Franz Kuntke

Dissertation · 2024

RESILIENT SMART FARMING

CRISIS-CAPABLE INFORMATION AND COMMUNICATION TECHNOLOGIES FOR AGRICULTURE

TECHNISCHE
UNIVERSITÄT
DARMSTADT

RESILIENT SMART FARMING

CRISIS-CAPABLE INFORMATION AND COMMUNICATION TECHNOLOGIES FOR AGRICULTURE

Vom Fachbereich Informatik
der Technischen Universität Darmstadt
genehmigte

DISSERTATION

zur Erlangung des akademischen Grades
Doktor-Ingenieur (Dr.-Ing.)

vorgelegt von

Franz Kuntke, M. Sc.
(geboren in Meißen)

Erstreferent:	Prof. Dr. Dr. Christian Reuter
Korreferent_in:	Prof. Dr. Jörg Dörr (Rheinland-Pfälzische Technische Universität Kaiserslautern-Landau)
Tag der Einreichung:	16. Oktober 2023
Tag der Disputation:	6. Dezember 2023
Hochschulkennziffer:	D17

PEASEC
Wissenschaft und
Technik für Frieden
und Sicherheit

Franz Kuntke, *Resilient Smart Farming: Crisis-Capable Information and Communication Technologies for Agriculture,* Dissertation, Technische Universität Darmstadt, 2024.
Veröffentlicht unter Urheberrecht

Dies ist eine Zweitveröffentlichung des folgenden Werkes: *Resilient Smart Farming: Crisis-Capable Information and Communication Technologies for Agriculture*, 2024, Springer Vieweg, vervielfältigt mit Genehmigung von Springer Fachmedien Wiesbaden GmbH. Die finale authentifizierte Version ist online verfügbar unter: https://doi.org/10.1007/978-3-658-44157-9

Wissenschaft und Technik für Frieden und Sicherheit (PEASEC)
Fachbereich Informatik
Technische Universität Darmstadt
Jahr der Veröffentlichung: 2024
Tag der mündlichen Prüfung: 6. Dezember 2023
URN: urn:nbn:de:tuda-tuprints-264969
URL: https://tuprints.ulb.tu-darmstadt.de/id/eprint/26496

FOREWORD

For many years, it was assumed that the world market, along with globalization, would enable society to buy and received all kinds of products, such as food, at any time. The crises of recent years, such as COVID-19 with shortages of hygiene products or certain foods, e.g., rice, or Russia's war against Ukraine with shortages of food, grain, and energy supply, show that the general supply of food to the world's population is by no means guaranteed in the long term and that societies need to become resilient. The failure of digital infrastructures can also have an enormous impact on digitalized agriculture.

This dissertation by Franz Kuntke addresses the tension between digitalization and resilience from the perspective of business continuity in the agricultural domain. In this context, agriculture is regarded as an essential infrastructure for food security, which means that this sector is attributed a high criticality for society. As current research on the intersection of resilience and agriculture focuses mainly on the topics of climate change and social changes, the topic of resilient digitalization has received less attention.

The dissertation uses qualitative and quantitative methods to understand the extent to which the technologies currently used by farmers are at risk of failure. Furthermore, new software is designed and implemented that increases the resilience of these technologies due to a failed internet connections. Overall, the dissertation fulfills my expectations. This thesis looks at a highly relevant topic. It is characterized in particular by the innovative combination of human-computer interaction, distributed systems and resilience in the context of digital agriculture with empirical findings, as well as conceptual and technical approaches. As such, this dissertation is pioneering work in this field.

The studies included in this PhD thesis have been published as seven peer-reviewed papers. In addition to working on his dissertation and his 22 scientific publications, Franz was involved in project management of various projects of agricultural IT (e.g., AgriRegio or GeoBox), research-oriented teaching in our program-ming courses and our lecture series Secure Critical Infrastructures as well as in the management of our internal IT infrastructure, thus contributing to the future development of PEASEC.

Franz Kuntke has proven that he is capable of independent scientific work. Thus, in December 2023, his dissertation was accepted by the Department of Computer Science at the Technical University of Darmstadt for the degree of Dr.-Ing. — as the fifth PhD thesis in our research group PEASEC. I would like to see a further focus on topics of such high importance. Franz, thank you for your contribution and for allowing me to ac-company you on your way to your PhD. I wish you all the best and every success for the future.

Prof. Dr. Dr. Christian Reuter
Professor for Science and Technology for Peace and Security (PEASEC)
and Dean of the Department of Computer Science at Technical University of Darmstadt

ACKNOWLEDGEMENTS

At the beginning, I would like to express my sincere gratitude to the many individuals who have contributed to the success of this dissertation. Without their support and assistance, this work would not be possible. Firstly, I wish to thank my doctoral supervisor, *Prof. Dr. Dr. Christian Reuter*, for his trust, guidance, and unwavering commitment to address my questions and concerns. Furthermore, I thank my co-examiner *Prof. Dr.-Ing. Jörg Dörr*, as well as *Prof. Dr. Felix Wolf*, *Prof. Dr.-Ing. Matthias Hollick*, and *Prof. Dr. Zsolt István* who kindly join the doctoral committee.

Additionally, I wish to express my appreciation for the whole team of *Science and Technology for Peace and Security (PEASEC)* at the Department of Computer Science at the *Technical University of Darmstadt*. The exchange of ideas and insights with colleagues has enriched my understanding of various topics and provided valuable perspectives on potential solutions or projects. Here, I would like to thank *Sebastian Linsner* as a particularly important collaborator, especially during the initial two years of my PhD position. Moreover, I wish to thank many other colleagues who have provided insightful conversations, sometimes offering new ideas or perspectives on various topics. Here, I would like to single out *Philipp Kühn*, *Jasmin Haunschild*, *Dr. Thea Riebe*, and *Dr. Marc-André Kaufhold* for many valuable discussions throughout the research process, especially during the final phase of my PhD studies. I would also like to thank the former student assistants who provided invaluable support in software development, research, and even careful proofreading of various publications: *Anel Muhamedagic*, *Franziska Bujara*, *Sabrina Neuhäusel*, *Laura Utz*, *Alexander Praus*, and *Julian Marcel Schindel*.

I would also like to thank all the co-authors of the published papers, in addition to those mentioned above, in particular: *Enno Steinbrink*, *Jonas Franken*, *Daniel Eberz-Eder* and *Dr. Lars Baumgärtner* for their valuable contributions to the conducted research. Parts of this work were also supported by funds of the German Government's Special Purpose Fund held at Landwirtschaftliche Rentenbank in the projects Geobox-I, Geobox-II, AgriRegio, by the German Federal Ministry for Education and Research (BMBF) in the project HyServ (01IS17030B), and by the LOEWE initiative (Hesse, Germany) within the emergenCITY centre.

Finally, my deepest thanks go to my family and friends who have supported me throughout this journey. In particular, I would like to thank my girlfriend *Lena Cibulski*, who supported me during these difficult times marked by the pandemic, remote work, and doctoral studies.

どうもありがとうございます
(Domo arigato gozaimasu)
Thank you very much.

Franz Kuntke

ABSTRACT

Like many sectors, agriculture is experiencing a continuous digitalization, i.e. an increase in data-driven technologies used. In contrast to companies of other critical infrastructures — e.g. energy or telecommunication — a typical farm is comparatively small and often run as a family business. Accordingly, the demands on farming technology, its implementation, and regulations are different in many terms. Furthermore, the circumstances that influence crisis risks and crisis management are different in agriculture — and as digitalization introduces new potential risks, this process should be reviewed critically. Currently, the most advanced approaches for agriculture are typically referred to as smart farming and agriculture 4.0, which incorporate more precise cultivation with less manual effort. But such new agriculture technology developments usually lack an assessment about its impact on the sector's resilience and dependencies on other infrastructures. The research domains of crisis informatics and information technology security (IT security) mostly focuses on other topics, apart from agriculture. The resilience research in agriculture itself is currently intensifying, however, this line of research focuses more on problems resulting from the climate crisis and social change. For these reasons it remains unclear, how digitalization impacts the resilience of food production and food safety. Therefore, it is not well researched which technological developments may lead to undesired effects in the future. How modern systems should be designed to allow for both, positive impacts on efficiency, and prevention of negative effects in terms of reduced resilience capacities, is also not answered by current literature. The aim of the present work is to close this research gap at the intersection of agriculture, digitalization, and resilience.

To answer the question to what extent current technologies used by farmers are at risk of failure, the dissertation first presents a snapshot of the resilience state of agricultural companies and the technologies used. This involves interviews with stakeholders, mainly farmers, as well as surveying security issues of the Long Range Wide Area Network (LoRaWAN) protocol, a transmission technology especially useful for agricultural Internet of Things. Which desires of farmers exist regarding software focusing on aspects of business continuity and secured operations, is another open question. This dissertation aims to also answer this question with empirical methods, mainly focus groups and usability tests. Then the rise of Internet of Things in agriculture raises another question, whether such technologies acquired for smart farming could also have benefits for resilience against internet-connection-lost situations. This question is answered by empirical evaluation of LoRaWAN range characteristics in agricultural landscapes, as well as artifact generation for resilient communication channels on top of LoRaWAN transmission devices.

Several findings are derived from the conducted research: There is a lack of understanding of how strong the used tools in agriculture depend on Information and Communications Technology, and many tools require a working internet connection. Moreover, information technology employed by agricultural enterprises presents security concerns similar to those encountered in other domains. Based on these findings, developments, and evaluations of new software approaches are presented: Derived design criteria and own system designs that allow for modern data-driven business operations, including Internet of Things integration based on LoRaWAN. The developed solutions show an increase in resilience capacities by enhancing the communication possibilities in crisis situations. The detected low absorption capacities against communication infrastructure outages shows room for improvement. To improve agricultural information technologies' resilience, software engineers could use the concepts and designs of this dissertation for their product development, like a modular offline-capable farm management storage that allows an exchange of small data in an autarkic manner via commodity LoRaWAN hardware. But also technology advisors and farmers benefit from the technological analyses and suggestions embedded in this work, like using multiple LoRaWAN gateways with an overlapping coverage to mitigate security vulnerabilities.

CONTENTS

III Appendix

AUTHOR'S PUBLICATIONS

In sum, 23 publications have been published in the context of the authors work.

The following 7 publications are published as chapters in part II of this thesis:

1. Kuntke, F., Linsner, S., Steinbrink, E., Franken, J., & Reuter, C. (2022). Resilience in Agriculture: Communication and Energy Infrastructure Dependencies of German Farmers. *International Journal of Disaster Risk Science*, *13*(2), 214–229. https://doi.org/10.1007/s13753-022-00404-7

2. Linsner, S., Kuntke, F., Steinbrink, E., Franken, J., & Reuter, C. (2021). The Role of Privacy in Digitalization – Analysing the German Farmers' Perspective. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, *2021*(3). https://doi.org/10.2478/popets-2021-0050

3. Kuntke, F., Romanenko, V., Linsner, S., Steinbrink, E., & Reuter, C. (2022). LoRaWAN security issues and mitigation options by the example of agricultural IoT scenarios. *Transactions on Emerging Telecommunications Technologies*, 1–20. https://doi.org/10.1002/ett.4452

4. Kuntke, F., Kaufhold, M.-A., Linsner, S., & Reuter, C. (2023). GeoBox: Design and Evaluation of a Tool for Resilient and Decentralized Data Management in Agriculture. *Behaviour & Information Technology*. https://doi.org/10.1080/0144929X.2023.2185747

5. Kuntke, F., Bektas, M., Buhleier, L., Pohl, E., Schiller, R., & Reuter, C. (2023). How Would Emergency Communication Based on LoRaWAN Perform? Empirical Findings of Signal Propagation in Rural Areas. *Proceedings of Information Systems for Crisis Response and Management (ISCRAM)*, 1–8. http://dx.doi.org/10.59297/QBHV2089

6. Kuntke, F., Sinn, M., & Reuter, C. (2021). Reliable Data Transmission using Low Power Wide Area Networks (LPWAN) for Agricultural Applications. *Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES 2021)*, 1–9. https://doi.org/10.1145/3465481.3469191

7. Kuntke, F., Baumgärtner, L., & Reuter, C. (2023). Rural Communication in Outage Scenarios: Disruption-Tolerant Networking via LoRaWAN Setups. *Proceedings of Information Systems for Crisis Response and Management (ISCRAM)*, 1–13. http://dx.doi.org/10.59297/WZMQ1124

The following 16 papers are not included in the thesis, although their findings are supplementary to it:

8. Schmid, D., Kuntke, F., Bauer, M., & Baumgärtner, L. (2023). BPoL: A Disruption-Tolerant LoRa Network for Disaster Communication. *2023 IEEE Global Humanitarian Technology Conference (GHTC)*, 440–447. https://doi.org/10.1109/GHTC56179.2023.10354717

9. Höchst, J., Baumgärtner, L., Kuntke, F., Penning, A., Sterz, A., Sommer, M., & Freisleben, B. (2023). Mobile Device-to-Device Communication for Crisis Scenarios Using Low-Cost LoRa Modems. In H. J. Scholl, E. E. Holdeman, & F. K. Boersma (Eds.), *Disaster Management and Information Technology* (pp. 235–268, Vol. 40). Springer International Publishing. https://doi.org/10.1007/978-3-031-20939-0_12

10. Kuntke, F., Eberz-Eder, D., Trapp, M., & Reuter, C. (2023). RSF-Lab'23: Konzepte und Anwendungen zur resilienten digitalen Landwirtschaft. *INFORMATIK 2023: 53. Jahrestagung der Gesellschaft für Informatik – Informatik für Gesellschaft (Workshop-Beiträge)*, 1–7. https://doi.org/10.18420/inf2023_156

11. Orlov, D., Kuntke, F., & Reuter, C. (2023). Optimierte Messenger-Applikation zur Notfallkommunikation via LoRaWAN-DTN. *INFORMATIK 2023: 53. Jahrestagung der Gesellschaft für Informatik – Informatik für Gesellschaft (Workshop-Beiträge)*, 1–6. https://doi.org/10.18420/inf2023_160

12. Guntrum, L., Güldenring, B., Kuntke, F., & Reuter, C. (2022). Using Digitally Mediated Methods in Sensitive Contexts: A Threat Analysis and Critical Reflection on Security, Privacy, and Ethical Concerns in the Case of Afghanistan. *Zeitschrift für Friedens- und Konfliktforschung (ZeFKo)*, *11*(2), 95–128. https://doi.org/10.1007/s42597-022-00088-2

13. Eberz-Eder, D., Kuntke, F., Brill, G., Bernardi, A., Reuter, C., Wied, C., Nuderscher, P., & Reuter, C. (2023). Prototypische Entwicklungen zur Umsetzung des Resilient Smart Farming (RSF) mittels Edge Computing. *43. GIL-Jahrestagung: Informatik in der Land-, Forst- und Ernährungswirtschaft*. https://dl.gi.de/handle/20.500.12116/40264

14. Linsner, S., Steinbrink, E., Kuntke, F., Franken, J., & Reuter, C. (2022). Supporting Users in Data Disclosure Scenarios in Agriculture through Transparency. *Behaviour & Information Technology (BIT)*, *41*(10), 2137–2159. https://doi.org/10.1080/0144929X.2022.2068070

15. Reuter, C., Kuntke, F., Trapp, M., Wied, C., Brill, G., Müller, G., Steinbrink, E., Franken, J., Eberz-Eder, D., & Schneider, W. (2022). AgriRegio: Infrastruktur zur Förderung von digitaler Resilienz und Klimaresilienz im ländlichen Raum am Beispiel der Pilotregion Nahe-Donnersberg. In D. Demmler, D. Krupka, & H. Federrath (Eds.), *INFORMATIK 2022: 52. Jahrestagung der Gesellschaft für Informatik – Informatik für Gesellschaft (Workshop-Beiträge), Lecture Notes in Informatics (LNI)* (pp. 961–972). Gesellschaft für Informatik e. V. https://doi.org/10.18420/inf2022_81

16. Reuter, C., Eberz-Eder, D., Kuntke, F., & Trapp, M. (2022). RSF-Lab'22: Resilient Smart Farming Laboratory: Für eine widerstandsfähige und intelligente Landwirtschaft. In D. Demmler, D. Krupka, & H. Federrath (Eds.), *INFORMATIK 2022: 52. Jahrestagung der Gesellschaft für Informatik – Informatik für Gesellschaft (Workshop-Beiträge), Lecture Notes in Informatics (LNI)* (pp. 931–934). Gesellschaft für Informatik e. V. https://doi.org/10.18420/inf2022_78

17. Eberz-Eder, D., Kuntke, F., & Reuter, C. (2022). Sensibilität für Resilient Smart Farming (RSF) und seine Bedeutung in Krisenzeiten. *42. GIL-Jahrestagung: Informatik in der Land-, Forst- und Ernährungswirtschaft*. https://dl.gi.de/handle/20.500.12116/38375

18. Kuntke, F., Sinn, M., Linsner, S., & Reuter, C. (2021). Low Power Wide Area Networks (LPWAN) für krisentaugliche Datenübertragung in landwirtschaftlichen Betrieben. In A. Meyer-Aurich, M. Gandorfer, C. Hoffmann, C. Weltzien, S. D. Bellingrath-Kimura, & H. Floto (Eds.), *41. GIL-Jahrestagung: Informatik in der Land-, Forst- und Ernährungswirtschaft* (pp. 193–198). Gesellschaft für Informatik. https://dl.gi.de/handle/20.500.12116/35671

19. Eberz-Eder, D., Kuntke, F., Schneider, W., & Reuter, C. (2021). Technologische Umsetzung des Resilient Smart Farming (RSF) durch den Einsatz von Edge-Computing. *41. GIL-Jahrestagung: Informatik in der Land-, Forst- und Ernährungswirtschaft*, 79–84. https://dl.gi.de/handle/20.500.12116/35651

20. Kuntke, F., Reuter, C., Schneider, W., Eberz, D., & Bernardi, A. (2020). Die GeoBox-Vision: Resiliente Interaktion und Kooperation in der Landwirtschaft durch dezentrale Systeme. In C. Hansen, A. Nürnberger, & B. Preim (Eds.), *Mensch und Computer 2020 - Workshopband* (pp. 1–6). Gesellschaft für Informatik e.V. https://doi.org/10.18420/muc2020-ws117-407

21. Höchst, J., Baumgärtner, L., Kuntke, F., Penning, A., Sterz, A., & Freisleben, B. (2020). LoRa-based Device-to-Device Smartphone Communication for Crisis Scenarios. *Proceedings of Information Systems for Crisis Response and Management (ISCRAM)*, 996–1011. http://idl.iscram.org/files/jonashochst/2020/2291_JonasHochst_etal2020.pdf

22. Linsner, S., Kuntke, F., Schmidbauer-Wolf, G. M., & Reuter, C. (2019). Blockchain in Agriculture 4.0 - An Empirical Study on Farmers Expectations towards Distributed Services based on Distributed Ledger Technology. In F. Alt, A. Bulling, & T. Döring (Eds.), *Mensch und Computer 2019* (pp. 103–113). ACM. https://doi.org/10.1145/3340764.3340799

23. Kalle, T., Kaufhold, M.-A., Kuntke, F., Reuter, C., Rizk, A., & Steinmetz, R. (2019). Resilience in Security and Crises through Adaptions and Transitions. In C. Draude, M. Lange, & B. Sick (Eds.), *INFORMATIK 2019: 50 Jahre Gesellschaft für Informatik – Informatik für Gesellschaft (Workshop-Beiträge), Lecture Notes in Informatics (LNI)* (pp. 571–584). Gesellschaft für Informatik e. V. https://doi.org/10.18420/inf2019_ws60

I

SYNOPSIS

1 INTRODUCTION

"There are two types of PA [Precision Agriculture] systems: those that have been hacked and those that will be."

(West, 2018)

1.1 Motivation and Problem Statement

Digitalization is a major issue in the agricultural sector. The desired positive aspects are an increase in efficiency and effectiveness and also a more resource-friendly production of food. The terms *agriculture 4.0* and *smart farming* are currently used to summarize the technological trends of knowledge management and intelligent, networked systems for agricultural production (Gandorfer et al., 2017; Weltzien, 2016). According to Weltzien (2016), the digitalization could open up new paths to a profitable agriculture accepted by society accepted, from which the environment, biodiversity and farmers would benefit. At the same time, it is important to bear in mind that the right to food is a human right recognized by the Universal Declaration of Human Rights: "Everyone has the right to a standard of living adequate for the health and well-being of himself and of his family, including food, ..." (UN General Assembly, 1948, Art. 25). Accordingly, the food sector is a critical infrastructure, i.e. of major importance to society's well-functioning. Depending on the administration, some countries officially include (large) farming businesses into security and safety regulations of critical infrastructures. For example in Germany, according to the German Federal Ministry of the Interior (Bundesministerium des Inneren), a farmer is considered be operating a critical infrastructure as soon as they have an annual production of 434,000 tonnes of food or 350 million liters of beverages (Bundesministerium des Inneren, 2016). Regardless of whether these limits seem appropriate, this shows that even purely agricultural businesses in private hands can in principle be perceived as critical infrastructure.

In the ongoing fourth agricultural revolution (*agriculture 4.0*) – also referred to as *smart farming* – technologies of the category *Internet of Things (IoT)* play a particularly big role (Liu et al., 2021). The main point of IoT is to make environmental parameters accessible from computer networks. The gathered data allows for monitoring and automation of many aspects in farms. Among the most common use cases of IoT based smart farming solutions are crop monitoring and irrigation control (Navarro et al., 2020). Sensors record environmental parameters, such as humidity or temperature and feed this data into computer networks for further processing. Evaluating the data allows for data-driven decisions, e.g., controlling the indoor temperature of a greenhouse. Although large-scale effects on an economic and ecological level are not well evidenced, expectations of IoT applications are high. However, questions arise when thinking about the increasing dependencies to the technologies and their operational stability. A problematic scenario that could be drawn is the potential high dependency on smart farming technologies for future agricultural practice, in combination with the vulnerability of non-resilient designed technical systems. Yet, as expectations are high, smart farming technologies should not be avoided. Therefore, such systems must be designed with high demands on resilience.

Looking at the connectivity of IoT devices for large-scale agriculture, modern far-reaching network technologies such as LoRaWAN are able to connect sensors within the agricultural areas even over long distances with little technical effort (Chen et al., 2016; Davcev et al., 2018; Ojha et al., 2015). The analysis of Wireless Sensor Networks (WSNs) for precision agriculture by Jawad et al. (2017) shows that current approaches typically require an internet connection to cloud services to analyze the sensor data, on the one hand, and enable later access via other conventional computer technology, such as tablets, on the other hand.

Cloud solutions are currently also a trend when it comes to the data management required by smart farming, at least for software dedicated to the agricultural sector with applications such as 365FarmNet, Trimble Farmer Core, Top Farm, etc. Advertised benefits of cloud software are often usability aspects, for example easy-to-use interfaces or synchronization between multiple devices. However, some of the aspects mentioned together with cloud software — such as modern User Interfaces (UIs) — do not depend on an underlying cloud architecture. Furthermore, the paradigm of outsourcing data and software to third parties (cloud service providers) itself raises questions about data protection and the vendor lock-in effect. But cloud solutions require a working connection to the internet, which is an additional dependency when comparing cloud software with classical on-premise software. This leads to the preliminary conclusion that modern IT products in the agricultural sector are currently subject to a decreasing resilience trend by introducing an additional dependency in terms of a working internet connection. It is unclear whether new types of software actually need this dependency, or whether the data management requirements for smart farming can also be met with other principles. To meet social responsibility, new technologies for farmers should be as focused on safe, decentralized, and resilient smart farming as possible, which, in line with Reuter et al. (2019) is necessary to be best prepared for possible disasters.

When thinking about disaster scenarios, communication in rural areas during telecommunication network outages has not been well researched. A study by Hobe et al. (2019), conducted in 2017, investigates how farmers in Germany tend to communicate under normal circumstances and which developments are expected in the following five years. Even today, farmers seem to prefer a direct and personal conversation, but a significant increase in the usage of digital communication systems like messengers and cloud services, as well as e-mail, is expected. In cases where farmers cannot communicate their needs and working routines at all, some farms are not able to operate, e.g., their harvest at home, as many tasks require multiple stakeholders or businesses to work together and coordinate their schedules (Lucas et al., 2019). For this reason,

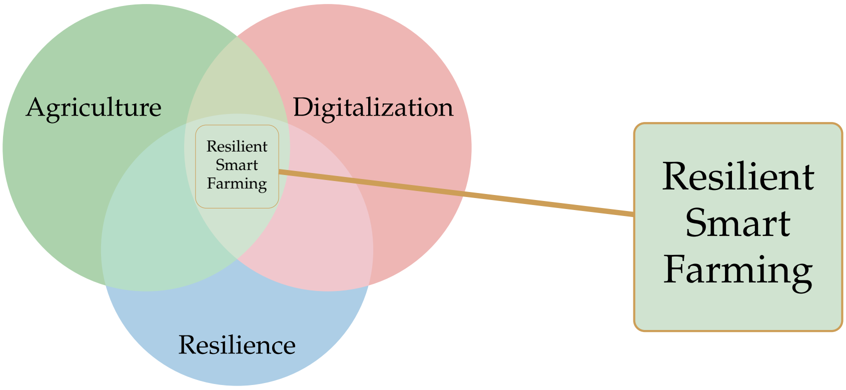


Figure 1.1: This work's theme is the intersection of agriculture, digitalization and resilience.

communication systems should be as reliable as possible to help users maintain as many of their routines as possible, even during a crisis. This means that a resilient form of digital communication is required, firstly for direct exchanges between actors in the agricultural sector and, secondly, with distributors or directly with customers.

In summary, computer science has so far paid little attention to the question of how to deal with possible crisis scenarios in agriculture. An example of such a scenario is a medium- to large-scale communications infrastructure failure that could be triggered by a natural disaster such as the European floods of 2021. One major aspect of possible solutions has to be the reliable communication between several farms, as collaboration between individual companies is typical for agricultural tasks (Gardner & Lerman, 2006), e.g., when harvesting before imminent weather changes is demanded or is coordinated as a joint task. The reduction of dependencies from the agricultural sector to Information and Communications Technology (ICT) should be of particular interest for future developments. A holistic approach, which allows using available tools, like LoRaWAN based devices with high range transmission capabilities, has also not been analyzed so far. The questions that arise within the thesis are formulated within the following definitions of aim and research question (RQ):

1.2 Aim and Research Question

Today, many software architectures do not seem to be resistant to unexpected events. This also applies to the agricultural sector, which is undergoing an ongoing digital transformation. The overarching goal of this dissertation is therefore to examine the agricultural sector in terms of the threats and problems associated with advancing digitalization in order to design more resilient approaches. Hence, the focus of this thesis is on the interplay between agriculture, digitalization and resilience (see Figure 1.1).

The main RQ of this work is the following:
"How should ICT for agriculture be designed to enhance the technological resilience of agriculture?"

The thesis answers this main RQ by elaborating three sub-fields:

> First, the thesis researches typical resilience capacities and vulnerabilities of farming businesses. It involves analyzing dependencies between farm companies and other infrastructures, mainly energy and communication. The state of security of the technologies in use is also of interest. This leads to the first sub-question:
>
> > *RQ1: To what extent are the technologies used by farmers at risk of failure?*
>
> Second, based on the results of working on RQ1, the food sector should be supported by developing and evaluating new concepts and software artifacts, that enhance resilience regarding natural disasters and attacks of cyber criminals. This leads to the second sub-question:
>
> > *RQ2: How to support information technology (IT) resilience for farm management?*
>
> Third, based on an increasing usage of IoT in agriculture, the question arises if available sensors communication technologies could be used as arbitrary data channels, e.g., for crisis communication. This leads to the third sub-question:
>
> > *RQ3: How could IoT technology be used to enhance farmers' resilience?*

1.3 CONTENT AND STRUCTURE OF THE THESIS

This dissertation consists of two parts: a synopsis (I) and publications (II).

Part I: Synopsis

The first part presents the conceptual foundations.

Chapter 1 (Introduction) introduces to the topic of digitalization in agriculture and the need for Resilient Smart Farming in combination with a crisis-capable ICT. This chapter contains the motivation, aims, objectives and the structure of the work.

Chapter 2 (Background) gives an overview of the state of agriculture, defines relevant terms and presents recent research in the areas: smart farming, farm management information systems (FMIS), sensors and wireless sensors networks, and resilient networking approaches.

Chapter 3 (Research Design) outlines the research approach, setting and methods used in this work: design case studies based on empirical study, conception of ICT artifacts and evaluation.

Chapter 4 (Findings) presents the main results of the conducted research and its implications for agricultural ICT in three parts: (1) Farms' Digital Dependencies and Vulnerabilities, (2) Towards a Resilient Software Architecture for Farm Management and (3) LoRaWAN-based IoT Developments Towards Resilient Communications.

Chapter 5 (Discussion) summarizes the requirements, concepts and implementations of ICT to pave the way for resilient smart farming, as well as the theoretical and practical implications.

Chapter 6 (Conclusion) emphasizes the contribution on resilience-enhancing ICT for farmers, states the overall conclusion and presents perspectives for future work in the area of crisis-capable agricultural IT.

Part II: Publications

The second part presents partial results for the questions presented above. The chapters in this part consist of previously published and similar papers (journal articles, and conference papers), with minor changes. Chapter 7 to Chapter 9 are empirical studies and analyses of current technologies or processes. Chapter 10 to Chapter 13 contain concepts, implementations of ICT artifacts and practical evaluations. For most (6 of 7) of the papers that are part of this dissertation, I was the first and corresponding author, but the contributions of the co-authors, which were gratefully provided, are also very important, as I will describe in the following. The purpose of this section is to list the independent scientific contributions that have been approved by all authors. Additional, Table 1.1 gives an overview of all included papers of Part II: Publications.

Table 1.1: Overview of the publications that are part of this dissertation.

Title	Authors	Published in
Resilience in Agriculture: Communication and Energy Infrastructure Dependencies of German Farmers	Franz Kuntke, Sebastian Linsner, Enno Steinbrink, Jonas Franken, and Christian Reuter	International Journal of Disaster Risk Science (IJDRS, IF 4.0)
The Role of Privacy in Digitalization – Analyzing Perspectives of German Farmers	Sebastian Linsner, Franz Kuntke, Enno Steinbrink, Jonas Franken, and Christian Reuter	Proceedings on Privacy Enhancing Technologies Symposium (PETS, Core-A)
LoRaWAN Security Issues and Mitigation Options by the Example of Agricultural IoT Scenarios	Franz Kuntke, Vladimir Romanenko, Sebastian Linsner, Enno Steinbrink, and Christian Reuter	Transactions on Emerging Telecommunications Technologies (ETT, IF 3.6)
GeoBox: Design and Evaluation of a Tool for Resilient and Decentralized Data Management in Agriculture	Franz Kuntke, Marc-André Kaufhold, Sebastian Linsner, and Christian Reuter	Behaviour & Information Technology (BIT, IF 3.3)
How Would Emergency Communication Based on LoRaWAN Perform? Empirical Findings of Signal Propagation in Rural Areas	Franz Kuntke, Merve Bektas, Laura Buhleier, Ella Pohl, Rebekka Schiller, and Christian Reuter	Proceedings of the 20th Annual Global Conference on Information Systems for Crisis Response and Management (ISCRAM 2023)
Reliable Data Transmission using Low Power Wide Area Networks (LPWAN) for Agricultural Applications	Franz Kuntke, Marcel Sinn, Sebastian Linsner, and Christian Reuter	Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES 2021)
Rural Communication in Outage Scenarios: Disruption-Tolerant Networking via LoRaWAN Setups	Franz Kuntke, Lars Baumgärtner, and Christian Reuter	Proceedings of the 20th Annual Global Conference on Information Systems for Crisis Response and Management (ISCRAM 2023)

Chapter 7 (Resilience in Agriculture: Communication and Energy Infrastructure Dependencies of German Farmers) presents the results of interviews and questionnaires with farmers, to answer: *How dependent are farmers on communication and energy infrastructures? To what extent do farmers take precautions for risk minimization?* This leads to new knowledge of current and actual measures for recovering in disaster scenarios of agricultural companies. This chapter has been published in the *International Journal of Disaster Risk Reduction* (Kuntke, Linsner, et al., 2022) (Paper A).

AUTHOR STATEMENT As corresponding and leading author, Franz led the overall research design, management and writing process of the paper. The literature was collected by all authors. The research design and choice of the study design for the pre-study were done by Franz and Sebastian together. Franz and Sebastian planned and conducted the interviews as well as the clustering of results. The survey was designed and conducted by Franz. Enno contributed to the evaluation of the quantitative data from the questionnaires. The results and discussion were written by all authors, with Enno focusing on the statistical analysis of the questionnaires. The central implications of this work were mainly derived by Franz. Christian was a general advisor for this work and contributed with continuous feedback during all phases of the paper writing process.

Chapter 8 (The Role of Privacy in Digitalization – Analyzing Perspectives of German Farmers) discusses how technological progress is disrupting various domains, including agriculture. The chapter presents a qualitative study involving 52 German farmers to investigate the impact of ongoing digitalization in agriculture and its implications for privacy. It highlights emerging challenges for farmers regarding privacy and how privacy issues also impact the adoption of digital tools. This chapter has been published in *Proceedings on Privacy Enhancing Technologies Symposium* (Linsner et al., 2021) (Paper B).

AUTHOR STATEMENT As corresponding and leading author, Sebastian led the overall research design, management and writing process of the paper. The literature was collected by all authors, where Jonas contributed a major part. The research design and choice of the study design were done by Sebastian and Franz together. Sebastian and Franz planned and conducted the interviews and the clustering of results. The results and discussion were written by Sebastian and Enno, where Sebastian focused on the agricultural part and the findings regarding privacy, and Enno on the implications for research. Franz contributed thoughts and ideas especially to the discussion. The central implications of this work were mainly derived by Sebastian. Christian was a general advisor of this work and contributed with continuous feedback during all phases of the paper writing process.

Chapter 9 (LoRaWAN Security Issues and Mitigation Options by the Example of Agricultural IoT Scenarios) provides an overview of current IoT (specific LoRaWAN) developments and use cases for agriculture. The main part of this chapter evaluates security vulnerabilities from existing literature, and investigates the possible impacts for agricultural applications, and also takes the newest LoRaWAN standard (to date) into consideration. Additionally, mitigation options are described, to allow users and developers to choose a secure way for specific IoT setups. This chapter has been published in *Transactions on Emerging Telecommunications* (Kuntke, Romanenko, et al., 2022) (Paper C).

AUTHOR STATEMENT As corresponding and leading author, Franz had the idea, led the overall research design, management and writing process of the paper. Vladimir developed the foundations within his bachelor thesis in 2019, supervised by Franz and Christian. Based on this, Franz drafted the whole paper. The conducted literature research of Vladimir was used and updated in 2020 and 2021 by Franz in particular, but also by all other authors. The domain specifics of agricultural Internet-of-Things were elaborated by Sebastian and Franz. Enno contributed to the introduction, as well as with editorial improvements and feedback. Christian was a general advisor for this work and contributed with continuous feedback during all phases of the paper writing process.

Chapter 10 (GeoBox: Design and Evaluation of a Tool for Resilient and Decentralized Data Management in Agriculture) provides the concept, implementation and evaluation of a decentralized software solution for the agricultural sector. It integrates the recommendation for a resilient communication technology for agriculture from the previous chapters. An evaluation of the UI with domain experts also gives further details on what to consider when developing farm management systems for agriculture. This chapter has been published in the *Behaviour & Information Technology* (Kuntke, Kaufhold, et al., 2023) (Paper D).

AUTHOR STATEMENT As corresponding and lead author, Franz directed the overall research design, management, and writing process of the paper. Literature was collected by all authors. Christian and Marc selected the study design and planned and conducted the first round of the preliminary empirical study (interface requirements). Franz and Sebastian planned and conducted the second round of the preliminary empirical study (architecture requirements). Clustering of the results of the preliminary study was done by Marc and Franz. The design and implementation of the user evaluation was done by Franz. The results and discussion were written by all authors. The key implications of this work were mainly derived by Marc and Franz. Christian was a general advisor to this work and contributed with continuous feedback at all stages of the writing process.

Chapter 11 (How Would Emergency Communication Based on LoRaWAN Perform? Empirical Findings of Signal Propagation in Rural Areas) presents results from empirical LoRaWAN signal coverage tests in rural regions, which is especially useful for smart farming applications. With two different hardware setups, multiple regions were experimentally evaluated, to allow for better coverage estimations in different circumstances. Tested objects were forests in different conditions, as well as classic fields without large obstacles. This chapter will be published in the *Proceedings of the 20th Annual Global Conference on Information Systems for Crisis Response and Management* (Kuntke, Bektas, et al., 2023) (Paper E).

AUTHOR STATEMENT As corresponding and lead author, Franz directed the overall research design, and writing process of the paper. Literature was collected by all authors. Merve, Laura, Ella and Rebekka selected the study design and planned the empirical evaluation in consultation with Franz. Franz, Merve, Laura, Ella, and Rebekka conducted the empirical tests. The results and discussion were written by all authors. Christian was a general advisor for this work and contributed with continuous feedback at all stages of the writing process.

Chapter 12 (Reliable Data Transmission using Low Power Wide Area Networks (LPWAN) for Agricultural Applications) works out a concept for building up TCP/IP based data communication via LoRa. This could be used as a redundant data channel or to let legacy hardware communicate via the far-reaching wireless coverage of the LoRa technology. An implementation and evaluation of a test setup gives an indication in which circumstances (distance, bandwidth) the concept could be used. This chapter has been published as a Workshop Paper of the *International Workshop on Frontiers in Availability, Reliability and Security (FARES)* in the *Proceedings of the 16th International Conference on Availability, Reliability and Security* (Kuntke, Sinn, & Reuter, 2021) (Paper F).

AUTHOR STATEMENT As corresponding and leading author, Franz had the idea, led the overall research design, management and writing process of the paper. Marcel developed the foundations within his master thesis in 2020, supervised by Franz and Christian. Based on this Franz drafted the whole paper. Christian was a general advisor for this work and contributed with continuous feedback during all phases of the paper writing process.

Chapter 13 (Rural Communication in Outage Scenarios: Disruption-Tolerant Networking via LoRaWAN Setups) examines an idea of exploiting commodity IoT hardware for building up a resilient communication network within farm neighborhood communities. The main parts of this chapter are an analysis of farm distribution in Germany to determine network requirements, and a simulation of two disruption-tolerant networking (DTN) routing approaches on farm neighborhood positions, retrieved by OpenStreetMap. The resulting concept and implementation is a resilience-enhancing technology, which might also be useful for other domains, with a high demand for local communication even in disaster situations. This chapter has been published in the *Proceedings of the 20th Annual Global Conference on Information Systems for Crisis Response and Management* (Kuntke, Baumgärtner, & Reuter, 2023) (Paper G).

AUTHOR STATEMENT As corresponding and lead author, Franz directed the overall research design, management, and writing process of the paper. Literature was collected by all authors. Franz and Lars selected the study design and planned the distance evaluation and simulation. The concept and implementation were written by Franz. The results and discussion were written by all authors. Christian was a general advisor for this work and contributed with continuous feedback at all stages of the writing process.

Summary – Introduction

- Agriculture is important, being an essential part of the critical sector food.
- There is a lack of research on how dependent agriculture is on ICT.
- The following chapters address this gap with both empirical studies and artifact generation:
  - Analyses of the current situation can be used by politics to make well informed decisions for enhancing food security
  - Evaluations of existing solutions help farmers to improve their own business security and resilience
  - Implementations and concepts could be used by software companies for a new generation of farm-management-systems, respecting security and privacy, and providing resilience-enhancing capabilities

2 BACKGROUND

This dissertation is about the infrastructural resilience of data-driven agriculture and requires a basic understanding of both the application scenario of agricultural practice and digital resilience as it is used in this work. Therefore, this chapter first provides a brief introduction to agriculture in Germany by referring to recent statistical investigations. Afterward, this chapter introduces terms, such as *smart farming*, *precision farming*, and *farm management information systems (FMIS)* and characterizes digital technologies in the field of *resilient network approaches*.

2.1 Characteristics of Agriculture in Germany

Agriculture differs in many ways around the world because of different climatic, political, and social conditions. Similarly, the definition of agriculture in terms of specific areas of activity slightly differs from region to region. This work focuses mainly on agriculture in Germany, as much of this work took place in the context of German projects. According to the Bundesministerium für Ernährung und Landwirtschaft, agriculture in Germany can be divided into the following economic sectors (sorted by monetary value of gross agricultural output, starting with the highest) : forage production, arable farming, animal production, horticulture, and permanent crops. Therefore, the most important economic areas correspond to a common understanding of agriculture: cultivated fields that produce grain, for example, and livestock for animal products such as milk and meat.

A look at official government statistics (Bundesanstalt für Landwirtschaft und Ernährung, 2023) allows for an overview of current practice and the derivation of trends. About 86.9 % of German farms in 2020 were mostly family-driven sole proprietorships, with an increased average of 1.5 full-time workers per business (+ 36.4 %) compared to 1999, where the average sole proprietorship was 1.1 full-time workers. The general trend is that the sector consists of fewer farms, thus each farm has to work more land (see Figure 2.1). This has been made feasible by implementing more effective procedures and by utilizing technical aids more frequently. Consequently, a lower number of individuals is required to cultivate the same amount of land. The number of people working in the agricultural sector in Germany has decreased by about 33.5 % in 25 years from 1,409,800 people (in 1995) to 937,900 people (in 2020), according to statistics. As not all workers are employed full-time on a farm, the labor output is recorded in addition to the number of individuals. Part-time employment is converted to full-time equivalents called labor units. For the year 1995, the labor output was

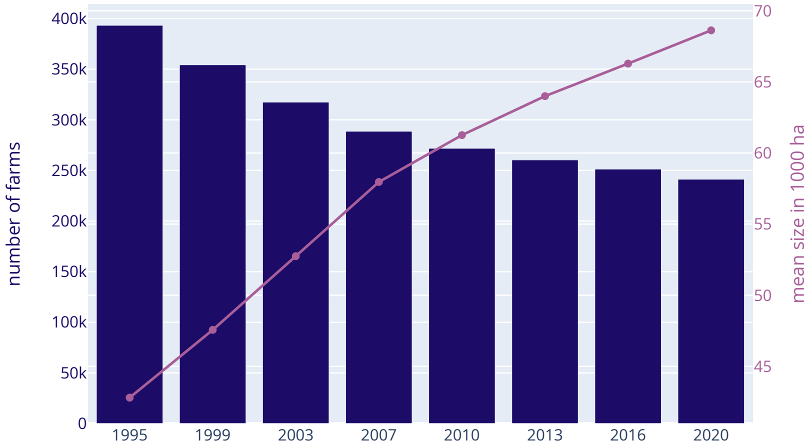


Figure 2.1: Development of the farm structure of agricultural holdings with 5 hectares or more of land in Germany; data from: Bundesanstalt für Landwirtschaft und Ernährung (2023, p. 24-25).

698,400 labor units and in 2020 it was 484,800 labor units, i.e., a decrease of about 30.5 % (Bundesanstalt für Landwirtschaft und Ernährung, 2023, p. 42). Those numbers represent work that takes place on the farm and in the stable, including administrative duties and other business functions, such as direct marketing, forest management, and extra-farm activities. It is difficult to determine how the lower quantity of workers and labor units affected yields qualitatively due to the different conditions per year. However, given a roughly similar size of agricultural land (a decrease of 4 % between 1995 and 2020) (Bundesanstalt für Landwirtschaft und Ernährung, 2023, p. 63), it can be assumed that, accordingly, agricultural processes have become more efficient in terms of labor input. An important role, especially in southwestern Germany with many smaller farms in comparison, is the coordination between actors in agriculture. Many activities require or benefit from more personnel and machinery than a single farm has on its own. Thus, the coordination of resources is an essential part of modern agriculture. Communication still tends to take place in person (Hobe et al., 2019), but rapid communication, such as harvesting a field before an imminent change in weather conditions, requires immediate communication, which then takes place by telephone or messenger. Apart from the increasing cooperation and coordination between companies, technology has also changed. Among other things, digitalization has led to an increase in the efficiency of existing machine classes and has also led to the use of new technologies.

2.2 Digitalization in Agriculture and Recent Findings of Resilient Technologies

There are some exciting areas in the research landscape that have already affected digitalization in agriculture and others that may benefit future digitized agriculture. The following subsections provide an overview of the information technology currently in use as well as an insight into recent findings from the scientific community. These include work that addresses key aspects of software for farmers, but also aspects of resilient communication infrastructures. The latter means that more and more digital tools and ways of working rely on functioning communication over long distances, and researchers investigate how to make this communication as robust as possible.

2.2.1 *Smart Farming*

Liu et al. (2021) recap the history of the *agricultural revolutions* up to the current trend of *agriculture 4.0* (see also Figure 2.2): Agriculture 1.0 is described as manual work from ancient times up to the end of the 19th century. The usage of agricultural machinery for mechanized agriculture between 1784 and 1870 leads to higher food production and less manual labors and is referred to as Agriculture 2.0. Starting with the third agricultural revolution, IT systems entered the food-production processes. In light of the current fourth agricultural revolution, data processing is even more crucial to allow for more precise processes all around the agricultural production and food supply chain management. Smart farming technologies in particular are gaining increasing attention, i.e., networked and semi-autonomously interacting devices that can perceive and communicate their individual status as well as their environmental context in real-time thanks to sensors (Fleisch & Thiesse, 2007; Porter & Heppelmann, 2014).

The opportunity of smart farming is to make the agricultural process more efficient and sustainable, while also increasing yields and reducing the environmental impact of farming. As the world's population continues to grow, the demand for food increases, which results in the need for more efficient food production. Smart farming can help farmers to produce more food with fewer resources and at a lower cost, making it an important tool in meeting the global food security challenge. As the survey of Schukat and Heise (2021b) states, 65.8 % of the participating German farmers ($n = 523$) reported using smart products in 2020.

Overall, smart farming is a key aspect of the agricultural sector, as it can help farmers to produce more food with fewer resources, reduce the environmental impact and increase the resilience to climate change. Nevertheless, several challenges and problems with the adoption of smart farming technologies are highlighted in the scientific literature:

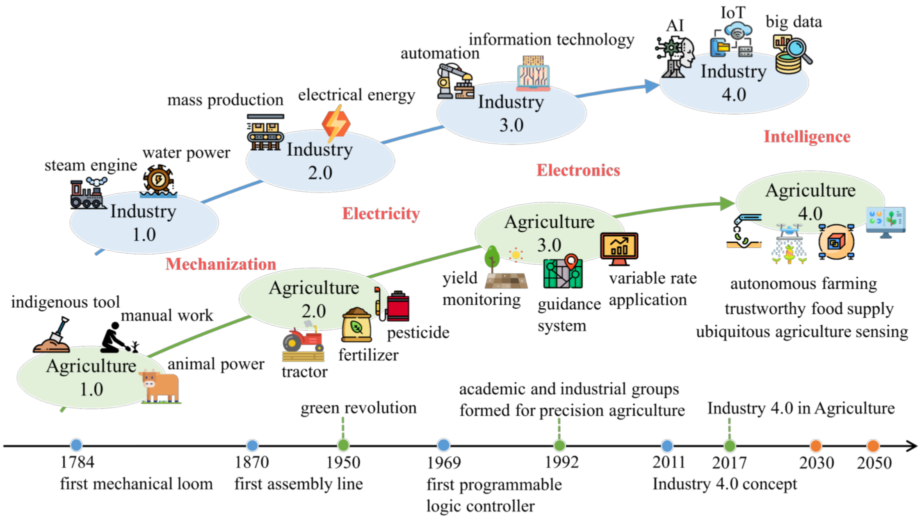


Figure 2.2: Timeline of agricultural revolutions aligned with industrial revolutions; source: Liu et al. (2021).

- High cost: Smart farming technologies can be expensive to implement, especially for small-scale farmers who may not have the financial resources to invest in them. (Balafoutis et al., 2020)
- Lack of standardization: There is currently a lack of standardization in smart farming technologies, which can make it difficult for farmers to choose the right equipment and software for their needs. (Bacco et al., 2018)
- Data privacy and security: Collecting and storing large amounts of data from smart farming technologies can raise concerns about data privacy and security, especially if the data is sensitive or personal in nature. (Gupta et al., 2020a; Hoeren and Kolany-Raiser, 2018, p. 115)
- Lack of technical knowledge: Some farmers may not have the technical knowledge or skills required to effectively use and maintain smart farming technologies, which can limit their effectiveness. (Jerhamre et al., 2022)
- Dependence on technology: Using smart farming technologies introduces a dependency on this technology. If there is an outage or malfunction, it can have a significant impact on the farming operations. (Demestichas et al., 2020)

2.2.2 *Farm Management Information Systems*

One essential part of a modern and technology driven farming business is the management of all relevant data. Data allows for monitoring processes and making reasonable decisions. Some modern farm equipment already depends on — or at least strongly benefits — from digital data, e.g., a field sprayer that allows for area-specific fertilizer application. Software that is dedicated to data management is so called FMIS.

Fountas et al. (2015) systematically analyzed 141 commercial FMIS focused on crop-production (arable farming). The authors state that the software products studied "tend to focus on solving daily farm tasks and aim to generate income for the farmers through better resource management and field operations planning" (Fountas et al., 2015, p. 48). The most common functions are field operation management (89 %), reporting (81 %), and finance (64 %), and most FMIS in their pre-2015 analysis were PC-based solutions (75 %); only some supported mobile (16 %) or web-based (15 %) applications. Among the ascribed benefits of using FMIS are less manual work on office tasks, like financial management and reporting, and the required data management for precision agriculture application, like partial area specific fertilization.

But there are also some challenges and problems associated with digitalization in agriculture, including FMIS. The most prominent challenge is increasing the low adoption rate of digital tools (Schwering & Lemken, 2020). The reasons for non-usage of FMIS are manifold and could range from a lack of knowledge, such as a low affinity for computer-based systems, to technical problems with the software itself, such as incompatible file formats or poor usability.

2.2.3 *Sensors and Wireless Sensor Networks*

To fill modern FMIS with data, sensors are a reasonable way to accomplish this. Sensor applications are manifold, for example sensors can be used to detect highly precise weather information for the given location, detect the soil moisture level or track animal health parameters. Besides the required physical sensing hardware itself, there must be a mechanism that forwards the gathered data. For sensors that are equipped on machinery, the sensor data is typically logged in the terminal unit. This allows to export data via a cellular connection (LTE, 5G) or manual transportation via a USB flash drive. But for the mass deployment of sensors in the field or on animals, there are special wireless transmission technologies of the category Low Power Wide Area Network (LPWAN). In contrast to *classic* wireless transmission standards like Wi-Fi or Bluetooth, LPWAN technologies allow for long range communication, up to several kilometers, as well as low battery consumption. A major drawback of LPWAN technologies is the low speed of connections, which is enough for most sensors' data transmission but not suited for the transmission of real-time multimedia streams. Table 2.1 presents three common representatives of LPWANs.

LoRaWAN is one of the most promising and popular LPWAN technologies, based on three useful properties: (1) comparatively long range, (2) availability of devices, and (3) possibility to build up own infrastructure or use existing public networks (mainly *The Things Network*), without additional transmission costs. LoRaWAN is an International Telecommunication Union (ITU) standard (ITU, 2021) managed by the LoRa Alliance. The most recent version to date is v1.0.4 (LoRa Alliance Technical Committee, 2020). A LoRaWAN setup consists of the following components (see also Figure 2.3):

- End device (ED)
    - Sensor or actor
    - Has cryptography keys onboard for device-to-application encryption
    - Connects with gateways (GWs) for sending/receiving data
- Gateways (GWs)
    - Receives LoRaWAN wireless transmissions and pushes data via common IP-based networks towards network server (NS)
- Network server (NS)
    - Manages GWs
    - Handles deduplication of multiple received LoRaWAN frames, when multiple GWs receive and forward an ED's transmission
    - Checks for transmission errors (e.g., *bit-flips*) and can request retransmission
    - Forwards data to the application server (AS)
- Join server (JS)
    - Handles (optional but recommended) Over-The-Air Activation (OTAA) process of an ED
- Application server (AS)
    - Decrypts payload to get raw data
    - Processes the raw data, e.g., forwarding the data towards an evaluation software system

The resulting topology of such LoRaWAN systems is stars-of-stars, i.e., multiple EDs can transmit data via one GW, and multiple GWs can connect to one NS, and so forth (see Figure 2.3). According to the LoRaWAN standard, a direct communication between GWs is not intended, as the advertised use cases are pure IoT applications. For this reason, neighbored LoRaWAN networks cannot be used to exchange data via the LoRaWAN physical layer (LoRa) innately.

Table 2.1: Comparison of three common LPWAN technologies, information taken from Mekki et al. (2019).

	SigFox	*NB-IoT*	*LoRaWAN*
Band	ISM	LTE/GSM	ISM
Network Operation	ISP	ISP	ISP/Private
Maximum Data Rate	100 bps	200 kbps	50 kbps
Range (rural)	40 km	10 km	20 km
Range (urban)	20 km	1 km	4 km

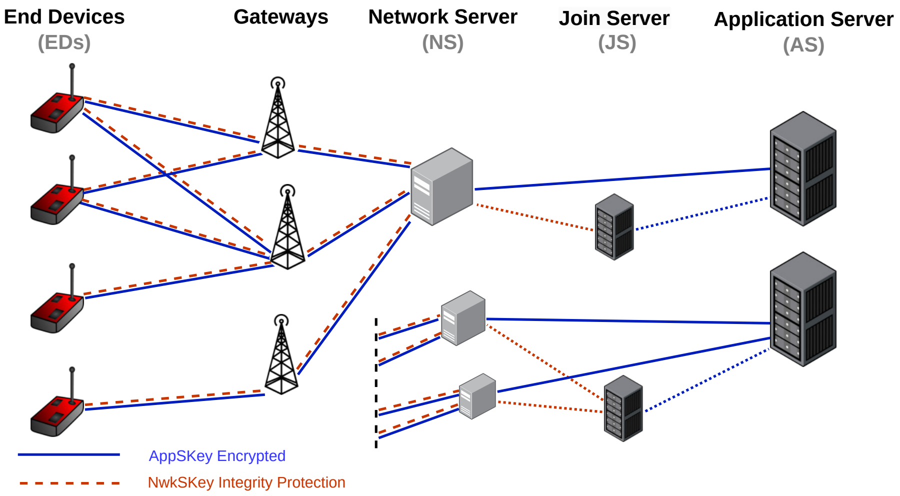


Figure 2.3: LoRaWAN stars-of-stars architecture with two cryptography keys for integrity protection (NwkSKey) and data protection (AppSKey).

2.2.4 *Resilient Networking Approaches*

In case of crisis events, communication becomes an especially essential tool. Rescue forces must be informed about individual emergency situations, and emergency personnel must be coordinated. But especially in dramatic crises, like natural disasters, existing communication infrastructures may break. The need for resilient networking thus leads to research in the context of autarkic peer-to-peer networking solutions.

A well-researched area is the use of Mobile Ad Hoc Network (MANET) for building up mesh networks with commonly available technologies like Wi-Fi or Bluetooth. But one limitation of such solutions is the limited range of those commonly available network technologies. In this realm, there are also some LoRa-based emergency communication solutions, like Meshtastic (Meshtastic LLC., 2023). One major drawback of these existing solutions is the need for specific LoRa modem boards, that are not widely distributed.

Unreliable devices are a big technical issue for network packet routing in crisis situations. This requires thinking of highly dynamic network topologies. The problem can be solved by relying on disruption-tolerant networking (DTN), also called Delay-Tolerant Networking. DTN was mainly developed for interplanetary communication by NASA, but gained attention in the emergency communication community. DTN solutions are commonly based on a *store, carry, and forward*-approach. With DTN, network packets are fragmented and the communication is no longer built up on guarantees of latency and hops. Network nodes act as data couriers, transporting data until an opportunity arises to exchange data with other nodes. Hence,DTN is not suitable for real-time applications such as videoconferencing or other applications that necessitate a stable end-to-end connection. However, it offers robustness and fault tolerance for applications that are capable of enduring delays in data transmission, such as messaging or sensor data transmission. Here, one area of application is disaster communication, when regular network infrastructure is disrupted, e.g., after natural disasters (Setianingsih et al., 2018; Zobel et al., 2022). The Bundle Protocol Version 7 (BP7) is the most recent Internet Engineering Task Force (IETF) standard (Burleigh et al., 2022) for such a DTN architecture. Additionally, different routing algorithms, e.g., *epidemic routing* or *Probabilistic Routing Protocol using History of Encounters and Transitivity* (PRoPHET) (Lindgren et al., 2012) can be used for distributing the bundles. This enables optimization for various properties such as fast/reliable bundle delivery or a minimum number of duplicates in the network. Besides advanced routing decisions that take into account, for example, geographic locations (Baumgärtner et al., 2020a; P.-C. Cheng et al., 2010; Sánchez-Carmona et al., 2016), there also exist other metrics which affect data dissemination across different convergence layers, e.g., duty-cycle restrictions when using LoRa (Msaad et al., 2021) or the workload of the involved nodes (W. Wang et al., 2021; S. Zhang et al., 2013). The `spatz` software uses some of these technologies (e.g., LoRaWAN, DTN, BP7) to provide a resilient emergency communication channel. The development and details of this software artifact are described in Chapter 13 (Section 13.7).

Summary – Background

- Forage production, arable farming and animal production have the biggest share of Germany's agriculture.
- Digitalization is an ongoing process in western farms, recent technology trends of smart farming involve more automation and data analysis for more precise processing.
- FMIS are important components of modern agricultural businesses, but still have a low adoption rate.
- The cloud pattern is omnipresent and heavily integrated into modern food production products, but it is not well compatible with technical-level resilience.
- Sensors generate the data required for precision agriculture.
- To be able to receive transmission from agricultural sensors, specific wireless transmission technologies are required that allow for long battery lifetime and large communication ranges.
- One prominent representative of such LPWAN technologies is LoRaWAN.
- DTN approaches are used for disaster communication systems, due to the property of transmitting data very reliably.

3

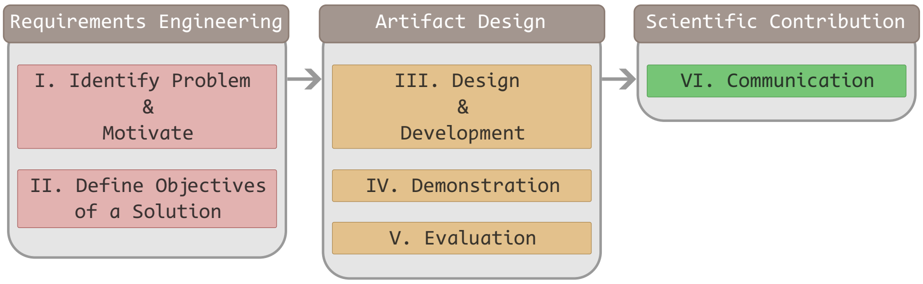
RESEARCH DESIGN

The motivation of this dissertation is to investigate threats to food security posed by the ever-advancing process of digitalization. Therefore, the strategy is to analyze the sector's current preventive measures, investigate security aspects of modern technology for smart farming, and develop artifacts that help to overcome the limitations of current technologies. This chapter presents the research approach, context, and methods used in this work.

3.1 Research Approach

> *'Design science research is a research paradigm in which a designer answers questions relevant to human problems via the creation of innovative artifacts, thereby contributing new knowledge to the body of scientific evidence. The designed artifacts are both useful and fundamental in understanding that problem.'* (Hevner & Chatterjee, 2010, p. 5)

The primary research field of this dissertation is crisis informatics, specifically informating crisis (Soden & Palen, 2018), with partial overlaps to the research areas of Human-Computer Interaction (HCI), Computer-Supported Cooperative Work (CSCW), and Wireless Sensor Networks (WSNs). As a common method especially in crisis informatics, design science research (DSR) was chosen as an overarching research paradigm. Peffers et al. (2007) propose a DSR methodology consisting of six major steps. From a methodological perspective, the six steps as applied in this dissertation can be divided into three groups: (1) requirements engineering, (2) artifact design, and (3) scientific contribution:



At first, the task is to identify a problem and motivate for the research. Analyzing the status quo leads to the problem and motivation of this dissertation.

Main parts are investigations (e.g., surveys) on how well farmers are aware of potential crises, and what precautions exist. The obtained empirical data is analyzed to get an impression of the status quo of the sector's resilience regarding digital technologies. Research about security of used technology (LoRaWAN) supplement the assessment. Based on the analyses' findings, the next step is to define objectives of solutions. One proper way for doing this is to derive requirements for new software artifacts. Based on the requirements, the next step is about the design and development of artifacts. Artifacts of this dissertation are system designs and graphical user applications with important parts in both, front end (UI) and back end (system logic). Typically, directly resulting from the implementations, a demonstration with prototypes as a proof-of-concept is done. The same software prototypes are also part of an evaluation. Depending on the generated software artifact, two different kinds of evaluations are used: real-world performance tests, and usability tests. Finally, the DSR methodology proposed by Peffers et al. (2007) argues for communication of the results, to spread the resulting knowledge. In the case of this cumulative dissertation, this is already integral, as only peer-reviewed and published (mostly with open access) papers are embedded.

3.2 RESEARCH CONTEXT

The research context is determined by several projects in which the co-authors of my publications and/or I were involved. Focus on the domain of agriculture was given by the participation in multiple projects, supported by funds of the German Government's Special Purpose Fund held at Landwirtschaftliche Rentenbank, namely: GeoBox-I, GeoBox-II, and AgriRegio. All those projects shared the desire for making digital technologies more resilient, or adapting already existing technology to enhance operational stability in outage scenarios. Ideas for working with networking technologies and the focus for crisis communication evolved from a short-time participation in the Collaborative Research Center (SFB) 1053 MAKI. Contacts from the projects allowed for an exchange of thoughts, ideas, and concepts, and also for sharing already developed tools or for organizing participants for empirical studies.

3.3 METHODS

As already described, multiple methods are applied to answer the RQs. Table 3.1 provides an overview of the specific methods used and their occurrence in the corresponding chapters. The following subsections present details on all applied methods.

Table 3.1: Applied methods at a glance.

Method	N	Chapter	Paper
Focus Group	52 52 67	7 8 10	A: Kuntke, Linsner, et al. (2022) B: Linsner et al. (2021) D: Kuntke, Kaufhold, et al. (2023)
Online Survey	118	7	A: Kuntke, Linsner, et al. (2022)
Systematic Literature Review	37	9	C: Kuntke, Romanenko, et al. (2022)
Usability Test	16	10	D: Kuntke, Kaufhold, et al. (2023)
Artifact Generation	1 1 2	10 12 13	D: Kuntke, Kaufhold, et al. (2023) F: Kuntke, Sinn, and Reuter (2021) G: Kuntke, Baumgärtner, and Reuter (2023)
Real-World Benchmark	1 1	11 12	E: Kuntke, Bektas, et al. (2023) F: Kuntke, Sinn, and Reuter (2021)

3.3.1 *Requirements Engineering*

According to Zave (1997), requirements engineering is "the branch of software engineering concerned with the real-world goals for functions of and constraints on software systems. It is also concerned with the relationship of these factors to precise specifications of software behavior, and to their evolution over time and across software families" (Zave, 1997, p. 315). There are a couple of scientific methods to acquire (Macaulay, 1996) and prioritize requirements (Riegel & Dörr, 2015). The concrete selection of useful methods depends on the goal of the requirements engineering process. In this dissertation, the application of requirements engineering methods is part of two phases:

I. Identify Problem & Motivate: Step one is about engaging with users to understand their needs. This enables the following steps to address real issues that are significant and relevant to all stakeholders involved. A mixed-method design (Johnson & Onwuegbuzie, 2004) is used in this dissertation to gain insights about the domain by getting information directly from stakeholders, who are primarily farmers. Mixed-method designs encompass both qualitative and quantitative methods to benefit from the advantages of each methodological approach.

Focus groups are an important part of the qualitative data in the dissertation, allowing an understanding of the field to be developed. Chapter 7 and Chapter 8 share one qualitative data set that consists of 12 focus group sessions with a total of 52 participants. The focus groups were conducted in different locations, with stakeholders of agriculture, mostly farmers. Recruitment was done with the support of collaborators in the research projects HyServ, and GeoBox-I. The focus group sessions were audio-recorded for a transcription. The inductive analysis of the transcripts by open coding allowed to sort and analyze the gathered statements. Qualitative findings based on this data set regarding technological dependencies of farm activities are used in Chapter 7 to create a question catalog for a quantitative survey. The resulting online questionnaire was distributed via the mailing list of a German association of farmers. In total 118 participants completed the survey. The resulting data made it possible to obtain further details about the precautionary measures taken by farms and to obtain an impression of the situation in Germany with concrete numbers.

A pure qualitative analysis in the form of Systematic Literature Review (SLR) (Kitchenham & Charters, 2007; vom Brocke et al., 2015) is used in Chapter 9 to collect security problems about modern technology with relevance for smart farming: LoRaWAN. Therefore, two RQs are formulated and used to derive keywords. The keywords are grouped into semantic similar words in the research context. Based on the groups of keywords, a search string as a *conjunctive normal form* is build. By using this search string on multiple scientific literature, databases are queried, which listed 403 publications. By utilizing inclusion criteria (e.g., "published between 2015 and 2021") and exclusion criteria (e.g., "not peer-reviewed"), these publications are filtered, resulting in a total of 37 relevant articles. Chapter 9 provides further details about the applied method, analyzes specific LoRaWAN security issues for the domain of agriculture, and compiles existing mitigation options.

II. Define Objectives of a Solution: Mainly by using focus groups as pure qualitative analyses, specific requirements are derived for software features and usability aspects. Parts of the focus group data set of Chapter 7 and Chapter 8 are also analyzed in Chapter 10, with the focus on software requirements that have an impact on the system architecture (back end) development. For interface design (front end) requirements, Chapter 10 evaluates also additional focus groups in a similar manner: inductive analysis by open coding of transcripts. In total, 69 participants contributed in 16 focus group sessions to the identification of 11 requirements (five UI design requirements, and six system architecture requirements). Chapter 10 contains further details on the requirements analysis process.

3.3.2 *Artifact Design*

Although sometimes more seen as an engineering approach, the creation of software artifacts is nevertheless an integral and important part of DSR that involves more than just writing program code lines. According to (Peffers et al., 2007, p. 55), this phase is even the core of design science. With certain objectives, the thoughts and necessary considerations regarding a feasible software architecture itself are important findings. Accordingly, step *III. Design & Development* is devoted to both, software architecture and implementation. This means, after a concept phase, that outlines the idea and desired software architecture, a concrete implementation is developed. The kind of implementation differs for each target, and incorporated frameworks and programming languages must be chosen wisely, to create an artifact that meets the requirements. Due to the research context in form of projects, there are also additional soft requirements, like compatibility to other project software artifacts, or usage of similar frameworks for easy integration of prototype parts into a larger application.

For the development of a UI application that should run on a multitude of end-devices (smartphones, tablets, laptops, etc.) a Progressive Web App (PWA) framework is used, called `Ionic`, in combination with `Angular`. Choosing such a framework allows using the same source code for multiple target device classes and operating systems with minor additional work. Chapter 10 provides further details on the concept and implementation. The artifact of Chapter 12 is a system architecture for using classic TCP/IP communication on top of LPWAN technology. In Chapter 13 farm distribution and distances between farms are analyzed to evaluate the possibilty of peer-to-peer connections between farms via autarkic wireless transmission technology. As no index of farm positions was found, a toolset for data mining and processing of geo-locations was developed. Hereby, `OpenStreetMap` as a public available source was used and processed with `Python` and `Jupiter Notebooks`. Another artifact of Chapter 13 is a server-software for building the main element of a crisis communication channel based on LoRaWAN technology. This software must run 24/7, should be efficient and also be reliable, which results in a `Rust` implementation.

In step *IV. Demonstration*, it must be shown, that an artifact is able to solve the given problem. Multiple ways are possible, according to Peffers et al. (2007), e.g., simulations, case studies, or proofs. Some of the artifacts of this dissertation themselves are part of a larger research effort, some serve just to demonstrate feasibility of solving an identified problem — and how it could be done. In this way, developed software artifacts of Chapter 12 and Chapter 13 are directly used for demonstrating underlying ideas and concepts in the most simple way: proof by example. Most of the implementations of this dissertation are also distributed as open source software[1] (artifacts of Chapter 13). This allows reproducability and enables researchers to build on top of the existing demonstrators.

As the development of a system itself is usually not sufficient to answer a dedicated RQ, the developed concepts and artifacts must be part to some extent of step *V. Evaluation*: "Without evaluating their new systems, designers can never know which techniques or methods are more effective, or why certain approaches fail. It is only through evaluation that designers come to understand the nuances of their design and add to the body of knowledge for other future designers to learn from." (Hevner & Chatterjee, 2010, p. 111) To check the usability of the created UI and its concepts, classic usability testing with 16 participants is performed as part of Chapter 10. Real-world tests are performed in Chapter 11 and Chapter 12. Simulations of DTN networks based on obtained real-world positions allow the comparison of two common routing algorithms for given conditions in farm neighborhoods in Germany (Chapter 13).

[1] open source software is released on GitHub: https://github.com/PEASEC/LoRaWAN-DTN, https://github.com/PEASEC/distance-statistics

3.3.3 *Scientific Contribution*

The step *VI. Communication* is necessary to distribute the knowledge gained. Goal is to "communicate the problem and its importance, the artifact, its utility and novelty, the rigor of its design, and its effectiveness to researchers and other relevant audiences such as practicing professionals, when appropriate" (Peffers et al., 2007, p. 56). In the context of this dissertation, the previously published and embedded papers, along with the present document, serve as the primary means of disseminating knowledge. Through these publications, the most important research results are made available to the scientific community and interested public. Three of these seven papers are conference papers, i.e., research talks at the conferences were part of the publication process. Additionally, in the context of this dissertation's topic, the two-time organization and moderation of a scientific workshop "RSFLab" (Kuntke, Eberz-Eder, et al., 2023; Reuter, Eberz-Eder, et al., 2022) were also part of the research and allowed to spread (partial) research results.

Summary – Research Design

- This work presents both analyses and solutions towards a more resilient, modern agriculture.
- The research conducted was mostly embedded in projects of the agricultural sector.
- A design science research (DSR) methodology with six phases was applied:
  I. Identify Problem & Motivate
  II. Define Objectives of a Solution
  III. Design & Development
  IV. Demonstration
  V. Evaluation
  VI. Communication
- Different methods were used in each phase, e.g.:
  - Focus groups (up to $n = 67$)
  - Systematic Literature Review
  - Software development
  - Usability test ($n = 16$)

4 FINDINGS

This chapter presents the main findings of the conducted research and its implications for the agricultural ICT. Key findings are separated into the following three areas: (1) Farms' Digital Dependencies and Vulnerabilities, (2) Towards a Resilient Software Architecture for Farm Management, and (3) LoRaWAN-based IoT Developments Towards Resilient Communications.

4.1 Farms' Digital Dependencies and Vulnerabilities

Multiple findings are part of the empirical, mixed-method research of this dissertation (Chapter 7 and Chapter 8), including qualitative focus group interviews ($n = 52$) and quantitative questionnaire surveys ($n = 118$). The incorporation of digital tools in agricultural operations often relies on the internet, making farms highly dependent on this infrastructure. Most farmers are not aware of how the internet and mobile network infrastructure affect their agricultural system and do not take any precautions for ICT breakdowns. Only 21 % (out of 46 participants who answered the corresponding question) indicated that their FMIS in use would work offline without limitations. But other applications and equipment are also indicated to be dependent on an internet connection, e.g., herd management systems (42 % of 39) or even agricultural machinery (27 % of 50). Another dependency in the software landscape of farm software stems from incompatibility — also known as *vendor lock-in*. Among the participants that use FMIS, 68 % (32 of 47) indicated incompatibility issues, i.e., data from a FMIS could not be used in another tool or machinery. Within the context of operational reliability in the focus groups, security of digital products itself was not mentioned as an issue. Also, the quantitative survey shows that only a small part of the farmers take measures against cyber attacks. Power supply is the most important requirement for software based systems. About 57.5 % (68 of 118) of the asked farmers stated that the time of operability is less than 24 hours after a blackout, on the other side, 14.4 % (17) stated that they could operate at least one week. Only 55 % (65) state that their farm owns an emergency power generator. However, farmers that are active in the livestock sector more often take precautions against outages than other farmers, both for higher dependency on continuous-working machinery and because of legal requirements.

As the empirical findings show, most farmers do not prepare well against digital "dangers" like data loss through software errors, hardware defects, or cyber attacks — even though according to research (Nikander et al., 2020a; Salam, 2020; Sontowski et al., 2020), IT security is one of the main issues for

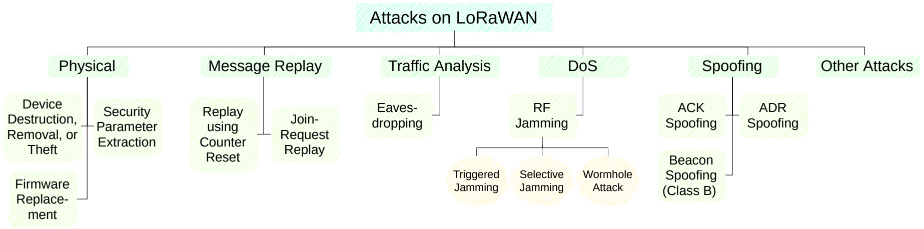


Figure 4.1: Attack types of the LoRaWAN vulnerabilities. Figure from Chapter 9.

sustainable, digital agriculture that relies on IoT applications. In particular, unsupervised EDs significantly increase the potential attack surface in contrast to other “smart” application areas, such as “smart home”, where most sensors are located in a physically protected environment. In order to further investigate this topic, a systematic literature review was conducted on LoRaWAN security issues and mitigations (see Chapter 9). The literature review identified several security issues with LoRaWAN, including RF jamming, physical attacks, and spoofing attacks (see Figure 4.1). While many LoRaWAN vulnerabilities have been addressed with version 1.1, some important issues still remain. Some of the detected mitigations for the existing issues, are rather easy to implement, including using multiple GWs with overlapping coverage, monitoring and traffic analysis, and avoiding Activation By Personalization (ABP). It is also important, to rely on devices with modern LoRaWAN versions (v1.0.4 or v1.1). Most farmers are unlikely to read into the security details of LoRaWAN, but most of these mitigations could be advertised in a software. For example a user could be warned before integrating an ED via ABP during the necessary sensor setup process.

4.2 TOWARDS A RESILIENT SOFTWARE ARCHITECTURE FOR FARM MANAGEMENT

As part of the digitalization in agriculture, farm management software is becoming increasingly important to control, plan, and document farming activities. The evidence from the previously described empirical findings and the existing literature (Fountas et al., 2015) revealed that modern farm software solutions require an internet connection for optimal operation and are not highly interoperable. One of the objectives of this dissertation is to analyze an offline-first software concept for farm management software, which is capable of resolving issues related to digital dependencies and vulnerabilities through a specific software architecture (Chapter 10). In order to be able to design a valuable farm management software base, end user requirements were derived from potential users and other stakeholders of agriculture. This process involved in total 57 experts who were interviewed using the focus group method. The derived 11 requirements were categorized into two groups: front-end (see Table 4.1) and back-end (see Table 4.2) requirements.

Table 4.1: List of identified requirements for interface design (front-end). Table from Chapter 10.

Requirement	Description
Tailorability for diverse agricultural subdomains	Support of different domains, customization according to their needs, i.e., granularity of information, and interfaces for interoperability with third-party systems.
Low complexity of field data filtering operations	Establish usability for personnel with less technical expertise, integrate usable data filtering views for field data, and automate the setup of background maps.
Location-independent technology support for field works	Support different devices, such as personal computers and smartphones (e.g., by responsive design) to allow operation both in field or office settings.
Prioritization and monitoring of field processing tasks	Allow for the prioritization of fields, display the progress of a task execution, facilitate the documentation of wage workers' days, and support time recording.
Navigation and recommendation system for wage workers	Provide a routing component for wage workers considering the width of paths and vehicles, giving tips for navigation, and suggesting the order of field processing.

The identified requirements led to the development of a conceptual framework for a comprehensive farm management software. The goal of the design was to be "crisis-capable", ensuring that it works as well as possible in outage scenarios, e.g., without relying on a working internet connection. The core element of the architecture is a small, local server that fulfills the purpose of a software backend, for a dedicated farm management interface that can be run on typical EDs like desktop computer, laptop, smartphone, or tablet (see Figure 4.2). It is a local data storage and can also serve local (in-house) server applications, for example a LoRaWAN NS.

Evaluation of the software via usability tests revealed a series of findings about the user perspective: Farmers appreciated the capabilities for offline operation. Aspects related to data protection were particularly requested by many participants, which is in line with the results regarding privacy issues of German farmers with digital products (Chapter 8). The included map functionality of the design was appreciated, but the used icons derived from classic geographic applications were not understood. The embedded form functionality was well understood, and the journal functionality was seen as important but with room of improvement in terms of usability and used specific terminology.

Table 4.2: List of identified requirements for system architecture (back-end). Table from Chapter 10.

Requirement	Description
Offline capability for infrastructure disruptions	Allowing the basic functionality without a proper internet access, e.g., by introducing caching mechanisms to offload data on the end-device pro-actively. Synchronization between multiple devices must be ensured.
Extendable and modular feature design	The basic feature set could be small but must be extendable by future modules (e.g., task monitoring and navigation features) that could be individual for different workflows.
Data sovereignty for confidentiality and privacy	Privacy and confidentiality are very important factors in this domain and must be respected. Therefore, outwards data transmission must be reduced to just permitted traffic.
Data safety and recovery mechanisms	Safety of data must be ensured, that is to say proper backup and recovery mechanisms. The whole backup process must be an integral property of the system, with a minimum on required user interaction.
Affordability for small and medium enterprises	The complete solution must be cheap in both acquisition and time for initial setup to align with the limited budget of small and medium-sized enterprises.
Integration of multiple and open data formats	To allow the integration into existing work processes, an easy exchange between established software must be possible by simple file exchange based on compatible file formats.

4.3 LoRaWAN-based IoT Developments Towards Resilient Communications

As LoRaWAN is one IoT protocol advertised with many properties that are especially useful for agriculture, like high ranges, low battery consumption, and the possibility of building own/autarkic networks, it is of interest, how well it performs in real life conditions. As there is a large gap between different ranges achieved in experimental setups, this work contributes a structured test series with range tests in Germany with common hardware (Chapter 11). For this purpose, protocols were established to document the results and circumstances, such as the weather and geographical setting, to ensure the reproducibility and comparability of all tests. The main tests allowed measuring effects of different geographical surroundings, by placing the LoRaWAN GW at a static position and moving away from the GW with EDs with varying distances and obstacles. The tests were conducted in different environments with varying degrees of vegetation, namely urban areas, dense forests, less dense forests, and agricultural fields with smaller hills, hedges, and groups of trees. The Global Positioning System (GPS) data of EDs and the GW, as well as a description of the surroundings, were recorded for future evaluation. During the tests, packets

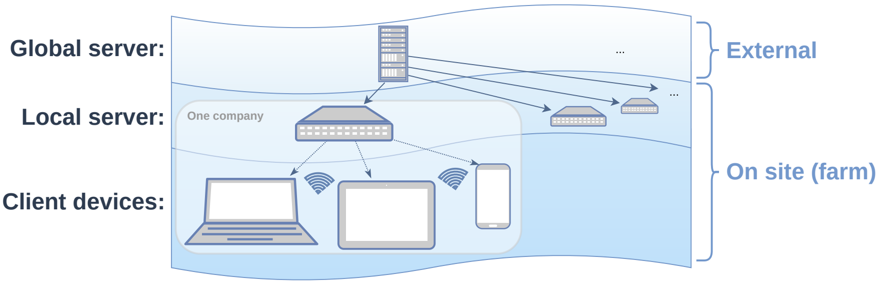


Figure 4.2: Scheme of the complete system, with the three different classes of devices: global server, local server and client devices. The concept of local (mini) servers is used to have a resilient data storage on the company level. Figure from Chapter 10.

were sent by the ED at regular intervals. Additionally, one of two hardware setups allowed the recording of received signal strength indicator (RSSI) and Signal-to-Noise-Ratio (SNR) values. In the tests conducted in urban areas, it was found that houses could impede and block the transmission, whereas trees and bushes did not have a significant effect on the transmission with the used hardware. In an agricultural environment, it was noticed that whenever a small difference in elevation, such as a small hill, blocks the direct line of sight (LoS) between the transmitter and receiver, the signal quality drops dramatically, usually resulting in a failed transmission. This effect, which potentially reduces the communication range from several kilometers to just a few hundred meters, seems to be especially a problem when both – transmitter and receiver – are on a rather low level near the ground, which could be the case for some emergency communication settings when holding communication devices in hands, like the one of Höchst et al. (2020). Additionally, it was found that transmission was possible as long as a direct LoS connection was ensured, meaning only until the transmission was blocked by trees.

As LoRa-based communication gained much attention in the recent years, one idea was to find a concept that allows for the usage of classic IP-based communication protocols via a LoRa communication channel, where a WiFi transmission range is not sufficient (Chapter 12). Such a concept has the potential to be useful in a variety of scenarios, such as creating redundant data transmission for critical information like error messages of cattle shed air-ventilation systems or connecting multiple stakeholders in cases of an internet outage. Based on an assessment of requirements and available technical options, such a concept with two LoRa-modems as a relay, was developed. One use case is to have a communication solution that could operate without relying on an internet connection, while still being able to transmit data reliably and securely. To test the feasibility of the concept, a test bed implementation allowed to confirm its general usability for different application protocols, distances, and settings. The implementation was successful and allowed the transfer of some classical network protocols to the LoRa physical layer, like HTTP, and, depending on the settings, even SSH-bidirectional-connections.

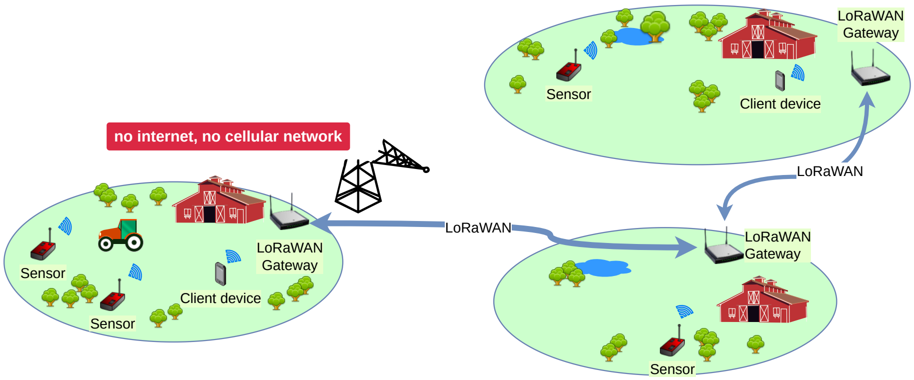


Figure 4.3: The concept of connected *farm islands* during an infrastructure outage.

To think the above-mentioned concept one step further, the connection of LoRaWAN-setups could build an emergency communication network, that is independent of the internet, and could be of use, when the regular network infrastructure has an outage (Chapter 13). The conceptual idea is depicted in Figure 4.3. Especially when farms already rely on IoT, the idea could be interesting, but requires also that farms are in a typical LoRaWAN communication range. By evaluating distances between neighboring farms, the feasibility of connecting them via LoRaWAN (or other wireless transmission technologies) could be evaluated. As access to a farm address database was not available, data provided by the OpenStreetMap project was used. A tool was developed in python to retrieve, process, and present the data. The tool's jobs can be grouped into three parts: retrieving, processing, and presenting. OpenStreetMap data was queried and filtered using the tag "landuse=farmyard" to approximate current farm business areas. Center points for each farm were calculated based on the filtered farmhouses, and a distance matrix was created. The matrix was used to evaluate the minimum distances between farms and the count of neighboring farms within a range of $[1, 2, 3, 4, 5]$ km. For example, the majority of detected farms (80,133 of 117,744; 68 %) has five or more neighboring farms within a 2 km radius, which is a feasible range for LoRaWAN devices in rural areas. In addition, it was tested how well multi-hop clusters can be formed in the data set using DBSCAN. Here, the high potential of a coverage was shown accordingly, if for example a radius of 2 km and a minimum size of a cluster of 5 farm buildings was set — in this case there are only 18,199 buildings (15.5 %) that are not part of a cluster (see Figure 4.4).

With the knowledge that many farms can connect to form clusters within a feasible radio range for LoRaWAN devices, the idea follows to create a software artifact that enables such clustering for disaster communication purposes. Integral to the derived concept is the use of robust DTN routing approaches to transmit data via neighboring farms. To determine feasible DTN parameters to start with, two scenarios were simulated: (1) only LoRaWAN transmission from one fixed farm building to another and (2) mixed-mode with additional moving pedestrians, having smartphones that allow WiFi ad-hoc data exchange between farms and other pedestrians. The simulation is based on real geographic data

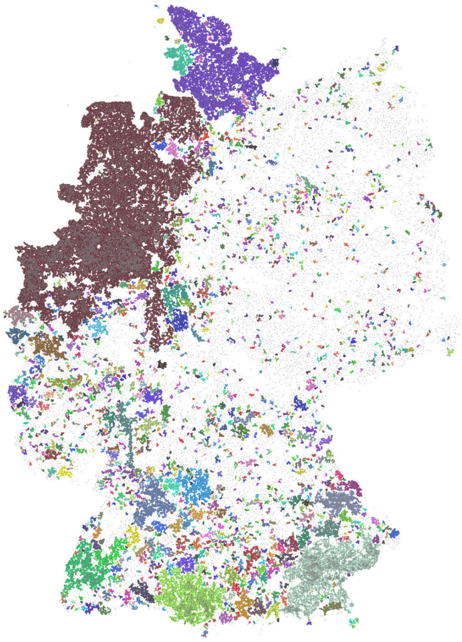
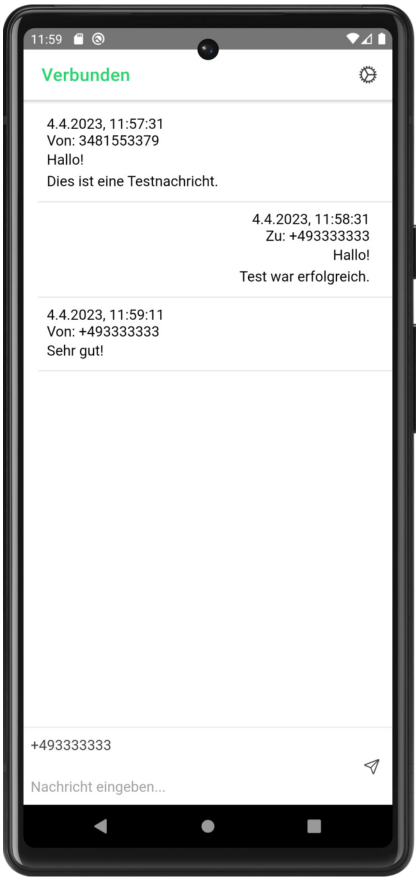


Figure 4.4: Visualization of farm clusters with DBScan and euclidean distance ($\epsilon = 2000\mathtt{m}$; $\mathtt{minPts} = 5$). Different colors represent different clusters of five or more farms, that could be connected via an wireless transmission channel with 2 km range. Light gray dots represent the detected farm buildings. In the eastern German states, there are statistically fewer but larger farm holdings, so that the average distance between farm buildings is greater. Accordingly, small clusters with few farms tend to form. Figure from Chapter 13.

extracted from OpenStreetMap. The ONE DTN simulation software is used for simulation of the network approach. The farm location dataset is further processed using k-means to reduce the size of large clusters to obtain more realistic sizes of neighborhood communities. The simulation is conducted on 40 randomly chosen clusters based on the 95 % confidence interval. Each cluster element is considered as a static node representing a farm and both PRoPHET and Epidemic routing protocols are used to evaluate the DTN routing performance. The simulation duration is 12 hours and both scenarios are simulated for all 40 clusters with 0.05 seconds update intervals. Results show that Epidemic routing outperforms PRoPHET routing in both settings. Especially the setting (1) with LoRaWAN transmission just between the static farms in combination with Epidemic routing performs very well with an average delivery probability of 99 %.

As the simulation results of the concept were promising, an implementation of a DTN on top of a LoRaWAN network followed. The goal of the DTN is to provide emergency communication capabilities between farmers in the case of a network disruption caused by natural disasters, infrastructure damage, or any other event that may cause a communication blackout. LoRaWAN GWs should connect neighboring farms in a multi-hop communication network.

The concept is implemented on top of the ChirpStack LoRaWAN NS, using the MQTT protocol to read LoRa frames and send messages through GWs. In the first version, a simple routing logic that processes bundles and identifies destination GWs based on the phone number of the recipient is implemented. The DTN bundles are encoded in CBOR, and the BP7 protocol is used for message delivery. As a requirement for the implementation, any farm should have a local server with an own NS software running, to collect and process data without limitations and running expenses. The proposed DTN software adds an emergency communication layer without interrupting the IoT setup in its regular operations. Additionally, a browser-based messenger client verified the functionality with a real hardware setup, consisting of three nodes. In a follow-up project, the existing system was also supplemented with an optimized UI for use on smartphones (see Figure 4.5).



4.4.2023, 11:57:31
Von: 3481553379
Hallo!
Dies ist eine Testnachricht.

4.4.2023, 11:58:31
Zu: +493333333
Hallo!
Test war erfolgreich.

4.4.2023, 11:59:11
Von: +493333333
Sehr gut!

+493333333

Nachricht eingeben...

Figure 4.5: Screenshot of messenger UI that works with the LoRaWAN emergency channel for smartphones from Orlov et al. (2023).

Summary – Findings

- Degree of own ICT-dependency on farming operations is unknown to most farmers.
- LoRaWAN as an IoT protocol with security-by-design has quite a number of security flaws, but most of those flaws can be mitigated.
- From the focus groups conducted, 11 requirements for operations management software could be identified.
- A software prototype and its usability evaluation have demonstrated that (and how) an architecture and UI for decentralized data management can be designed to improve farm resilience through capabilities for offline operations.
- LoRaWAN can achieve up to 3 km range in farm areas with simple setups.
- The majority (68 %) of detected farms have five or more neighboring farms in a 2 km range.
- Based on the investigation of farm location distribution, an emergency communication network for rural communities exploiting commodity IoT hardware was developed.
- LPWAN technology allows for building up a redundant transmission channel for mission-critical technology that usually requires classic TCP/IP connections.
- A developed software allows to equip already installed LoRaWAN GWs with an emergency communication channel for exchange of text messages between farms.

5 DISCUSSION

This chapter answers the RQs by discussing the findings (Chapter 4) and draws a bigger picture of how the results could enhance the stability of the farming system by designing crisis-capable software systems. At the end of this chapter, limitations of the conducted research are described as well.

5.1 The Risk of Failure of Technologies Used By Farmers

Based on the empirical findings (see Section 4.1), several factors were detected that influence resilience. A finding is that power outages can lead to serious problems for crop and animal husbandry farms — which can be treated as somewhat trivial, as those farms usually use devices that require electrical energy. Crop farms may only experience issues with office activities like documentation and billing, but animal husbandry farmers may experience downtime of devices crucial for the health of their animals, such as ventilation systems and milking robots. On the one side 57.5 % of the survey participants state, that their time of operability after a blackout is less than 24 hours. But on the other side, the average estimated fuel capacity allows to cover a few days to one week with emergency generators, which is consistent with statements made in the 2010 German report on technology assessment of long-term power outages (Petermann et al., 2010). The difference between both statements is important. Despite having an emergency generator and fuel supply, there is no guarantee that a power outage can be effectively managed. The generator could be for example to weak for powering all important devices. In any case, most operations will experience serious problems if there are outages lasting a few days or longer. Assessing consequences due to telecommunication outages is more complex for agricultural systems. Most studies indicate that these systems do not crucially rely on (wireless) network connections. However, there is a trend towards more digital communication technologies and interconnected devices in agriculture, creating greater vulnerabilities to outages in the future, as also noted by other research (Gupta et al., 2020b; Nikander et al., 2020b; Sontowski et al., 2020).

As the need for efficient farming processes increases, the adoption of sensor-based smart farming solutions is likely to increase (Sinha & Dhanalakshmi, 2021) – even if some issues remain, such as economic aspects, compatibility problems and usability aspects that must be adressed (Dörr & Nachtmann, 2022, p. 33, 386). Smart farming solutions have a strong dependency on the energy supply and on the telecommunications infrastructure, as well. While the sensors are often powered independently by long-life batteries, the rest of the process chain (GWs and computers for processing and evaluation) is usually supplied by the power grid and data are typically accessible through a web service. The introduction of offline-capable modes for new agricultural applications that rely on ICT would increase the resilience of the systems, as the continuity of agricultural processes is crucial even in the event of an infrastructure failure. Such modes must allow users in the community to work in offline scenarios, e.g., by always caching the most important data on the client side as well as in the application itself, as it is also part of the proposal of *local-first* software by Kleppmann et al. (2019).

When it comes to stationary sensor applications for agriculture, LoRaWAN is a promising technology, possibly the most relevant transmission standard for IoT applications in agriculture. However, it faces several issues that are independent of the application domain. The literature study revealed that newer versions of LoRaWAN, have much fewer known attacks compared to older ones. Despite the improvements brought by the latest 1.0 release (v1.0.4), it still has more known vulnerabilities than its successor, v1.1. But most devices — even new devices in 2023 — rely on a v1.0 protocol version. Some of the vulnerabilities can be particularly dangerous when agricultural IoT systems are targeted. For instance, an attacker could gain unauthorized access to an ED and potentially manipulate data or even take control of an entire irrigation controlling system. Unfortunately, this is not a hypothetical threat as multiple commercial EDs advertised for the agricultural sector (such as electric valves and soil moisture sensors) are still equipped with LoRaWAN v1.0.2 or v1.0.3. This makes these devices susceptible to various attacks, some of which can only affect a specific ED while others may compromise the entire IoT system by feeding incorrect or potentially malicious data into an irrigation controlling system. To ensure the security and reliability of agricultural IoT systems utilizing LoRaWAN technology, it is crucial to stay informed about the latest vulnerabilities and implement appropriate countermeasures, such as regular software updates and strong encryption protocols, as the findings have shown.

The relevant points for RQ1 (*To what extent are the technologies used by farmers at risk of failure?*) include:

- Most farmers state that they could keep their operations for less than 24 hours after a blackout.
- Animal husbandry farms are more severely affected from outages, but also tend to have more precautions in the form of emergency generators.
- Digital solutions like sensor networks have additional vulnerabilities in the realm of IT security.
- LoRaWAN is a promising representative for agricultural sensor networks that has some vulnerabilities despite built-in security features.
- If existing sensors do not allow updates to newer, more secure protocol versions, then other measures can help depending on the situation to reduce the attack surface.

5.2 Concepts and Prototypes as Demonstration of Resilient Smart Farming Technologies

Resilient IT for Farm Management. Based on the empirical findings, an average farm is well prepared against vulnerabilities of electrical devices, e.g., by having an emergency power generator as well as enough fuel to let it run for multiple days. With increasing digitalization, however, the basic software should also be given an "emergency operating mode". The objective is to guarantee that modern operating practices will continue to function, even in the event of a disruption affecting the digital realm, such as large-scale power outages or destroyed network infrastructure, despite the fact that they rely on smart farming technologies. The idea of an operational mini-server (Hofbox) is founded on precisely this line of thought. In the GeoBox projects, in which parts of the dissertation were developed, a corresponding mini-server was designed and partially implemented. This mini-server is used for caching and synchronization purposes. Multiple ex- and import functions within the client-application to manually manage data in unforeseen situations should counteract the problem of lock-in effects, especially for crisis situation that may need a quick adaption of workflows. The main point of this concept is that data storage and data management take place directly on farm site. This is in line with the suggestion of Kleppmann et al. (2019), who note that more application developers should work towards decentralized systems, for example by improving offline support or improve UI for such offline-capable "next generation of applications". The conducted usability test did not find major drawbacks and user statements did not indicate problems or negative preconceptions of the *offline-first* designed implementation. Several years ago, the overall concept of a mini-server would not have been economical feasible, because of both high hardware costs of capable devices and high energy demands. Nowadays, computer manufacturers offer affordable hardware that can be used as a mini-server while consuming not much energy (Kaup et al., 2018). The software developed in the projects is running on a rather small device (Advantech UNO-2271G with 4 GB RAM and Intel Celeron N6210, 2x 1.20 GHz), that consumes about 3.2 Watt with regular load , which is less than the consumption of a typical WiFi access point or network-attached storage (NAS) and comparable to single board computers like a Rasperry Pi 4. The developments and prototypes created in the context of this dissertation are adapted to the mini-server concept and its implementation. These results suggest that *offline-first* software development is not a matter of limited usability, but is an engineering task that should be considered for any software used for serious tasks.

The relevant points for RQ2 (*How to support information technology (IT) resilience for farm management?*) are:

- Change of currently dominant software distribution as remote running, centralized software (pure *cloud* software) towards decentralized systems is mandatory for increasing resilience.
- Offline-first or local-first principles can achieve such infrastructure independence, for example, a simple computer can be used as an internal

server, running applications and providing interfaces for other farm devices.

- A shift away from the cloud pattern, especially for management software, need not have a major, negative impact on usability.

USING IOT TECHNOLOGY TO INCREASE RESILIENCE. It was shown that LoRaWAN as a radio technology for smart farming applications can achieve a good range in agricultural areas of up to more than three kilometers without targeted optimizations. These results complement the previous test series under "practical conditions" (low transmission altitude, inexpensive equipment), which have so far mostly been carried out in urban regions and were able to achieve shorter ranges (Mdhaffar et al., 2017; Petrariu, 2021; Petrić et al., 2016). Building on this, several resilience-enhancing measures were designed using LoRaWAN. Developed proof-of-work prototypes were used to demonstrate their technical feasibility. One example is how conventional TCP/IP protocols can be translated into LoRa communication. This allows easy upgrading of older smart agricultural devices with long-range transmission capabilities. Another finding is that a majority of farms in Germany have a neighboring farm within a two-kilometer radius. Based on this neighborhood clustering result, the idea was developed that self-sufficient communication networks for short messages in emergency scenarios could be established using LoRaWAN hardware, which may be available for smart farming use anyway. This would significantly increase resilience to infrastructure failures and serve as a cost-neutral redundant data channel (with low bandwidth) during network outages. Based on this idea, a prototype was written in Rust that demonstrates the feasibility of such a system. It is able to route messages via several intermediate stations (multi-hop), i.e., sender and receiver do not have to be directly connected to each other, but can also exchange messages via several intermediate stations. An important aspect of this solution is, that this emergency addition has no major drawbacks regarding the usual IoT functionality, when the system is in an idle mode, being ready for usage in an emergency situation. The main difference to previous solutions (Baumgärtner et al., 2020b; Höchst et al., 2023; Suryadevara & Dutta, 2022) is that no specific device with custom firmware is needed – the wireless transmission is done with *off the shelve* hardware. As described above the developed system of this dissertation works in combination (but also standalone) with the remaining Hofbox ecosystem. By addressing]RQ3, this dissertation contributes valuable insights into how IoT technology can be harnessed to strengthen farmers' ability to withstand various challenges and maintain their operations.

The relevant points for RQ3 (*How could IoT technology be used to enhance farmers' resilience?*) include:

- It is possible to transmit classical TCP/IP communication over LoRa hardware for wireless data transmission of existing devices, such as barn climate control monitoring or data loggers with Ethernet.
- Hardware that originally serves for pure IoT applications can be used to build disaster communication networks.

- Specifically, this dissertation demonstrates that a multi-hop communication network can be implemented as an additional benefit of a regular sensor network. This system is capable of routing textual emergency messages in a neighborhood cluster, which is especially useful in the event of an infrastructure failure.

5.3 Limitations

In summary, while the results provide valuable insights into the potential applications of IoT technologies in agriculture, there are some limitations to note. First, the prototypes were primarily tested with real hardware, but not always on a farm. This raises questions regarding the evaluation of these concepts in real-world scenarios. In addition, while the prototypes show promising capabilities, they are largely artifacts intended to demonstrate scientific issues and have not been fully readied and tested for production use.

In addition, uncertainty about the concrete future of smart farming applications in agriculture itself and the extent to which potential disasters will have an impact are also important aspects to consider. For example, it is unclear whether it is necessary for farmers to communicate with neighboring farms at all in the event of a disaster. However, the system we have developed could also be useful in situations where infrastructure is unavailable for an extended period of time after the damaging event. This was the case, for example, in the Ahr Valley region of Germany in 2021, where some areas faced significant problems for several months due to the unavailability of fixed-line Internet connections.

It is also uncertain, how useful emergency communication channels over LoRaWAN will be when affordable satellite-based Internet, such as Starlink, have already become available. However, such a redundant system may also be beneficial here. This is because (agricultural) businesses usually only buy one of the two Internet connections - satellite or fixed network - and both can fail without affecting the LoRaWAN hardware and thus continue to function (free of charge).

Summary – Discussion

- Short power outages can be mitigated by most farms.
- Currently no business-critical dependency on the digital realm in the sector, which would be problematic in the event of short-term outages.
- Unknown how large-scale blackouts or ICT outages affect agriculture.
- Farmers are not able to take care of prevention regarding ICT just by themselves.
- A shift of software concepts towards decentralized systems could increase resilience capacities towards ICT outages.
- Usability is little to unaffected by the choice of a resilient system architecture.
- IoT transmission technologies have the potential to be used in times of crisis, e.g., by equipping commercially available devices with software that enables message exchange.

6 CONCLUSION

The topic of this dissertation concerns the resilience of modern agriculture, both in the present and in spite of software-based systems. The aim is to improve technical resilience, with the goal of reducing the susceptibility to failure and vulnerability of new software-based systems, and providing greater flexibility for unforeseeable events. It is only through the progressive development of interconnected systems in the field of smart farming that the questions of systemic security arise. One question to be answered is, how the negative effects of increased dependency can be counteracted through the clever design of software architecture and the use of existing (hardware) technology.

6.1 Key Findings and Implications

The first step was to examine how the sector perceives current problems and dangers, both in terms of direct dependencies and preparedness for infrastructure incidents. The core statement here is that in the case of "analog" threats such as power outages or logistical problems, it would be possible for average companies to continue operating for several days. An internet failure, on the other hand, would be difficult or even impossible to mitigate, precisely because many applications depend on a functioning internet connection. However, due to the lack of hard dependency of such software services, a corresponding outage is not critical to operations at the time of the survey. With increasing networking and reliance by industry on a functioning internet connection for products, this could change quickly in the future. In order to look in the direction of future-proof farm software, and what can be achieved with a clever choice of architecture under the premise of operational reliability, the GeoBox software was (co-)developed. The resulting system is based on the idea of a decentralized mini-server (called "Hofbox"), that stores all necessary data inside a farm. Parts of the development, conception and primarily also the evaluation are parts of this dissertation. Among other things, it could be shown that the decentralized architecture does not contradict a pleasant UI and was regarded as a positive or even desirable feature by the test persons.

As a future-proof wireless transmission protocol for sensor data, part of the thesis has taken a closer look at LoRaWAN and, among other things, summarized security problems and mitigations at the application level with a special focus on agricultural applications. Many of the problems would be solved with a more recent LoRaWAN protocol version, but the majority of available devices rely on a simpler and often outdated protocol version – however, even for these versions, ways have been found to make certain attacks more difficult, though not all vulnerabilities have been closed. As further research results with LoRaWAN in agricultural environments have achieved good ranges of over 3 km despite simple antenna locations, we continued to examine how the protocol might lend itself to further "enhancing resilience" use cases. Here, the results show that, on the one hand, classic IP (UDP and TCP) based applications could be adopted to transmit data via the LoRa transmission channel, if they have low bandwidth and latency requirements. On the other hand, an emergency communication system could be developed that integrates non-invasively into an existing LoRaWAN NS, running for example on a Hofbox inside a farm. This extension allows users to send short messages via the self-sufficient LoRaWAN-based network in multi-hop mode using smartphones or PCs that are connected to the Hofbox via WiFi or Ethernet.

The dissertation has shown that there are no major issues with digital dependencies for resilience in German agriculture at this time. Still, digitization has not yet that advanced on a broad scale, so that many farms have not yet started using smart farming solutions. Nonetheless, given that such solutions are deemed to possess significant potential for enhancing the efficacy and resource efficiency of farming, their widespread adoption is likely to occur in the future. But these technologies also come with a higher risk of being vulnerable. This dissertation demonstrates that it is possible to design and implement system architectures that continue to function in the event of infrastructure failures and are accepted and even valued by potential users. Another discovery is that IoT technologies can be utilized for other communication purposes, such as long distance, power-saving data transmission without disrupting regular operations. This could prove to be a valuable tool, particularly in crisis situations, as it allows individuals to communicate independently of external network operator technologies, even if those individuals are not technically proficient. To summarize, the following key messages for developers and researchers with focus on agricultural systems emerge from this dissertation:

1. *Preparation for power outages takes place:* An average farm can power itself for several days in an emergency situation based on emergency power generators and the fuel stock. Energy for essential (low power) IT equipment could be provided for longer period of time. (See Chapter 7)

2. *No well-known preparation against ICT outages, yet:* The whole idea of preparation against multiple days long ICT infrastructure outages is a new territory. There is only few research and there are no known *ICT crisis capable* tools in practice. This also means that as a researcher or developer you can (and must) discover new paths. (See Chapter 7)

3. *Crisis-capable development does not influence user perception:* Software design patterns that target the ability to act in times of crisis, e.g., requirement for local data storage hardware or extensive import and export capabilities, were not perceived negatively by most participants in tests and were even desired. Accordingly, from the user's perspective, if there were a choice between pure cloud applications and offline-capable applications, the latter would be preferred, with otherwise identical features. (See Chapter 10)

4. *LPWAN technologies are options for resilience enhancement:* LoRaWAN as a popular LPWAN technology has served for two resilience enhancing solutions. Especially noteworthy is the emergency communication layer, for a messenger application that connects rural neighborhoods. Such a system could allow neighbored farms to communicate via text messages, when ICT infrastructure is not available. (See Chapter 12 and Chapter 13)

5. *Crisis preparedness features as an integral "bonus" feature:* Pure solutions for crisis preparedness are generally not purchased without further reason. Even where there is a legal obligation, there seem to be exceptions where no provision is made accordingly. The advantage of software systems here is that emergency functions, such as an autarkic communication system, can be delivered directly with the system or even added via an update. Emergency functions can thus be distributed more quickly and easily as part of a larger system. (See Chapter 13)

6.2 Future Work

Future work should test the practicality of the emergency communication system to identify further potential for improvement with end users. Furthermore, more research should be done on systems and architectures that ensure at least rudimentary functionality even in cases of infrastructure failure. This is because progressive miniaturization is making it possible to pack more and more computing power with high storage capacities into a small form factor, which means that local data processing can be established at a high level with available resources. For example, smartphones are already sufficiently powerful even for many productive software applications and, accordingly, sophisticated data processing and storage can take place directly on these devices, which could then synchronize with each other. Also, more research should be done in the future on actual security vulnerabilities of agricultural equipment and software. This is because, with increasing digitization and, at the same time, greater importance of optimized farming for global food safety, the motives of malicious attackers are also increasing, who, for example, paralyze farms with ransomware or carry out politically motivated large-scale attacks on widespread systems in agriculture.

Summary – Conclusion

- ICT for agriculture needs to be critically questioned regarding its dependencies.
- Especially with the trend towards more digitalization, agricultural software-based systems should follow a resilient system design.
- This work highlights the yet less emphasis of technology resilience in the sector.
- Also this work shows some approaches, e.g.:
  - A decentralized approach can be built and have a usable UI.
  - IoT network technologies can be exploited for building an additional emergency communication channel, that might help rural areas in times of crisis events.

II

PUBLICATIONS

7

RESILIENCE IN AGRICULTURE: COMMUNICATION AND ENERGY INFRASTRUCTURE DEPENDENCIES OF GERMAN FARMERS

ABSTRACT Agriculture is subject to high demands regarding resilience as it is an essential component of the food production chain. In the agricultural sector, there is an increasing usage of digital tools that rely on communication and energy infrastructures. Should disruption occur, such strengthened dependencies on other infrastructures increase the probability of ripple effects. Thus, there is a need to analyze the resilience of the agricultural sector with a specific focus on the effects of digitalization. This study works out resilience capacities of the interconnected technologies used in farm systems based on the experiences and opinions of farmers. Information was gathered through focus group interviews with farmers (N = 52) and a survey with participants from the agricultural sector (N = 118). In particular, the focus is put on the digital tools and other information and communication technologies they use. Based on a definition of resilience capacities, we evaluate resilience regarding energy and communication demands in various types of farm systems. Especially important are the resilience aspects of modern systems' digital communication as well as the poorly developed and nonresilient network infrastructure in rural areas that contrast with the claim for a resilient agriculture. The result is a low robustness capacity, as our analysis concludes with the risk of food production losses.

ORIGINAL PUBLICATION *Kuntke, F., Linsner, S., Steinbrink, E., Franken, J., & Reuter, C. (2022). Resilience in Agriculture: Communication and Energy Infrastructure Dependencies of German Farmers.* International Journal of Disaster Risk Science, 13*(2), 214–229. https://doi.org/10.1007/s13753-022-00404-7*

NOTE Supplementary material of the qualitative and quantitative studies can be found in Appendix A.

ACKNOWLEDGMENTS This work was supported by funds of the German Government's Special Purpose Fund held at Landwirtschaftliche Rentenbank in the projects Geobox-II and AgriRegio, by the German Federal Ministry for Education and Research (BMBF) in the project HyServ (01IS17030B), and by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation)—251805230/GRK 2050.

7.1 INTRODUCTION

Digitalization, especially the interconnection of modern equipment for agricultural production, is a major issue in the agricultural sector. The desired positive aspects are an increase in efficiency and effectiveness and a more resource-friendly production of food. Digital, interconnected tools could open up new paths to profitable and socially accepted agriculture that benefits the environment, biodiversity, and farmers (Weltzien, 2016).

Smart farming tools can be useful in gaining precise information about crop conditions for planning farming practices according to specific phenological stages and thus improving, for instance, the timing for harvest, pest control, and yield protection (Braun et al., 2018; Yalcin, 2017). But the increasing usage of digital solutions may also increase agriculture's dependence on digital infrastructures. Current resilience assessments (Meuwissen et al., 2019; Perrin & Martin, 2021; Snow et al., 2021) for agriculture lack a specific view about the digitalization of agricultural systems and the possible consequences of its interactions with other key systems like the energy and communication sectors. Unintended consequences could be new risks and threats to the business of farms and - from a global perspective - also to food safety. As Darnhofer (2021, p. 3) states: "While much research has focused on developing efficient processes and increasing productivity, much less research effort has gone into understanding what enables agricultural systems to navigate unexpected change". Going further within the research area of food system resilience, we will investigate organizational behavior in (technical) emergencies as well as the digitalization process from a farmer's point of view, and draw conclusions about potential risks in relation to the current digitalization process, using the situation in Germany as an example for modern, technology-driven agriculture. This study is guided by the following research questions:

- *RQ1:* What potential risks are associated with the use of digital tools, especially related to infrastructure failures for farm systems?
- *RQ2:* What are the resilience capacities associated with the use of digital tools of agricultural companies?

The remainder of this article is structured as follows: In Sect. 7.2, we present the definition of resilience used for this study as well as the problems and vulnerabilities associated with modern agricultural technology, for example, smart farming tools. Section 7.3 describes the focus groups we conducted, in which a total of 52 farmers participated. In order to verify our preliminary findings of the qualitative study, we conducted a quantitative survey on specific topics with 118 agricultural experts, which is described in Sect. 7.4. Subsequently, in Sect. 7.5, we contribute to the existing literature by relating the answers of both the qualitative and quantitative studies to the definition of resilience and to the digitalization process in agriculture. Finally, in Sect. 7.6, we conclude with a summary of key findings and set out possible future research.

7.2 State of Research

In order to meet the social responsibility of agriculture as critical infrastructure (CI), digitalization through the incorporation of new technologies in agriculture has become a major issue. We present the current state of digitalization as well as already known risks coming along with the increased usage of information systems. We also present a framework for resilience assessment of farm systems and derive a research gap.

7.2.1 *Interconnected Technology in Agriculture*

Scrutinizing the current literature, various obstacles and problems as well as current trends regarding the effective and efficient use of digital, interconnected technology in farming business can be identified. First, the use of communication tools is changing. Communication is of great importance in the daily work routine of a farmer. Arrangements with employees or external contacts, such as suppliers, subcontractors, or clients, are increasingly incorporated into new technologies. A study by Hobe et al. (2019) investigates the ways farmers communicate and expected developments between 2017 and 2022. According to their results, in 2017 only 15% of German farmers considered digital services (email, messenger, and cloud services) as their most important means of communication for their everyday work routine, while 36% anticipated digital services as their principal means of communication in 2022. Braun et al. (2018) state that in the agricultural sector, smooth communication and information exchange along the supply chain is essential; only limited attention has been drawn to this topic. Shang et al. (2021) propose a framework for modeling adoption and diffusion of digital farming technologies based on reviewed literature. As the authors state “only a few recent studies highlight the importance of attributes of technology (e.g. compatibility to existing farming equipment, complexity and data safety)” (Shang et al., 2021, p. 12) .

Another important issue is the demand for Internet connectivity. The analysis of wireless sensor networks for precision agriculture by Jawad et al. (2017) discovers that current approaches typically propagate an Internet connection to cloud services as a means to analyze sensor data and provide access via client computing devices, such as tablets. At the same time, technologies like cloud services have proven vulnerable to threats such as cloud-service breakdowns or Internet outages (Aceto et al., 2018). Moreover, the digital infrastructure in Germany is characterized by a digital divide, which means that rural areas have less access to high-bandwidth Internet connections than urban areas; for example, 4G networks provide 73.5% coverage in rural areas, 82.2% in urban areas (Rizzato, 2019). Faults in interconnected technology may be caused by several factors. For a first overview, it is useful to distinguish between information and communication technology (ICT) related and energy-related failures.

ICT-RELATED INCIDENTS: In general, there are many different causes of ICT disruptions that are not energy-related. Aceto et al. (2018) offer a categorization that evaluates incidents on three axes: origin (natural/human), intentionality (accidentally/intentional), and type of disruption (physical/purely logical). An example of ICT outages caused by natural circumstances that result in the physical damage of ICT infrastructure is the fiber cable cut by undersea currents that put the Commonwealth of the Northern Mariana Islands offline for three weeks in 2015 (Aceto et al., 2018; SubCableWorld, 2015). As far as human-caused failures are concerned, there are cases of intentionally caused ICT outages. The Internet shutdown in Egypt and Libya in 2011, for example, was carried out by the government for censorship reasons (Dainotti et al., 2011), as were ransomware or distributed denial-of-service (DDoS) attacks that resulted in large cyber crises in the UK in 2017 and Estonia in 2007 (Backman, 2021). A common example that accounts for the majority of Internet backbone disruptions is the accidental damage to submarine cables through fishing activities and dragged anchors (The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2019). Purely logical disruptions, like prefix hijacking, can also lead to major constraints with regard to the accessibility of a web service (Ballani et al., 2007). Even on the level of farms, network technology like wireless sensor networks could be attacked (Kuntke, Romanenko, et al., 2022).

ENERGY-RELATED INCIDENTS: On many farms, especially in livestock farming, certain facilities (like ventilation) depend on a permanent power supply. Power outages can therefore result in the loss of an entire livestock population. Storms and floods are the most prevalent causes of major power outages in Central Europe (Mahdavian et al., 2020). For example, during a three-day power outage after a blizzard in northwest Germany in 2005, most of the farmers had to secure their livestock facilities through generators (Gerhold et al., 2019). In some cases, livestock farms without functioning backup energy supply lost all their livestock within hours of disconnection (Pfohl, 2014; Schröder & Klaue, 2005), as weather conditions prevented taking animals outside and multiple critical situations at different locations at the same time required triage. Obviously, most of the interconnected technology also depends on electrical energy. While some of these systems, such as outdoor sensors, could run on battery, information technology (IT) hardware, monitoring of a ventilation system, or smart valves could require a stationary power source. The increasing reality of cyber hazards, and the related need for systems to become more resilient, has pushed CI protection and resilience in the information system sector up the agendas across a range of domains.

7.2.2 *Resilience Assessment of Farm Systems*

In this article, we focus on the impact of digital technology for farm systems on resilience. The term resilience varies depending on the context of application, such as engineering (Francis & Bekera, 2014) or ecology (Holling, 1973) which is why a universal definition is not possible. According to Tendall et al. (2015,

p. 18), for food systems “resilience can be broadly defined as the dynamic capacity to continue to achieve goals despite disturbances and shocks”.

To assess the resilience of a system, however, a suitable framework is needed. A contribution by the European SURE-Farm project highlights the complexity of agricultural systems and states that previous studies mostly focused on agricultural production processes (Meuwissen et al., 2019). The authors therefore propose a resilience assessment framework that incorporates not just agricultural production properties, but also farm demographics and governance. Even more important for this paper, the authors define three resilience capacities, which are needed to evaluate a systems’ resilience: robustness, adaptability, and transformability. According to Meuwissen et al. (2019, p. 4) robustness is the resilience capacity “to withstand stresses and (un)anticipated shocks”[sic]; adaptability is the capacity that allows a system to adjust to undesirable situations by undergoing some changes, but without changing the internal structures; transformability represents the capacity to significantly change internal structures to return to normal or improved operations.

We understand resilience not only as crisis management but also as a preventive and foreseeing concept. The goal of resilience is the regular continuity of the system under every circumstance. This is especially important when taking into consideration the characterization of farm systems as CI.

7.2.3 *Research Gap*

Nearly all of the scientific literature on ICT for agriculture is concerned with improving agricultural operations through greater automation or increased precision - see, for example, Gu and Jing Y. Gu and Jing (2011) and Wolfert et al. (2017). Few works describe dangers resulting from increased dependency on other infrastructures like electricity generation and telecommunication (Moteff et al., 2003; Reuter et al., 2019), which are very important to consider in light of possible disaster situations. Against the backdrop of agriculture being CI and the increasing use of smart farming technologies, the investigation of IT resilience in the context of agriculture seems to be even more crucial. Gurschler et al. (2017) point out that the usage of ICT in CI creates new risks and threats for the IT infrastructure, and for that reason, it is important to engage all actors in proper risk assessments.

Beyond agriculture, providers of other CI also should be aware of their responsibility and possible precautions for potential risk scenarios (O’Rourke, 2007; Rademacher, 2013). This is essential in order to build a shared understanding of disasters and to comprehensively evaluate past incidents (Monteil et al., 2020). Existing case studies (Meuwissen et al., 2019) or other recent works (Perrin & Martin, 2021; Snow et al., 2021) do not cover our work’s technology-driven subject of study, but rather focus on aspects of socioeconomic resilience. In contrast, we focus on the impact of the increasing usage of digital tools on the resilience of agriculture. To our knowledge there are currently no empirical studies that address this aspect of resilience and the preparation for disasters in the sector of agriculture in general and especially for agricultural IT systems.

7.3 QUALITATIVE ANALYSIS

In this section we document the methodological procedure within our qualitative study. To answer our research questions (see Sect. 7.1), focus group interviews (Kitzinger, 1995; Morgan, 1997) were conducted with a concentration on resilience in agriculture, especially ICT, and how ICT disruption is considered a possible danger for the regular working procedure on farms.

7.3.1 *Method and Data Description*

To avoid (subjective) biases, the focus groups were led by two of our researchers in face-to-face meetings in 2019. The researchers did not have the impression that the participants had hidden agendas or intentionally tried to hide information (Kontio et al., 2004). The researchers conducted 12 focus group interviews (Table 7.1) can be considered expert interviews since all the participants were experts in agriculture. The entire process, which comprised the creation of an interview guideline, recruitment of participants, conducting the focus groups, and data analysis and storage, followed the guidelines of the ethical commission of the Technical University of Darmstadt. The original guideline can be found in Appendix A.1.1. Some results of these focus groups have already been published in a scientific journal (Linsner et al., 2021); however, the data were analyzed with a different scope and purpose.

Table 7.1: Distribution of participants of the focus group interviews.

Focus Group	Participants
fg1	P1, P2, P3, P4
fg2	P5, P6, P7
fg3	P8, P9, P10
fg4	P11, P12, P13, P14
fg5	P15, P16, P17, P18
fg6	P19, P20, P21, P22
fg7	P23, P24, P25, P26, P27
fg8	P28, P29, P30, P31
fg9	P32, P33, P34, P35, P36
fg10	P37, P38, P39, P40, P41, P42
fg11	P43, P44, P45, P46, P47
fg12	P48, P49, P50, P51, P52

Participants

Since we are working in publicly funded research projects (HyServ and GeoBox) with partners from the private sector, federal institutions, and associations for farmers, such as machinery rings, their clients and members were invited to participate in our focus groups. Participation was voluntarily and no compensation was paid. Each participant was informed about the objectives and topics of the study and how their answers would be processed via an informed consent form, which was signed by each person. Every participant (N = 52) in our study owns or leads an agricultural business. This characteristic has ensured that participants at decision levels were involved. Most of them run farms, but some also are service providers for other farmers. Seven of the participants identified as female and 45 as male. Thus, the proportion of female participants is 13.5%. The latest numbers of the 2016 Eurostat database estimate that the gender ratio of the agricultural workforce in Germany is 32.4% women overall and 9.0% at the operational level of farm management (Eurostat, 2016). Hence, the gender proportion of our study depicts the gender ratio of farm managers in Germany closely. A large percentage (81%, N=42) of the participants are younger than 40 years. While their age group represents less than 15% of German farmers in 2016 (Eurostat, 2018), they represent current or future farm managers and therefore are an interesting target group for this study. Our sample covers multiple branches of agriculture, but these are not equally distributed (see Table 7.2).

Table 7.2: Branches the participants are working in (multiple answers possible)

Branch		**Amount**
Cultivation of grain		22
Viticulture		3
Cultivation of vegetables		1
Animal husbandry	Dairy cattle	12
	Beef cattle	4
	Pig housing	4
	Laying hens	3
	Biogas production	3
Service provision		6

Data Collection and Analysis

Data of the focus groups were collected through sound recording followed by transcription. We segmented the data into meaningful expressions using the constant comparison analysis method, which, in its first stage, is characterized by open coding (Onwuegbuzie et al., 2009). These included codes such as: general understanding; IT-risks; IT-prevention; Hardware/PC; Hardware/Tablet, and so on, to name just a few of the 34 codes in total (see Appendix A.1.2). Subsequently, we formed five categories by grouping the statements/codes: digitalization in agriculture, infrastructure on farms, processes, data protection, and resilience. The research process involved two researchers during both the focus group interviews and the process of coding. They both applied the method of constant comparison analysis independently from each other and compared and consolidated their results afterward. This allowed us to derive our results, as presented in the following section. Because the recorded interviews are in German, we translated the statements into English as literally as possible.

7.3.2 *Results of the Focus Groups*

In this section, we present the results of our interviews, where the constant comparison analysis method led to a grouping of all statements into the following aspects: (1) digitalization in agriculture and (2) resilience. An overview of the insights from the focus groups (Sects. 7.3.2 and 7.3.2) is given in Fig. 7.1.

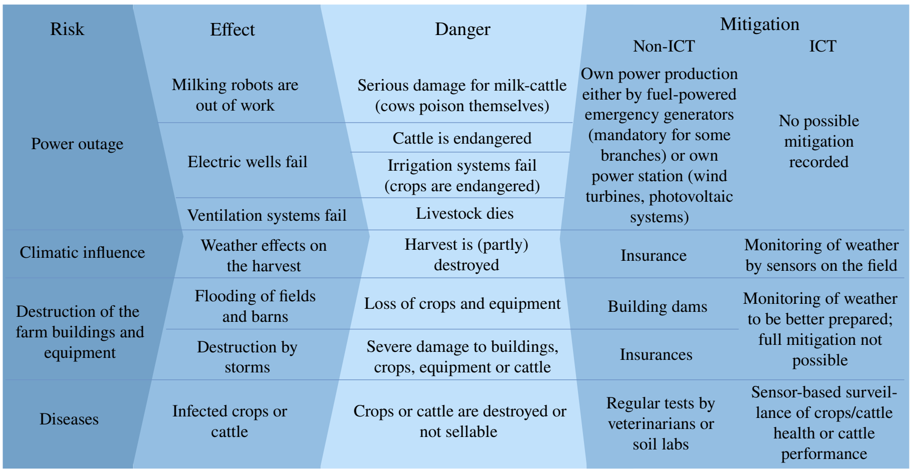
Digitalization in Agriculture

One central aspect regarding the general understanding of digitalization is summarized in the following statement: "What we used to write on paper is now digital on the PC" (fg5). Other statements mention that digitalization in agriculture contains the use of modern technologies for increased efficiency in conventional working processes as well as the automatic recording of processes on the field (abolishing the unpleasant task of manual recording).

When it comes to an individual's own experiences and examples, most but not all (7 of 52) of the participants state that they use digitalized hardware in their everyday work processes. As a result, a wide range of experience is represented. Whereas some participants with an already-digitalized work routine use digital tools for direct on-site recording and highly automatized vehicles with digital steering systems and section control, that is, a precise fertilizer application, others in contrast state: "Everything is still handwritten in our case" (fg8). Companies that practice arable farming mostly take advantage of section control, which heavily relies on satellite navigation of the tractors (fg4, fg8, fg10). Some of this hardware already relies on (mobile) network technologies for data exchange: "When I'm at the [fertilizer] injection, I just enter what kind of spray and how much. Then it's uploaded, and I read it on my computer, and I'm done" (fg11). Regarding livestock farming, there are also robots and corresponding software involved, for example, for monitoring the milk yield and milk quality of each cow. The aggregated data in the case of a dairy farm allows a highly detailed insight, which was commented as follows: "you see everything [. . .] the ingredients, the amount of milk from each cow [. . .]" (fg11). Office tasks that have to be performed on farms use common ICTs, such as telephone, computers, fax, or the Internet. Most participants' companies have a digital crop field card to keep track of all processes on their land. Processes such as application for state subsidies or invoicing as a temporary employment company require operational data of the company, precise recording of work, and transmission of digital forms. Such recording is typically done automatically by modern, digital tools, such as tablet-like tractor additions for recording all processes, "[. . .] just to be safe in billing" (fg10).

In line with these reported experiences, personal feelings and opinions differ greatly when it comes to digitalization in agriculture. Here, some of the participants see the small size of their company as an obstacle and express opinions like "Do you even need something like that?" (fg10). In contrast, others outline the possibilities, especially for small-sized agricultural companies, as for example: "With small structures, I actually think it makes sense to drive with things like RTK [Real Time Kinematic] or section control [...]. You get [the fertilizer] much better on the target areas" (fg10). Some participants would even like to see (more) digitalized solutions in their companies and describe their current condition of a nondigitalized company as "quite backward" (fg5). There are also some neutral statements, mostly with the central message that digital tools do not seem necessary and that the real benefit is hard to determine at the moment, like: "I think at the moment it is still a bit too early to draw conclusions. [...] In five or ten years, when the technology is even more mature, and even smaller companies can afford it, things will look different." (fg6). Negative opinions revolve around fears, risks, and problems and are mainly associated with the loss of data sovereignty and related consequences. Some participants have already thought about possible problems that could arise from the exploitation of their business data.

Another fear refers to the increasingly high level of dependence on technology, which, if it fails, can only be repaired by experts: "You are so dependent on the technology. In former times, one could still detect the cause [remark: of technical failures, e.g., in machinery] somehow by oneself or could try to get it [agricultural machine] back by oneself. And now there are error messages, and then it's over." (fg7). This is related to the dissatisfaction about the unreliability of certain products, incompatibility of devices, or frequently crashing software: "And when that [software error] happens several times a day, it's annoying." (fg7). A similar problem is the incompatibility of iOS and Android applications because some machine vendors only offer useful companion applications exclusively for one of these operating systems (fg4). A further, often mentioned problem is poor education on how to use digital products (fg6, fg7). Especially concerning is data sovereignty; one focus group mentions that it would be great to educate the owners of small-sized farms on how to build up a local Wi-Fi network that is secure and allows sharing certain data with third parties if required. It would be great "[. . .] if there would be training or enterprises offering a simple intranet or the possibility to just built up Wi-Fi on our farm with a server owned by ourselves, where we store the data and [. . .] which offers the possibility to share data [. . .]." (fg9), "We really want to share, in order to process it [the data]. [. . .] The only problem really is data protection." (fg9). Participants are generally aware of the importance of backups and the security of their computers, but report a lack of necessary knowledge. No participant mentioned the increasing dependencies on other infrastructures, like the Internet or the power grid, as a risk of digitalization, before the interview questions explicitly referred to this subject.



Risk	Effect	Danger	Mitigation	
			Non-ICT	ICT
Power outage	Milking robots are out of work	Serious damage for milk-cattle (cows poison themselves)	Own power production either by fuel-powered emergency generators (mandatory for some branches) or own power station (wind turbines, photovoltaic systems)	No possible mitigation recorded
	Electric wells fail	Cattle is endangered		
		Irrigation systems fail (crops are endangered)		
	Ventilation systems fail	Livestock dies		
Climatic influence	Weather effects on the harvest	Harvest is (partly) destroyed	Insurance	Monitoring of weather by sensors on the field
Destruction of the farm buildings and equipment	Flooding of fields and barns	Loss of crops and equipment	Building dams	Monitoring of weather to be better prepared; full mitigation not possible
	Destruction by storms	Severe damage to buildings, crops, equipment or cattle	Insurances	
Diseases	Infected crops or cattle	Crops or cattle are destroyed or not sellable	Regular tests by veterinarians or soil labs	Sensor-based surveillance of crops/cattle health or cattle performance

Figure 7.1: Tabular listing of the recorded risks within the focus groups with possible effects, and the resulting dangers as well as appealed countermeasures, with or without information and communication technology (ICT) to mitigate specific dangers

Resilience in Agriculture

Regarding the resilience of agricultural businesses, we focus on the domains of electricity and ICT, as we see both dependencies as possible sources for a reduction of resilience. We start with statements about the perceived threats of resilience followed by statements based on the definition of resilience capacities given in Sect. 7.2.2, which includes (1) robustness, (2) adaptability, and (3) transformability. The following statements are grouped into the domains we perceive to be possible causes for ripple effects—electricity supply and communication and Internet infrastructure:

RESILIENCE OF ELECTRICITY SUPPLY: Although many agricultural tasks involve tools that need electrical power, some technologies are particularly vulnerable (see Sect. 7.2.1). In order to (1) cover power outages, power can be self-produced: “We generate electricity via our wind turbine. Also, our whole stable area is equipped with photovoltaics.” (fg8). Many participants stated that cattle and pig breeding companies are required by law to have an emergency power generator (including sufficient fuel reserves for its operation) for (2) adaption in power outage scenarios. However, dairy farms that usually use milk robots would have to switch to a manual mode. This could decrease the milk yield, but harm in the form of diseases for their animals would be prevented (fg8). Based on these results, we can see that cattle farmers’ operations are weakened in terms of production quality and efficiency in power outage scenarios. Therefore, we hypothesize that farms that are also active in the livestock sector more often take precautions against outages (H1). Typically, the (3) restoration after a power outage is easy and fast in the domain of agriculture. But for some digitalized tools, a restart could take a long time. After a short power outage in a dairy farm "all the robots and boxes were off, the cows were still inside. So, nothing worked anymore. Until the whole system was started up again and running faultlessly, two days went by." (fg7).

Resilience of communication and internet infrastructure. The necessity of thinking about communication and Internet infrastructure in the form of both landline and mobile radio networks arises because the regular operations of agricultural companies require communication with various actors. Therefore, access to reliable communication infrastructure is essential. Since we assume a rising dependency on various digital communication products, we are interested in the opinion of the participants regarding the current state of reliability and possible dangers and risks in this field. In 2019 (as in 2021), many areas in Germany were still not covered by cellular networks. Since most of these blind spots happen to be in rural areas, the big majority of the general public is not affected, but farmers are disproportionately impacted. We hypothesize that the incorporated tools of agricultural operations are often dependent on the Internet (H2), based on the insight that machine vendors create new products that rely on - or at least take advantage of - a permanent Internet connection, and that this requirement intensifies problems such as missing coverage by cellular networks: "We have technical possibilities to use apps and to do everything. And then it depends on simple things like the bad internet. [...] I know two years ago that it took me all day to download an application." (fg4). Capacities for absorbing ICT outages appear to be difficult to build up, as there are rarely any suitable mechanisms for this improvement. In fact, no absorbing measure was mentioned by the participants. However, there are some ways to adapt in situations of failing telecommunications. In order to share data between companies, the usage of a USB flash drive is considered sufficient and secure and is not perceived as more demanding than sending it to the tractor directly, although it requires more time for data transport (fg2, fg9). This applies also for the exchange between employees of the same farm or between different devices or for business communication: "Yeah, well, you know where the contractor lives. You can still go there in an emergency and discuss everything with him/her." (fg4). The restoration after a communication and Internet infrastructure outage is seen to be as simple and fast as electricity supply. It was not mentioned as problematic at all, since all the tools reconnect automatically and phones are working again on both sides.

7.4 Quantitative Analysis

Based on survey data, we are able to test hypotheses derived from the qualitative study (Sect. 7.3.2) and gain more insight into the topic of technological resilience in agriculture. This section elaborates on both descriptive results and hypothesis testing.

7.4.1 *Method and Data Description*

Using an online questionnaire, we asked German farmers about resilience in agriculture, dependencies on other infrastructures with a focus on ICT, and potential outage scenarios that could harm their agricultural operations. Initially, this survey was planned to be conducted offline at different agricultural events in 2020. However, these were canceled due to restrictions during the COVID-19 pandemic.

Participants and Procedure

The participants were recruited via the mailing list of a German association of farmers. In the survey, we asked for the participants' specific working conditions. Most of the participants (111) worked as farmers in Germany, and five worked in related business segments, such as food production or agricultural machinery production. Two participants did not specify their employment, but they are also active in the domain of agriculture as recipients of the mailing list. The survey includes farmers working in larger businesses (see Table 7.3) and covers a more diverse selection regarding age and location than did the focus groups (Sect. 7.3). Participation was voluntary and not compensated. Within the survey, we collected demographic information and information about the agricultural enterprise in which the participants worked. The age distribution was recorded in categories (see Table 7.4) with 73% of participants in the age groups 31-60. The geographical distribution of the participants' work areas in Germany is shown in Fig. 7.2.

Data Collection and Analysis

For the collection of data, the software `LimeSurvey 3.17.0` was used on a self-hosted server. The questionnaire consisted of 50 items with a closed-ended answering scheme. Not all of the questions were relevant for this study. A list of questions used for this evaluation can be found in Appendix A.1.3. The survey was conducted in German. For the data analysis, only completely filled out questionnaires (N = 118) were included. For the statistical evaluation and the graphical visualizations, the authors used `R 4.0.2` and the package `ggplot2`. Because the questionnaire was in German, we translated the items into English as literally as possible.

Table 7.3: Companies size in number of employees.

Employees [number]	**1**	**2**	**3**	**4**	**5–10**	**>10**	**N.A.**
Rel. freq.	19%	35%	15%	7%	11%	5%	8%
Number	23	41	18	8	13	6	9

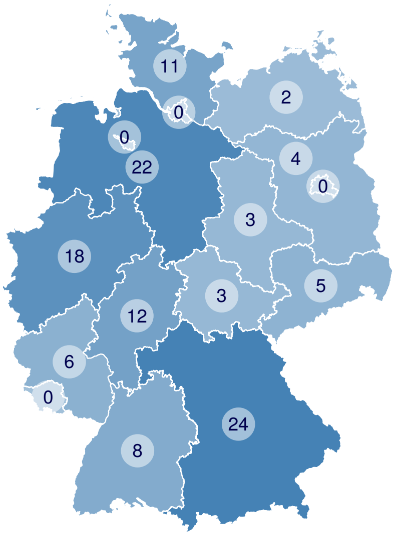


Figure 7.2: Geographical distribution of participants in the online survey by German federal state of the company's main activity.

Table 7.4: Age distribution of participants.

Age [years]	21–30	31–40	41–50	51–60	61–70	>70	N.A.
Rel. freq.	15%	23%	28%	22%	9%	2%	1%
Number	18	27	33	26	11	2	1

7.4.2 *Results of the Online Survey*

To gain quantitative insights into the (technological) resilience domain of German farmers, we used an exploratory approach in addition to hypothesis testing to evaluate interesting and relevant aspects. Since the online survey also included items on other topics, we have limited ourselves here to the areas of technical resilience and digitalization. We split the presentation of results into two categories: (1) incidents and precautions and (2) estimation of operability. Within these categories, we investigate assumptions we have gained from analyzing the focus groups' statements (Sect. 7.3.2).

Incidents and Precautions

We asked the participants to give numbers regarding actual outages. As depicted in Fig. 7.3, especially ICT-related incidents were present in the previous 12 months of the survey, with a quite high proportion of failures of mobile network (cellular phones) and mobile Internet: Participants reported failures of mobile network (27.1%) and mobile Internet (31.5%) more than three times within this time frame. Classical infrastructures like transportation, water, and gas were

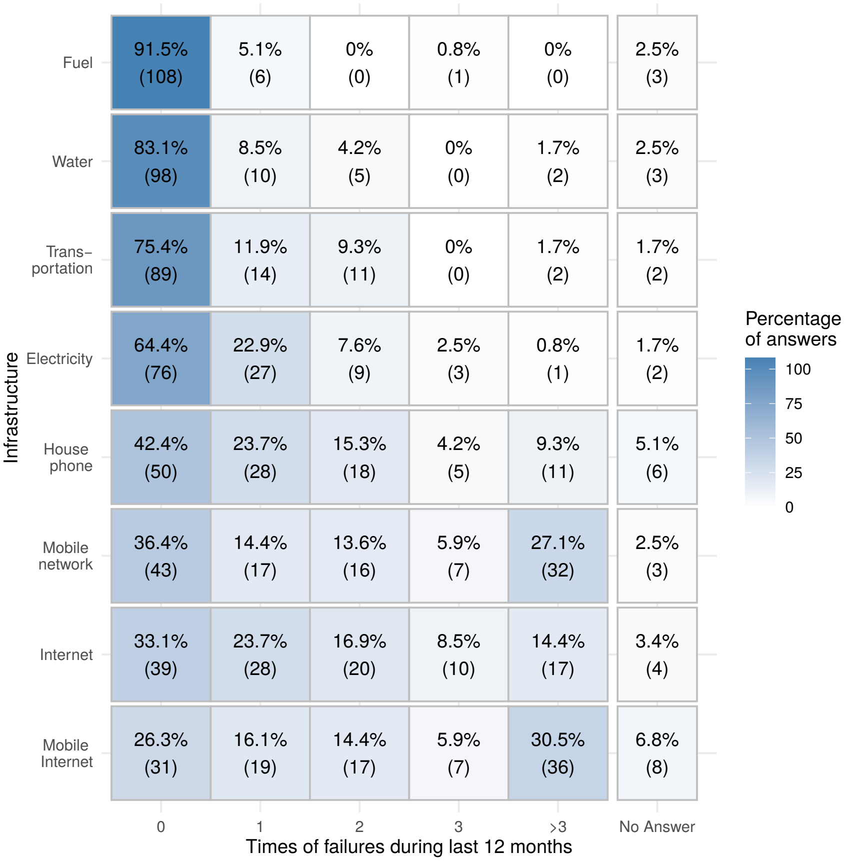


Figure 7.3: Heat map for failures within the last 12 months depending on infrastructure type. The numbers represent the percentages of the answering options and add up to 100% per row. The numbers in brackets represent the absolute numbers of answers.

relatively stable within the same timeframe. Electricity – which is especially important according to the focus groups – was attributed to have caused some outages, with more than 30% having at least one power outage in the past 12 months.

Further, we asked whether the farms possessed different precautionary measures and whether those measures have already been used in the past. The results are depicted in Fig. 7.4. In contrast to the focus group statements, the share of companies possessing a power generator is unexpectedly low. Just slightly above half of the participants state that their company owns a power generator. This may be a result of the overall stable power grid. As we can see from the data, only about half of those who own a power generator already had the need to use it. Other infrastructures that increase the independence in outage or crisis scenarios (for example, gas reserves) are higher in both possession and need of usage.

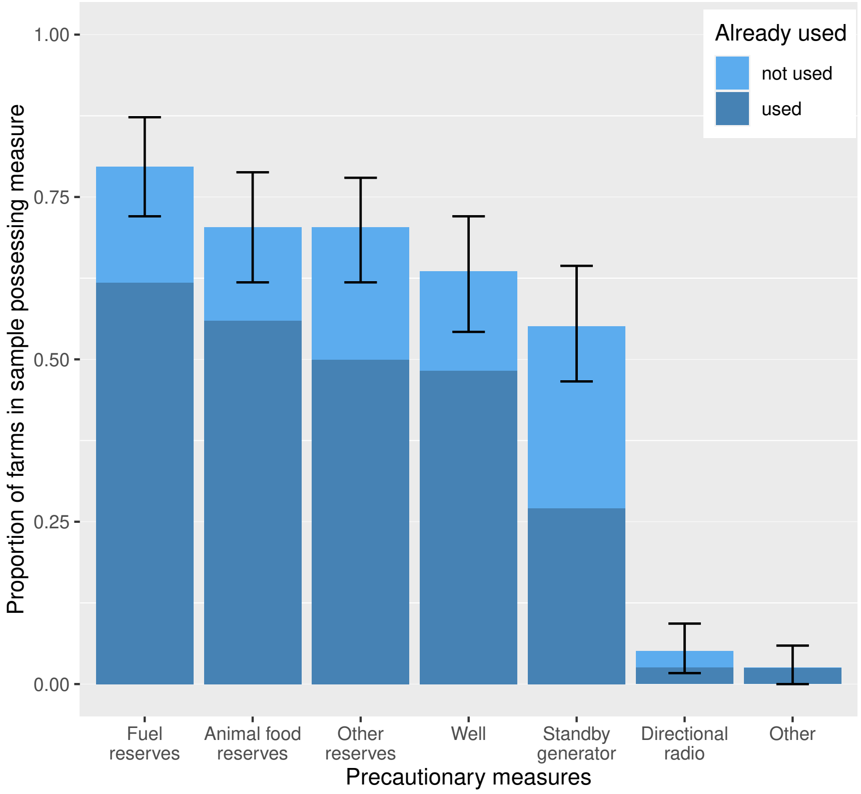
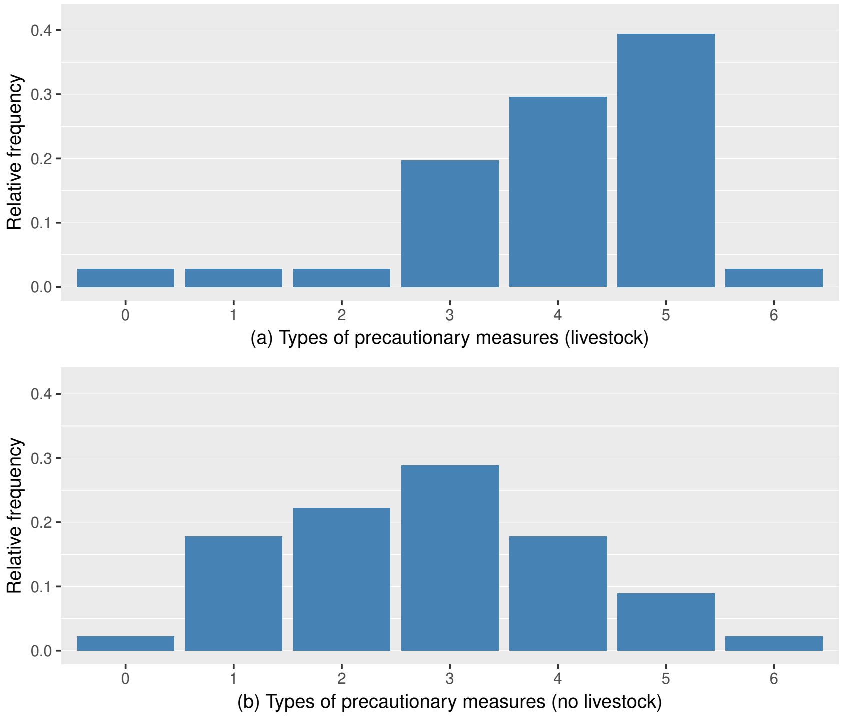


Figure 7.4: Relative frequency of possession of precautionary measures with bootstrapped 95% confidence intervals. Embedded is information on the percentage of facilities that had to use the precautions in the past.



(a) Types of precautionary measures (livestock)

(b) Types of precautionary measures (no livestock)

Figure 7.5: Relative frequencies for the number of different types of precautions for infrastructure failures per farm, with livestock farms in the upper chart ($n_1 = 71$) and farms without livestock below ($n_2 = 47$).

Based on the survey data, we are able to test the following hypothesis, which came up in our focus group (Sect. 7.3.2) – *H1: Farms that are active in the livestock sector more often take precautions against outages.* To test this hypothesis, we compared the number of precautionary measures per farm of farms that did not keep livestock with the ones that did keep livestock. This includes farms that also engaged in other agricultural sectors in addition to livestock. The distributions for farms with or without livestock can be found in Fig. 7.5). TTo test the hypothesis H1, we conducted a Wilcoxon rank-sum test. The results indicated a significantly higher level of precautions ($W = 2417$, $p < .001$) for farms with livestock ($n_1 = 71$, $Mdn = 4$) compared to farms not keeping livestock ($n_2 = 47$, $Mdn = 3$), thus, the results confirm our hypothesis.

Estimation of Maintaining Operability

Similar to the focus groups, we also asked the interviewees to estimate the duration of maintaining operational capability in case of different infrastructure outages. Results are rather inconclusive. Only electricity has a rather clear result, with 57.6% (68) stating that the time of operability is less than 24 hours, and 14.4% (17) stating that it is one week or longer. In case of an Internet outage, the

Table 7.5: Percentage of answers to the question which (digital) tools would continue to function without an Internet connection. Note: Last column (n_i) is total number of owners of the application. Answer options were *Does not work offline* (−), *Works offline with limitations* (−/+), *Works offline* (+).

Application	**Works offline [%]**			
	−	−/+	+	n_i
Communication platforms	72	18	3	82
Other	50	20	10	8
Farm mgmt. information system	36	40	21	46
Herd mgmt. system	17	25	55	39
Calculation aid	16	28	53	72
Farm machinery with ISOBUS	12	15	69	50
Autom. milking system	0	33	67	9

anticipated problems have fewer operational consequences as expected: 35.6% (42) of participants think that they are operable less than 24 hours, and 18.6% (22) estimate one week or longer.

In the analysis of our focus group data (Sect. 7.3.2), we also formulated the following hypothesis – *H2: The tools used are often dependent on the Internet.* To test this hypothesis, we asked the survey participants to estimate how much the technology used on their farms depends on the Internet. Answer options and respective distribution of answers were: *Not dependent* (5.93%), *A little dependent* (16.95%), *Medium dependent* (28.81%), *Quite Dependent* (26.27%), *Very Dependent* (20.34%), and *Prefer not to say* (1.69%). It should be emphasized that 46.61% of the participants stated that the technology used is quite or very dependent on the Internet.

Relative and absolute frequencies of the answers to the question "Which of your digital tools would continue to function without an internet connection (e.g., due to a communications network disruption), i.e., would continue to function in 'offline' mode?" are depicted in Table 7.5. Not surprisingly, especially the communication platforms are expected to need an active Internet connection. Unfortunately, 36% (17) of the participants using farm management systems expect their systems not to work in offline scenarios.

In the case of ICT failures, classical cloud services are not accessible by definition. To get an idea of how frequently cloud storage is used, we asked which digital tools' data are stored in a cloud. The relative and absolute frequencies of the answers can be found in Table 7.6. Here we see to some degree an explanation for the previously mentioned high dependency of farm management systems on the Internet, as data of 67% (29) of the farm management system users are stored in a cloud.

One problem stated in the focus groups was the incompatibility of some (digital) tools. Among the users of farm management information systems (47), 68.1% (32) affirmed having problems due to incompatibility issues, and 23.4% (11) did not. The participants that already use digital tools (108) replied to the question

Table 7.6: Percentage of answers to the question whether data of an application are stored in a cloud. Note: Since not all participants used every system, the total absolute number (n_i) of participants varies per row. Missing values were not included within the relative frequencies.

Application	**Data in cloud [%]**		
	Yes	**No**	n_i
Farm mgmt. information system	67	33	43
Communication platforms	49	51	81
Herd management system	45	55	40
Automatic milking system	44	56	9
Other	38	62	8
Calculation aid	25	75	69
Farm machinery with ISOBUS	11	89	47

"Is your data secured by regular on-site backups?" as follows: 72.2% (78) said yes, 22.2% (24) no, and 5.6% (6) did not give an answer.

7.5 Discussion

Sections 7.3 and 7.4 present insights from the focus groups and survey, respectively. In the following section, the answers to the questions underlying this article are summarized and discussed.

7.5.1 *Potential Risks of Digital Tools*

During power outages, serious problems arise for different types of agricultural systems. Since digital tools necessarily require electrical power, their use results in a dependency on a working power supply for the long run – even if mobile devices like tablets and laptops could bridge a couple of hours using built-in battery capacity. Crop farms may only experience problems regarding office activities, like documentation and billing. But in animal husbandry, farmers may be faced with the downtime of devices that are crucial for the health of their animals, such as ventilation systems and milking robots. Usually, the general power grid is responsible for delivering an uninterrupted power supply. From the interviews and the study, however, we learned that there are recurring power outages for some companies up to three times a year. Whereas the focus groups indicated that most agricultural companies have an emergency power generator as a precaution, this does not seem to be the case for 42% of the participants in the quantitative survey. As the average estimated fuel capacity covers a few days to one week, longer-lasting power outages and broken emergency power generators represent harmful risks, even for those taking precautions. As more battery-powered devices and vehicles are likely to be used in agriculture in the future (Koerhuis, 2020; Spykman et al., 2021) as well as with the good application prospects of photovoltaic systems on farms (Friha et al., 2021), the need for large fuel reserves could decrease.

Assessing the consequences due to telecommunication outages is more complex. Looking first at human-to-human communication, we are in line with the survey results of von Hobe and his colleagues Hobe et al. (2019), namely that the agricultural actors are well-connected, many players know each other personally, and appreciate the personal contact that promises support in times of trouble. But at the same time there is recognition that there is a countervailing trend towards using more digital communication technologies. Accordingly, all focus groups perceived mobile phones and especially messenger apps to be an essential everyday tool for task coordination. Even though this constitutes just one aspect of communication in agricultural systems, the crucial question concerns the importance of this part of the overall communication for the continuity of agricultural operations. In fact, most agricultural systems in our studies do not vitally rely on (wireless) network connections, but we can confirm a trend towards more digital communication technologies and inter-connected devices in agriculture (Ojha et al., 2015), creating greater vulnerabilities to outages in the future.

Another problem can arise when required machine-to-machine communication is done over air channels, like mobile Internet. Surprisingly, such risks were neither mentioned by the farmers themselves nor present in the literature. We see the first reason for this missing awareness in the lack of extensive implementation, possibly due to risk aversion in the adoption of new technologies (Marra et al., 2003), data protection concerns (Linsner et al., 2021), or the partly unreliable mobile data connection in Germany, especially in rural areas (Fig. 7.3). The second reason may be a missing understanding of the machine-to-machine aspects of already implemented technologies (Cavallo et al., 2014).

Since precautions regarding telecommunication and Internet outages are difficult to take, especially when personally knowing important points of contact that are essential for business continuity seems to offer advantages. The interviewed farmers (both focus groups and questionnaire) do not own stand-alone radio/wireless technology that would allow them to communicate over the air in case of an ICT breakdown. We strongly recommend the implementation of backup mechanisms for new agricultural applications that depend on ICT, since the operational continuity of agricultural processes during infrastructure outages is essential. Such backup mechanisms should allow community users to work in off-line-scenarios, for example, by having the most relevant data always cached on the client side as well as with the application itself. In general, (new) strong dependencies should be avoided where possible.

7.5.2 *Factors that Affect the Resilience Capacities*

Based on our qualitative data and quantitative verification, we are able to assess the level of the three resilience capabilities (Meuwissen et al., 2019) for the domain of modern agricultural businesses.

Robustness

In case of failures in the energy or communication infrastructures, almost all companies are unable to contain disruptions. While livestock farming has a great need for electricity, arable farming is rather independent of electricity but has high demands on a functioning communication infrastructure. Disturbances in both infrastructures, electricity and communication, are hard to absorb, especially for small and medium enterprises. Solutions that absorb power grid outages are available, for example, in the form of microgrids or decentralized energy systems (Panteli & Mancarella, 2015), although typically these are not considered by small companies. Rare exceptions are self-sustaining companies with photovoltaic and/or wind power stations, which allow the absorption of general power grid outages. ICT failures in the form of Internet service breakdowns are hard to absorb, since required technology changes are currently not available to customers. Especially agricultural businesses in rural areas usually do not have a consistent Internet connection due to frequent gaps in broadband and mobile Internet coverage. About 35.6% of the respondents (Sect. 7.4.2) think they can only remain operable for less than 24 hours in case of an Internet outage. In the future, communication network redundancy could be established by affordable orbital Internet connections (Harris, 2018) or the use of wireless sensor networks for communication in disaster scenarios (Adeel et al., 2019) to further improve the technical resilience of agricultural companies.

Adaptability

Most of the surveyed companies own power generators – either voluntarily or required by law. Because agricultural machinery depends on fuel, a sufficient stock of fuel is expected to be available in most companies to fuel the power generators for multiple days on average. The effort and time to put a power generator into operation range from "easy"/"quick" to "enormous"/"couple of hours" (both statements in fg3), depending on the company's system construction and the technologies involved. In total, the adaptability capacity regarding power outages is high due to the ability to completely restore full operation after a power outage for a limited time. Adaption of communication can also be realized by switching from phone-based communication to face-to-face conversations. These personal conversations are locally possible and often preferred by well-networked farmers (Fecke et al., 2018; Hobe et al., 2019).

Transformability

When the regular power grid returns to normal operation after an outage, companies just have to disconnect the temporarily installed power generators. In some cases, this process requires modern digital equipment and time-consuming actions to reset the whole agricultural system into a fully operational mode. Looking at communication infrastructure, there was no required effort mentioned for restoration into regular operational mode. This may be because these devices will typically reconnect automatically after the recovery of the ICT infrastructure. In such a case, the regular way of communicating via telephone, email, or similar digital options is working again without the need for active interventions.

7.5.3 *Limitations*

It has to be considered that our sample for the focus groups and the questionnaire consisted only of farmers. Other possible stakeholders, such as their business partners or people working on agricultural ICT, were not involved. The participants in the focus groups run their agrarian businesses in southwestern Germany, consisting of small structured areas, which is not representative for the whole country (Bundesministerium für Ernährung und Landwirtschaft, 2018). In contrast, with the quantitative study (questionnaire), we had participants from all parts of Germany. Moreover, the familiarity with and expertise in agricultural digital technologies of our samples may be biased. Most of the participants in focus groups took part in a federal education initiative that incorporates digital tools for farming businesses as a subject. As is the case with all mixed methods approaches, we decided for a trade-off between the detailed, subjective information of qualitative statements against quantitatively measurable dimensions. The individual results of the sub-studies should therefore only be interpreted collectively, as the hypotheses generated in Sect. 7.3 and their verification in Sect. 7.4 successively build on each other.

7.6 Conclusion

As mentioned by related literature, digitalization can increase the efficiency and effectiveness of agricultural operations (Walter et al., 2017; Wolfert et al., 2017). Trends also point to an increasing use of digital services in this area (Fecke et al., 2018; Sundmaeker et al., 2016). To critically challenge the predominantly tech-positive body of literature on digitalization in agricultural systems, we looked at the specific risks of digital tools for farm systems and their impact on resilience capacities. This is inevitable in terms of the development of sustainable and future-proof systems. For this purpose, we used a mixed methods approach to first generate hypotheses through qualitative focus group interviews (N = 52), which we verified in a second step through quantitative questionnaire surveys (N = 118). To gain insight into dependence on digital technologies, we asked explicitly about aspects of digitalization on household-level agricultural systems, but also inquired about risks and disasters experienced, as well as explored precautions taken. Key insights about potential risks associated with the use of digital tools (RQ1) are as follows:

- The incorporated tools of agricultural operations are often dependent on the Internet.

- A power failure of a few hours to a few days would not be very harmful to those farms having a power generator. Longer failures would realistically result in complete harvest failures and lethal consequences for animals.

Key findings related to resilience capacities (RQ2) are as follows:

- Most of the farmers are not aware of how the Internet and mobile network infrastructure affect their agricultural system and do not take any precautions for ICT breakdowns.
- Just slightly above half of the farmers own an emergency power generator.
- Farms that are active in the livestock sector more often take precautions against outages than do other farmers, both for higher dependency on continuous-working machinery and because of legal requirements (Sect. 7.3.2)

Especially problematic for farms (Fig. 7.3) is the trend of increasing dependency on Internet infrastructure along with the fragility of the Internet. Additionally, the statements by interviewed farmers show the diversity in the usage of digital tools. Some farmers are limited in the usage of digital tools by external factors, like high investment costs, missing information on these modern farming tools in their education and experience, or a bad/missing Internet connection in their region.

Our assessment regarding resilience capacities with a focus on the two infrastructures of electric supply and communication shows that there are high robustness and adaptability capacities in these systems, but that transformability capacity is low due to mainly technical reasons and should therefore be of particular interest for future work. When looking at the digitalization of the agricultural sector, it is important to keep in mind that all advantages must go hand in hand with strong operational reliability. Currently, there is no publication investigating the operational reliability of present tools, nor are there descriptions of technical approaches for resilient communication that would allow strengthening the robustness capacity of farming companies. More research in this field is needed. Market analyses inspecting digital products for agriculture with regard to resilience criteria would allow for a more precise assessment of the current situation. Also, research on utilizing the increasingly distributing Internet of Things networks for self-operated communication between neighbored farms could help to achieve greater resilience capacities.

8

THE ROLE OF PRIVACY IN DIGITALIZATION — ANALYZING PERSPECTIVES OF GERMAN FARMERS

ABSTRACT Technological progress can disrupt domains and change the way we work and collaborate. This paper presents a qualitative study with 52 German farmers that investigates the impact of the ongoing digitalization process in agriculture and discusses the implications for privacy research. As in other domains, the introduction of digital tools and services leads to the data itself becoming a resource. Sharing this data with products along the supply chain is favored by retailers and consumers, who benefit from traceability through transparency. However, transparency can pose a privacy risk. Having insight into the business data of others along the supply chain provides an advantage in terms of market position. This is particularly true in agriculture, where there is already a significant imbalance of power between actors. A multitude of small and medium-sized farming businesses are opposed by large upstream and downstream players that drive technological innovation. Further weakening the market position of farmers could lead to severe consequences for the entire sector. We found that on the one hand, privacy behaviors are affected by adoption of digitalization, and on the other hand, privacy itself influences adoption of digital tools. Our study sheds light on the emerging challenges for farmers and the role of privacy in the process of digitalization in agriculture.

ORIGINAL PUBLICATION *Linsner, S., Kuntke, F., Steinbrink, E., Franken, J., & Reuter, C. (2021). The Role of Privacy in Digitalization – Analysing the German Farmers' Perspective.* Proceedings on Privacy Enhancing Technologies (PoPETs), 2021*(3). https://doi.org/10.2478/popets-2021-0050*

ACKNOWLEDGMENTS This work was supported by the German Federal Ministry for Education and Research (BMBF) in the project HyServ (01IS17030B), by funds of the German Government's Special Purpose Fund held at Landwirtschaftliche Rentenbank in the project Geobox-II and by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) — 251805230/GRK 2050.

8.1 INTRODUCTION

Digitalization in agriculture is a process with very heterogeneous implementations by different actors. This makes this domain an interesting field of investigation in terms of the extent to which certain factors influence the adoption of digitalization. According to Gandorfer et al. (2017), privacy is a factor that tends to slow the process of digitalization. The processing and exchange of data is a key element of digitalization, but not everyone is in favor of this development. Nevertheless, agriculture is an economic domain that relies heavily on the division of labor and collaboration Braun et al., 2018. Farmers usually cannot grow crops or breed cattle on their own. Multiple actors are involved in the whole process, from planning a season to delivering products to retailers. For these cooperations to function smoothly in times of digitalization, it is necessary to share data in order to be able to plan the individual production steps effectively.

Since data exchange is a major issue, privacy concerns are raised and trade-offs are necessary: High-tech machines can help to save resources and protect the environment, but they require comprehensive and processed data. This data is generated from a variety of information sources and is more useful the more information is available. However, at the same time, this availability can also be a problem: If farmers disclose too much information to their business partners, they run the risk of being put at a competitive disadvantage by individualized prices. Such fears paralyze enthusiasm for digitalization, especially if data flows and purposes are not clearly communicated and contractually secured. To find out how the heterogeneous adoption status and the long duration of the digitalization process in agriculture are influenced by data protection aspects and how digitalization affects the work processes of stakeholders, we conducted an empirical study to answer the following research question:

> **How does privacy affect the adoption of digital technology in agriculture?**

This paper is structured as follows: Section 8.2 presents the background and related work of digitalization and privacy in agriculture, as well as the research gap. Building on this, Section 8.3 describes our methods, the participants involved in our study, the study design, and the data analysis. Section 8.4 presents the results of our empirical study, including the attitudes and concerns of the farmers. Based on our findings, Section 8.5 discusses our results with reference to our research question. Section 8.6 concludes our study by recapitulating the main findings.

8.2 Background and Related Work

This section provides a brief overview of the context of our study: digitalization in agriculture. Although this paper focuses on privacy for and perceptions of farmers, background information on digitalization in general is helpful to understand the statements of the study participants in this context.

Even though the digitalization of agricultural processes is not a new idea, it is an ongoing development, especially in relation to the current introduction of modern concepts such as IoT or big data in this field Lokers et al., 2016; Tzounis et al., 2017. In this context, data privacy appears to be an important factor in the adoption of new digital technology Aldehoff et al., 2019; Ferris, 2017; Melicher et al., 2016. However, studies conclude that digitalization in agriculture is lagging behind expectations (Gandorfer et al., 2017). Accordingly, other domains are more advanced in the integration of business models and processes. In the following section, we will summarize recent developments in the field of digitalization in agriculture (8.2.1), also called Smart Farming or Precision Agriculture, to provide context for the reader. We will then focus specifically on privacy and data ownership issues (8.2.2). Futhermore, we will discuss the role of user perceptions in relation to data privacy (8.2.3). The section concludes by identifying a research gap that our study addresses (8.2.4).

8.2.1 *Background on Digitalization in Agriculture*

Several benefits of digitalized agriculture are mentioned in previous research: First, it improves traceability. Retailers could offer their customers information about the origin of their crops. This could prevent or limit food scandals even more efficiently. One example from research Kamath (2018) suggests that better traceability may simplify countermeasures during food contamination scandals. Here, the author refers to two food scandals, in 2006 in the U.S. and 2011 in China, where contaminated products from a single farm damaged the image of the entire sector due to a lack of traceability. In this context, a blockchain-based approach is presented to enable transparency and traceability in agriculture. Similar approaches to this objective exist in further research Bermeo-Almeida et al., 2018; Ge et al., 2017.

Second, digitalized agricultural machinery and equipment could also bring monetary benefits. So-called smart farming approaches promise to increase efficiency and effectiveness Y. Gu and Jing, 2011; Wolfert et al., 2017 through precise maneuvering and application of seeds, fertilizer, and other resources. Taking advantage of these benefits can save time and financial resources. Elijah et al. (2018) also see the benefits of IoT in reducing needed resources while feeding a growing population. Rosskopf and Wagner (2006) conducted annual studies from 2002 to 2005 to investigate the usage of computers and electronic devices in German agriculture. Main challenges were lack of understanding of computers and time spent without perceived benefits. In 2017 Gandorfer et al. (2017) confirmed these findings and stated that privacy is a particularly relevant issue.

Third, the precise application of agents and better calculation based on sensor data could reduce pesticide contamination and thus environmental pollution. As early as 2007, Pinaki and Tewari (2010) show in their review of trends in precision farming that there is enormous potential for environmentally sustainable agriculture, an argument which Finger et al. (2019) also provide. A meta-study of energy use in precision farming is provided by Pelletier et al. (2011). The authors compare different approaches and sub-domains, such as livestock or crop production.

8.2.2 *Privacy in Digitalized Agriculture*

The adoption of digital tools is closely linked to the handling of data, which makes privacy an important factor. Shepherd et al. (2018) approach the topic of digitalized agriculture from a socio-ethical perspective: They point out that digitalization in agriculture could help feed the growing population, but success depends on business models that can ensure data privacy and security. The desired increase in agricultural efficiency depends on the establishment of new technologies such as IoT and data analytics in agriculture. The need for security and privacy as well as data ownership is also emphasized by Elijah et al. (2018). In addition to general security issues in the IoT world, agricultural IoT devices are also vulnerable to physical tampering, such as theft or animals attacks. Looking at the cloud-based backend infrastructure, successful attacks can lead to unauthorized data access. The problem of data privacy is not exclusive to agriculture. Privacy and secure data processing are also important in other areas where IoT is used to prevent de-anonymization or re-identification of individuals Naeini et al., 2017.

The increasing impact of aggregated and processed data on agriculture is highlighted by Sykuta (2016). The author proclaims principles of big data for agriculture and mentions privacy as an issue. Nery et al. (2018) name knowledge engineering as a proposed solution. The authors point out challenges such as the semantic gap, dealing with spatial and temporal information, and correlation issues. Fleming et al. (2018) present perspectives of the industry with a focus on big data. The authors note the need to address issues such as trust, equity, distribution of benefits, or access.

Research also focuses on different countries and their attitudes toward digitalization: Specific drivers for digitalization in Australian agriculture are presented by A. Zhang et al. (2018). The authors interviewed 1,000 Australian farmers from 17 subsectors about their expectations and needs regarding digital agriculture. One striking finding was that the majority of farmers were highly critical of various data assets and wanted more privacy, but were still keen to share data with other stakeholders in agriculture, such as big companies. Fountas et al. (2005) asked 198 farmers in the U.S. and Denmark about their attitude towards precision agriculture. They found that the main problem was too time-consuming data handling and that 80% of farmers wanted to store their data themselves. Carbonell (2016) sees power asymmetry between farmers and agribusinesses as a problem. The author calls for open source tools and open data for a fairer use of big data. An overview of the adoption of digital tools in agriculture in different EU countries is provided by the study of Kernecker et al. (2020). A total of 287 participants from seven countries participated in this study. It revealed that farmers wanted more instructions and security. It also became clear that most farmers with more than 500 ha land run fully digitalized businesses. Especially the smaller farms still lack digitalization.

The fact that small enterprises in particular lack digitalization has also been concluded by Regan et al. (2018). As an example, the authors refer to agriculture in Ireland, which consists mostly of family-run farms. They present an interesting view on data ownership and maintaining privacy for farmers. The researchers found a general distrust towards companies, but a very open attitude towards actors with whom the farmers had longstanding partnerships. The authors assume that the reason for this is the family-owned business model. This theory is supported by the work of Cravotta and Grottke (2019). They conducted a study that highlights the tendency of family-run enterprises to favor old-fashioned over innovative solutions. In Germany the demographic situation is similar, as shown by federal statistics Statistisches Bundesamt, 2019: The majority of farmers cultivate less than 200 ha of land. This circumstance makes it worth investigating whether small and medium-sized enterprises (SMEs) in particular are lagging behind in digitalization and whether the lack of viable privacy solutions is a reason for this. For the purpose of this paper, we use the definition of the European Union when referring to SMEs[1].

Furthermore, previous work has outlined that access to corporate data is an existential problem for farmers, as noted by Fraser (2019). Increasing "data grab" can lead to "land grab". Once companies have access to the business data, they can easily overtake the farm. By acquiring many smaller farms, companies can manage large scaled agricultural businesses with the data they obtained from former owners. With less effort, the companies are able to gain much more profit from the land than many small farms before. Ferris (2017) sees opportunities in precision agriculture, but also dangers arising from the massive collection of data: Exposure of personal data, income, or yield of the fields. The author states that farmers fear disadvantages if this data is accessible for their competitors. Therefore, the author calls for the need for governmental regulation.

8.2.3 *The Influence of Users' Perception on Privacy Preferences*

The previous section has shown that privacy is an important issue that requires specialized techniques to protect end-user data. However, when developing privacy-enhancing solutions for specific use cases, it is necessary to investigate the behavior and preferences of the target audience. Not only privacy and security behavior Biselli and Reuter, 2021, but also user perception and reality often differ, as research in other domains shows:

Malkin et al. (01 Oct. 2019) investigated the perception of users with regard to smart speakers and found serious misconceptions. About half of the participants were unaware that smart speaker recordings are permanently stored. Furthermore, most users were not familiar with the available privacy functions. 23,8% plan to use them in the future. Users' perceptions of smart home technology were studied by Zimmermann et al. (2019). The researchers conducted 42 semi-structured qualitative interviews with inexperienced users of smart home technology and found that users not only fear attacks, but also feel they are losing control. Another example of differences between the mental model of users and real-world technology was found by Han et al. (01 Jul. 2020). Their study

[1] https://ec.europa.eu/growth/smes/sme-definition_en,
based on headcount (micro < 10, small < 50, medium < 250) and turnover (micro $\leqslant$ 2 million €, small $\leqslant$ 10 million €, medium $\leqslant$ 50 million €) of the enterprises

examined the differences between free apps and their paid versions. After assessing which mental model the users had regarding these apps, the researchers found that only 3,7% of the 5877 pairs of apps had significant differences in their use of permissions and data usage. This contradicted most users' impression that paid apps were more privacy protective than free versions. Reasons for specific perceptions regarding privacy and digital tools were investigated by Smullen et al. (01 Jan. 2020), who found that users' preferences are related to a specific purpose. Coopamootoo and Groß (01 Oct. 2017) found that privacy preferences and willingness to share data are based on a person's personality. The researchers identified specific personality traits and their influence on attitude towards privacy. However, these approaches focus on the private individual and their use of technology in their everyday lives. Considering that digitalization affects the business aspects of peoples' lives, it has to be expected that factors other than personality are key to understanding the motivation to adopt or not to adopt. Career implications must also be considered. An approach that considers these perceived negative consequences of online tracking was conducted by Melicher et al. (2016). The qualitative interviews showed that users are distrustful of tools in the context of tracking and fear risks such as price discrimination. Although this addressed a monetary factor that influences privacy attitudes, the impact of tracking on individuals is less severe than in a business context.

8.2.4 *Research Gap*

In the previous sections, we presented the state of research on digitalization in agriculture and the role of privacy. Agriculture relies on the division of labor and therefore the sharing of operational data Braun et al., 2018. Additionally, farmers have reporting obligations to authorities and retailers strive for transparency to provide traceability to their customers. While most of the privacy research mentioned focuses on the issue of privacy in consumer applications, the implications of digitalized tools and data collection in a commercial context need to be considered as well. In a context where the disclosure of proprietary or sensitive data can lead to financial damage or competitive disadvantages for a business, privacy considerations take on great importance. One industry that is particularly vulnerable to these risks is agriculture. This results from multi-actor supply chains and high demands for transparency and traceability from both commercial and governmental sides. While many studies exist on the establishment of digital tools for transparency Bermeo-Almeida et al., 2018; Ge et al., 2017; Kamath, 2018, few examine farmers' perception and their roles in the transforming domain of agriculture. While the aforementioned study by A. Zhang et al. (2018) provides some insight into the situation in Australia, it also raises new questions: Why are farmers willing to share their data with third parties when they actually consider it critical in principle? Is this related to the specific economic circumstances in Australia, or does it result from a misconception of privacy, as studies in other areas suggest (see Han et al., 01 Jul. 2020; Malkin et al., 01 Oct. 2019)? In terms of structural reasons, Kernecker et al. (2020) show for Europe that digital tools are less adopted by smaller enterprises. However, their sample for Germany consists mostly of larger farms, while the agricultural sector in Germany is predominantly characterized by small farm structures. Hassan et al. (2020) demonstrate that the decisions of German SMEs to adopt cloud computing are influenced not only by their perceptions of usefulness, security aspects, and the implementation costs, but also by the internal capabilities of an SME. Moreover, the main drivers of technological innovation are larger companies upstream and downstream in the supply chain. Therefore, the incentives for new technologies come from actors with a significantly stronger market position than SME farmers. This creates an imbalance of power and leaves the perspectives of farmers underrepresented. Considering this situation, where SMEs predominate in the middle of the agricultural supply chain, the perceptions of farmers could provide valuable insights into the challenges and barriers to digitalization adoption, and thus privacy attitudes across this sector.

To conclude: To our knowledge, a study with German SMEs in agriculture with a focus on perceived privacy and their experiences with digitalization is currently both entirely lacking and urgently needed. The contribution of this paper is to provide information about farmers' views on the issues of digitalization and privacy. Further, we elaborate how these aspects correspond to the adoption of new technologies. This provides a broad information basis for future studies and allows to address these topics appropriately, taking into account the subjective perspective of farmers.

8.3 Method

Our study aims to find privacy-related issues and obstacles in the adoption of digitalization in agriculture. In the context of this paper, the notion of privacy is not limited to the field of private data, but is extended to the usage for operational data owned by individuals. In this section, we present our overall methodology to address our research question, as mentioned in Section 8.1, as well as the design and conduction of the actual study.

8.3.1 *Participants*

We conducted a qualitative study with 52 participants from agricultural businesses. The study took place at the machinery ring[2] "Maschinen und Betriebshilfsring Rheinhessen-Nahe-Donnersberg", "John Deere European Technology Innovation Center (ETIC)" and "Hofgut Neumühle", a training and research farm. In preparation for the actual study, we consulted stakeholders from agriculture, such as farmers, machinery manufacturers, and representatives of farmers' associations, in regular meetings every 2 weeks for more than 8 months, and discussed typical work routines and technological innovations, as well as the challenges of data sharing in agriculture, the parties involved, and regula-

[2] Machinery rings are associations of farmers which organize collaborative work orders and the use of shared machinery

tions. This helped in the preparation of the interview guidelines by pointing out relevant topics and potential conflicts in advance.

We are working in a publicly funded research project called HyServ with partners from the private sector, federal institutions, and associations for farmers, such as machinery rings. Their clients and members were invited to participate in our focus groups. Everyone participated voluntarily and no compensation was paid. Each participant was informed about the objectives and topics of the study via a informed consent form, which was signed by each person. On the advice of our project partners, we launched events for farmers to meet and exchange ideas and expertise or learn about new products and services offered by one of our project partners. In this way, we planned events that were conducted over five days. The first event was a collaboration with the machinery ring, the second with John Deere ETIC. With Hofgut Neumühle we held events on three days due to the high number of participants. During the events, the farmers had the opportunity to attend different program points. One was the focus group interview presented in this study, the second was an agronomy workshop, and the third was a presentation of a NIER-sensor for the analysis of liquid manure. Offering multiple program points increased the motivation to participate by providing a better cost-benefit ratio of travel and offered content. We interviewed the participants in focus groups of 3 to 6 people Lazar et al., 2017; Morgan, 1997 with a duration of 25 to 30 minutes. These focus groups were conducted by two of our researchers and explored the participants' experiences regarding digitalization and privacy in their systems. In this way, we were able to recruit 52 participants, who own family-run farms in south-western Germany, which can be considered as SMEs. This region is quite rural and has a long history of agriculture. Furthermore, the climate and soil in this region is suitable for viticulture, which allowed us to investigate this particular branch of agriculture.

Our aim was to involve participants at the decision-making levels. Therefore, each participant in our study owns or manages an agricultural business. Most of them run farms, but some also provide services to other farmers. Additionally to farmers, we interviewed one service provider who runs a soil laboratory for farmers and two representatives of the administration, including the head of the local machinery ring and a counselor from a federal administration. For further studies it would be interesting to approach stakeholders downstream or upstream the supply chain in order to broaden the perspective.

Seven of the participants identified themselves as female and 45 as male, thus the proportion of female participants is 13.5%. According to the 2016 Eurostat database, the overall gender ratio of agricultural workers in Germany was 32.4% female compared to 67.6% male at the date of the census. Nevertheless, as this paper focuses on the operational level of farm managers, the gender ratio of the survey is very similar to the gender ratio of 9.0% for female farm managers in Germany (see Eurostat, 2016).

We recruited most of the participants in the three events with Hofgut Neumühle through a nationwide advanced training institution for agriculture that offers different degrees for farmers after a few years of practical experience. In fact, it is mainly relatively young farm managers who attend this institution to further their education and skills. Therefore, these 42 participants are in the age segment between 20 and 30 years, which is why our study has a focus on the younger generation. However, all these participants grew up on farms and have been familiar with the daily work of a farmer since childhood. The rest of the participants were between 30 and 60 years old.

It should also be mentioned that all of the businesses surveyed were small and medium-sized enterprises. This is because most of the farms in this domain are family-run farms which are inherited over generations. Additionally, according to Cravotta and Grottke, 2019; Regan et al., 2018, the adoption of digitalization is a major challenge, especially for SMEs, e.g., in raising equity capital for the adoption. Furthermore, Cravotta and Grottke (2019) point to social reasons as challenges for family-run enterprises, such as focusing on owner vision rather than efficiency. This makes these businesses interesting for investigation of the role of privacy in their adoption decisions. For an overview of the fields of work of our participants, see Table 8.1.

Table 8.1: Branches the participants work in (multiple possible)

Branch			Amount
Cultivation of grain			22
Viticulture			3
Cultivation of vegetables			1
Husbandry	Beef raising	Dairy cattle	12
		Breeding	4
	Pig housing		4
	Laying hens		3
	Biogas production		3
Service provider			6

8.3.2 *Study Design and Ethical Considerations*

We interviewed the participants in focus groups Lazar et al., 2017; Morgan, 1997 because this gave them the opportunity to discuss among themselves as well. In our case, these discussions brought to light new aspects that might have remained undiscovered in individual interviews. All focus groups were led by two researchers to mitigate the likelihood of subjective bias. The entire process, including the creation of an interview guideline, recruitment, conduction of the focus groups, and data analysis and storage followed the guidelines of the Ethics Committee of the Technical University of Darmstadt.

The 52 participants in this study were interviewed in twelve sessions: For the first focus group, we consulted the local machinery ring. This way, it was possible to form an expert panel that included the head of the machinery ring, the soil laboratory owner, and the federal counselor. The aim was to conduct an exemplary focus group interview with them and to review and validate our interview guidelines with these domain experts. The second and third focus groups were conducted with the help of our project partner, John Deere ETIC, who invited customers to participate in the interview. The participants split into two groups, avoiding any (unconscious) bias by manually selecting participants. The remaining nine focus groups were conducted during the three events with Hofgut Neumühle. The participants were farm managers who took part in a federal graduation program to earn the title "state-recognized technician in the field of agriculture (German: Staatlich geprüfte(r) Techniker(in), Fachrichtung Landbau)". Again, the participants divided into groups to attend the different sessions of the event. In view of the limited time available for the interviews, we decided to outsource some background information into a survey in order to give more room for discussion in the focus groups. The survey was filled out before the focus groups and contained some general information about the branches they work in and their experience with digital tools.

In the focus groups, we asked about their understanding of digitalization, positive and negative aspects, fears, and (if not mentioned by themselves) questions regarding privacy and data ownership. It has to be noted that nearly all groups mentioned privacy aspects on their own initiative. Therefore, we conclude that it is an important issue worth investigating from their perspective as well.

We encouraged the participants to discuss freely about the topics we gave them. Nevertheless, we prepared some questions to give impulses to the discussion, mainly aimed at exploring the perception and state of digitalized agriculture within the focus groups, as the direct question about privacy is susceptible to the acquiescence bias:

- *What is your perception of digitalization in agriculture?*
- *Which digital tools or machines do you use?*
- *Does your farm have its own server or other network infrastructure?*
- *What are your experiences with digitalization in the daily work routine?*

8.3.3 *Data Analysis*

Data from the focus groups were obtained through audio recordings. Later, these recordings were transcribed and anonymized for coding. We segmented the data into meaningful expressions using the open coding method Corbin and Strauss, 1990. We then grouped the codes into categories: digitalization in agriculture, privacy, and data ownership as an important aspect of privacy which was mentioned often. Based on this grouping, we were able to get an overview of all statements on the given topics. This allowed us to derive our results, which are presented in the following section. The categorization was performed by one of the researchers who conducted the focus groups. We decided to do so in order to ensure a homogeneous analysis of the data. To avoid subjective bias, the coding was reviewed by the second researcher who participated in the focus groups. The coding resulting from this process was then presented to the other authors. The recorded interviews are in German, however, we translated the statements as literally as possible into English..

In this paper, we refrain from disclosing the clear names of companies mentioned by the participants in order to guarantee a neutral perspective. These companies can be suppliers of agricultural machinery and equipment, e.g., tractors, irrigation systems, or soil sensors. They may also be contracting firms and suppliers of seeds, fertilizers, or animal feed.

8.4 Results of the Empirical Study

In this section, we present the results of the qualitative study. We derive general aspects of digitalization in agriculture, followed by a presentation of the interviewees' positions on privacy and data ownership in particular. We also present some direct citations of statements that expressed farmers' experiences in a concrete and precise way. In this section, citations refer only to the focus group (*fg*) in which they were mentioned in order to ensure the anonymity of the individuals. The quotes in this paper are numbered (e.g., *Q1*) for further reference in the discussion of the results.

8.4.1 *Heterogeneous Levels of Experience and Dependencies on Digital Tools*

This study found varying levels of decision-making regarding the adaptation of digital technology. Three branches stand out in terms of benefits and freedom of choice regarding adoption; they are provided as examples to illustrate potential differences: **cattle farms** that rely heavily on digitalization, **plant farms** that reported benefits of digitalization but do not necessarily need to take advantage of it, and **winery productions** that benefit the least from digitalization and therefore have the least motivation to use digitized tools. Reasons for this are highly heterogeneous levels of available technology to benefit from, the need for technology (e.g. milking robots), or legal requirements, such as animal welfare laws which require every affected farmer to provide emergency generators for ventilation systems or milking robots in order to ensure animal health.

Cattle farms rely on digital solutions, as they cannot maintain their operations without machines and robots. Dairy farms cannot guarantee the welfare of the animals without milking robots (fg8), as dairy cows need to be milked daily, otherwise they suffer from severe pain and poisoning that can lead to death. Without robots, this work would be impossible to accomplished, as it takes 30 minutes to milk a single cow manually. In breeding farms, it is necessary to install intelligent ventilation systems, as the evaporations of the animals would otherwise lead to suffocation. For this reason, farmers who raise animals are under legal obligation to possess generators to keep the machinery running in the event of a power outage.

Since cattle farms rely on the use of state-of-the-art technology, there is little inhibition to adapt to digitalization. Moreover, subjects reported additional optional advantages, such as digital automatic feeding machines, which allocate the optimal amount of nutrients to each individual animal and optimize the performance of the animals (fg11).

Plant production companies are representatives of businesses who do not necessarily rely on the use of high-tech machines and robots, but can rely on a wide range of digitized agricultural machinery and administrative tools. The focus groups in our study also report on the advantages they have experienced through the use of new technologies. These include, for example, agricultural machines that are automatically controlled by satellite signals and can seed fields by making the best use of land and resources. These machines are particularly suitable for angled fields (fg12). This form of precision agriculture is particularly useful in the context of legal requirements such as distance regulations that define zones where agricultural substances may not be used or regulations to protect groundwater and soil quality. In such cases, digitized machines help to apply resources precisely and use them optimally.

Winery productions are least affected by digitalization. Usually, production steps are carried out manually or with non-digitized mechanized equipment, because there are rarely any digitized machines for viticulture (fg2). Only logistics and administration can be optimized by digitalization, but the few advantages are hardly an incentive for winery productions to invest in it. Therefore, some wine producing companies do everything manually or handwritten and even without computers or other machines.

The fact that farmers differ in the way they are affected by digitalization influences their privacy behavior due to heterogeneous experience or external motivation to expose themselves and their businesses to digital services and privacy risks. In Figure 8.1, we have illustrated the three prominent agricultural branches of our study in relation to their dependency on digitalization and the benefits of technologies for their subdomain. This figure can be used to estimate the likelihood of adoption and thus exposure to privacy-related technologies of other subdomains.

8.4.2 *Attitude towards Digitalization*

To provide context for the privacy issues within agriculture, we will present some insights into the general attitudes of farmers towards digitalization in agriculture. Overall, interviewees displayed a balanced view on improvements within their field of work. However, we will elaborate more on the negative aspects, since these are more related to privacy concerns and impede digitalization. Regarding the production steps in the field, automated precision farming is evaluated as helpful for farming within complex field boundaries resulting from the small-scale and fragmented land structure in rural southwestern Germany (fg9), where the group interviews were conducted Doll et al., 2001. Not only is work on the fields affected, but office work is also transforming. Farmers

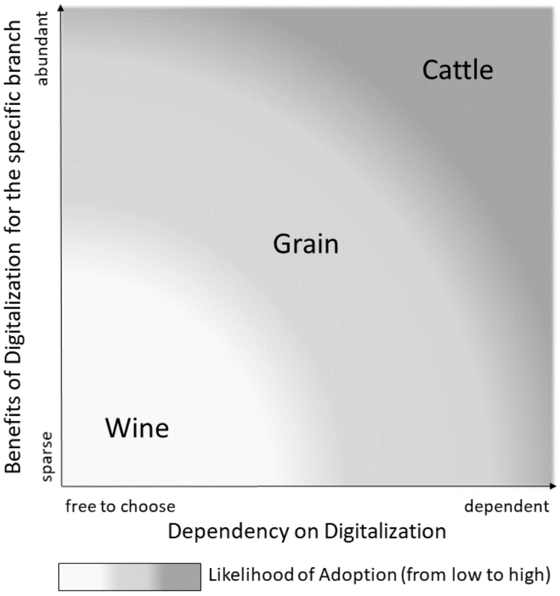

Benefits of Digitalization for the specific branch
abundant
sparse
Cattle
Grain
Wine
free to choose
dependent
Dependency on Digitalization
Likelihood of Adoption (from low to high)

Figure 8.1: Different agricultural subsectors and how they are affected by digitalization, influencing attitudes toward privacy and the likelihood of adopting new technologies

already need to document their work in order to fulfill reporting duties towards authorities. This type of work can be done more efficiently with digitalized farm tools (fg8).

However, not all farmers were generally positive about digitalization and repeatedly mentioned arguments why digitalization is not adopted in all agricultural businesses. One argument is the high price, that is not yet affordable for owners of small and medium-sized enterprises (fg1). Farmers have to decide whether to adopt digital technologies, which ones to adapt and how this will influence their daily work routine (fg9).

> *Q1 (fg10): [...] it is my experience so far that we do not save any work, we just distribute it differently. And perhaps the documentation will then be more centralized, but the skill is to keep the overview*

Another topic that was addressed was that digitalization creates new dependencies. These mainly concerned the technical infrastructure and external services. This refers not only to support for the mechanical components, but also to software failures or mandatory internet connection which causes machines to exit automation mode. Farmers are only left with the option of restarting and hoping that the machine will work again. Otherwise, they have to lay down their work and wait for support services (fg4). The increased dependency on external services results from the need for external staff to fix problems that do not occur with non-digital farm equipment. Another dependency mentioned was availability: Especially the problem of poor mobile data reception in rural areas is a major issue for farmers, because it hinders the effectiveness of their processes on the field (fg10).

8.4.3 *The Value of Privacy: What is Being Done with Data in Digitalized Agriculture?*

Besides general challenges perceived by farmers, we were especially interested in privacy concerns, which were an important factor for most of the focus groups, based on a lack of trust in the intentions and motives of agricultural companies.

The Importance of Privacy for Farmers

The role of farmers is shifting in the process of digitalization. This also affects the different perceptions of the consequences of data transfer towards companies. The scale ranges from fearing the end of the concept of the professional farmer on one side to the opinion that data can be seen as another important resource within the agricultural business on the other side.

> Q2 (fg7): *I see a danger that the farmer might fall behind at some point if the data is really processed in such a way that the companies can take over the planning of the cultivation by themselves.*

Some farmers perceive that they are disclosing more than just data when they give companies access to their documentation:

> Q3 (fg5): *There are people who want our information, how we proceed in the field, or what we have acquired over the years so that someone can analyze it. If they know who did what, where, and when, then almost everyone can copy that. We could be replaced through the many years of experience that we have built up when someone gets this information.*

These statements display the skepticism of some participants that companies are collecting data not only to improve technologies, but also to generate fundamental change in agricultural production itself. Experience and lifelong learning in farming, especially in regions with small to mid-scale farms, is perceived as an important factor for effective production. Replacing the factor of human experience with the appliance of accumulated movement patterns and activities could therefore lead to increasing automation and gradual de-professionalization of agriculture. Most fundamentally, by giving up the exclusiveness of the knowledge of how to work in a specific field, farmers are at risk of being bought out by companies in the future.

Data as a Valuable Resource

Then again, there are also opinions on how to balance the interests of companies in data collection in order to improve technology and the threats that comprehensive transparency poses to farmers. By regarding agricultural data not as a secondary product but as a precious core resource of farming, the prices for data should be commensurate with the advantages companies gain by obtaining data.

> Q4 (fg9): *As long as the data remains within a farm, and I have control over the data, I still see the whole thing [digitalization] relatively relaxed. But as soon as other companies want to gain access to the data, then of course they can also get it at a certain price. So, depending on what kind of data they want, they have to offer something in return.*

From this perspective, there is a need to restrict data access by companies to a certain extent, e.g., only for a short period of time or exclusively for the recipient and not for third parties.

> Q5 (fg6): *The companies that manage the digital crop field cards*[3] *can use the data to create their own personalized profile of you and also predict how you will act in certain situations in the future. That's actually frightening. And who guarantees me that the data will not be sold to other companies?*

Farmers fear that they will be at a market disadvantage if companies can predict their harvest and the effort a farmer has spent in one season. Thus, the perception of data collection is quite negative: if a farmer does not get any benefit from his data, the collection is just additional work with benefits for third parties. This is a serious hindrance to digitalization.

> Q6 (fg10): *We collect a lot of data and do nothing with it. We do collect them, but we cannot use them automatically.*

To conclude, none of the focus groups expressed indifference towards their privacy. Given the perceived risk of professional farmers becoming obsolete and the current situation of data exchange without substantial financial compensation, a need for a solution can be derived by limiting the visibility and accessibility of data by agricultural companies.

8.4.4 *Different Actors with Distinct Intentions regarding Data Ownership*

As a specific aspect of privacy, many concerns about loss of data ownership were expressed by the participants.

[3] crop field card: administrative tool for planning what measures are applied to which piece of land

> Q7 (fg5): *Concerning the digital crop field cards[3] and their cloud versions too, we all agree on the issue of data ownership. That we reveal a lot about ourselves, a lot goes somewhere unknown or maybe people have access to it, and we don't notice.*

Furthermore, farmers argue that they like to stick with the old-fashioned ways of documentation in order to prevent others from getting insight to operational data:

> Q8 (fg2): *If you write your stuff on paper, you know you have it at home in your office. And if you just type it into a cloud, you don't know who can look in and where the data ends up. That's an unsafe context, because it's about important operational data. I think that is the biggest problem.*

Unintended Use of Data

As already mentioned in 8.4.3, if companies gain access to agricultural data, farmers run the risk of giving up part of their economic foundations. However, not only economic actors such as big companies or retailers may benefit from data, but also criminal groups or the authorities.

> Q9 (fg6): *I see opportunities in digital agriculture, but I also see risks in digital agriculture in the form of making the whole documentation transparent. That all the data that you collect, that you have on the farm, can or will become public. If data is in clouds, it can fall into the wrong hands, through hackers, for example, and then they can spy on our entire production data, analyze our professional knowledge and then evaluate what we do.*

But hackers are not the only ones who should be kept out: A much more present danger for farmers than ominous hackers are companies. That companies are trying to collect data from farmers is no secret, and some already have business models to share data with third parties:

> Q10 (fg4): *So, in some way, you can follow some [digitalization] trends, but you should always have a critical look at them and avoid jumping in headfirst. Because otherwise, you're transparent for the companies. With too much data provided, they can take too much advantage.*

> Q11 (fg9): *It is already quite sure that many companies are interested in the data. When I see offers for a digital crop field card[3], where every process on the field is documented, that you get the ten euros cheaper per month, but company "XY" can look into the data. [German Chemistry Company], for example, can look at this data to see what crop protection is being done, what is needed, and for what reason. [...] Not everyone needs to know what I do and what kind of strategy I apply.*

Instead of uploading their data to the servers and clouds of third parties, farmers who already adopted digitalization prefer their own solutions to store and manage their data in order to keep control over it.

> Q12 (fg1): *The PC on which the system runs has a security system of its own, then another NAS system is attached to it, then there used to be a cloud backup all the time.*

Negative Experiences with Existing Systems

On the other hand, some farmers are using cloud-based systems on their farms, which, however, brings some disadvantages: The fact that many technological innovations in agriculture are developed and offered by the leading companies results in a dependency of farmers on company-specific systems. Another reason that makes farmers dependent on third parties is security. Digitalization is already increasing the office workload, and farmers who want to concentrate on farm work cannot guarantee cyber-security.

> Q13 (fg3): *Data protection, also with regard to the security of my data per se, can hardly be guaranteed by myself anymore. I assume that we will soon be looking for a company that will take over the whole thing, where you rent a server, and they take over the data protection part.*

Many responses displayed the skepticism about cloud servers offered by companies, which could potentially profit from the data. Indeed, at the same time, reading the privacy policies is perceived as too complex for farmers without in-depth knowledge of privacy law. One participant stated how frustrating it is to be confronted with privacy policies and unintended consequences of accepting them without fully understanding them:

> Q14 (fg3): *[Digitalization] is of course a great relief, and you can put an end to all this paperwork, but I don't know where my data will end up. It makes no difference whether I read through their privacy policy or not. Nobody can figure it out anyway. And in the end, there is somehow a [German chemistry company] behind it, which then has my data. And a few weeks later, a letter comes and there are some offers that happen to fit well for my farmland. (approving laughter by other participants) Yes, so you really wonder where this comes from.*

Traceability versus Privacy

According to the statements of the participants, newly developed field sensor methods are mostly perceived as convenient and helpful. New technology can provide benefits for the whole supply chain. Being able to trace products from their origin to the end consumer is helpful for marketing, trust building, and avoiding food scandals. Nevertheless, at the same time, this could also provide a loophole for companies like traders or upstream industries to collect data from farmers.

> Q15 (fg8): *Just the other week, I have read a report about field sensors from [two German technology companies], which measure all factors like precipitation, nitrogen level, soil compaction, and vegetation. If a company owns this data, they can do everything with it. They can send you your exact fertilization planning. Actually, that is none of their business.*

Technical innovations in the fields of tracking and navigation systems, automated driving, fertilization, irrigation, sowing, and harvest generate large amounts of data, that can be traced back. On the one hand, this is helpful for the farmers themselves, as it simplifies the operational management of a farm. On the other hand, the enhanced traceability of actions through permanent data collection increases the monitorability and accountability of farmers. For this reason, some participants perceive it as a risk that human as well as sensor errors during the whole process of data collection may result in more frequent, unjustified sanctions by the authorities, e.g., for violation of environmental protection rules due to sensor errors.

> Q16 (fg8): *A drawback is then, through the accurate data collection, on the one hand, that it is easier for inspectors to retrace activities, but that makes it harder for you to adhere to everything. Just because they see it that way does not mean that it went exactly that way. These are small things like typos or something that can get you into big trouble.*

But not only authorities demand traceability. Customers of farmers, especially in the subsector of organic food grocers, are increasingly requesting traceability in order to serve the demands of the final consumers. Accordingly, the provision of retraceable data serves not only to meet the mandatory requirements of authorities, but can also work as a purchase incentive for customers. At this point, market mechanisms put indirect pressure on farmers to offer more transparency.

> Q17 (fg7): *For retail, I have to provide all my data: when I sprayed [plant protection agents], what I sprayed, when, and what I fertilized. That is what the retail trade wants. In other words, all the encryption [of data] we want for the companies stands in contrast to the traceability that the retail trade wants from us. [...] We have to supply it to the retail trade, because they want traceability, but we don't want to give the data to the plant protection agent companies or [two German fertilizer producers]. But then they get the data from retail trade.*

Offering traceability for customers and consumers does not pose a problem as such for farmers, as it provides only small sets of operational information. At the same time, big retailers may gather a large quantity of data, which could possibly be sold to big agricultural companies (fg5). In this context, some of the focus groups identified a loophole for data leakage towards undesired recipients.

8.5 Discussion

In the following, the results obtained in the study are analyzed and placed in the overall context of privacy in this domain, and it is shown why agricultural SMEs are particularly vulnerable with regard to privacy. First, the impact on farmers is explained and reasons for (or against) adoption are discussed. We then look at the domain as a whole and identify facets that play a role in the adoption of digital tools for agriculture. Subsequently, we elaborate on the conflict between transparency and privacy along the supply chain. Further, we briefly highlight existing approaches from research which could potentially help address the identified problems in the future and place them into the context of our results.

8.5.1 *The Impact of Digitalization on Farmers*

When talking about privacy, the focus is always on management of digital data and its dissemination or protection. Therefore, privacy relies on digitalization to provide the infrastructure for privacy-relevant services and products. In 8.4.1 and 8.4.2 we presented some information on the impacts of digitalization on farmers. Building on the results of our study, this section analyzes the general impact of digitalization on the domain to provide a contextual basis for the privacy implications.

Technological change affects the work processes of a modern farm in a far-reaching way and changes the profile of professional farmers in the long term. Especially for SMEs this poses a big challenge, since the adoption of automation and digitalization processes are the more profitable the larger the area of tilled land or the number of cattle is. Moreover, the increased workload in the office is problematic for family-run farms with low workforce.

Before digitalization, farmers mainly had to perform manual work. This includes not only work in the field or barn, but also the maintenance of agricultural machinery. Although planning phases and agreements with other stakeholders also existed in the past, as modern agriculture is dependent on a large number of actors and specialized staff, the participants report that the planning and office workload is significantly increased by digitalization. Some even state that the promised reduction in workload due to digitalization is not noticeable, as work simply shifts to the office (see Q1, Q6). The process of data collection for automated machines is perceived as a nuisance by farmers, especially since the benefit for the own business is much smaller (see Q6), compared to the benefits for third parties through the collected data (see 8.5.2). The shift of work to the office requires the farmers, who formerly managed all work steps themselves, to rely on other parties for maintenance or data management. Thereby the risks posed by data propagation are increased even more. This problem of further dependencies also applies to customer retention by the manufacturers of digital tools. Customers may obtain all their digital tools from one supplier only, thus creating a vendor lock-in effect. Furthermore, farmers today are not only dependent on the weather, as they were in the past, but also on good network connections, nationwide mobile communications, and the availability of satellites.

Considering the identified privacy problems of farmers, it is not surprising that the adoption of digitalization is very heterogeneous in this domain. The results presented in section 8.4.1 showed that the subsectors differ regarding the likelihood and the extent of adoption based on the expected benefits and the need to adopt due to market pressure or legal requirements. A higher dependency on the use of technology can have different effects on the privacy behavior: On the one hand, more experience with the technology allows prejudices to be reduced which therefore have less influence on the data management behavior. On the other hand, the dependence on certain technologies can lead to a feeling of being forced to give the data away in any case. Both factors, prior knowledge and resignation, seem to decrease inhibitory factors resulting from privacy concerns. This shows, that privacy is a relevant factor that affects the adoption of digital technology. Another important point, is that in addition to financial and physical resources, farmers have to spend time, share their data, and have to be flexible to take advantages of the benefits of digitalized agriculture.

8.5.2 *Conflicts of Interests regarding Privacy and Transparency*

Privacy concerns do not only affect the adoption of digital tools, they also play an important role in the everyday life of farmers, since emerging technologies and trends force farmers to provide transparency along the supply chain. The transfer of data along the supply chain is a central feature of digitized processes in agriculture: Data from various parties involved have to be aggregated and exchanged in order to feed machines with the optimal farm data or to guarantee the traceability of certain quality characteristics along the entire supply chain. However, because all the parties involved have their own agendas, conflicts of interests arise.

Many **Farmers** consider the demand for transparency as problematic, as they fear competitive disadvantages. While transparency along the supply chain offers advantages for food safety, it weakens the market position of farmers, who have to fear price dumping if retailers know how the season went for each individual (see Q9, Q10, Q11). The constellation of the supply chain, in which producers consist of a large number of SMEs that are supplied by large companies and deliver to large wholesalers and processing companies, is very specific to agriculture. This puts farmers in a weak bargaining position when it comes to protecting their interests. Some of the interviewees reported about tailor-made offers for their farms (see Q14) which placed them in a subordinate position of power. Due to their weakened market position, farmers also have to fear take-over by large corporations, which are able to carry out cost-effective land

Table 8.2: Legitimate reasons for transparency and the fears of farmers regarding different actors

	Machine manufacturer	Suppliers and buyers	Government authorities
Legitimate reasons for transparency	• Better maintenance due to telemetric data	• Better compliance to quality standards (e.g. 'organic') • Increased food safety	• Better execution of restrictions and regulations for public safety
Fears of farmers	• Vendor lock-in effect • Extradiction of agricultural knowledge and experience	• Price dumping	• Interference and control by government authorities • Loss of funds

management by unskilled workers, as they were able to obtain all relevant data from the farmers' experience (see Q2, Q3). Hence, it is difficult for farmers to assess whether the collection and transfer of data for a certain legitimate purpose, such as regulative reporting obligations or more precise services from service providers, may not lead to an unintended disadvantage (see Q17). Therefore, providing transparency and exchanging data is economically not necessarily in the farmers' interests.

However, when discussing about digitalization in agriculture and the impact of privacy (concerns) on the adoption of digital tools, the farmers' perspective is not the only one to be considered. There are several important actors and stakeholders with legitimate data collection intentions which conflict with the before mentioned fears stated by the farmers in the focus groups. Table 8.2 summarizes these conflicts of interests. In the following, we present three prominent stakeholders and their respective interest in receiving data as well as the farmers' concerns with which they are associated.

Agricultural machinery manufacturers: By accessing farmers' operational data and, in particular, telemetry data from machines, agricultural machinery manufacturers can improve their own products and offer optimized maintenance. If a certain part is found to wear out particularly quickly or frequently, farmers' data can be used to better reconstruct and understand the cause and thus optimize maintenance and product design. In this way farmers can hope for better service and warranty evidence, but they must trust that the data is kept and managed securely so that data leakage or deliberate collaboration with third parties do not have a detrimental effect on the farmers. Thus, farmers need to trust business partners, as they have no control over the further use of their data. If this trust is not assured, farmers will refrain from using digitalized services (see 8.4.4). This does also apply to cloud services and reflects the fear of loss of control of sensitive business data. The feeling of loss of control is not only limited to the domain of agriculture, as shown by Zimmermann et al. (2019).

Further tensions arise from producer dependencies: Manufacturers may benefit from high customer loyalty, but farmers thereby become dependent and are not protected from arbitrary pricing. This is the case, because to a certain extent it is more expensive for the farmer to change supplier and convert the entire farm than to pay higher fees from the current supplier. In addition, farmers fear that their farming operations will be recorded and then, after the agronomic knowledge has been appropriated, used to oust the farmers (see Q2, Q3). This results in fears of becoming obsolete, in that companies could gather the experience and knowledge of their profession, take over the farms and use cheap work forces to do the work.

Suppliers and buyers: Farmers depend on suppliers who supply them with seeds, feed, fertilizers, or pesticides. In this area, farmers benefit from transparency, as they can ensure that they receive products that are compliant with the regulations they face, e.g. legal regulations concerning plant protection and fertilization. It is therefore important that farmers document and plan exactly what they apply on their land. Furthermore, this way food scandals could be prevented or detected more efficiently Kamath, 2018 and in the case of food with certain quality characteristics (e.g. "organic") it is easier to prove that the product meets the quality requirements.

In the opposite direction, however, transparency causes problems: If the suppliers know how the farmers cultivate their fields and what they earn from it, the farmers are strongly dependent on the good will of the suppliers. One interviewee reported that suppliers could increase prices for the products in such a way so that hardly any profit remains for the farmers (see Q10). In this way, prices are at a level at which farmers just barely avoid bankruptcy, but at the same time can hardly generate any profit and thus no reserves. A similar problem arises with the buyers: if they get insight into the farm data they can offer individualized, lower prices, which is a enormous disadvantage for the farmers. Our participants stated their own experiences with these offers (see Q14). This problem of unfair competition also endangers existing structures in agriculture. As Linsner et al. (2019) showed, farmers tend to think of business partners as part of their social environment and do not want to give up partnerships that lasted for generations.

Government supervisory authorities: Farmers receive subsidies from public funds, for example from the European Union. In order to receive these subsidies, they must comply with certain conditions such as upper limits for fertilizers, use of certain plant protection products, or distance zones to water bodies in order to protect drinking water. In this regard digitalization would make it easier to document processes on farms, but many farmers feel at the mercy of government control. Also, trust in technology is not very strong. Farmers know from their daily work how susceptible to faults high-tech agricultural machinery is. Therefore, they do not trust that the automatic recording of operational processes by sensors is so precise that they would make their subsidies dependent on it (see Q16).

To conclude, agriculture is a domain in which a large number of small and medium-sized farms depend on large companies to supply them with machines and working materials, offer services such as soil sampling or buy up the yield. Additionally, the farmers are often reliant on IT service providers to digitalize their businesses. Governmental actors need access to data to ensure compliance with regulations. Within this large number of stakeholders, each actor has its own interests and expectations regarding digitalization and data handling. Above all, the transparency and traceability of agricultural products creates tensions in the sector. In order to resolve those, suitable and data protection sensitive processes and tools are needed that take into account the needs of individuals and make the advantages of digitalization available to all.

8.5.3 *Outlook on Future Research Possibilities*

Concluding our findings on the effect of privacy on digitalized agriculture, we very briefly want to point towards possible measures to address these problems in the future and hence give some impulses for future research.

Our results show that one of the key problems for SMEs lies in their position in the middle of the supply chain and their size resulting in a weaker bargaining position. Sharing too much data towards commercial purchasers or suppliers of necessary primary products and machinery can lead to higher prices and economic pressure. Hence, it is crucial for SMEs to retain the control over the access to and flows of their farm data. This is also important from the perspective of potential (interstate) conflicts Reuter, 2019 or data breaches Saleem and Naveed, 2020, that may affect farmers. Privacy-enhancing technologies could help to achieve this, by creating usable solutions and access control mechanisms. This could be done with tools based on blockchain-technology, which has the additional benefit of non-repudiation and is favored by the food industry for providing transparency for supply chains Bermeo-Almeida et al., 2018; Ge et al., 2017; Kamath, 2018. However, granting control over data flows for the data owner remains a challenge. For example, if a machinery manufacturer collects data to perform computations on it, even with data access management, data leakage or misuse of data for personalized offers cannot be ruled out. For this purpose, secure multiparty computation methods could enable the manufacturer to perform computations on encrypted or obfuscated data without having access to the actual data. By this, a misuse of data for personalized offers and similar issues could be prevented. While this technology has been suggested for the use in other domains Froelicher et al., 2017; Pham et al., 2017, future research could work on creating more possibilities for such an application in agriculture.

Last but not least, we want emphasize the importance of raising awareness for privacy. A situation, in which the sharing of data leads to financial advantages (see 8.4.3), could create economic pressure for other producers to share data as well to remain competitive. Hence, in this situation the producers are played off against each other and put under pressure to give up their privacy. As a consequence, greater awareness for these problems could foster the demand for privacy-enhancing technologies and rule out any privacy risks that hinder digitalization in agriculture.

8.5.4 *Limitations*

Although our study addresses our research question, it still has limitations. (1) Because of the qualitative methodology of this study, the value of it is exploratory and hypothesis-generating. Thus, no quantitative insights can be gained from it and the results may not be applicable to all farms. (2) Moreover, our study focuses on SMEs, because they are the least likely to use digital tools and are therefore worth investigating. However, this is also a limitation, since our findings do not represent every type of agricultural business. (3) While representing the gender ratio of farm managers closely, our study consists of mostly younger participants. A more diverse sample regarding age could offer additional insights.

8.6 Conclusion

In our study, we examined how privacy affects the process of digitalization in agriculture. Such a study might be a valuable background for the research on privacy-enhancing technologies, provided that it presents empirical evidence on privacy-related obstacles and conditions. First, we presented the influence of digitalization on the daily work of farmers and their wishes with regard to privacy (8.5.1). Furthermore, we have shown that different actors along the supply chain have different interests regarding digitalization (8.5.2). Concluding from this analysis, we have presented challenges and possibilities for future development in this domain (8.5.3).

The role of transparency in the industry is controversial. While it offers advantages especially for downstream actors in the supply chain such as retailers, it also creates conflicts of interest for upstream actors such as suppliers who fear being overcharged in price. Asymmetries in market position between SMEs and large agricultural companies seem to amplify these conflicts. For the successful adoption of digitalization without individuals being left behind, it is necessary to establish mechanisms that make relevant data accessible to all without exposing the operational data of individuals for misuse. Therefore, privacy and especially the fear of its violation by new technologies and business practices remains an important factor in the adoption of digitization in agriculture. Many businesses of different sizes have to weigh up whether the promised advantages outweigh the feared disadvantages. Transparency in particular is a double-edged sword: it creates trust, but can also be threatening if business secrets are disclosed to third parties.

9

LoRaWAN Security Issues and Mitigation Options by the Example of Agricultural IoT Scenarios

ABSTRACT The IoT is a major trend that is seen as a great opportunity to improve efficiency in many domains, including agriculture. This technology could transform the sector, improving the management and quality of agricultural operations, e.g., crop farming. The most promising data transmission standard for this domain seems to be *LoRaWAN*, a popular representative of LPWAN technologies today. LoRaWAN, like any wireless protocol, has properties that can be exploited by attackers, which has been a topic of multiple research papers in recent years. By conducting a systematic literature review, we build a recent list of attacks, as well as collect mitigation options. Taking a look at a concrete use case (IoT in agriculture) allows us to evaluate the practicality of both exploiting the vulnerabilities and implementing the countermeasures. We detected 16 attacks that we grouped into six attack types. Along with the attacks, we collect countermeasures for attack mitigation. Developers can use our findings to minimize the risks when developing applications based on LoRaWAN. These mostly theoretical security recommendations should encourage future works to evaluate the mitigations in practice.

ORIGINAL PUBLICATION *Kuntke, F., Romanenko, V., Linsner, S., Steinbrink, E., & Reuter, C. (2022). LoRaWAN security issues and mitigation options by the example of agricultural IoT scenarios.* Transactions on Emerging Telecommunications Technologies*, 1–20. https://doi.org/10.1002/ett.4452*

ACKNOWLEDGMENTS This work was supported by funds of the German Government's Special Purpose Fund held at Landwirtschaftliche Rentenbank in the project Geobox-II as well as by the German Federal Ministry for Education and Research (BMBF) in the project HyServ (01IS17030B) and by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – 251805230/GRK 2050.

9.1 Introduction

The Internet of Things (IoT) is a hot topic with various use cases, which are usually prefixed by the term *smart*, like *smart home*, *smart city*, and *smart farming*. The idea of IoT is to use networks ("internet") to connect sensor devices or actor devices ("things") with IT systems. This allows for monitoring or automated controlling of the environment in the real world. One essential component of each IoT system is the data transmission technology. Depending on the use case, the requirements for wireless transmissions differ. Smart home solutions may just have to bridge a couple of meters to the next gateway. But in other scenarios, this can be a lot different - the distance to the next gateway can be many meters (smart city) or even kilometers (smart farming). Wireless transmission protocols that suit this long range requirement for IoT applications are grouped by the term LPWAN, covering several network protocols from different vendors, e.g., LoRaWAN, SigFox, NB-IoT, LTE-M. Compared to more traditional wireless network protocols like Wi-Fi, LPWAN protocols allow for a much higher transmission distance between devices, up to several kilometers, as well as having a low power consumption (Rana et al., 2021). The most popular solution – at least in the domain of agriculture – seems to be LoRaWAN, a specification designed by the LoRa Alliance (2017). In comparison with the direct alternatives, LoRaWAN achieves a lower power consumption (i.e., higher battery life) alongside support for rather high data transfer rates while embedding authentication and encryption by default (Mekki et al., 2019).

With the increased use of IoT systems using LoRaWAN for data transmission, the risk of malicious participants taking advantage of any vulnerabilities of the LoRaWAN technology also increases. Therefore, a specific analysis of attacks on LoRaWAN as one promising protocol for IoT is necessary.

Since LoRaWAN has existed for several years now, surveys (Butun et al., 2018a; Yang et al., 2018) inspecting the protocol's security were already conducted to some extent. However, in the time between those surveys were conducted, more vulnerabilities were detected, and the LoRa Alliance has published new LoRaWAN versions that affect the vulnerability to some of the older attacks. Therefore, this paper will provide a recent survey on the security of LoRaWAN. To illustrate use cases and attacks, we choose agricultural IoT applications as we see rather challenging use cases (from a security perspective) here that combine many properties which demand LPWAN solutions like LoRaWAN. But the findings will also hold for LoRaWAN applications of other domains. The research questions (RQ) of this work are:

- [RQ1:] *What are the known vulnerabilities of LoRaWAN?*
- [RQ2:] *Which mitigations against the known vulnerabilities should be considered when developing a LoRaWAN-based IoT solution?*

To answer these questions, we first outline some IoT applications in the use case of agriculture to give an idea of how IoT applications work and which requirements make LPWAN, e.g., LoRaWAN, necessary. By conducting a systematic literature review, we extract domain specifics as well as known LoRaWAN vulnerabilities.

By providing a comprehensive list of countermeasures to to reduce the vulnerability of an (agricultural) IoT setup, we aim to help developers and scientists to employ LoRaWAN applications. Developers that aim to work on an IoT project may be the main beneficiaries of this paper. The contributions are the following:

- overview of the LoRaWAN technology,
- a review of IoT specifics for wide area applications (considering agricultural IoT as an example),
- a recent overview of vulnerabilities of LoRaWAN and its mitigations, and
- security recommendations for IoT application developers using LoRaWAN.

The structure of the paper is as follows: Section 9.2 gives background information about LoRaWAN and the state of research. Section 9.3 provides specifics of IoT applications that require wide area transmissions, using the example of agriculture. Section 9.4 describes the literature selection method. In Section 9.5, the selected literature is used to list the vulnerabilities of LoRaWAN setups. In the same section, preventive mechanisms are proposed for each attack - primarily from the perspective of an IoT application developer. Section 9.6 presents the discussion, and Section 9.7 concludes the paper.

9.2 Background and Research Gap

Overview about LoRaWAN The LoRa Alliance[1] published the LoRaWAN protocol standard, which is primarily used for connecting battery-powered end-devices, like environmental sensors. This protocol is popular in industry and science, which may be due to the fact that it combines a high range with acceptable bandwidth and comparatively low cost (Cambra et al., 2017). At the time of writing, v1.0.4 (LoRa Alliance Technical Committee, 2020) (released in 2020) and v1.1 (LoRa Alliance, 2017) (released in 2017) are the two suggested protocol specifications for new developments. But when looking at commercially available end-devices, it seems that the former standards LoRaWAN v1.0.2 (released in 2016) and v1.0.3 LoRa Alliance, 2018 (released in 2018) are dominating – unfortunately, such devices cannot be easily upgraded as there are different hardware requirements for v1.1 and v1.0.4.

According to the specifications, a typical LoRaWAN network consists of the following components: EDs, also called *nodes*, GWs, NSs, JSs and, ASs (see Figure 9.1). EDs communicate with GWs, and GWs forward raw data frames to the NS over standard IP connections, e.g., via Ethernet or cellular data connections. The NS is responsible for validating and decoding packages, as well as forwarding them to the AS. It also manages other LoRaWAN features like the adjusting adaptive data rate (ADR). The communication between an ED and a GW is done via the LoRa specification (physical layer and data link layer). When considering the Open Systems Interconnection (OSI) model, LoRa is filling the physical layer and LoRaWAN forms the data link layer and the network layer (see Figure 9.2). LoRa uses a wireless modulation utilizing the chirp-spread spectrum Berni and Gregg, 1973 for transmission.

Khutsoane et al. (2017) present an overview of (scientific) applications of LoRa and LoRaWAN, e.g., measuring urban greenhouse gas emissions, monitoring

[1] https://lora-alliance.org

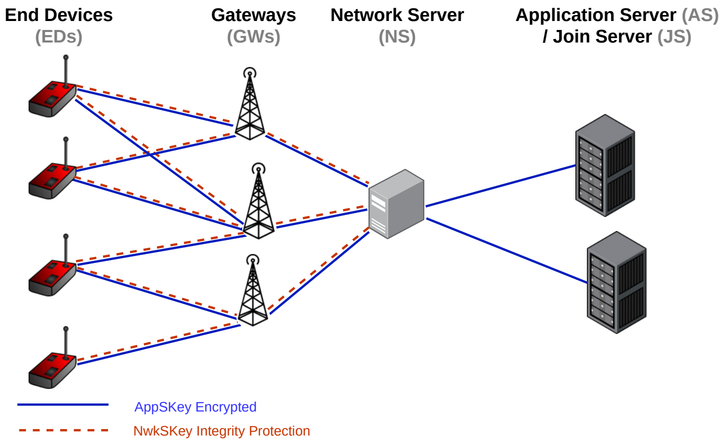


Figure 9.1: LoRaWAN Architecture and Key Usage (own illustration)

the temperature of blood fridges, and water grid management. The physical layer LoRa can also be used without the LoRaWAN part (data link layer and network layer) for different use cases, like wide-area point-to-point communication (Kuntke, Sinn, & Reuter, 2021) or communication devices for network outage scenarios (Baumgärtner et al., 2020a). But in this present paper, we concentrate on the rather common usage of LoRaWAN in terms of IoT setups.

LoRaWAN specifics The LoRaWAN specification (LoRa Alliance Technical Committee, 2020) defines three ED classes: Class A, Class B, and Class C. These three classes differ in the frequency of open receive window time slots, which has a direct impact on the power consumption and battery life.

- *Class A* can send data at any time (uplink), but the other direction from the NS towards the ED (downlink) is restricted. There are up to two short downlink receive windows, followed by each uplink transmission (see Figure 9.3). For this reason, all downlink communications from the NS must wait until an uplink is initiated by the ED.

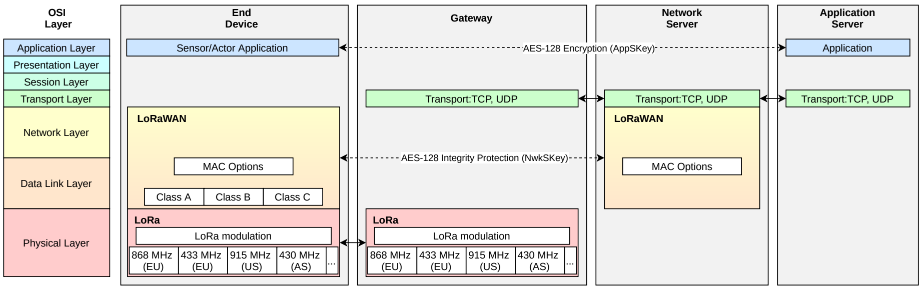


Figure 9.2: Simplified LoRaWAN technology stack in the OSI model (own illustration)

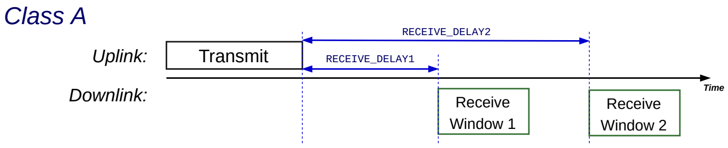


Figure 9.3: Class A ED receive-slot timing (own illustration)

- *Class B* differs from Class A by having more and scheduled receive slots. In order for the Class B-enabled EDs to open the extra receive windows at scheduled times, it receives a time-synchronized beacon from the gateway. In this case, the NS knows when the ED is listening and must not schedule the downlink message for an ED to an ED-initiated transmission. Battery consumption is higher compared to Class A-enabled EDs.

- *Class C* goes one large step further and has continual receive windows. Class C-enabled EDs listen almost continuously for downlink messages. The receive windows are just closed during the transmission of an ED. Obviously, having the radio device listening all the time consumes more energy, and, therefore, the battery life is shortest with Class C-enabled EDs.

The topology of LoRaWAN networks is "star-of-stars," where one NS can talk with multiple GWs, and each GW can communicate with multiple EDs. An NS forwards packets received by one or more GWs to the responsible AS and vice versa. There is no hard relation between an ED and a specific GW. If an uplink transmission by an ED is received by multiple GWs, all GWs forward the LoRaWAN packet to the connected NS, which performs *deduplication* of the multiple receptions of the same packet. In case a downlink transmission should be sent to an ED, the NS chooses the GW for transmission.

LoRaWAN transmissions use two session keys for safeguarding a message's security and integrity (see Figure 9.1): The `AppSKey` is used to end-to-end encrypt the payload between ED and AS via Advanced Encryption Standard (AES). The integrity of messages between an ED and an NS is ensured by integrating message integrity codes (MICs) in the transmitted packets, calculated via AES-CMAC.

The `AppKey` is the personalized, unique 128-bit AES root key of each ED that must be pre-configured by the device manufacturer. Based on this `AppKey`, the session key `AppSKey` is derived during the ED activation process.

Device Activation Schemes For registering an ED, two activation modes exist: ABP and OTAA. In both modes, the desired ED is provisioned with three keys: a device address (`DevAddr`), a network session key (`NwkSKey`), and an application session key (`AppSKey`). When using ABP, all three individual keys are directly stored on the ED before it can participate in the LoRaWAN network. In the specifications of LoRaWAN v1.0.4 and v1.1, it is recommended to use OTAA for "higher security applications". When using OTAA, all EDs must be personalized with a global unique ED identifier (`DevEUI`), the JS identifier (`JoinEUI`), and an AES-128 root key `AppKey`. The `AppKey` allows the derivation of the session keys `NwkSKey` and `AppSKey` when the device joins via OTAA.

LoRaWAN Specification History The first specification was released with *LoRaWAN v1.0* in January 2015. *LoRaWAN v1.0.1* was introduced in February 2016 with some minor changes and clarifications of the specifications. *LoRaWAN v1.0.2* was introduced in July 2016 and added the encryption of the Uplink Frame Counter (`FCntUp`) and added this counter (`FCntUp`) to the confirmation messages (ACK downlinks) as a preventive measure against replay attacks. Starting with that release, regional parameters were also shipped as a separate document. *LoRaWAN v1.1* was introduced in October 2017 with many drastic changes that place higher requirements on ED hardware as well as new software requirements on NS. JS and NS are separated — prior, the functions were managed solely by the NS. Frame counters could not be reset, two keys (texttNwkKey, texttAppKey) for session security were introduced. *LoRaWAN v1.0.3* was introduced in July 2018, bringing some changes of v1.1 into the v1.0.x branch, mainly for Class B devices. *LoRaWAN v1.0.4* was introduced in October 2020 with more changes and clarifications. But as there are also new hardware requirements (persistent storage for `FCnts`), it can be seen as a breaking change.

Security Issues of LoRaWAN Several studies have examined the LoRaWAN protocol and found various security gaps depending on the respective version. Aras, Small, et al. (2017) focused on LoRaWAN's physical layer (LoRa) and have shown that it is possible to jam a LoRa network using commercial off-the-shelf hardware. Another work that focuses on LoRaWAN security by Yang et al. (2018) presents five possible attacks to compromise confidentiality, availability, or integrity and provides a selection of countermeasures. Some known attacks have since been addressed by the release of LoRaWAN v1.1. This version introduced many security-related changes together with the option to support backward compatibility for v1.0. However, as investigated by Dönmez and Nigussie (2018), only session key derivation is addressed when using the backward compatibility mode – other security benefits are lost. Their work is the first to provide a full list of detailed attacks for both of the supported LoRaWAN versions. A similar list has been compiled by Butun et al. (2018a) for LoRaWAN v1.1 only, but it lacks detailed attack information and security recommendations, which we aim to provide within this work. Especially with the release of LoRaWAN v1.0.4, we have not found any security review of LoRaWAN that takes into account the changes of this protocol version.

Research Gap Several scientific papers recommend more research on IoT security in general, as well as in specific domains like smart farming (Demestichas et al., 2020; Gupta et al., 2020a; Sontowski et al., 2020). Unfortunately, it is currently difficult for developers or researchers to obtain simple, clear security recommendations for the development of IoT solutions in general and more difficult when it comes to the specific use scenario of agriculture. Another problem is the variety in today's deployed and actively used IoT technologies and protocols. In this work, we focus on LoRaWAN, as it seems to be popular in science and industry - and also in agriculture (Davcev et al., 2018; Grunwald et al., 2020). Even though LoRaWAN is just a couple of years old (v1.0 was released in 2015), multiple works that collate security issues exist (Butun et al., 2018a; Cambra et al., 2017; Yang et al., 2018). With the publication of more vulnerabilities, as well as new LoRaWAN specification releases, we see the need for an updated overview about security issues, as well as mitigation options.

The overall goal of this work is to provide a list of possible LoRaWAN attacks and to provide security recommendations that are not reliant on protocol changes and are therefore usable by developers working in the field. As an example for attack illustration, we choose the agricultural IoT environment, as this example allows to argue for multiple requirements in one use case. The following section (Section 9.3) collects IoT specifics on the example of agricultural applications.

9.3 Specifics of IoT in Wide Area Applications

This section presents specifics of IoT in applications that must cover large areas, as LoRaWAN is especially for those use cases a relevant technology. We have chosen agriculture as a tangible example for listing example applications of IoT and for rendering known attacker profiles by real-world use cases with a demand for IoT security.

9.3.1 *Specifics of Wide Area IoT by the Example of Agricultural Applications*

According to the American Heritage Dictionary of the English Language (2021), agriculture is the *"science, art, and business of cultivating soil, producing crops, and raising livestock"*. It is an essential part of the food chain and responsible for feeding the world's population. Therefore, agriculture is typically considered to be a critical sector and should be treated as such. For that reason, all the necessary technologies and tools of agriculture must be designed carefully with regard to safety and security.

There are many kinds of specific agricultural businesses that are part of agriculture, e.g., livestock breeding, viticulture, crop farming. In this paper, we take conventional crop farming as our exemplary IoT use case, as we see both a trend in increasing offers for crop farming specific smart devices and also an increasing demand for high efficient production that requires modern technologies, like IoT networks deployed in large areas. In the following, we list specifics building on contributions of multiple publications (Bokusheva & Kimura, 2016; Elijah et al., 2018; Geil et al., 2018; Gupta et al., 2020a; Hamami & Nassereddine, 2020; Nikander et al., 2020a; Popescu et al., 2016; Sanjeevi et al., 2020; Terence & Purushothaman, 2020; Tzounis et al., 2017; West, 2018), where a), b), c) are rather relevant for the success and applicability of attacks and d), e) are rather influencing the motivation of adversaries:

a) Physically Accessible Devices When looking at the surveillance of sensor/actuator units set up on the area of operation (agricultural fields), the majority of these EDs must be considered *unsupervised* without specific safety mechanisms, i.e., an attacker might easily access and modify it (Tzounis et al., 2017).

b) Area of Operation We have to deal with potentially large areas between connected devices, as this is may be one reason to choose LoRaWAN. As rural areas are rather sparsely populated, usually, there are not any or just a few electronic devices between EDs. Additionally, IoT devices are potentially exposed to harsh environmental phenomena (Tzounis et al., 2017).

c) Lack of IT Knowledge The end-users (e.g., farmers) should not be treated as IT experts with knowledge about specifics of IT security (Geil et al., 2018; Linsner et al., 2019; Nikander et al., 2020a) as well as IoT specifics (Elijah et al., 2018). Facing an heavy workload, the farmers' time budgets are limited (Linsner et al., 2021; Petit et al., 2010). Therefore, agricultural IoT solutions need to be ready to use without difficult and time-consuming manual steps.

d) Sensing and Acting Devices used in IoT scenarios are both sensors and actuators. In agriculture, sensors are used for weather conditions, supervision of plant growth, nutrition, and water level. They generate the data that are the basis for a decision, like how many fertilizers could be applied or what is the optimal water inflow. Controlling the water flow of an irrigation system is an example use case for actuators (Hamami & Nassereddine, 2020; Sanjeevi et al., 2020; West, 2018). Especially the potential modification of the environment makes agricultural IoT use cases worthy of protection.

e) Increasing Responsibility of Single Companies As for social responsibility, we see a trend that fewer companies (e.g., farms) are responsible for supplying more people (e.g., with food), at least in the western world (Bokusheva & Kimura, 2016; Popescu et al., 2016). This is due to the increased operational performance though the use of more precise methods and further improvements in technology.

9.3.2 *Security of IoT Systems on the Example of Agricultural Applications*

Different works have investigated possible benefits and challenges for IoT in agriculture, with Elijah et al. (2018) stating that they believe the adoption rate will increase in the following years. However, the authors warn that additional

Table 9.1: Agricultural IoT application area according to Demestichas et al. (2020) with ED examples

IoT Application Area	**Example**
Continuous land monitoring	Surveillance cameras
Water management	Smart valves or pumps
Monitoring and reporting of crop growth	Cameras
Identification and management of soil characteristics	Sensors for temperature, humidity, and light
Detection and recognition of diseases in crops and/or plants	Optical sensors on leafs of a representative plant; multi-spectral cameras on multicopters for big areas
Enhanced food preservation and quality control	Gas, temperature, and humidity sensors
Smart livestock	Smart collars for cattle

research in security is required to ensure continued growth. Barreto and Amaral (2018) support this statement, showing the importance of IT security across the software and hardware landscape in agriculture by drawing high-level scenarios like *agroterrorism*, the agricultural branch of cyber terrorism. One given example concerns the malicious manipulation of smart farming devices in a way that may lead to a refusal of the produced food by the food supply chain. The threat of malicious misinformation is further highlighted by Gupta et al. (2020a). In their overview of smart farming and general security threats, the authors cite the flooding of a field by feeding erroneous data into the system as an example of such an application.

Demestichas et al. (2020) give an overview of more general security threats in agricultural IoT and also grouped applications into seven areas. We take their grouping and give examples of ED that could be used to fulfill the application in Table 9.1.

ATTACKER DESCRIPTION The focus of our work is on the wireless link between ED and GW and the physical access on the EDs itself. In the following, we use the terminology and proposed attacker profiles for cyber-physical systems by Rocchetto and Tippenhauer (2016) and tailor these profiles to the agricultural IoT use cases by adjusting the profiles for the context of agricultural IoT:

The *basic user* is the attacker profile without a clear target of harming a specific company, but with time and interest to understand the technique. This profile includes hobbyists that want to see how things work and could also be a threat to agricultural IoT by having fun to exploring technologies like LoRaWAN in a rather offensive manner, comparable to war-driving. Their monetary budget is limited, but they have quite a lot of time for experiments.

The profile *insider* includes people with a lot of knowledge about concrete installed setups. In the case of agricultural IoT, this profile matches (past) employees of IoT service providers who installed IoT setups on the field. Their motivation could be to discredit the IoT service provider by disturbing the IoT setups on the field. Their time and money budget is limited, but they have insider information, e.g., which device is accessible on which position.

Hacktivists could especially be a problem in agriculture, as debates about environmental threats often include agricultural practice. Their time and money budget is rather high, and also the knowledge could be treated as high.

The *terrorism* profile does not match too well with the agricultural IoT scenario we consider in our paper. Although there is a general threat to the domain by agrifood-terrorism, we see just a low motivation for attacking single IoT setups, but rather attacks on the cloud-domain of much-used software, which is not in the scope of this present paper.

Agricultural IoT could also be of interest to *cybercriminals*, especially when considering bigger farms with a bigger financial pad that could be the target of attacks (e.g., Denial-of-Service (DoS)) in combination with blackmailing.

Like *terrorism*, we did not see *nation-state* attackers as a real danger for the scope of this paper, as this attacker profile usually aim for greater targets and less on single IoT setups.

9.4 Literature Selection Method

This section describes the method that formed the upcoming section: The systematic literature review (Kitchenham & Charters, 2007; vom Brocke et al., 2015) for collecting vulnerabilities and mitigations specific to LoRaWAN (Section 9.5).

The questions for the literature review are:

- [Q1:] Which attacks or vulnerabilites exist for LoRaWAN (and LoRa)?
- [Q2:] Which mitigations exist to prevent known vulnerabilities for LoRaWAN (and LoRa)?

We selected the following keywords to build our search string:

- LoRaWAN, LoRa
- Vulnerability, Attack
- Security, Cybersecurity, Mitigation.

Based on the keywords we built the search string: `("LoRaWAN" OR "LoRa") AND ("Vulnerability" OR "Attack") AND ("Security" OR "Cybersecurity"`

`OR "Mitigation")`. The following databases/publishers served as data sources: ACM Digital Library, IEEE Xplore, Science@Direct, Springer, Taylor and Francis. After performing the queries on the databases, we collected 403 articles. Further filtering was done based on:

- Inclusion criteria:
  - Published in between 2015 and 2021
  - Describes at least one attack, vulnerability, or mitigation
  - Provides technical details of the attack, vulnerability, or mitigation.
- Exclusion criteria:
  - Not peer-reviewed
  - Not published in English
  - No relation to LoRa(WAN).

After filtering based on these criteria, we obtained 37 articles (Table 9.2) we used for the compilation of vulnerabilities and mitigations (Section 9.5).

Table 9.2: Detected publications of the systematic literature review, together with the referenced LoRaWAN version, and described attack-types, according to our categorization (Figure 9.4).

Author, year	**Referenced LoRaWAN version**	**Described Attack-Type**
J. Lee et al., 2017	v1.0	Other (MitM)
Na et al., 2017	v1.0	Message Replay
Aras, Ramachandran, et al., 2017	v1.0	Physical, Message Replay, DoS
Tomasin et al., 2017	v1.0	Message Replay, DoS
Aras, Small, et al., 2017	v1.0	DoS
Kim and Song, 2017	v1.0.2	Message Replay
Gladisch et al., 2018	v1.1	Message Replay, Traffic Analysis
Yang et al., 2018	v1.0.2, v1.1	Message Replay, DoS
Sung et al., 2018	not defined	Message Replay
Danish et al., 2018	not defined	DoS
Benkahla et al., 2018	v1.0	Spoofing, Other (MitM)
Skorpil et al., 2018	v1.0.2, v1.1	Message Replay, Spoofing, Other (MitM)

Continued on next page

Table 9.2: Detected publications of the systematic literature review, together with the referenced LoRaWAN version, and described attack-types, according to our categorization (Figure 9.4). (Continued)

Author, year	Referenced LoRaWAN version	Described Attack-Type
Y. Cheng et al., 2018	not defined	*No described attack*
Dönmez and Nigussie, 2018	v1.0.2, v1.1	Message Replay, Traffic Analysis, DoS, Spoofing, Other (MitM)
Butun et al., 2018a	v1.1	Message Replay, Traffic Analysis, DoS, Other (MitM)
Mundt et al., 2018	v1.1	Message Replay
van Es et al., 2018	v1.0.2, v1.1	DoS
Ruotsalainen and Grebeniuk, 2018	v1.1	Traffic Analysis
Coman et al., 2019	v1.0.1, v1.0.2, v1.0.3, v1.1	Other (Packet Forging)
Wadatkar et al., 2019	v1.0	DoS
Raad et al., 2019	v1.1	Other (MitM)
J. Xu et al., 2019	v1.0.3	Other (Side-Channel)
Hill et al., 2019	not defined	DoS
Saxena et al., 2019	not defined	DoS
Kamble and Gawade, 2019	not defined	DoS, Other (MitM)
Eldefrawy et al., 2019	v1.0, v1.1	Message Replay, DoS
Mikhaylov et al., 2019	v1.1	DoS
Bala et al., 2019	v1.0	*No described attack*
Thomas et al., 2020	v1.1	Other (MitM)
Philip et al., 2020	v1.0, v1.1	DoS
C. Gu et al., 2020	v1.0.2	DoS
Perković and Sirišćević, 2020	v1.1	DoS
Singh et al., 2020	v1.0	DoS
Noura et al., 2020	v1.0.1, v1.0.2, v1.0.3, v1.1	Physical, Message Replay, Traffic Analysis, DoS, Spoofing, Other (MitM)
Hessel et al., 2020	v1.0.2, v1.0.3, v1.1	Spoofing
X. Wang et al., 2020	not defined	Spoofing

Continued on next page

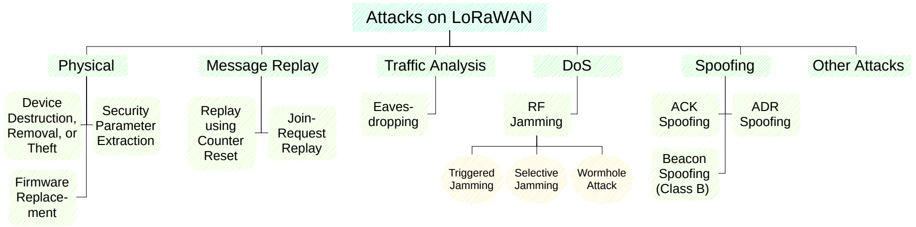


Figure 9.4: Attack types of the LoRaWAN vulnerabilities

Table 9.2: Detected publications of the systematic literature review, together with the referenced LoRaWAN version, and described attack-types, according to our categorization (Figure 9.4). (Continued)

Author, year	**Referenced LoRaWAN version**	**Described Attack-Type**
Lv et al., 2021	not defined	Message Replay

9.5 Vulnerabilities and Mitigations

This section compiles the collected vulnerabilities of LoRaWAN, which we found through the previously literature selection (Section 9.4). The presentation includes an attack procedure to increase understanding and special cases, which might not be immediately apparent for some selected attacks. As no found literature inspected the most recent LoRaWAN v1.0.4 (see Table 9.2), we checked the specification (LoRa Alliance Technical Committee, 2020) for having the same characteristics that made the described attack working. Additionally, within each attack, we include an assessment of the potential impact on confidentiality, integrity, and availability, such as that used by the CVSS Impact Metric (FIRST — Forum of Incident Response and Security Teams, 2019) to evaluate various attacks. Subsequently, known countermeasures to prevent or reduce the impact of the attacks are proposed for each attack type. We roughly grouped the attacks based on the attack type in Figure 9.4. A listing of all countermeasures together with the mitigated attacks is presented in Table 9.3.

9.5.1 *Physical Attacks*

Being placed out in the open and lacking any strong physical protection, EDs can be subjected to multiple direct, physical attack options - especially in agriculture; this is a serious threat. Those options can be grouped into the following three attacks (Na et al., 2017): *(a) ED destruction, removal, or theft*, *(b) Security parameter extraction*, and *(c) ED cloning or firmware replacement*.
All of these attacks are not specific for LoRa devices but important to consider

when designing a robust system. Being agnostic to the transmission data technology, the attacks are possible in each version of the LoRaWAN specification.

a) *ED destruction, removal, or theft.* Destruction, removal, or theft of an ED limits the information available to the system by disabling a responsible ED. While theft is only possible by a malicious entity, multiple sources for device damage or removal exist, e.g., environmental effects, animals, or destruction by humans due to an accident - to name some of the more likely ones. It is important to note that this list is incomplete as other sources of device damage might exist depending on location.

For IoT in agriculture, this attack presents a high threat for availability, permanently removing an ED from the system and forcing additional replacement costs. However, the attack has no effects on confidentiality and integrity.

b) *Security parameter extraction.* An attacker with physical access on an ED can attempt to extract security parameters. A serial interface, if available on the ED, can be used to extract all key exchanges due to the lack of built-in encryption between the host microcontroller and radio module in contemporary radio modules. However, such an attack would only comprise data stored in the specific ED, as root keys are uniquely generated. Nonetheless, this can be combined with firmware replacement to allow the reuse of keys (Aras, Ramachandran, et al., 2017; Butun et al., 2018a).

Security parameter extraction would allow an attacker to read all data sent by the ED, and represents a clear threat for confidentiality, however, the impact is low in agriculture. As mentioned earlier, root keys are unique, and most of the data from a single sensor can be accessed using other methods, or is not enough to disclose relevant business information. Extracting security parameters in itself provides no threat for availability or integrity.

c) *Firmware replacement.* Physical access can also be used to intercept all data exchange between the host microcontroller and the radio module and use this information to create a mock device with the same credentials. The attacker could also resort to advanced tampering to potentially modify or replace the firmware, which could lead to key reuse being possible (Butun et al., 2018a).

This is the most dangerous of all the physical attacks. Allowing for key reuse allows an attacker to potentially obtain information from many sensors and leak business secrets like soil composition, we therefore rate the impact as high for confidentiality. Furthermore, an attacker could use the replaced firmware to feed any data into the controlling subsystem, which could prove fatal when dealing with automated irrigation for example. We therefore rate the impact on integrity as high as well. A firmware attack that modifies the sensor to produce gobbled data is equivalent to removing it from the system entirely in regards to availability and is classified as high, similar to the destruction-based physical attacks described earlier.

Countermeasures Physical attacks are a problem for the IoT world as some usage scenarios do not allow EDs to be physically protected from unauthorized third parties. Ways to mitigate physical access like surveillance via cameras and hiding through unobtrusive design are known, but some strategies can help to further reduce the impact of such attacks:

a) To ensure authentication and integrity of the software, the firmware should be verified using ultra-low-power cryptographic hash functions (Butun et al., 2018a). Also secure hardware elements could enhance the security level against physical attacks (Noura et al., 2020).

b) EDs should be checked routinely for unauthorized hard- or software modifications as well as damage Butun et al., 2018b.

c) Extracted cryptographic parameters will change upon initiating a new session when using OTAA, making extracted parameters useless. This is not the case for ABP, and, therefore, OTAA should be preferred.

9.5.2 *Message Replay*

Replay using Counter Reset

There are two activation modes available in a LoRaWAN setup: *ABP* and *OTAA*. In ABP-mode, EDs use static keys that can't be changed for the duration of the EDs' lifetime. Non-volatile memory for frame counters that is allowed up to LoRaWAN v1.0.3 (LoRa Alliance, 2018) results in a vulnerability to replay attacks. In OTAA-mode, EDs are safe from replay attacks caused by manual devices resets but are still vulnerable to counter resets caused by overflowing as the session keys remain the same (LoRa Alliance, 2018).

The ED reset vulnerability can be abused by an attacker to replay messages from previous sessions, thereby withholding changes from the GW. Resetting the counter after an overflow can be used to replay pre-reset messages to desynchronize the GW and ED counters and thereby cut the communication between those two (LoRa Alliance, 2017). An attacker has to monitor and store messages, which can be done in the radio range of GW and ED, but does not require knowledge of the exact location of either. Because the counter value is not encrypted during the message transmission, it is readable by eavesdropping the LoRaWAN transmissions. Additionally, counter values are also predictable since the counter is a sequence number, either encoded by 16bit ($\leqslant$ v1.0.3) or 32bit (optional in $\leqslant$ v1.0.3, forced in v1.0.4/v1.1). After the counter resets (after an overflow or after a device reset in ABP-mode), the attacker can replay an old message that fits into a sliding window with a set up gap (default value of 16384). All future messages that are received with a lower counter value are discarded on the receiving device. When replaying single messages that max out the sliding window borders, this procedure is basically a DoS attack.

In agricultural applications, an attacker can just drop a small malicious battery-powered device in the coverage area of both the targeted ED and GW for executing the attack. As the attack is dramatically improved in the time requirement by a manual device reset (in $\leqslant$ v1.0.3), physical access to an ED makes this attack more applicable, but also more expensive in terms of manual work. Therefore, we see here danger for the most critical single devices, e.g., smart valves used for controlling water management. Such devices when under attack could be randomly manipulated in the water flow to obfuscate the attack.

Those attacks were addressed in LoRaWAN v1.1 due to the obligation of a persistent memory for counter storage and a re-join possibility to re-key the device during a running session. Nonetheless, it should be noted that re-keying is not possible when running in backward compatibility mode, making this attack a threat for a system relying on backward compatibility (Dönmez & Nigussie, 2018).

When discussing the attack impact, we classify it as none for confidentiality, as no data is leaked. The impact on integrity is classified as high, because serious harm is possible, e.g., by feeding incorrect data to an automated gate or a water pump. Although an attacker is limited in the ability to discern values due to encryption, the open location of the sensors and the ease of observing specific phenomena makes discerning important values easier than in other IoT domains. The impact on availability is low in our opinion, as it is possible to remove an ED by resetting the counter and replaying high counter value messages, but important data should most often be available from other sources due to the distributed nature of IoT systems in general.

Special Case: Fake Session Creation A fake session is possible between an attacker and an NS (Yang et al., 2018), as well as between an attacker and an ED (Dönmez & Nigussie, 2018). Both of those attacks exploit the weakness in `nonce` reuse and allow the attacker to proceed with a normal replay attack once the fake session is created. Both of those attacks are no longer possible in LoRaWAN v1.1 and only work in backward compatibility mode if the victim is the one running v1.0. Thus, a fake session on the ED is only possible if the ED is running v1.0.

Countermeasures Both types of replay attacks are only possible for LoRaWAN v1.0 (and v1.1 in backward compatibility mode). Using LoRaWAN v1.1 would, therefore, solve this issue. For LoRaWAN v1.0 deployments, the following countermeasures can be performed to reduce the risk of being attacked:

a) Prefer using OTAA. ABP uses static keys, and the counter will reset to 0 every time the device resets, which could be exploited by an attacker.

b) Yang (2017) advises protecting devices against physical access, as being able to reset the device manually can decrease the waiting period for an attacker attacking an ABP-activated device. Of course, in some use scenarios of agricultural IoT, physical protection is not possible to a sufficient degree.

c) In a backward compatibility scenario, if the NS is v1.1 with a v1.0 ED, the NS should be configured to discontinue communication with an OTAA activated v1.0 ED upon recognition of a frame counter saturation to force the node to initiate another activation, as it is the only available way of re-keying, as described by Dönmez and Nigussie (2018).

d) Another suggestion is discontinuing communication with an ABP-activated ED upon detecting a frame counter saturation. As re-keying is not possible, this approach results in additional costs as the ED needs to be replaced.

e) X. Wang et al. (2020) suggested a solution *SLoRa* as an ED authentication scheme, that leverages two physical layer features: Carrier Frequency Offset and spatial-temporal link signature. Based on the fingerprint-like transmission characteristics of each device, a new (malicious) ED could be detected at the GW side.

Join-Request Replay

When using OTAA for activation, join-request messages are unprotected against replay attacks before LoRaWAN v1.1. The NS only stores most recently used `DevNonce` values, as repetition is possible due to the pseudo-random character. This can be abused by the attacker by replaying previously captured join-request messages, while the ED attempts to connect to the NS.

In the beginning, the attacker installs a sniffing device in the target area, e.g., in the vicinity of a farmhouse, and proceeds to collect join-request messages from different EDs, aiming to acquire as many as possible. The second phase is about analyzing collected messages to determine EDs that send join-request messages frequently and regularly; those devices are the target of this attack. Additionally, the attacker stores the devices' expected join-request cycles, calculating the optimal time for an attack. Phase three starts when enough messages are collected, and the joining pattern of a given ED is figured out. Now, the attacker needs to wait for the usual device's join-time. Right before this moment, the attacker starts to replay the cached join-request messages. The NS attempts to connect to the attacker's device, as its message arrived first, discarding join-requests from the regular node. After a while, the timeout limit exceeds, and the NS drops the unconfirmed session. However, the attacker can replay the next cached join-request to restart the procedure until he runs out of cached messages (Dönmez & Nigussie, 2018; Na et al., 2017). This results in the ED being unable to participate in the network until all join messages have been used.

This attack is still possible when running in backward compatibility as a security context switch is not possible when one participating device is using LoRaWAN v1.0 (Na et al., 2017; Yang et al., 2018).

It is hard to exclude agricultural application areas from this attack scope, but this attack will be easily detectable, as it hinders complete ED from joining the network, and there are no ways known for obfuscation of this attack.

The attack has no impact on confidentiality or integrity; no data in the system is disclosed or modified. Furthermore, the attack has a low impact on availability, being severely limited by the number of messages an attacker has captured, which happens the attack duration, as well as affecting a single ED only.

Countermeasures against the Join-Message Vulnerability This vulnerability relies on insufficient replay protection for join-request messages in LoRaWAN v1.0 versions. As the attack is not possible in LoRaWAN v1.1, using this version would solve the problem. If the system requires the usage of LoRaWAN v1.0, we recommend the following security measures that can be applied to reduce the impact:

a) Avoiding clear patterns to server reboots and resetting devices at *random* times will make it impossible for the attacker to disconnect multiple devices at once, severely lowering the impact of the attack.

b) Resort to block-chains for EDs' authentication in real-time could eliminate the attack possibility and build trust among LoRaWAN EDs and NSs (Danish et al., 2020).

c) Modifying the join procedure to account for potential replays while keeping the existing packet structure; an exemplary method using two types of join-requests is presented by Kim and Song (2017).

9.5.3 *Traffic Analysis: Eavesdropping*

LoRaWAN implements channel confidentiality through AES in counter mode, where the block counter value is used as an input. During a counter reset, the key will remain in place, meaning that the block cipher will recreate the same key material. An attacker can exploit this behavior to decrypt messages, as described by Yang et al. (2018).

This attack is possible in LoRaWAN $\leqslant$ v1.0.3 due to the ability to reset the counter by restarting the device. In a second attack variant, the attacker exploits the lack of the `ForceRejoinReq` command, as the counter is resetting to 0 upon overflowing according to the specification (Dönmez & Nigussie, 2018). Despite the attack variant, the attacker has just to monitor and store messages, which can be done in the radio range of GW and ED, but does not require knowledge of the exact location of either.

Eavesdropping can be combined with a replay attack to allow the attacker to replay specific messages based on his needs and feed erroneous data to the backend.

This attack is especially applicable for getting deep insights into a farm's operations by eavesdropping the results of the sensor nodes, e.g., soil analysis sensors of arable farming businesses. In combination with the replay attack, this could be especially dangerous for modern food systems by introducing wrong data that manipulate calculations that determine the amount of applied fertilizer.

Considering the findings from the last paragraph, we classify the impact on confidentiality as low in the general case. However, as shown earlier, an attacker using background knowledge to target specific EDs could be able to obtain crucial business information, which in turn would raise the attacks impact to high. The attack itself has no impact on integrity or availability.

COUNTERMEASURES As Eavesdropping is only possible for LoRaWAN v1.0 (and LoRaWAN v1.1 in backward compatibility mode), using LoRaWAN 1.1 would solve this issue. In the case where the system has to contain LoRaWAN 1.0 components, the following countermeasures can be used to reduce the risk for an attack:

a) Prefer using OTAA. ABP should only be used in special circumstances, as resetting the ED is the easiest way to obtain messages from the same node with the same session keys and the same counter value, which are required to derive keys used (Yang et al., 2018). Physically protecting ABP nodes makes the attack much more difficult to perform as a counter overflow takes time to occur, and a considerable amount of messages with the same session key and counter value are required. This could be interesting for in-house sensors, like cattle monitoring. Especially actors (e.g., smart locks, valve controllers) should not rely on ABP.

b) When running in backward compatibility mode, implement a re-keying procedure without ways to reset the counter so the attacker can't perform an eavesdropping attack.

9.5.4 *Denial of Service: Radio Frequency Jamming*

Radio Frequency Jamming is one of the more general problems for IoT technologies. The adversary transmits a powerful radio signal in the proximity of the application devices, disrupting transmissions. In agricultural applications, this may be used to reduce or completely destroy the quality-of-service, applicable to all application areas of agricultural IoT. Motives could be the denunciation of a competing IoT-service provider or obtaining ransom money by criminals.

While such an attack is typically in need of dedicated hardware, Aras, Small, et al. (2017) as well as Perković and Siriščević (2020) have shown that it is possible to jam LoRaWAN using commercial (low-cost) off-the-shelf hardware. This poses a real threat for LoRaWAN networks as throughput can be decreased by up to 56 % (Martinez et al., 2019). The attack is possible for LoRaWAN v1.1 as well v1.0. We differentiate the following types of jamming attacks: *Triggered Jamming*, *Selective Jamming*, and *Wormhole Attack*.

a) *Triggered Jamming* can be used by the attacker to increase package loss in the network, in addition to providing a good basis for more sophisticated attacks like selective jamming. The technique is based on the functionality of LoRa radio

Table 9.3: Tabular listing of countermeasures, together with the scope of application, related (vulnerable) LoRaWAN versions and mitigated attacks. (v1.1* is v1.1 in backward compatibility mode)

Countermeasure	LoRaWAN Version			Scope			Mitigation for
	v1.0	v1.1*	v1.1	ED	GW	NS	
Traffic analysis	x	x	x			x	RF Jamming
Multiple GWs with overlapping coverage	x	x	x		x		RF Jamming ADR spoofing
Monitoring SNR values	x	x	x			x	ADR spoofing
Physical protection (EDs)	x	x	x	x			Physical attacks
Physical protection (GWs)	x	x	x		x		Class B attacks; ACK Spoofing ($\leqslant$ v1.0.3)
Keeping multiple unconfirmed messages per ED	x	x		x			Join-Request Replay
Ending session with OTAA when counter saturated and force re-keying	x	x		x		x	Replay Attack Eavesdropping
Avoiding ABP	x	x		x			Replay Attack; Eavesdropping ($\leqslant$ v1.0.3)
EDs resend mission critical messages	x			x			ACK Spoofing ($\leqslant$ v1.0.3)

modules to scan a certain channel to detect an ongoing transmission. Upon detection, the attacker can proceed with jamming.

b) *Selective Jamming* requires a low-level configuration to allow reading a message while it is being received. During the attack, the radio module starts in receiver mode and waits for a LoRa modulated signal. Once a message is detected and its physical header is proven correct, the module reads the FIFO until it reaches the device address. If the message triggers the jamming policy, the module switches to jamming mode. Once jamming is done, the module switches back to receiving mode again (Aras, Ramachandran, et al., 2017). As this attack could be used to manipulate messages of single devices, there is a danger for the most critical EDs, e.g., smart valves used for controlling water management. Such devices, when under attack, could be randomly manipulated to obfuscate the attack.

c) A special case is the combination of selective jamming and a replay attack to perform a so-called *Wormhole Attack*. Two types of devices are required in this case, a *sniffer* capturing the packet and a *jammer* signaling the successful capture. The captured message can then be replayed at a later date since there is no time-related information in LoRaWAN messages. The attack is limited by the jammer's reaction time, which needs to be lower than the packet's airtime minus the airtime of the first five bytes of the device address; otherwise, the jammer will not have time to act before the packet reaches the gateway. This attack was addressed in v1.1 but is still possible in v1.0 versions and when running in backward compatibility mode (Aras, Ramachandran, et al., 2017; Chacko & Job, 2018). We do not see specific attack scenarios for this attack in agricultural IoT applications.

The attack has no impact on confidentiality or integrity. However, the impact on availability is high, as the attacker is able to disconnect multiple EDs and is not limited by external factors like stored messages or specific timings.

COUNTERMEASURES Jamming is limited by the number of nearby GWs, packet airtime, and channel hopping. Those limitations can be used to implement the following countermeasures:

a) Creating a dense LoRa network with overlapping GW coverage makes a jamming attack much more difficult to perform. In this way, an attacker needs to make sure the message of an ED is not received by any of the different located GWs, as the success of the attack depends on physical proximity to the GW (Aras, Small, et al., 2017; Hessel et al., 2020). In case any GW receives the message of an ED, the message will be forwarded to the NS, which de-duplicates the message if multiple GW have received the same message. Of course, the feasibility to set up multiple GWs in distinct locations depends on the present circumstances on the farm. Another countermeasure is to maximize the use of channel hopping (usually used to reduce packet collision), which makes the jammer need to become more complex and expensive as it must listen to more channels at once.

b) In the case of wormhole attacks, the signal frequency and the packet size can be lowered to reduce air-time and beat the jammers' reaction time (Aras, Small, et al., 2017). It should be noted that a lowered signal frequency results in lower reliability and a lowered communication range.

Mikhaylov et al. (2019) noted that network adaptation, e.g., switching to a higher signal frequency or transmitting power, can be abused by an attacker to drastically increase energy consumption, thereby shortening the remaining device lifetime. As of now, there is no known solution. Hence, it should be considered when deploying IoT devices.

d) A jamming attack may be detected by performing a traffic analysis at the GW or at the NS level. When there are regular transmission rates known, abnormal message quotas could be detected and trigger an alarm or a network adaption (Aras, Small, et al., 2017).

9.5.5 *Spoofing Attacks*

ACK Spoofing

The attack exploits the lack of association between acknowledgment and message. The frame counter of the ACK is the sequential number of all downlink messages. Therefore, a captured and delayed ACK can be used to acknowledge another unrelated message without its arrival at the backend provider (Yang et al., 2018).

An attacker will observe the network waiting for the NS to acknowledge any message from the ED. Afterward, the attacker will proceed to selectively jam the ACK message, capturing it in the process. Now the attacker can abuse the lack of association to be able to acknowledge any next single uplink message without its arrival at the backend by replaying the cached ACK. The ED then believes the message arrived and will not attempt to resend potentially mission-critical data. This attack can be used to prevent the communication of a status change of an actor, like a smart lock of a cattle farm, or water valve of an irrigation system.

This attack is possible in LoRaWAN v1.0 versions and was addressed in v1.1 by the changes to MIC calculation. However, this attack is still possible when running in backward compatibility mode (Dönmez & Nigussie, 2018; Yang et al., 2018).

The attack reveals no information, and therefore it has no impact on confidentiality. The impact on integrity is low, as during modification of the data, the attacker is limited to single messages and hindered by encryption. The impact on availability is low as well; some messages are gobbled by the flip and unusable to the system. However, in an agricultural IoT system, it should be easy to recreate those missing data pieces.

COUNTERMEASURES Using LoRaWAN v1.1 would solve the issue. If the system requires LoRaWAN v1.0, the following countermeasures can be performed to reduce the risk of being attacked:

a) Protecting access to GWs as the attack requires the adversary to be in control of the GW. A common method to attack a LoRaWAN gateway is using physical access (Yang et al., 2018).

b) Confirmed messages should be treated carefully, and EDs should be programmed to resend critical data or requests. Even if the message is acknowledged, the *critical* state remains.

ADR Spoofing

This attack forces an ED to use insufficient transmission power and data rate to reach a GW by manipulating ADR control messages, as described by Hessel et al. (2020). The intention of LoRaWAN's ADR function is to find an appropriate data rate as a compromise of coverage and transmission time. By selective forwarding messages with a wormhole setup, an attacker is able to capture and jam the ADR initiating message, which was sent by an ED. This captured message can be manipulated in its metadata to fake the signal strength indicators, which are evaluated on the NS to calculate appropriate transmission parameters. By transmitting the ADR answer message back to the ED, the ED applies the transmission parameters, which are insufficient to reach the GW. As a result, the ED's coverage is too low to be able to communicate directly with the GW.

This attack has no impact on confidentiality or integrity because it does not leak or modify any data. However, the attack has a high impact on availability because it is possible to permanently disconnect EDs from the system, which in turn severely limits an agricultural IoT setup.

COUNTERMEASURES This attack is also possible with LoRaWAN v1.1. Abandoning the ADR feature and manual setup of the network parameter would prevent this attack. Mitigating this attack could be achieved by monitoring the SNR values and averaging the SNR at the NS to prevent abrupt changes (Hessel et al., 2020).

9.5.6 *Other Attacks Found in Literature*

There are additional attacks linked to LoRaWAN that can be found in the literature. The following attacks are presented for completeness, but we did not develop security recommendations for those attacks as they are either not possible to our knowledge or unspecific for LoRa/LoRaWAN devices. Nevertheless, developers have to also be aware of those vulnerabilities when developing any IoT application, regardless of the chosen technology.

a) *Man-in-the-Middle (MitM) / Bit Flipping.* LoRaWAN messages are encrypted and equipped with a MIC. However, these two layers of security (encryption and integrity check) are handled at different locations inside a message frame: The payload encryption is handled by the AS, while the MIC is checked and terminated by the infrastructure provider. *"This means that in between the infrastructure operator's network server and the IoT solution provider's application server, the content cannot be checked for integrity and authenticity"*, as stated by Yang et al.Yang et al., 2018. An attacker can attempt to intercept anywhere between the NS and the AS (J. Lee et al., 2017; Skorpil et al., 2018; Thomas et al., 2020). This can be done via different approaches, ranging from routing-based ones, like BGP-prefix hijacking or IP source routing to physical and link-layer based ones, like a compromised device on the path. While normal AES is resistant to bit flipping due to the avalanche-effect, LoRaWAN is not using authenticated encryption and therefore terminates the integrity check too early. This allows the attacker to potentially modify the content of sensor readings and abuse the ciphertext, which affects the exact bit position in the plain text in a predictable manner (Yang et al., 2018).

b) *Side Channel.* J. Xu et al. (2019) have demonstrated that based on electromagnetic radiation (EMR) of an ED and the knowledge about the communication mechanisms of the LoRaWAN protocol, the full `AppSKey` could be recovered with less than 100 transmissions in the ABP mode, utilizing neuronal networks (deep learning). To tackle EMR based attacks electromagnetic shielding like a Faraday cage around the computational hardware elements could be applied.

c) *Class B Device Attacks.* There are three classes of LoRaWAN EDs described by the standard: class A, B, and C. While all EDs can send messages to a GW at any time, the class determines when an ED can receive messages from a gateway. Class A nodes are able to receive messages right after sending a message. Class C ("Continuous") nodes never sleep and always listen to incoming messages. Class B devices aim to balance power consumption with the possibility to receive messages periodically. However, they have a vulnerability: To open receive windows at fixed times, gateways need to broadcast a beacon synchronously to provide a time reference. As beacons messages contain GPS coordinates of the sending GW in plaintext, its position can be easily eavesdropped or spoofed when combining the attack with triggered jamming. Another class B attack is a *rogue beacon* that could be set up by the attacker and used to send random or extreme wakeup times to class B EDs. This leads to a distortion of receiving operations due to the device waking up at a different time than expected by a legitimate GW. Hessel et al. (2020) use this behavior for a *beacon spoofing* attack, which could result in a DoS.

d) *Network Flooding.* When attempting a network traffic flood, the adversary captures the EDs and misuse those to perform an attack against the rest of the network. Such an attack can degrade the network by flooding it with packages (Butun et al., 2018a).

e) *Network Traffic Analysis.* A network traffic analysis is a passive attack where the attacker sets up a rogue GW and uses the received packages to deduce some knowledge about the data being transmitted or key material used (Butun et al., 2018a).

f) *Self-Replay Attack.* To our knowledge, a self-replay attack is not possible but was referenced in another paper (Butun et al., 2018a). To our understanding, this was a misconception or mixing of properties of LoRaWAN and another LPWAN technology, *SigFox*. The latter one has a communication quota with a maximum number of messages per day.

9.6 Discussion

Multiple papers have investigated security aspects of LoRaWAN and have shown that, while LoRaWAN is a promising technology, it bears multiple issues independent of the application domain. The works by Yang et al. (2018) and Butun et al. (2018a) are probably the most prominent works in this category, while the work of Noura et al. Noura et al., 2020 is the most recent survey, that covers multiple vulnerabilities, we have detected in our literature review. The result of our literature study shows that the newer the LoRaWAN 1.0 version, the fewer attacks are known. But also the newest 1.0 release (v1.0.4) has more known vulnerabilities compared to v1.1.

When looking at the attacks, some of the more dangerous vulnerabilities require or benefit from physical access to an ED, which is especially for agricultural IoT systems a real threat – in contrast to many other IoT use cases that have EDs deployed in physically protected environments, like buildings. When talking about attack complexity, we can see that almost all attacks exhibit a low complexity. For the most part, attacks can be performed with of-the-shelf hardware and rely on well-known and documented attack patterns; other attacks are easy to perform due to the ease of physical access inherent to the agricultural IoT domain. Another important aspect of IoT in agriculture is that none of the attacks we discovered require any kind of system privileges or legitimate user interaction. The scope of attacks varies while some attacks only affect a specific ED, others can harm the entire IoT system, e.g., by feeding incorrect or potentially malicious data into an irrigation controlling system.

Unfortunately, multiple commercial EDs that are advertised for the agricultural sector like electric valves, soil moisture sensors, or general-purpose EDs, which could be equipped with different sensors or actors, are still delivered with LoRaWAN v1.0.2 or v1.0.3. We did not cover hints about possible firmware upgrades for the inspected products. Together with the promise to have a battery runtime of up to +10 years, this situation is critical from an IT security perspective.

This paper is, to our knowledge, the first work that uses a systematic literature review to provide a full list of LoRaWAN vulnerabilities for the multiple versions up to v1.0.4 and gives security recommendations as countermeasures that do not require a change on the LoRaWAN standard itself. The tabular listing

(Table 9.3) of countermeasures should help developers to minimize risks and improve IoT security.

Limitations The presented attacks and security recommendations are (only) based on documents of existing LoRaWAN specifications and results stemming from the performed literature review. However, most of the attacks included in this document have been practically proven by their corresponding paper. We analyzed the examplary wide area IoT part through extensive research in the domain of agriculture, resulting in five IoT specifics for wide area applications (see Section 9.3.2). This allowed us to investigate the attacks considering domain-specific constraints, e.g., physical access-based attacks are a greater threat for wide area applications than any other IoT domain, and to provide domain-specific recommendations when possible. Since our work is of theoretical nature, a practical analysis should follow in the future.

9.7 Conclusion

This work inspects the state of security of the communication technology LoRaWAN, that is especially useful for wide area IoT applications, e.g., smart agriculture. After giving a short summary into LoRaWAN details, we compile some properties of wide area IoT applications from a security perspective. Especially unsupervised end devices increase the possible attack surface a lot. As the main contribution, we investigated on the research questions, (1) "What are the known vulnerabilities of LoRaWAN?", and (2) "Which mitigations against the known vulnerabilities should be considered when developing a LoRaWAN-based IoT solution?", based on results from a systematic literatur review.

This paper is intended to help both researchers and developers in the field of wide area IoT due to its completeness and the nature of our provided recommendations. To our knowledge, it is the first work that provides a systematic literature review of LoRaWAN security issues and mitigations. Another unique point of this paper is the novel, full list of known LoRaWAN attacks regarding v1.0, v1.1, and backward compatibility mode.

Research has shown that while many LoRaWAN vulnerabilities have been addressed with v1.1, some important issues still remain, e.g., RF jamming, physical attacks, and spoofing attacks. With our proposed mitigation options, the risks to be vulnerable to attacks could be reduced.

Future work could include performing a practical evaluation of our findings concerning social responsibility, which are mostly based on theoretical considerations. In this context, we see a deeper investigation of physical attacks and the development of related mitigation strategies to be of prime importance, especially in the domain of agricultural IoT.

10

GEOBOX: DESIGN AND EVALUATION OF A TOOL FOR RESILIENT AND DECENTRALIZED DATA MANAGEMENT IN AGRICULTURE

ABSTRACT Farm Management Information Systems (FMIS) are an important core component of modern farming companies as they allow, e.g., to document activities, create fertilization plans, and feed digital equipment with required data. Since the entire agricultural sector is an essential component of food production, high standards of resilience should be established in the involved companies. Accordingly, the used software should also be designed with high standards on reliability and crisis capability. Based on a literature review, we found that software for farmers with certain resilience needs is lacking. Thus, we designed and evaluated a new FMIS concept with the user-centered design method. By conducting focus groups (two rounds, total N=57) in 2017 and 2019, we raised specific front-end and back-end requirements of farmers. Based on the requirements, we developed our concept for both front- and back-end in terms of a decentralized and offline-working FMIS. Through the evaluation with practitioners (N=16) of the implemented concept, we derived findings and implications, highlighting the need for privacy, stability, and offline-capability, as well as the UI-requirement to be supportive, e.g., with easy to understand icons and terms.

ORIGINAL PUBLICATION This is an Accepted Manuscript of an article published by Taylor & Francis in Behavior & Information Technology on 10th of March 2023, available at: https://doi.org/10.1080/0144929X.2023.2185747. *Kuntke, F., Kaufhold, M.-A., Linsner, S., & Reuter, C. (2023). GeoBox: Design and Evaluation of a Tool for Resilient and Decentralized Data Management in Agriculture.* Behaviour & Information Technology. *https://doi.org/10.1080/0144929X.2023.2185747*

NOTE Supplementary material of the qualitative and quantitative studies can be found in Appendix A.1.3.

ACKNOWLEDGMENTS This work was supported by funds of the German Government's Special Purpose Fund held at Landwirtschaftliche Rentenbank in the projects Geobox-II and AgriRegio, and by the German Federal Ministry for Education and Research (BMBF) in the project HyServ (01IS17030B). We would also like to thank our project partners as well as Elmar von Radziewski and Roxanne Keller for their valuable support during the first pre-study. Furthermore, parts of the second pre-study have already been published in two

different papers, but were analyzed with a different scope focusing privacy (Linsner et al., 2021) and resilience (Kuntke, Linsner, et al., 2022).

10.1 Introduction

In many countries, agriculture is considered part of the critical infrastructure to safeguard food production and security. Recently, the term *agriculture 4.0* was coined to discuss and research the use of ICT to improve agricultural processes Liu et al., 2021. For instance, precision farming is expected to offer monetary advantages, allow the precise application of resources, and improve the traceability of production. A frequently used term is that of FMIS, which can be defined as "a planned system for the collecting, processing, storing and disseminating of data in the form of information needed to carry out the operations functions of the farm" Sørensen et al., 2010. The most prominent functionalities of FMIS comprise field operation management, reporting, and finance Fountas et al., 2015. However, several barriers interfere with the successful adoption and use of FMIS. For instance, the farmers' reliance on cloud-based, third-party FMIS raises questions about data ownership and, consequently, adequate regulatory frameworks Atik, 2022. Other issues relate to privacy, security, and data availability in particular, should centralized infrastructures fail Wolfert et al., 2017.

Failing infrastructures is a serious challenge for the *resilience* of a farm and, if large-scale disasters occur, for the critical sector of agriculture as a whole. Developing resilience, which means to "successfully deal with uncertainty and dynamic environments" Slijper et al., 2022 is therefore crucial for the agricultural sector. Furthermore, research indicates a low adoption rate of FMIS in small and medium-sized farms and enterprisess (SMEs) due to lacking awareness (of potentials) (Bucci et al., 2018) and unclear economic advantages (Schulze Schwering & Lemken, 2020). Yet, there is a lack of user-centered evaluation studies examining the perceived usefulness of functionality, usability, and user experience of FMIS in general. There is an even greater lack when it comes to resilience-enhancing concepts, such as decentralized systems. While such concepts have already found significant consideration in the development of conceptual frameworks for digital farming systems Bökle et al., 2022; Kuntke et al., 2020, so far, prospective users have not been involved in design and evaluation studies of concrete FMIS adhering to these principles. Other empirical design and evaluation studies focus on different agricultural technologies, such as decision support systems Parker and Sinclair, 2001 and smartphone apps Bonke et al., 2018; Kenny and Regan, 2021; Michels, Bonke, and Musshoff, 2020. The dependence of farmers' business operations on software is increasing and more crises are expected to cause ICT infrastructures to collapse in some regions (e.g., following the 2021 floods in Europe). We therefore see a need for further research into appropriate information systems that implement crisis-ready features for end users. Thus, this paper seeks to answer the following RQ:

> **How should an architecture and user interface for decentralized data management be designed to improve farm resilience and fit the farmers' requirements in agriculture?**

By answering this RQ, the paper makes several contributions to the discipline of human-computer interaction Wobbrock and Kientz, 2016. First, Section 10.2 provides a literature review on digitalization and its impact on resilience in agriculture. Then, Section 10.3 and Section 10.4 provide *empirical contributions* by the user-centered requirements elicitation for the architecture (R1-R5) and interface (R6-R11). Our findings highlight that crisis capability is considered an essential feature, a strong desire for customization, the importance of supporting multiple end-user devices, as well as UI requirements for specific groups of farmers. The concept and implementation of the FarmBox tool for resilient data management are the *artifact contribution* described in Section 10.5. Details of the scenario-based evaluation are outlined in Section 10.6, and the resulting additional *empirical contributions* are presented in Section 10.7. The subsequent *theoretical implications* on decentralized and resilient data management are discussed in Section 10.8. Finally, a concise conclusion is given in Section 10.9, which also discusses limitations and avenues for future research.

10.2 Literature Review: Digitalization and Resilience in Agriculture

Our literature review introduces the foundations of digitalization and resilience in agriculture, discussing both potential and current issues. Furthermore, a short overview of technologies for agriculture is given before outlining a research gap.

10.2.1 *Digitalization in Agriculture: Higher Precision and other Advantages*

Digitalization through the incorporation of new technologies in agriculture has become a major issue. Liu et al. (2021) recap the history of the *agricultural revolutions* up to the current trend of *agriculture 4.0*: Agriculture 1.0 is described as manual work from ancient times up to the end of the 19th century. The usage of agricultural machinery for mechanized agriculture between 1784 and 1870 leads to higher food production and less manual labors, and is referred to as Agriculture 2.0. Starting with the third agricultural revolution, IT systems entered the food-production processes. In light of the current fourth agricultural revolution, data processing is even more crucial to allow for more precise processes all around the agri-food production and agri-food supply chain management. In this context, smart farming technologies in particular, i.e., networked and semi-autonomously interacting devices that can perceive and communicate their individual status as well as their environmental context in real time thanks to sensors Fleisch and Thiesse, 2007; Porter and Heppelmann, 2014, are becoming increasingly important. In the survey of Schukat and Heise (2021b), 65.8% of the participating German farmers (n=523) reported to utilize smart products in 2020.

The precise processing made possible through digitalization offers several benefits: First of all, digitalized farm machines and equipment could offer *monetary advantages*. Smart farming approaches promise an increase in efficiency and effectiveness Y. Gu and Jing, 2011; Wolfert et al., 2017 by evaluating the recorded data and calculating a more precise and area-specific application of seeds, fertilizers, and other resources. By utilizing these advantages, time and money can be saved. The same applies to smartphone apps that offer decision support to farmers. In 2019, Michels, Bonke, and Musshoff (2020) asked German farmers in an online survey about smartphone apps in crop protection. Among the most useful considered features of crop protection apps by the 198 respondents are weather information (77%), pest scouting (75%), and infestation forecast (64%), even though actual app usage is often less widespread Michels, Bonke, and Musshoff, 2020. Hence, there is still potential for improvement, especially considering that another 2019 survey found that 95% of farmers use a smartphone Michels and Musshoff, 2021. The number of agricultural apps used is affected by individual factors such as age and education Michels and Mußhoff, 2020. Elijah et al. (2018) see benefits of the IoT also in a resource reduction for feeding a growing population. Secondly, the precise application of resources (e.g., fertilizer) and specific calculations (e.g., nutrient requirements) could *reduce environmental pollution and enhance animal welfare*. Pinaki and Tewari (2010) show that there is a huge potential for an environmentally friendly, sustainable agriculture by utilizing precision farming technologies. In general, the use of ICT might reduce CO_2 emissions in agriculture if potential rebound effects are addressed properly Buhleier et al., 2022. A metastudy on energy use in agriculture is provided by Pelletier et al. (2011). The authors compare different approaches and sub-domains, such as livestock or crop production, and predict an increasing energy demand for agriculture due to population growth and changing consumption patterns. Similar results are found by Finger et al. (2019). With regard to livestock farming, Schukat and Heise (2021a) argue that smart farming technologies have the potential to enhance animal welfare. Thirdly, *traceability is improved*. Retailers could offer their customers information about the origin of their crops, and food scandals could be fought more efficiently. Kamath (2018) points out that better traceability may simplify countermeasures during food contamination scandals. The author refers to two food scandals in the USA (E. coli outbreak in 2006) and in China (pork mislabeling debacle in 2011).

All the named advantages require the incorporated tools and equipment to have access to data about the real-world conditions, like soil moisture, weather, plant condition, and more. Thus, FMIS seek to collect, process, store, and disseminate all kinds of farming-related data to carry out operational functions of farms Sørensen et al., 2010. These agricultural data include farm activities, such as fuel consumption or routes driven, the documentations and reports, but also planning for future operational considerations. In an analysis of 141 commercial FMIS, Fountas et al. (2015) identified eleven distinct functions and grouped FMIS into four clusters, i.e., basic, sales-oriented, site-specific, and complete systems. Their analysis reveals that field operation management (89%), reporting (81%), and finance (64%) are the most common functions. Most FMIS are PC-based solutions (75%); only some supported mobile (16%) or web-based (15%) applications.

The review of Birner et al. (2021) investigates the role of different actors in digital farming, such as suppliers, software companies and differently sized farms. One of the authors' conclusion is that there is concern about a potential increase in the market power of large companies through digital farming tools. As a result, smaller companies would be less competitive. Unfortunately, we have not found reliable statements about the concrete benefit of using digital technologies for farming. Most works, like the ones of Ammann et al. (2022), Annosi et al. (2019), Chandra and Collis (2021), Gautam et al. (2021), Liu et al. (2021), OECD (2019), Schukat and Heise (2021a), and Zscheischler et al. (2022) describe the potential benefits of using FMIS or other digital tools, without the proof of society-wide positive impacts (Lioutas et al., 2021) or considerations regarding needed investments of farmers in terms of finances and time to build up knowledge and expertise for using the tools. First and foremost, most tech-positive works calls for greater dissemination so that the promised environmental and economic advances are more evident in practice. Interviews with 38 stakeholders of agriculture in the south-west of Germany conducted by Pfaff et al. (2022) support the assumption that the financial hurdles in small-structured regions are an issue for higher adoption rates. As a result, it would be difficult for these very companies to benefit from tools from the field of smart farming.

10.2.2 *Open Challenges: Increasing Adoption Rate and Making Systems Resilient*

The process of digitalization in agriculture has been investigated by researchers for several years now. Liu et al. (2021) detected some open challenges of multiple research areas to complete the fourth agricultural revolution. When it comes to Big Data, important aspects are the standardization of file formats for an exchange between software products and social issues, i.e., privacy and the agricultural stakeholders' understanding of technology. Additionally, complexities in the creation, collection, maintenance, and dissemination of big data with many precision agricultural systems impair the effective provision of actionable and valuable decision support for farmers, thus impeding their further adoption Mitchell et al., 2018. Artificial intelligence (AI) has the potential to improve the management of big data and to simplify these processes even in safety-critical situations Kaufhold, 2021. However, farmers' self-confidence in their abilities to use AI systems and personal attitudes towards AI influence the acceptance of such systems Mohr and Kühl, 2021.

A study with Iranian agricultural specialists found that, among others, both perceived *triability*, i.e., the possibility of testing technologies in a small area, and *observability*, i.e., the extent to which the results of technologies can be observed, have a positive impact on the intention to use precision agriculture technologies (Kurosh & Saeid, 2010). While various other quantitative studies have employed a variety of theoretical models to explore factors that influence the intention to adopt agricultural technology, the research community has attributed particular attention to individual factors, whereas only few models have recognized the significance of environmental and social factors, as well as their interrelation with individual factors Carli et al., 2017. The study by Li et al., 2020 is an example of a more comprehensive approach. It found that the perceived relevance of technology features to Chinese farmers' requirements, the perceived risks and benefits of technology adoption, and the perceived presence of facilitating conditions, such as knowledge, resources, and access to consultant services, have a positive impact on the intent to adopt precision agriculture technologies. Similarly, a recent meta-analysis of 23 publications in this field points to an interplay of individual and social factors, as it found that on the one hand the perceived profitability of precision agriculture and individual computer use, and on the other hand the commitment of consultants have a positive effect on technology adoption Tey and Brindal, 2022. Unmanned aerial vehicles (UAVs) and autonomous field robots (AFRs), representing some of the latest technological innovations in agriculture Michels et al., 2021; Rübcke von Veltheim and Heise, 2021, are also of interest for understanding technology adoption. Studies found that Chinese farmers' intention to adopt UAVs is positively related to both individual factors Zheng et al., 2019, and environmental and social factors, such as cultivated land area, presence of village cadres within the family and the number of borrowing channels for money Wachenheim et al., 2021. The same applies to the factors influencing the actual adoption of UAVs by German farmers Michels, von Hobe, and Musshoff, 2020. Michels et al. (2021) argue that the communication of UAVs' benefits and a tailored demonstration of drones to farmers may change farmers' perceptions and beliefs, thus enhancing the intention to adopt such systems. Rübcke von Veltheim and Heise (2021) formulate similar advice regarding AFRs and encourage farmers' involvement in the design process.

In the context of this study, previous research focusing on the challenges and prerequisites of the adoption of FMIS is of particular relevance. A survey with 184 participants from Denmark, Finland, Germany, and Greece in 2011 focused on potential benefits for introducing labor-saving FMIS in terms of budgeting procedures, field planning, and paperwork dealing with subsidy applications and public authorities Lawson et al., 2011. But a majority of the participants were unsure about the benefits of new technology. Particularly for the results of the German participants, the authors see the large amount of time needed to get used to the technology as the major problem. Additionally, smaller farms did not have enough labor capacity, nor the necessary time to concentrate on precision agriculture compared to bigger farms. A positive relationship between farm size and the adoption of precision agricultural enabling technologies was also found for Switzerland Groher et al., 2020 and with regard to Germany Gandorfer et al., 2017. Linsner et al. (2021) confirmed these findings in 2021, stating that privacy is an upcoming issue in the adoption of FMIS. The study by Paulus et al. (2022) shows that the adoption rate of smart farming tools is higher among full-time farmers. The authors call for further research into the specific digital technology needs of part-time farmers to provide this target group with easier access to smart farming tools.

Similarly, Schukat and Heise (2021a, 2021b) note that ambiguities regarding data sovereignty and security may be an inhibiting factor for the adoption of smart farming systems, as they affect farmers' trust. Atik (2022) thus recommends a holistic approach to issues of agricultural data ownership, involving both the design of legal regulations and of infrastructures.

Another important issue is the demand for internet connectivity. The work of Aceto et al. (2018) shows how fragile the internet itself is. They propose a taxonomy for internet outages and provide a selection of scientifically proven examples of concrete internet outages with impacts ranging from regional to global; each of the 15 examples is referenced by at least one scientific analysis. Obviously, any internet outage could suppress the use of applications that rely on an internet connection, e.g., cloud-only services, and there are typically no precautions for such ICT breakdowns (Kuntke, Linsner, et al., 2022). Apart from disruptions, insufficient broadband internet availability in rural areas is a major barrier to the use of agricultural information technologies Kenny and Regan, 2021. In order to meet the farmers' demands, digital links between the increasing number of IoT devices inside the farms and farmlands provide a reliable way of digital communication. Besides mobile ad-hoc networks (MANETs) for local communication Reuter et al., 2017, modern and far-reaching network technologies such as LoRaWAN (Davcev et al., 2018) can connect sensors within the agricultural areas even over long distances with little technical effort (Chen et al., 2016; Ojha et al., 2015). Furthermore, Kalle et al. (2019) show how different network technologies can be combined to enhance resilience during crises with (partial) infrastructure disruptions. The analysis of wireless sensor networks for precision agriculture by Jawad et al. (2017) shows that current approaches typically propagate an internet connection to cloud services to analyze the sensor data and to enable later access via client computing devices, such as tablets. But at the same time, fundamental technologies like cloud services have proven to be vulnerable in case of a specific cloud-service breakdown or a failing internet connection. Unfortunately, digital infrastructure in Germany is characterized by the digital divide, which means that rural areas have less access to 4G networks (73.5 %) than urban areas (82.2 %) (Rizzato, 2019).

By inspecting the data from the agricultural structure survey 2020 regarding agricultural holdings and utilized agricultural area by size Statistisches Bundesamt (Destatis), 2021c, we see that most (about 85.49 %) holdings in Germany do not exceed 100 ha, and there are about 3.6 worker per farm (Statistisches Bundesamt (Destatis), 2021a). In accordance with the EU Commission's limit for medium enterprises (Commission, 2015), those holdings can be seen as SMEs (small-size: less than 50 employees). SMEs, in general, are considered to be highly vulnerable to impacts from disruptions, such as the effects of increasingly extreme weather (Wedawatta et al., 2010). Despite their high vulnerability, especially SMEs seem to lack adequate strategies to prevent interruptions and to quickly return to normal continuity of their operations. Reasons identified for this are high standards for business continuity, risk and security management that SMEs cannot easily adopt Kaufhold et al., 2018. Hence, experts call for simplified concepts (Reuter, 2015; Thiel et al., 2010). Pipek and Wulf (2009) coin the notion of "infrastructuring" and highlight the importance of understanding users' activities for improving IT infrastructures. Since triggers of IT infrastructure perturbations can remain simple even in complex or complicated use situations, the authors suggest a frequent reflection on available strategies to handle such perturbations. Furthermore, research indicates that agricultural software solutions must be tailorable to (changing) local regulatory policies and legal frameworks Elijah et al., 2018; and user interfaces as well as information visualization should be simple in order to be usable for all farmers Michels and Mußhoff, 2020.

10.2.3 *Research Gap: Decentralized Farm Management Based on User Centered Design*

Based on our literature review, we identified two central research gaps. First, the *need for research on decentralized FMIS* became apparent. With the emergence of big data analytics, cloud computing, and IoT, Wolfert et al. (2017) envision two extreme scenarios, i.e., "closed, proprietary systems in which the farmer is part of a highly integrated food supply chain" or "open, collaborative systems in which the farmer and every other stakeholder in the chain network is flexible in choosing business partners". Looking at the first scenario, the reliance on cloud-based, third-party FMIS raises not only issues concerning data ownership, privacy, and security, but also regarding data availability if centralized infrastructures fail. For this reason, the integration of decentralized communication infrastructure – the second scenario – seems promising to increase resilience in crises Elijah et al., 2018, as well to increase farmers' acceptance (Linsner et al., 2021). There is a large body of literature comprising conceptual models Sørensen et al., 2010, software architectures Nikkilä et al., 2010, infrastructures Nikander et al., 2015, and comparisons of existing FMIS Fountas et al., 2015. But none of those related works investigate decentralized software systems for agriculture, nor make suggestions for the development of resilience enhancing software systems.

Second, the review revealed a *need for the analysis of farmers' demands and involvement in the design process*. Involving users in design has been shown to lead to developing more usable satisfying designs as well as to establishing new technologies and innovation (Cajander et al., 2021; Shin et al., 2017). Yet, only a small number of studies focuses on such designs in the agricultural environment, like the ones by Bonke et al. (2018), Kenny and Regan (2021), Michels, Bonke, and Musshoff (2020), and Parker and Sinclair (2001). The main objective in a user-centered design processes is to involve end-users in the computerized design process (Wallach & Scholz, 2012). The ways in which users participate vary: They may be consulted about their needs and participate in usability testing (more passive role of users) or participate actively throughout the design process as partners in the design. User-centered design has been shown to lead to developing more usable satisfying designs as well as to establishing new technologies and innovation (Cajander et al., 2021; Shin et al., 2017). Therefore, it was the preferred method for the design process of the FarmBox software, which is explained in the following Section 10.3 starting with the requirements engineering.

10.3 Empirical Study: Focus Groups to Derive Requirements for Architecture and Interface Design

We conducted two rounds of focus groups in 2017 and 2019 to derive requirements for the design of a novel tool for decentralized data management and resilient regional networking. This section presents the study design, participants, analysis, and a summary of results, outlining design requirements. Some results from the second round of focus groups have already been published in scientific journals (Kuntke, Linsner, et al., 2022; Linsner et al., 2021); however, the data were analyzed with a different scope, i.e., not for the requirements elicitation.

10.3.1 *Study Design*

We decided to interview agricultural practitioners in focus groups Lazar et al., 2017; Morgan, 1997 because this gave the interviewees the opportunity to discuss with each other. In our case, these discussions brought up new aspects that might have gone undetected in individual interviews. All focus groups were conducted by two researchers in order to provide inter-subjective comprehensibility (Jenner et al., 2004). The entire process containing the creation of an interview guideline, recruitment, conduction of the focus groups, and data analysis and storage followed the guidelines of the ethical commission of the Technical University of Darmstadt university. With regard to the limited time available for interviews, we decided to outsource some background information into a survey in order to give more space for discussion in the focus groups. The survey was filled out before the focus groups took place and contained some general information about the branches they work in, their roles, and their experience with digital tools. We conducted two rounds of focus groups.

In the first round, we invited practitioners in 2017 to discuss the potentials for technology support. The participants were divided into four focus groups; each group consisted of three to six participants, and each session took about one hour. Based on this, we derived *requirements for the design of the envisioned interface* of the novel tool. In the second round, we asked practitioners about their understanding of digitalization in 2019, including positive and negative aspects, fears, and questions regarding privacy- and data ownership. The participants were invited to twelve one-hour focus groups, whereof each session consisted of three to six participants. The output of the focus groups of the second round was analyzed to identify *requirements for the envisioned architecture*. The used session guidelines of both rounds started with a short welcome and introduction, conveying the goals of the focus groups, and asking for approval to record the session. During the focus groups, participants were asked to share their experience with agricultural technologies and to discuss possibilities for future improvement.

10.3.2 *Participants*

Our participants were recruited in the context of public-funded research projects called HyServ Bernardi et al., 2019 and Geobox-II Kuntke et al., 2020, which comprises partners from the private sector, federal institutions, and associations for farmers. We recruited most of the participants at a federal advanced training institution for agriculture, which offers different degrees for farmers with practical experience. The clients and members of the project were invited to our focus groups for requirements elicitation. Everyone participated voluntarily, and no compensation was paid. Each participant was informed about the aims and topics of the study via informed consent, which was signed by each person. In total, 67 agricultural practitioners participated in two rounds of our focus groups.

The first round involved 15 practitioners (2 female, 13 male), which were organized into four focus group sessions: The first focus group was composed primarily of water conservation advisors that had little to no experience with FMIS. Group two had a mixed composition: one person was a teacher and consultant for viticulture, one participant was a participant for electronic area applications, and one participant worked first as a farmer in viticulture and then in a machinery ring (association of local farmers) in the field of fertilization technology. The third group consisted of three farmers, two of whom already had experience with FMIS. Finally, the fourth group consisted of a technical instructor for viticulture and plant protection, a vintner and member of the board of directors of the machinery ring, as well as a vintner's wage worker. The strong role of vintners was not forced, but resulted from the recruitment of the focus groups in an area in Germany that has a comparatively large number of viticultural areas. Nevertheless, most participants had experience in other areas of agriculture in addition to their current occupation.

The second round involved 52 participants (7 female, 45 male) who were interviewed in twelve focus group sessions: For the first focus group, we consulted a machinery ring. This way, an expert round was established, including the head of the machinery ring, a soil lab owner, and federal counselors. The aim was to conduct an exemplary focus group interview with them and to validate our interview guidelines with these very domain experts. The second and third focus groups were conducted with the help of our project partner John Deere, who invited customers (farmers) to be interviewed. The remaining nine focus groups were conducted with farm managers and farm worker who took part in a federal graduation to earn the title of state-recognized technician in the field of agriculture. Especially in this second-round focus group, the participants had quite a broad background regarding their affinity to digital technologies in their business, as some of the participants had no software for farming in use.

10.3.3 *Analysis*

The focus group sessions were audio-recorded, transcribed, and anonymized for coding. In our subsequent analysis, we employed open coding according to Strauss and Corbin (1998), i.e., gathered data into approximate categories to reflect the issues and requirements raised by the respondents based on repeated readings of the data and organized them into similar statements. The resulting categories are reflected by the requirements outlined in Table 10.1 and Table 10.2. The categorization of the first-round focus group was conducted by the second author, while the first author coded the second-round focus groups. We decided to do so in order to grant a homogeneous analysis of the data in the first stage of coding. To prevent subjective biases and to achieve an intercoder consensus, the first and second authors reviewed, discussed, and revised, if required, their codings mutually (Cascio et al., 2019). Thereafter, the coding was presented to the other authors for a second round of review. As most of the analysis was conducted in German, selected quotes were translated into English by the authors.

10.4 Empirical Study: Summary of Findings

All four first-round groups were made up of different members: water conservation advisors, agronomists, vintners, machinery ring employees, and agricultural students. Only a few participants already had experience with FMIS. It turned out that the participants used the FMIS either to communicate between farmers and (water conservation) advisors or to communicate between farmers and contractors (with forms and route planners for drivers). Used FMIS were compared several times with GIS systems, with which some participants have already gained experience. Three groups independently expressed the wish to be able to include a route planner for drivers. Other frequently requested features were clarification of access permissions for the app, a possibility to rename column names, conflict resolution in case of conflicting changes to files, and a possibility to indicate the current status of jobs. In addition, one participant expressed the wish to being able to tick off areas he had already visited and also note how far he had come with e.g., fertilizing a field. A similar practice already seems to be done with paper and pencil.

An employee from a machinery ring told us some usability weaknesses of older technologies, such as a difficult installation, missing explanations for features, or the selection of a file export directory. Also, a vintner contractor briefly described their approach to planning with Google Earth, as they were unable to find affordable planning tools suitable for viticulture. They make tables and maps for drivers so that they can find their customers and use the contractor's tables to complete the necessary documentation. As a contractor, they create their own maps for customers, which they described as a time-consuming process. When analyzing the different points of discussion in the four focus groups, we identified five major requirements, which are summarized in Table 10.1.

Table 10.1: List of identified requirements for interface design

Requirement	Description
Tailorability for diverse agricultural subdomains (R1)	Support of different domains, customization according to their needs, i.e., granularity of information, and interfaces for interoperability with third-party systems.
Low complexity of field data filtering operations (R2)	Establish usability for personnel with less technical expertise, integrate usable data filtering views for field data, and automate the setup of background maps.
Location-independent technology support for field works (R3)	Support different devices, such as personal computers and smartphones (e.g., by responsive design) to allow operation both in field or office settings.
Prioritization and monitoring of field processing tasks (R4)	Allow for the prioritization of fields, display the progress of a task execution, facilitate the documentation of wage workers' days, and support time recording.
Navigation and recommendation system for wage workers (R5)	Provide a routing component for wage workers considering the width of paths and vehicles, giving tips for navigation, and suggesting the order of field processing.

Also the twelve second-round focus groups were made up of different members: agronomists, farming advisors, machinery ring employees, farm managers and agricultural students. Only a few participants already had experience with FMIS. The intention of the second-round focus groups was to develop and understand more basic requirements, important for the design of a system's architecture (backend). We received many statements that are on a more abstract level than directly connected to possible user interface requirements. For example, harvesting could be scheduled in narrow time frames due to possible weather changes, that makes any system's faults involved in this operations not tolerated. Especially combined with bad internet connectivity in rural areas, a desire for internet-independent solutions arises, meaning pure cloud solutions are opposed. Besides the technical requirements, we were often confronted with statements that management operations, which typically take place via computers in offices, are tasks conducted rather reluctantly. As a result of the analysis of the twelve focus groups, we identified six requirements for architecture design, which are summarized in Table 10.2.

Table 10.2: List of identified requirements of the system architecture

Requirement	Description
Offline capability for infrastructure disruptions (R6)	Allowing the basic functionality without a proper internet access, e.g., by introducing caching mechanisms to offload data on the end-device pro-actively. Synchronization between multiple devices must be ensured.
Extendable and modular feature design (R7)	The basic feature set could be small but must be extendable by future modules (e.g., task monitoring and navigation features) that could be individual for different workflows.
Data sovereignty for confidentiality and privacy (R8)	Privacy and confidentiality are very important factors in this domain and must be respected. Therefore, outwards data transmission must be reduced to just permitted traffic.
Data safety and recovery mechanisms (R9)	Safety of data must be ensured, that is to say proper backup and recovery mechanisms. The whole backup process must be an integral property of the system, with a minimum on required user interaction.
Affordability for small and medium enterprises (R10)	The complete solution must be cheap in both acquisition and time for initial setup to align with the limited budget of small and medium-sized enterprises.
Integration of multiple and open data formats (R11)	To allow the integration into existing work processes, an easy exchange between established software must be possible by simple file exchange based on compatible file formats.

10.5 Concept and Implementation: A Toolbox for Decentralized Data Management and Resilient Regional Networking in Agriculture

As the next step, we conducted a synopsis of requirements to derive and explain design decisions that led to both the back-end and front-end concepts and implementations of FarmBox.

10.5.1 *Synopsis of Requirements*

The identified requirements for the interface design (Table 10.1) and the system architecture (Table 10.2) were considered as a whole for developing the concept of the complete FarmBox system. The concept and implementation phase started in 2017 with first prototypes, and lead to a continuous development in multiple stages until the user evaluation in late 2020 and early 2021. Some parts of conceptual ideas at a higher level were already part of other publications during this time (Eberz-Eder et al., 2021; Kuntke et al., 2020). By inspecting the requirements, we came up with high demands for a flexible system, which must be: extendable (R1) and fast to use (R2), as well as supportive by reducing the interface complexity (also R2) and being able to run on multiple (common)

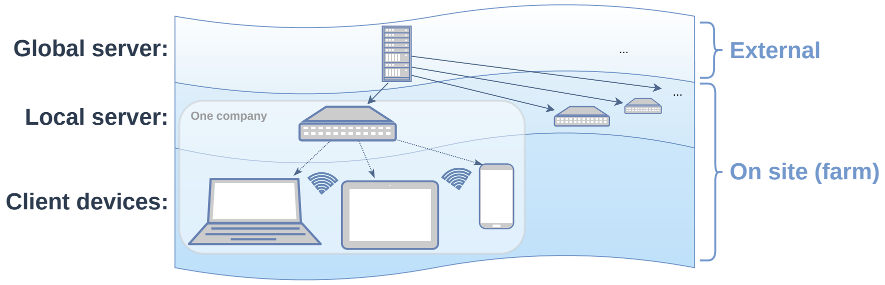


Figure 10.1: Scheme of the complete system, with the three different classes of devices: global server, local server and client devices. The concept of local (mini) servers is used to have a resilient data storage on the company level.

devices (R3). For this reason we decided to build the front-end with the PWA pattern. Using this pattern allows for developing the app with web technologies and being able to run the application on several operating systems and device classes with just one code base. As computational end device categories tend to flow into each other — e.g., convertible laptops with touchscreens, or smartphones than can fold up to tablet-size — web apps with responsive designs seem to be an easy way to handle this situation with the increasing range of *typical* screen-sizes and input-modalities. Demands for specific functions, like task monitoring (R4) or navigation feature (R5), could therefore be outsourced to own function modules and be part of later revisions. In this way, we first focused on developing a back-end concept, that is able to fit the system architecture requirements.

Figure 10.1 presents a simplified schema of our target architecture. We have grouped the architecture in three clusters of device classes: global (external) server, local server and client devices. The focus in this present paper lies mainly on the client devices' application. However, the overview of the complete system's architecture is helpful to understand some design considerations. Especially the used concept of the local (mini) server, which allows for some system architecture requirements by design and is a concept that is rather rarely used in practice, today. The conceptual introduction of a mini-server is a result of the demands for offline capability (R6), data sovereignty (R8) and data safety (R9). Our conceptual requirement for additional hardware – local server – negatively affects the demand for affordability (R10). As we think of small and rather cheap hardware, we therefore refer to *mini-servers*.

10.5.2 *Back-End: Multi-Purpose Mini-Server*

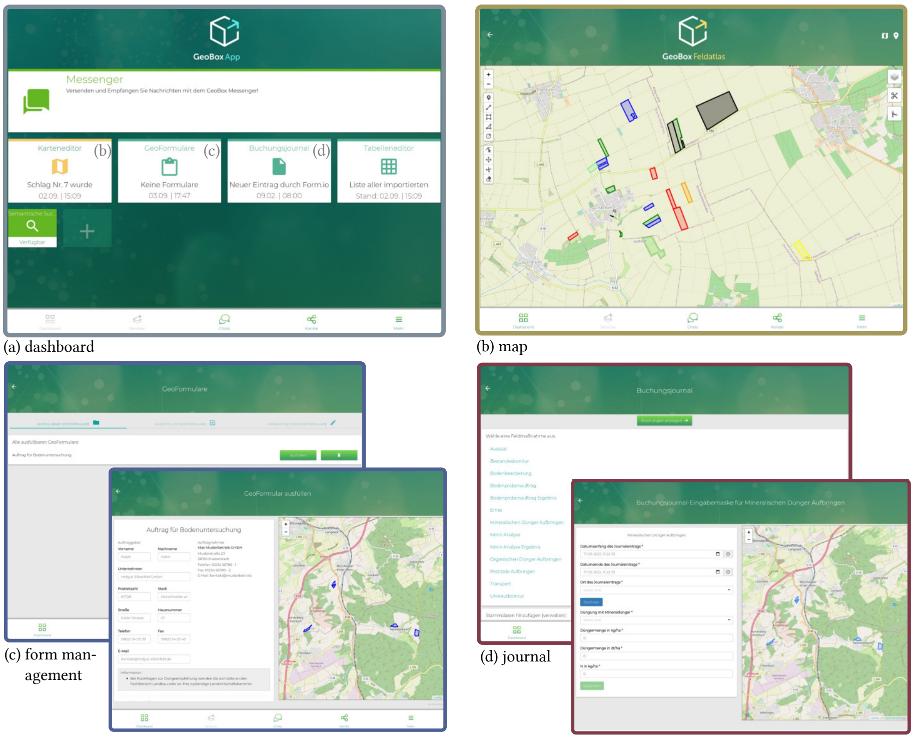
The local mini-server is designed as a central hardware unit, that is used in first instance to synchronize data between different end-devices. Often, modern software is designed with a *cloud* pattern, meaning that the entire data storage is outsourced to external servers, and synchronizing between devices is done via a complete data alignment of each device with the external server. But based on our identified requirements, our goal should be to reduce the data flows to third-parties to ensure privacy (R8). Just the requirement of reducing data synchronization to external servers could also be fulfilled by peer-to-peer transmissions between the end-devices. Yet, we see a higher practicability when all devices of a company could synchronize with one server instance at all the time. Additionally, such a mini-server can also host local server apps (R7) similar to the *cloudless* approach (Grosmann & Ioannidis, 2020) and cache data from the internet for the front-ends. In cases of limited internet bandwidth, those transfer speed limits could be exceeded, assuming the local network, e.g., WiFi, is faster than the internet link. A local network for field applications can be established via LPWAN technologies for small data (Kuntke, Sinn, & Reuter, 2021), in addition to WiFi for high bandwidth applications in specific areas, like machine building, workshop and farm office. In cases of internet outages, the databases of those local mini-servers could be reached from inside the company (R6), in contrast to pure cloud solutions. A simple data safety consideration is the mirroring of the used database between end-devices and the central mini-server (R9), so a single broken device should be able to recover. By keeping the hardware-requirements low, we are able to run the complete server distribution on cheap hardware (R10).

10.5.3 *Front-End: Interacting with Temporal and Spatial Data*

The end-users mainly interact with the whole system by using the front-end. To reach multiple devices (R3) within the same code base, we decided to develop a PWA, that could be translated into software for smartphones, tablets, and desktop computers and their different operating systems (Microsoft Windows, Apple macOS, GNU/Linux, Google Android, Apple iOS/iPadOS). Our first development stage should establish a basic functionality set with a low complexity (R2), but a cross-domain usage (R1). We decided to implement the following application features to have a usable application:

- visualization of spatial data on a *map* (e.g. all cultivated fields of a company),
- documentation of processes in a *journal* (e.g. applied fertilization),
- sending/receiving orders/jobs in a *form management* (e.g. soil sample examination),
- creating *calculations* (e.g. calculation of optimal amount of fertilizer), and
- getting an overview of business data in a *tabular* view (e.g. how many fields have been fertilized).

Those functions are represented by own modules on the main dashboard (see Figure 10.2). For the evaluation, we focused on the features *map*, *form management*, and *journal*: The *map* function allows for both getting a visual overview about the own area and adding, modifying or removing geographic references



(a) dashboard

(b) map

(c) form management

(d) journal

Figure 10.2: Navigation inside the application starts on (a) dashboard, that allows to open the distinct functions; (b) map; (c) form management; and (d) journal.

of the database, primarily used for own fields, but also paths, buildings or arbitrary polygons. The *form management* function is used to import forms of a specific file format and fill those. Most forms require a geometric reference, that automatically show a map view side-by-side next to the form view. A convenience function allows to directly send the form to the recipient through the integrated messenger or via e-mail, based on the integrated metadata of a form file. Each filled form could also be exported as a file to being able to manually hand it over to the recipient. The *journal* function allows to document tasks or operating material. The UI to document something has a similar interface to the form management.

One implementation detail of the developed application is a specific database scheme, i.e., every entry is a triple of {location, time frame and change set}. A change set itself consists of one or more object-values tuples, whereas objects are defined by multiple ontologies. By having these rules for aligning data that are stored into the system's database, we allow for some automatic evaluation processes inside the functions and reduce necessary user input in cases, the semantic of input field is retrievable via the stored data. Reducing required user interactions also reduces the complexity of the user input forms (R2). The home screen of the application (see Figure 10.3) is a grid view (dashboard) with shortcuts to sub-functions, that are called partial apps.

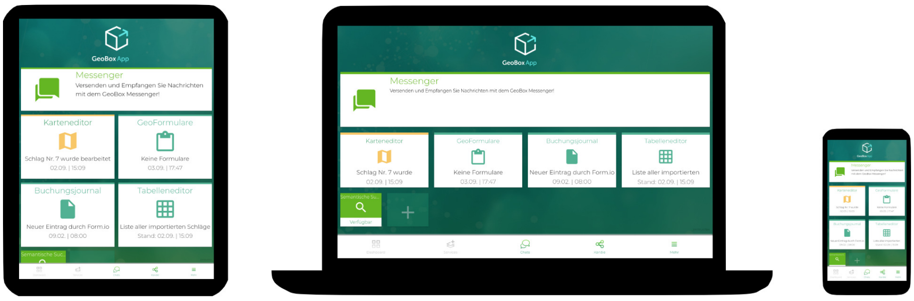


Figure 10.3: Responsive home screen (dashboard) on three most used client devices of the targeted end-users: tablet, laptop (desktop computer) and smartphone. The tiles represent distinct functions of the app, like visualization of cultivated fields on map, documentation of done actions, etc.

In summary, this concept utilizes a novel approach, taking advantage of a small hardware server (*mini-server*), which acts primarily as a local database for the purpose of synchronization between multiple clients. By keeping data local, in contrast to existing solutions, this approach achieves privacy-by-default, as well as a high offline capability. In addition, various import and export functions expand the possibilities of using the managed data to work even in unfamiliar situations.

10.6 Empirical Evaluation: Usability Tests with Agricultural Practitioners

We conducted an evaluation of FarmBox with three major objectives in mind. First, we performed a usability test to reveal positive and negative aspects of the interface, stated by the participants. Second, we worked in an offline scenario to test the understanding of the offline-first character of the developed architecture. Finally, we analyzed ideas and inspirations for future improvements of both the front-end and back-end. The philosophy behind the evaluation process was derived from the notion of *situated evaluation* Twidale et al., 1994, in which qualitative methods are used to draw conclusions about real-world use of technology using domain experts. The aim here is not only to measure the relationship between evaluation goals and outcomes but to derive subjective views from experts about how useful and relevant the technology might be in use. The entire process comprising the creation of an interview guideline, recruitment, evaluation, and data analysis and storage followed the guidelines of our ethical commission. As a limitation, it should be noted that the individuals who developed the prototype are affiliated with the individuals conducting the research, in the form of being colleagues in the same research group or collaborating on the same research projects.

10.6.1 *Study Design*

Due to the ongoing COVID-19 pandemic, we decided to conduct the evaluation in a remote setting with the help of a video conference software between 12/2020 and 03/2021. The participants were once again recruited in the context of a public-funded research projected called GeoBox-2 as described in Section 10.3. However, the participants were not the same as in the focus groups. Everyone participated voluntarily, and no compensation was paid. At first, the participants were informed about the ideas of this evaluation and the involved data processing. To proceed, the participants had to agree with the audio recording and later data processing of all the results. To get some socio-demographic and farm structural data for a rough categorization of the participants, we asked about age and location and high-level information about the job profile, as well as a standardized questionnaire about their technical affinity Karrer et al., 2009.

The main part of the evaluation constitutes supervised scenario-based walkthroughs (Twidale et al., 1994) and think-aloud combined with integrated semi-structured interviews at the end of each task. A scenario description was presented to help all participants to get their minds into the same hypothetical setting. The scenario itself starts with being without any internet connection in the local area due to a major technical problem on part of the responsible internet service provider. That means there is no online help available and the user has to use just the given system (decentralized data management). The tasks were (i) to migrate backup data from another (cloud-based) data management and update the data, (ii) to fill out a form for a soil analysis order, and (iii) to document a farming task. The tasks are considered as easy, but it is the first time the participants interact with this interface, so there is potential for some delays during the exploration of the overall application interface.

After the tasks, we asked the participants to fill out the standardized questionnaire called System Usability Scale (SUS) Brooke, 1996, so we are able to compare the state with other applications as well as previous states of our system and in the future with the next stages of development. At the end, we also gave participants room to settle down and recap the tasks. In this way, we hoped to receive additional helpful information about the evaluation itself and possibly more important statements about our developed software, as some people tend to be more open to sharing their thoughts when a formal setting is in its final stage. The paper contains an evaluation schedule summary (Appendix A.2.1) and a detailed evaluation guideline (Appendix A.2.2).

Age range [years]:	**21 - 30**	**31 - 40**	**41 - 50**	**51 - 60**
Count of participants:	7	5	2	2

Table 10.3: Age distribution of the 16 participants (I2-I17) of the usability tests.

10.6.2 *Participants*

Every participant has to agree to the recording and proper data analysis. We did not keep track of sensitive personal data, and after transcription of the audio recording, we deleted the recorded audio files. A test run of the complete test setup was performed with a HCI expert, while the main evaluation was performed with 16 participants in total (I1-I16). Most of these 16 participants work on agricultural farms (N=10); the others are official advisors (N=3), researchers (N=2), or educators (N=1) — all in the domain of agriculture. The age distribution is shown in Table 10.3. We acknowledge that our set of participants cannot be seen as representative regarding their age, as our participants are rather young with a median of 31 – 40 years. In the domain of working people of agriculture in Germany just about 24 % are below 35 years old, and 49 % are 45 years or older (Bundesministerium für Ernährung und Landwirtschaft, 2020). This reduces the likelihood that our results will be transferable to the entire domain. However, since our results should be of interest for future software in agriculture, the focus on a currently below-average aged target group is to some extent justifiable in our view.

10.7 Empirical Evaluation: Presentation of Findings

Due to our test strategy, we got impressions of how new users interact with the user interface, out-spoken opinions about the software prototype, aspects that should be considered for future development, and statements about the software landscape for agriculture. Based on the comparable SUS (Brooke, 1996), we also have a value that can be compared to and be aligned with existing systems. The SUS-values ranged between 62.5 and 82.5 (mean 73.75, SD 5.84), which could be interpreted as a good (but not great) value according to Bangor et al. (2009). The distribution among all questions of the SUS is shown in Figure 10.4. Most participants stated that they found the system easy or very easy to use. 88 % said they would like to use the system frequently. Notably, 81 % stated that they would not need the help of a technophile person to use the system. But 19 % saw too many inconsistencies in our prototype, with 13 % unsure.

In the following, we highlight positive as well as negative reactions to the tested parts of our system, as well as further considerations for future developments that seem to be of particular interest to the targeted domain of agricultural professionals. In this way, we gain better insights to understand this specific target group and their needs.

10.7.1 *Reactions to the overall system*

The general design of the app was mostly seen as *"comprehensibly structured"* (I02), and mentioned positively by 14 of the 16 participants. Also, we could not see any problems regarding the understanding of the internal navigation,

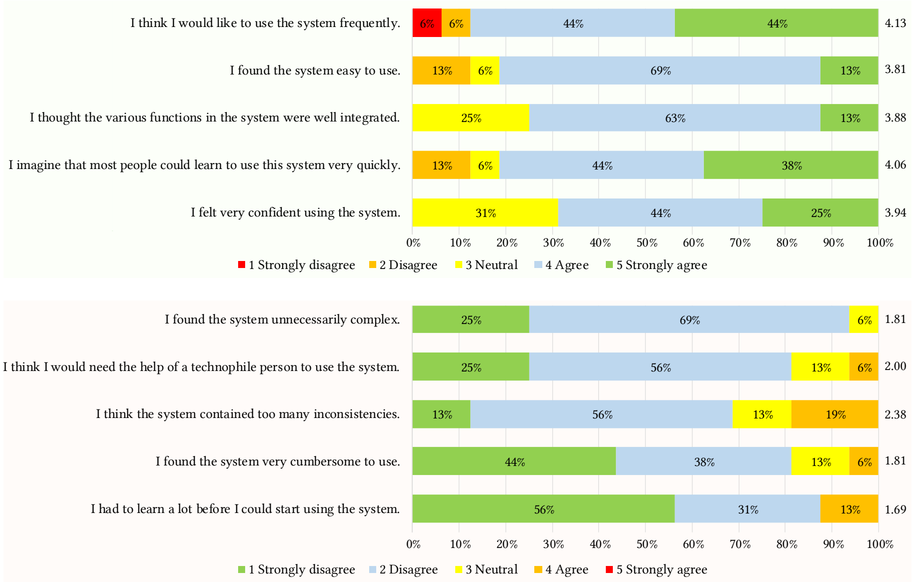


Figure 10.4: Results of the SUS questionnaire. The number on the right of each bar indicates the mean score for the question (ranging from 1 to 5).

i.e., to open a specific function (partial app), one has to go to the app's home screen (*dashboard*) and in every partial app (e.g., *map*) one can go back one step by clicking on a back-arrow in the upper-left, or directly to the dashboard, by clicking the appropriate symbol on the lower left (see Figure 10.2). We also got some positive mentions regarding the used colors (I10, I15) and icons (I10, I16).

One suggestion for improvement relates to the fact that the light font used may be difficult to read for some people, primarily older people (I16). Accordingly, one participant also had problems reading labels in a partial app:

> I10: " *This [headings in the form application] I can now read on my PC almost not at all.*"

Two participants considered the import functionality as too cumbersome (I12, I13). However, the possibilities of data exchange with open formats that are also compatible with other programs (e.g., spreadsheet files like `.csv`) were highlighted positively and considered important by 13 respondents. Particular attention was paid by participants to the choice of symbols and labels, which at the time of the tests were still partly based on the examples of the frameworks used (e.g., Leaflet [1]). Six persons pointed out that simpler descriptions should be chosen and that foreign words (English descriptions) should be avoided since this would be an obstacle, especially for the older generation. This is particularly interesting since there is a trend towards modern-sounding descriptions in other software.

[1] https://leafletjs.com

10.7.2 *Specific reactions to the tested functionalities*

THE MAP IS APPRECIATED, BUT ICONS ARE NOT UNDERSTOOD: There were no problems with the general navigation of the map application, which was described as "relatively easy to use" (I02), and comparable to other domain specific map applications. As farmers regularly have large areas to manage, map applications are used frequently and on a daily basis. Therefore, a good map experience is crucial for the overall acceptance of the app. When drawing in new areas, however, about half of the test persons had initial difficulties and could not find the correct tool right away. Geometric primitives typical for drawing on maps, such as polylines or polygons, were often unfamiliar: *"That strange thing there with the three points ...uh I don't know"* (I06). Potential improvements noted here are the direct display of size information when drawing lines and areas (I07, I09) and the display of cadastral data to directly mark existing properties (I05, I16).

THE FORM IS WELL UNDERSTOOD: Overall, the forms management was described as well-structured (I04, I06, I10, I11, I15, I16). The functionality of the auto-fill support of form input fields by already known business data of the app's internal database was also positively mentioned (I03, I04, I16). However, comfort functions were missed: the forwarding to the form input view after file import, more button icons for faster recognition of actions, and the identification of the processing status of forms in the overview. Furthermore, the buttons for import and export were often difficult to find and are therefore not yet optimally placed or insufficiently recognizable as such. But the idea of migrating the paper forms-based process - e.g., awarding contracts or ordering placements - into the digital farm management ecosystem was mostly seen as overdue.

THE JOURNAL IS SEEN AS IMPORTANT, BUT CAPABLE OF IMPROVEMENT: Overall, the journal was considered important. Its functionality and structure received positive remarks. Certain aspects were, however criticized, such as labels and unnecessary input fields. The function itself was also seen as important due to increasing regulations:

> I04: *"And when it comes to something like area applications, where you might have to fear penalties if you don't provide certain data, then it [having access to a journal of activities] could become important. I would say that such an independent system would fill a gap, so that you could at least provide proof or something similar: "Here, I have done this then and there"..."*

However, there is room for improvement with regard to the description of some elements. Thus, some terms were badly chosen and came across negatively to many test persons, e.g., the word "pesticides", which has a negative connotation in German and should be replaced with the term "plant protection products" (German: "Pflanzenschutzmittel").

10.7.3 *Farmers appreciate the offline-capable design*

As part of the evaluation, we also asked participants about the importance of aspects of offline capability in software, which is one of the unique features of the farm management concept compared to commercially available tools. The capabilities to have routines that are designed to work also offline (nearly) fully functional is seen as an important feature by some participants (I02, I03, I05, I09, I10, I13, I16), resulting in statements like:

> I09: *"It can be that a network line is somehow disrupted and that this can also happen over a longer period of time, there can be a power failure, there can be computer problems or something. So it's good that you can still continue to work there and that perhaps at a later time then reconciles again. Or that it is automatically synchronized, however that may be. So whether that happens actively or passively. So such a scenario should be taken into account."*

The increasing dependence of modern software on the internet is also creating problems for farms in some rural areas with poor internet connections, pushing the entire sector into an increasing dependence on infrastructure. Even in our rather small set of participants, we received statements about missing internet connectivity, which is not handled by current software:

> I04: *"Because here in the country, mobile internet is still very poorly developed. So I don't have 4G and so on. And you can't do anything with it in normal applications. Therefore, an offline application would not be bad."*

Also, outage scenarios are well-known and feared. In the event of power outages lasting from a few hours to a few days, some companies are still able to generate electrical energy themselves using emergency generators. The necessary fuel stock is also usually present as the agricultural machinery require it. But as the increasing dependence on data and network connectivity is new in this sector and therefore rarely considered - it is becoming increasingly important and difficult to overcome. Self-sufficiency in electrical power is well known, but it is not as easy to ensure communication in the event of outage scenarios, as happened after the 2021 flood in some rural areas of western Germany. And the possibility of being in an offline scenario at one point due to an outage was also considered likely. Even at the time of the evaluation - when no catastrophe had occurred in the area for a long time - network outages were very present:

> I16: *"actually, with regard to last week [a city-wide internet outage for about two hours], I will say that it [being offline for some hours to days] is very valid"*

One problem for the UI design was the trade-off between an easy-to-use design and elements to support the offline capability. A specific concern was to embed functionality for offline capability without limiting comfort, as it may be limited through more buttons or more cumbersome procedures. But eight participants explicitly did not see any danger or problem with this regard. With respect to managing a business in crisis scenarios, one respondent (I06) explicitly pointed out that the system has to react quickly in very hectic situations and must be fully functional precisely then. To our understanding, especially the property of offline capability allows continuing business operations in such scenarios, in contrast to cloud-based tools.

10.7.4 *Privacy aspects are scrutinized by some participants*

When asked about the perceived loss of control over data when using the software, opinions differed. This result is in line with the analysis of the privacy perception of the sector (Linsner et al., 2021). The investigated farmers tend to be privacy-aware stakeholders, who want to be very cautious with their own data, but are constrained by external circumstances. On the one hand, there were statements that the software was already *"confidence-inspiring"* (I02) and that there were no fears that the software would send any data on unknowingly (I07); on the other hand, there were also farmers who wanted to be convinced and approached the software with skepticism due to bad experiences (I03). Likewise, the desire to be informed about all data leaving the system was expressed (I04, I05, I11), e.g., they would prefer one additional confirmation button before sending a form to the contractor. In this context, the complexity of terms and conditions and privacy statements was also mentioned negatively, and the desire was expressed to present these in a language that is easy to understand (I04).

10.8 Discussion

In order to address our research question (Section 10.1) and the issues identified in our literature review (Section 10.2) and the elucidated requirements from practitioners (Section 10.3), we designed the FarmBox tool for resilient, decentralized data management in agriculture (Section 10.5). Then, we conducted a user-centered evaluation of FarmBox using scenario-based walk-throughs, semi-structured interviews and a usability questionnaire (Section 10.6). In the following subsections, we present our main findings and contextualize these into the existing body of knowledge. Also, we sum up our empirical and artifact contributions and discuss theoretical implications for the design of agricultural software and future research.

10.8.1 *Findings*

Our findings indicate that **crisis capability is considered an essential feature** for business continuity but is not available to currently used technologies. We found that the practitioners we interviewed in the empirical studies already had a sense for business contingency in crisis scenarios (*R6 Offline capability for infrastructure disruptions*). This whole topic of crisis-capability is not covered by recent related work that also analyzed requirements for farming software by empirical methods, like (Michels & Mußhoff, 2020). Especially in such difficult situations like extreme weather events that harm the environment, a farmer would not like to face the additional challenge of non-functional systems. Although this claim applies to several sectors, it has a particular flavor in agriculture because of the small farms and the large amount of time required for the necessary field activities. The time-consuming aspect prevents a high degree of self-organizing prevention mechanisms. Therefore, the used equipment must be designed with the crisis capability in mind. Other business domains usually have dedicated staff responsible for managing corporate IT and can take the necessary actions for the situation at hand. Also, in most domains, the job can often be delayed for some hours or days, and there are *only* additional employee costs or production losses with its corresponding consequences. The result of the work is delayed - but could be finished. In agriculture, field operations usually have to be carried out in narrow time slots; otherwise, sudden changes in weather can result in poor harvests or even the destruction of the crop. A technical problem in such a time slot can have dramatic effects on the company if the machinery is striking or not performing well due to missing data for precision agriculture. The identified requirements are also reflected by some statements of our software prototype evaluation (Section 10.6). For the reason of *crisis-capability*, the goal was to design an architecture that is able to withstand crises without the need for expensive specialized hardware (*R10 Affordability for small and medium enterprises*). As electrical power can be produced locally with *emergency power generators* in crisis situations, the concept of mini-servers could be analogously seen as *emergency data generators*, i.e., as local data storage for the businesses' end-devices (e.g., smartphone, tablet, laptop, IoT equipment). By developing the software with an *offline-first* mindset, we ensure that our system also works in scenarios without a proper internet connection.

Second, the **contrast between strong desire for customization and time-efficient operation** became apparent. One aspect mentioned in both the requirements engineering and our evaluation is the high need for customization of the farm management software to fit the demand for different workflows. From the outside, this is an interesting fact, as it seems that despite the different sizes of companies, the daily routines should be similar across the domain. On the other side, we also received statements saying the less time a software takes away from relevant tasks, the better. Farmers typically did not choose their profession because they like to do office work; they probably also do not want to spend more time than necessary with a software. However, since application customization is very time-consuming and requires a more detailed investigation of a software's capabilities, this seems to be a conflict of interest. Other commercial apps typically presuppose a specific way of doing things that might not fit every company's workflow, according to the statements of some participants. In this way, further research on this area of conflict may be required. Third, our participants highlighted the **importance of support for multiple end-devices**. As already mentioned, it is important to support multiple end-devices with modern software. This allows the software to fit to different user behaviors, and therefore might increase the target group. But most professional (business) software is dedicated for stationary devices or mobile devices and must not adapt to different screen sizes and user conditions. But farmers would like to do some simple management or documentation tasks on the go on a smartphone. Other tasks might profit from more screen space and are easier to do on a regular desktop computer / notebook. So the farmer user-base is a good example of the need for responsive enterprise software design. Finally, we identified different **UI requirements for the specific groups of farmers**. It is a rather trivial fact that a specific target group has its own specific needs and requirements regarding software design, which also holds for the group of farmers. Within our evaluation we got two surprising insights: (1) Although we thought that all farmers are experienced in digital map software, not all symbols and labels common to us are recognized. Therefore, we see the need for simplified icons and rather farming-related graphics to improve the visual understanding of map actions, like drawing a new area. (2) Foreign words should be introduced very carefully, even in cases where it seems to be common knowledge. To further improve the understanding of foreign words, they should be combined with illustrations like pictograms. Similarly, the demand for terms and conditions, as well as privacy statements, that are phrased easy to understand was underscored. In fact, we did not find any analysis on service agreements in lay language; this could be an interesting open topic for future research.

10.8.2 *Contributions*

First, this work provides the empirical contribution of **design requirements for the architecture and interface of a resilient farm management information system**. Empirical contributions provide "new knowledge through findings based on observation and data-gathering" using sources, including interviews, surveys, focus groups, and many others Wobbrock and Kientz, 2016. In Section 3, we summarized the findings of two rounds of focus groups to distill design requirements for the FarmBox tool-set. In terms of the interface, participants required a cross-domain usage and tailorability (R1), a low complexity of operation (R2), and location-independent technology support (R3). Furthermore, they asked for specific features, such as the monitoring of fields task progress (R4) and a navigation system for wage workers (R5). With regard to the system architecture, offline capability (R6) and data safety (R9) were mentioned requirements for a resilient system, while an extendable and modular design (R7) as well as multiple open data formats (R11) were required to ensure connectivity. Moreover, from a business perspective, participants desired an affordable solution (R10) that respects the confidentiality and privacy of data (R8).

There is little literature covering requirements analysis for management software for agriculture, like the one of Sørensen et al. (2010). Other works that adopt a user-centered perspective mainly cover domain-specific topics like the analysis of farmers' perspectives on smartphone usage for developing a geotag smartphone app (Kenny & Regan, 2021). Some of our detected requirements are consistent with existing analyses, i.e., a low complexity of operation ("information overload"), location-independent technology support ("on-line data acquisition in the field”), and monitoring of fields task progress (“monitor field operations”). But as previous works did not extensively elaborate on implementable requirements, our detected requirements are more extensive, and most of our detected requirements (e.g., offline-capability) are not covered by the existing body of literature. Other works do not analyze the needs from a user-centered perspective, but rather focus on existing solutions by inspecting the current usage of FMIS (Munz et al., 2020), detecting factors that influence the usage and adoption of smartphone apps for dairy heard management or crop production (Michels, Bonke, & Musshoff, 2020) or analyzing functions of existing FMIS (Fountas et al., 2015).

Second, an artifact contribution is achieved by the design and evaluation of **toolbox for resilient data management**. Artifact contributions arise from generative design-driven and invention-driven activities, resulting in “new systems, architectures, tools [and] toolkits” which then are “evaluated in a holistic fashion according to what they make possible and how they do so” Wobbrock and Kientz, 2016. In Section 10.5, we created the ready-to-use system FarmBox for potential users, mainly targeting farmers of crop or fruit production, but also usable for the livestock sector. First, we have shown our basic concept of the complete system that allows for cloud-like synchronization without the need for an internet connection to solve everyday tasks. And in accordance with this concept, we implemented a prototype with the most important features.

In Section 10.6, we present the results of the evaluation of FarmBox. The concept of the system with the decentralized approach as one core aspect was appreciated and could therefore be an aspect to increase the adoption rate of agricultural software. The general usability of the client application’s user interface was not seen influenced at all by the decentralized system’s design. In line with some of the related literature (Klerkx et al., 2019; Linsner et al., 2021), we received statements about the importance of privacy, especially for software that manage all relevant business data. However, users rely on trusting software developers to not spy on the generated data, with some statements conveying a general mistrust in software. But the feature to work without an internet-link could be a confidence building measure.

Finally, we provide theoretical implications by a **novel concept for decentralized and resilient data management**. Theoretical research contributions consist of “new or improved concepts, definitions, models, principles, or frameworks” Wobbrock and Kientz, 2016. Our paper contributes to the area of digitalization and resilience, applied to the domains of agriculture and, in particular, to farm management software, with implications also for other SME domains, especially where important operations are managed with the help of software. In both the requirements engineering as well as the evaluation, we received statements that highlight the importance of systems’ stability, even – or particularly – in crisis scenarios. It can be crucial in such situations to have the important applications running to do everyday tasks without a working internet connection, even when interacting with other people or hardware systems. An effective way to ensure the offline-capability is to design the whole software architecture so that the offline capability is not a specific function but an intrinsic architecture design, as is the case with decentralized systems. A rather uncommon element of our concept is the local mini-server to overcome the need for internet connectivity for easy-to-use data synchronization of multiple end-devices.

Furthermore, we have shown some details of the design of the front-end application for end-devices like smartphones, tablets, and desktop computers. The graphical design concept and color scheme were adjusted in an iterative manner. Especially the cloudless (Grosmann & Ioannidis, 2020) approach is new to the domain of agricultural applications, and in general, rarely considered as an alternative design for modern inter-connected systems concept. The similar (from a technical perspective) *fog* pattern itself is not a novel concept of this present paper, but mostly seen as an addition to cloud services for reducing network traffic, to ease pressure on the core server, and to improve network latency and speed. However, we have not seen works that use this approach for a resilient service distribution for business operations. Related approaches are community projects like yunohost [2] that share the privacy aspects, but are motivated more from an autonomy perspective, rather than the need for resilient services. But especially the hardening of new solutions against outage scenarios is important. Long-lasting network unavailability could also be the result of weather catastrophes, e.g., the 2021 European floods. Even if the power grid is rebuilt quickly, a couple of weeks could pass until basic internet connectivity is restored.

10.9 Conclusion

The digitalization process for agriculture is still ongoing, promising more precise and less labor-intensive farming production. One aspect that comes with this digitalization process is the need for farm management software to control, plan, and document farming activities. One of our contributions to this process is a recent requirements analysis (Section 10.3) in which 57 experts in the agricultural domain were interviewed using the focus group method. In contrast to related works, we grouped the requirements into front-end and back-end requirements. Based on the identified requirements, we created a concept for a complete farm management software system, which forms the second contribution. To our knowledge, this concept is the first technical description of a *crisis-capable* software design for farmers, which ensures that it works as well as possible in outage scenarios, e.g., without relying on a working internet connection. The third contribution is the evaluation (Section 10.6) of the implemented front-end application with 16 domain experts.

On the limitation side, we have only tested a subset of the functionalities of the front-end software in an artificial test environment. Overall, most participants emphasized the meaningfulness to reduce the dependency of software/hardware on a working internet connection. In this way, we provide an example of a business software with the ability to exchange data that is not developed based on the cloud pattern and thus does not require a reliable internet connection to interact with data. Our approach introduces a mini-server at the company level for caching and synchronization purposes, as well as many ex- and import

[2] https://yunohost.org - self-hosting of (web-)services

functions within the client-application to manually manage data in unforeseen situations.

Use-cases for decentralized systems seem to be underrepresented in the current scientific landscape. As decentralizing could increase the resilience in outage scenarios, there should be more engagement into developing and evaluating such concepts with regard to the users perspective, especially for critical businesses like food production. Furthermore, research on how to increase the adoption rate of precise farming tools is necessary, e.g., how to support the trust relating to the privacy behavior of a software.

11

LORAWAN SIGNAL LOSS IN RURAL AREAS

ABSTRACT Low Power Wide Area Network (LPWAN) technologies are typically promoted for Internet-of-Things (IoT) applications, but are also of interest for emergency communications systems when regular fixed and mobile networks break down. Although LoRaWAN is a frequently used representative here, there are sometimes large differences between the proposed range and the results of some practical evaluations. Since previous work has focused on urban environments or has conducted simulations, this work aims to gather concrete knowledge on the transmission characteristics in rural environments. Extensive field studies with varying geographic conditions and comparative tests in urban environments were performed using two different hardware implementations. Overall, it was found that the collected values in rural areas are significantly lower than the theoretical values. Nevertheless, the results certify that LoRaWAN technology has a high range that cannot be achieved with other common technologies for emergency communications.

ORIGINAL PUBLICATION *Kuntke, F., Bektas, M., Buhleier, L., Pohl, E., Schiller, R., & Reuter, C. (2023). How Would Emergency Communication Based on LoRaWAN Perform? Empirical Findings of Signal Propagation in Rural Areas.* Proceedings of Information Systems for Crisis Response and Management (ISCRAM)*, 1–8. http://dx.doi.org/10.59297/QBHV2089*

ACKNOWLEDGMENTS This work was supported by funds of the German Government's Special Purpose Fund held at Landwirtschaftliche Rentenbank in the project AgriRegio.

11.1 INTRODUCTION

Low Power Wide Area Network (LPWAN) implementations are continuously gaining interest in practice and research, especially for usage in Internet of Things (IoT) devices. Therefore, the Long Range (LoRa) Alliance invented the Long Range Wide Area Network (LoRaWAN) standard. Advantages in using LoRaWAN for device connection are primarily the low energy consumption and the high range that can be achieved (Bardram et al., 2018). LoRaWAN has also gained attention in the crisis informatics community, based on the high peer-to-peer range and rather cheap and available devices and development boards. Use cases for this technology are mainly (1) establishing communication capabilities after infrastructure breakdowns (Höchst et al., 2020; Kuntke, Baumgärtner, &

Reuter, 2023; Sisinni et al., 2020), or (2) environment monitoring as part of early warning systems, e.g., to warn in case of flooding events (Huyeng et al., 2022).

However, contrary to the proposed range of up to more than 10 km (Queralta et al., 2019), recent studies show a broad range of maximum communication distances depending on the setting: 50-90 m in a dense forest environment (Iova et al., 2017) to 3km in urban area with high buildings (Mdhaffar et al., 2017) in practice. While a communication range of 50 meters does not seem very useful, communication up to several kilometers distance would be a good means of communicating many concerns in emergency situations. Therefore, it can be concluded that further research is needed to examine the effects of the geographical conditions on the transmission characteristics. Thereby, the information on the achievable range could be used to derive the maximum distance between devices to achieve an optimal distribution and reliable communication. For this research, different infrastructure areas like groups of trees and houses need to be assessed. The results of this research can then be used to adjust the technical implementation regarding real-life conditions. Therefore, this work addresses the following research question: *What concrete values for the LoRaWAN transmission characteristics can be achieved regarding geographical conditions?*

By answering this research question, the paper makes several contributions for further development of LoRaWAN based emergency communication systems.

First, Section Foundations and Related Work provides a short technical introduction on LoRaWAN and presents use cases of LoRaWAN in the crisis informatics community and works that investigate on wireless transmission range. Our own test methodology and the used hardware is described in Section Methodology. Afterwards, Section Results presents concrete test results, and Section Discussion presents implications of these empirical determined data. Finally, a brief conclusion is drawn in Section Conclusion, which also discusses limitations and opportunities for future research.

11.2 Foundations and Related Work

This section explains the theoretical foundations of LoRaWAN, as well as later used software and hardware for the empirical evaluations, and also describes related work.

11.2.1 *LoRaWAN*

LoRaWAN is a popular Low Power Wide Area Network (LPWAN) technology, that was first released in 2015 (LoRa Alliance, 2015). It is said to allow for a high transmission range of up to several kilometers along with a relatively low energy consumption. Because of the long range, LoRaWAN is often used in large-area IoT applications in combination with sensors, for example soil moisture or temperature sensors in agriculture. Since such sensors are often battery powered and distributed over a wide range, LoRaWAN is one of the rather appropriate technologies. Although LoRaWAN has some security considerations in the protocol itself, there remain security issues that must be taken into consideration when building resilient network setups (Kuntke, Romanenko, et al., 2022). A LoRaWAN network consist of end devices, gateways and servers and follows a stars-of-stars topology. All data arriving at the gateway are forwarded to a network server, which in turn forwards them to an application server to present it to users. LoRaWAN is partially based on the LoRa physical layer, which specifies the wireless data transmission between gateways and end devices (see Figure 11.1).

The spreading factor (SF) controls the amount of signals (chirps) per transmitted data. It allows to adjust the tradeoff between speed and robustness of a LoRa data transmission, with values between 7 (fast) and 12 (robust). The gateway and network server as well as the network server and the application server communicate over a conventional network connection via TCP/IP. To join a LoRaWAN network, new end devices must conduct over-the-air-activation (OTAA) or activation by personalization (ABP). The difference here lies in the key exchange protocols. The end devices can be of one of three different types. End devices of type A wait for the reply package for two windows after sending information. End devices of type B wait for an additional interval and end devices of type C listen continuously for incoming data frames. Our study uses type A and type C end devices. The Received Signal Strength Indicator (RSSI) and Signal-to-Noise-Ratio (SNR) values can be examined to check the connection quality of LoRaWAN. These indicators are especially suitable since they allow for a quantification of the transmission characteristics. The RSSI value represents the reception strength in dBm with a higher value representing a better reception strength. The SNR represents the ratio of signal to noise in dB, where a higher value is preferable.

11.2.2 *Related Work*

Despite a multitude of studies investigating the influence of the geographic conditions on LoRaWAN range, most of them focus on urban areas (Cattani et al., 2017; Petrariu, 2021; Petrić et al., 2016) or test the range mainly by simulations (Khan & Portmann, 2018).

Khan and Portmann (2018) only simulated a LoRaWAN network to gain knowledge about the transmission characteristics. Two different scenarios were tested. In scenario 1, an end device moved away from the gateway with a constant direction on a distance of 1-7 km. In scenario 2, multiple end devices were positioned at different places in a 5 km radius around the gateway. The authors concluded that in scenario 1, adjusting the transmission rate would benefit the performance and in scenario 2, a higher quantity of maximum transfers would impair the performance. Most other works conduct field tests comparable to the ones executed in this work. However, some of these focus mainly on urban areas.

Petrariu (2021) focuses on urban areas and test Longley-Rice and ITU-R on the LoRa network coverage, choosing a communication interval of 10 seconds and a fixed communication channel (868.3 MHz). They also tested different SF from SF7 to SF12. In 200 measurements on a radius of 2 km, they focused on examining the Global Delivering System (GPS) Position, the RSSI values, the Signal-to-Noise Ratio (SNR) values, and the elevation. The maximum communication distance was 500 m. Similarly, Petrić et al. (2016) performed range tests on LoRa FABIAN with mobile end devices around a gateway and a measurement with fixed and devices in an urban area. Their findings were that position has an impact on transmission. Cattani et al. (2017) tested the reliability of LoRaWAN communication in three different locations, namely indoors, outdoors and underground on a university campus and concluded that temperature and humidity can influence the reliability. Other works have executed tests in more rural areas. Marfievici et al. (2013) conducted tests on Wireless Sensor Network (WSN) technology in different vegetation environments and at different times of the day. The conclusion was that all of these factors have an impact on the transmission characteristics for WSN, especially the Packet Delivery Ratio (PDR). Iova et al. (2017) investigated the effect of different types of vegetation in rural environments on the LoRa signal quality. In four different environments, they positioned the sender at a fixed point and the receiver at changing distances. Line-of-Sight (LoS) connections achieved a range of 450-550 m. A range of 50-90 m was achieved when the connection was blocked by vegetation. It was concluded that transmitter power had no effect on range, but temperature could affect the quality of the connection.

Ojo et al. (2021) focused on the usage of LPWAN for Smart Agriculture. The authors used 433 MHz and 868 MHz bands and varying SF values between 7 and 12. The gateway was placed at a height of 3 m and the end devices at different places with different vegetation between gateway and end device. Ranges of up to 860 m in dense forest and 2050 m in less dense forest areas were achieved. Mdhaffar et al. (2017) consider the usage of LoRaWAN networks to gather medical data. A coverage of 33 km2 with the gateway on a height of 12 m in rural environments was achieved. Also, a range of 2 km in dense urban environments and 3 km in less dense urban environments was recorded. Höchst et al. (2020) use LoRa capable micro-controller boards as companion devices for smartphones. A specific chat application allows the smartphone to connect via bluetooth to the LoRa board and let a user send SMS-like messages as LoRa signals to other users. A real-world evaluation for the device-to-device communication allows a range of up to 2.89 km.

Most of those results show that the environment can affect the LoRaWAN transmission characteristics and that further studies are needed to gain accurate values regarding the impact of geographical environment in rural areas on the RSSI/SNR values. With correspondingly more concrete empirically determined values, more precise expected ranges could be predicted in the future, systems could be planned accordingly, and recommendations could be made in the use of emergency communication and environment monitoring systems.

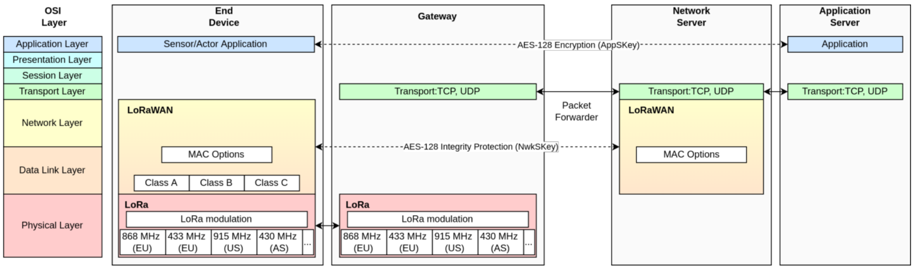


Figure 11.1: Simplified illustration of the LoRaWAN technology stack in the OSI model

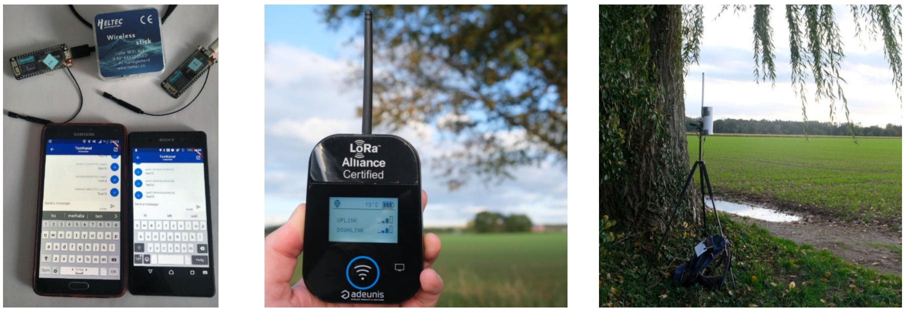
11.3 Methodology

The goal of this work is to determine typical ranges of LoRaWAN by means of empirical measurement series. For this purpose, test series with different hardware setups are to be carried out in order to compensate for the peculiarities of individual hardware and to be able to represent a certain range if there are differences in the hardware. Two different hardware setups were used for the field tests (see Figure 11.2 and Table 11.1): Setup H with two smartphones and two small companion LoRa boards for sending/receiving LoRa signals and setup A with an outdoor LoRaWAN gateway and a commercial signal test device.

11.3.1 *Setup Description*

The Heltec Wireless Sticks in setup H communicated with two Android smartphones to establish the data transfer over the BlueRa app (Höchst et al., 2020). For the field tests, one smartphone (the sender) stayed at a fixed position and sent a message at an interval of 15 seconds to the receiver smartphone, which moved in varying distances and with varying obstacles around the sender. The data was saved on the smartphones and was later evaluated with DB Browser for SQLite.

In setup A, the Adeunis Field Test Device (FTD) offers the IoT-Configurator interface to configure the different communication variables. The gateway was equipped with an open-source embedded Linux system and was connected to a ChirpStack v3 network server instance. The Adeunis FTD was registered in ChirpStack as a regular LoRaWAN end device, and a payload encoder allowed translating the received bits into human-readable data fields like the position (latitude, longitude) and SNR/RSSI values. ChirpStack stored its data in a PostgreSQL database, that allowed to export data for external processing and evaluation. The resulting data sets are uploaded for further processing by thirds (Kuntke, Bektas, et al., 2022).



(a) Setup H: Two Heltec Wireless Sticks, each connected to a smartphone

(b) Setup A: Adeunis FTD

(c) Setup A: LoRaWAN Gateway on a tripod, connected to a laptop

Figure 11.2: The used hardware setups of our empirical tests. (source: own pictures)

Table 11.1: Used hardware of both setups.

Setup H *(Heltec)*	Setup A *(Adeunis)*
• 1x Heltec Wireless Stick (RF95 Modem, ESP32 dual-core Microprocessor, IPEX-1 Spring Antenna 2) • 2x Android smartphone	• 1x Adeunis Field Test Device LoRaWAN EU863-870 (LoRaWAN V1.0 Protocol) • 1x DLOS8N Outdoor LoRaWAN Gateway • 1x Notebook with ChirpStack v3 (LoRaWAN network server)

11.3.2 *Field Tests*

During all field tests, protocols were made to document the results and circumstances, e.g., the weather and geographical setting. This ensures the reproducibility and comparability of all tests. The first tests focused on single-object obstacles to estimate if the impact of a single object on the transmission quality would be sufficient to calculate an obstacle's repeated impact. Setup A was used to test this assumption, since this implementation provides more detailed information on the transmission characteristics like RSSI and SNR. The test was conducted by placing the sender at a fixed point in front of the obstacle and then placing the receiver at two fixed positions, one with the obstacle between the devices and one without the obstacle between them. Since it could be concluded that the collected data wasn't accurate enough for this procedure, the following tests did not follow this procedure. In the other tests, the effects of different geographical surroundings were tested by placing the gateway at a static po-

Table 11.2: The conducted field tests in regard to the used hardware setups, and its location. Three conditions (weather/area) were tested with both setups simultaneously for comparison.

Tests with setup H	Tests with setup A
H1 (Frankfurt am Main, urban)	
H2 (Frankfurt am Main, urban)	
H3 (Darmstadt, urban)	
H4 (Hofgut Neumühle, agricultural)	
H5 (Hofgut Neumühle, agricultural)	A1 (Hofgut Neumühle, agricultural)
	A2 (Frankfurt am Main, forest)
	A3 (Frankfurt am Main, urban)
H6 (Frankfurt am Main, forest)	A4 (Frankfurt am Main, forest)
H7 (Frankfurt am Main, urban)	A5 (Frankfurt am Main, urban)
	A6 (Darmstadt, agricultural)

sition and moving away from the gateway with the end devices with varying distances and obstacles. During the tests, packets were sent by the end device at regular intervals. The tests were conducted in different environments with varying degrees of vegetation, namely (1) urban areas, (2) dense forests, (3) less dense forests, and (4) agricultural fields with smaller hills, hedges, and groups of trees. The GPS data of end device and gateway as well as a description of the surroundings was recorded for later evaluation. Additionally, the meteorological data was collected from the Deutscher Wetterdienst (DWD, *German Weather Service*), since Cattani et al. (2017) detected that weather conditions could influence transmission characteristics. While this is not the focus of this work, this also allows for better comparison. In the test with setup A, the RSSI and SNR values were documented as well. A depiction of the conducted test with corresponding location can be found in Table 11.2.

11.4 Results

In the following, the field tests will be explained in detail with the respective achieved results.

11.4.1 *Setup H*

Test H1 was conducted in Frankfurt am Main, thus a more urban area. This was the first test and mainly aimed at collecting a first test record. This mainly enabled an estimation of the achievable degree of detail as well as range. Test H2 was executed in a similar environment and was meant to deliver results on whether single obstacles would influence the transmission. For this reason, houses, trees and bushes were used as obstacles.

The results showed that trees or bushes did not have a sufficient effect on the transmission to be noticeable with the used hardware. Houses, on the other hand, could impede and block the transmission. It was therefore concluded that further tests should examine these results in urban areas as well as rural areas with varying degrees of foliage. Similar to Test H2, Test H3 was also executed in an urban environment, however this time in Darmstadt, to gather data that is not just based on one location. The same obstacles as in Test H2 were chosen, with one part of this test focusing on trees and bushes and the other focusing on rows of houses. In the first part, the highest range in general for setup H, with 412 m, could be achieved. Hofgut Neumühle, an agricultural environment with slight hills, single bushes, and forest, was chosen as the location for Test H4. The receiver was surrounded by fields, which enabled a range test without many obstacles. Noticeable was that whenever a small elevation difference, i.e. a small hill, blocked the direct LoS connection between sender and receiver, the transmission failed.

In a second test, a small group of trees was used as an obstacle between the two devices. Here, transmission was possible as long as a direct LoS connection was ensured, meaning, only until the transmission was blocked by trees. Lastly, a range test was conducted, whereby an LoS connection was ensured but only a slightly higher range than in the test before could be achieved. Test H5 was executed simultaneously with Test A1 again at Hofgut Neumühle. Another range test was conducted which showed setup A could achieve a much higher range than setup H. In a second part of this test, the connection in a near forest should be tested, but the transmission broke off again when a slight elevation difference blocked the transmission. To again test the range in a dense forest, a forest area in Frankfurt am Main Oberrad was chosen as the location for this test. Test H6 was also simultaneously conducted with Test A4 (setup A). First, an area of the forest with small buildings like a playground was tested and it was found that this did not result in different ranges for the setups. Secondly, an area only consisting of forest was tested, where setup A could achieve much higher ranges. Lastly, in Test H7 an urban area was tested again with both setups (Test A5 for setup A), to gain comparable data of both setups. As soon as some buildings blocked the connection, the transmission broke off again. In an area with more buildings, the setups performed similarly but in an area with less building and more park areas, setup A achieved the higher range.

11.4.2 *Setup A*

Test A1 was conducted simultaneously with Test H5. During this test, setup A achieved a range of 885 m in a small valley. It was also evident that in this case, the RSSI and SNR values no longer worsened. To conduct a first test in a forest area, a forest in Frankfurt am Main Louisa was chosen for this test. This area is characterized by having little undergrowth. In a second part of this test, allotments were also tested as an obstacle. In both parts the RSSI as

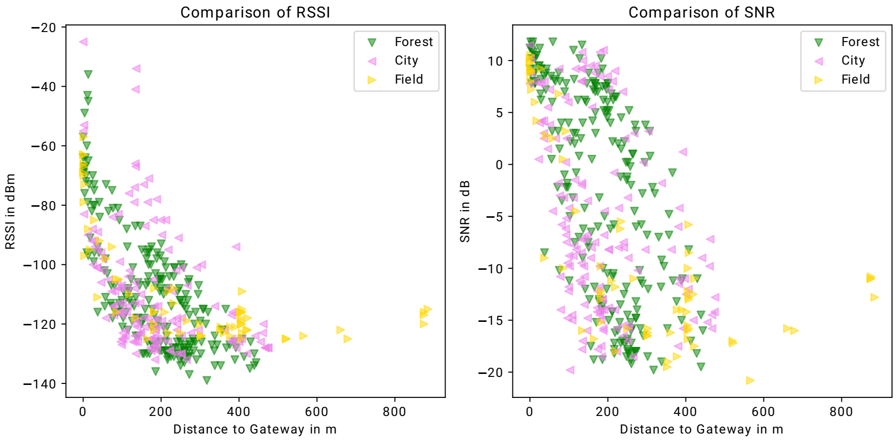


Figure 11.3: Comparison of RSSI and SNR as a function of distance with the Adeunis Tests A1-A5.

well as the SNR values decreased with increasing distance between sender and receiver. Test A3 was executed in the city center of Frankfurt am Main. In a first part of this test a maximum distance of 500 m could be achieved. However, a few minutes later only a distance of 160 to 170 m could be measured in the same environment. Similarly, the values for RSSI and SNR worsened. The only noticeable difference was a change in weather conditions. Test A4 was executed simultaneously with Test H6. In the dense forest area, a range of about 250 m and in the last part of the test a range of 300 m could be achieved. The main difference here were two buildings that additionally blocked the transmission in the first part. In test A5, the same area as in Test A3 was tested to further investigate the changing values. This Test was also conducted with setup H. The range was only slightly higher than in the last part of Test A3 with 250 m, but still much lower range compared to the beginning of Test A3 where a range of 500 m could be achieved. A comparison of some of the RSSI and SNR values in the conducted tests A1-A5 can be seen in Figure 11.3.

Test A6 was executed in an agricultural used area in the north of Darmstadt. This test had the purpose of conducting a rather maximum-distance evaluation (but with real-world conditions) by performing tests in a known wireless transmission friendly area. The positioning of the gateway allowed for several hundred meters of LoS and up to 3 km with just a few obstacles. We got a maximum distance of about 3.3 km in this test for setup A. This is also shown in Figure 11.4.

11.5 Discussion

Several observations can be made from the recorded results. First of all, both hardware configurations can be compared based on their usability for the given use case and test setups. For this purpose, the five field tests where both setups

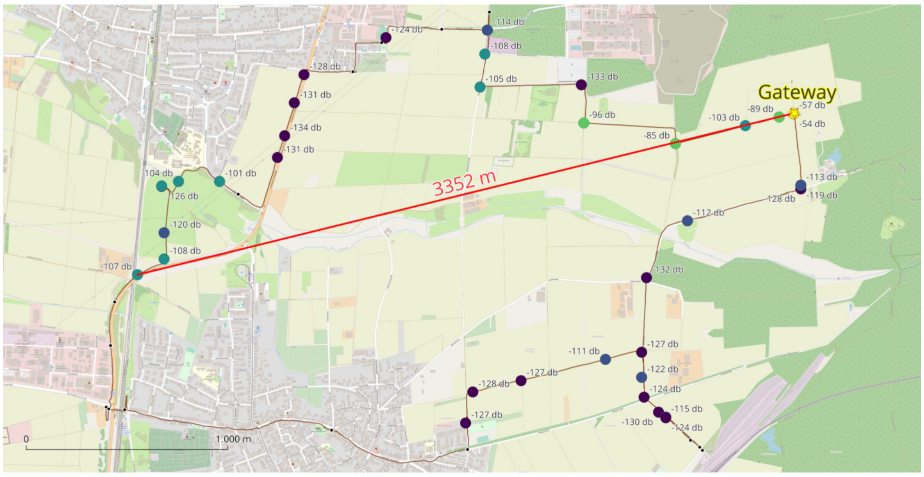


Figure 11.4: Test A6 (agricultural used area) with just a few obstacles achieved a range of 3352 m. Smaller black dots on the track mark failed transmission attempts. The gateway is on an elevation of 190 m NN. At the maximum distance, the sender is on an elevation of 175 m NN. This comes to an elevation difference of 15 m.

were used simultaneously can be considered. Especially in the tests H5a and A1a as well as H6b and A4c, setup A achieved better results than setup H, which in the first case might be explained by the high elevation difference that occurred just after a few meters and affected both setups equally. Another explanation could be that setup H partially could not hold a stable connection. In tests H5b and A1b as well as H6a and A4a, both setups performed similarly. In the urban environments in test H7 and A5, both setups could achieve similar maximum ranges as well. Especially the high range by setup A in test A1 (885 m) could not be reproduced by setup H (test H5), which achieved a maximum range of 412 m. Setup A, in particular, enabled the collection of detailed RSSI and SNR values. Regarding the RSSI and SNR values, as shown in Figure 1, several observations can be concluded.

The lesser dense forest can achieve better results in RSSI and SNR as the agricultural field with a distance of up to 400 m. In the environments urban-day 1 and less dense forest, better RSSI and SNR values could be achieved than in urban-day 2 and the denser forest. The difference in the two forest locations shows that the density of the obstacles can influence the transmission characteristics. Additionally, the transmission in the dense forest is generally worse with no connection beyond a range of 300 m. The difference in the transmission quality on the different days in the urban environments can be explained by the different weather conditions, which will be examined later.

Lastly, the open field achieves the highest range with 3352 m. Mdhaffar et al. (2017) could achieve a similar range of 3 km even in an urban setting, which can be explained by them placing the gateway at an elevation of 12 m compared to 1.3m - 2.0 m in this work. The results of Ojo et al. (2021) also could not be reproduced, as their higher placed gateway at 3 m and the fixed position of the end devices most likely enabling the higher range. However, our tests were conducted with mobile emergency communication systems in mind, like those described by Höchst et al. Such systems will be used at rather low heights of maximum 2 m, as they are typically used as handheld devices. It is also possible that the motion of the end devices could have influenced the connection. The simulations of Khan and Portmann, P. 3 (2018) with a range of 5 - 7 km can't stand as realistic compared to our field test results. In our most optimistic (but realistic) setting in test A6, 3.3 km between sender and receiver could be achieved. Based on our test results, we can confirm the approximate range of 500 m achieved by Iova et al. (2017) and Petrariu (2021) for area characteristics that potentially negatively impacts the LoRaWAN range, like many obstacles or mountain areas.

Although not the primary goal of this work, the meteorological data was collected as well. This enabled comparing the tests A3 and A5, which although conducted in the same environment resulted in different transmission characteristics. Test A3a conducted from 15:46 to 16:25 and test A5 conducted from 15:27 to 16:27 vary especially regarding the temperature, degree of coverage and vertical visibility. This suggests a correlation between the weather conditions and the transmission quality. These conclusions are supported by Cattani et al. (2017), who also deduce an effect of the weather conditions on the transmission characteristics. The differences in tests A3a and A3b/c, however, can't solely be based on the weather since technical difficulties occurred in this case that could have an effect on the range. Future works could focus more on the influence of the meteorological conditions specifically.

11.6 Conclusion

Two of the use cases of LoRaWAN based transmission in crisis informatics are environmental monitoring and digital emergency communication. By conducting field tests in varying environments (urban, forest, agricultural) this work could collect thorough data on the LoRaWAN transmission characteristics dependent of geographical circumstances. These results should help the design of developments for rural area LoRaWAN based systems, based on real world data. Consequently, the real values for the LoRaWAN range in urban and rural areas are significantly lower than the suggested theoretical values. Thereby, an impact of obstacles, the elevation and the meteorological conditions on the transmission characteristics could be recorded. Regarding the obstacles, it could be concluded that the density of the respective obstacles influences the transmission quality. To measure the effects of single objects, the used devices could not provide results that were detailed enough. The conclusion that a higher range can be achieved in valleys can also stand as one of the results of this work. Lastly, an influence of the meteorological conditions could be derived. The highest achieved range over all tests was 3352 m, with a good antenna, but not optimized location. We suggest to take this value as a real world maximum distance with current consumer grade electronics. For areas with a rather high obstacle density, like forests, this value goes down to about 800 m, which is also considered as a worst-case value for regular situations. In case of low-end equipment, the real world values are significantly lower, and achieved a maximal distance of 412 m in our test setup. This result is not convincing, and the use of such low-end boards for critical operations needs to be reconsidered strongly.

The results are obviously restricted by the limited number of conducted test, which were also only conducted in a limited time span and a limited area (all tests were conducted in Hesse or Rhineland-Palatinate, Germany). Additionally, the weather conditions were very similar in all field tests. Although two different hardware setups were used, a multitude of different configuration possibilities to implement a LoRaWAN network exists. Lastly, the field tests are limited by the assumption that multiple factors such as obstacles, distance, elevation, weather conditions and other circumstances could have influenced each one of the test results, thereby hindering a clear derivation of correlation. For a better generalization, further test should be conducted based on the results of this work. This would also serve the further collection of data to gain an empirical dataset. Additionally, further tests in different regional areas and with different meteorological conditions should be executed.

12

RELIABLE DATA TRANSMISSION USING LOW POWER WIDE AREA NETWORKS (LPWAN) FOR AGRICULTURAL APPLICATIONS

Abstract Reliable IT-based communication in agriculture is becoming increasingly important for regular operations. For example, if a farmer is in the field during a network outage, such as a failure of the mobile network, an alternative communication channel is needed to continue to connect to IT components and required data. With increasing digitalization, Low Power Wide Area Network (LPWAN) technologies are being used more and more frequently, e.g. for sensor networks. The LPWAN technologies offer a high range and can be used autonomously for the most part, but do not allow classic TCP/IP communication. In this work, a popular LPWAN technology, namely LoRaWAN, is experimentally supplemented by AX.25 on OSI layer 2 (Data Link Layer) to allow end devices TCP/IP-based communication over long distances. The evaluation shows that classic low-bandwidth applications are thus functional and can enable reliable, crisis-capable data transmission.

Original Publication © Kuntke, Sinn & Reuter | ACM 2021. This is the author's version of the work. It is posted here for your personal use. Not for redistribution. The definitive Version of Record was published in ARES '21: Proceedings of the 16th International Conference on Availability, Reliability and Security, https://dx.doi.org/10.1145/3465481.3469191. *Kuntke, F., Sinn, M., & Reuter, C. (2021). Reliable Data Transmission using Low Power Wide Area Networks (LPWAN) for Agricultural Applications.* Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES 2021), *1–9. https://doi.org/10.1145/3465481.3469191*

Acknowledgments This work was supported by funds of the German Government's Special Purpose Fund held at Landwirtschaftliche Rentenbank in the project Geobox-II as well as by the German Federal Ministry for Education and Research (BMBF) in the project HyServ (01IS17030B). A preliminary, earlier and much shorter version of this paper has been presented at the 41. GIL-Jahrestagung in March 2021 Kuntke, Sinn, Linsner, and Reuter, 2021.

12.1 Introduction, Background and Research Question

Digitalization is now more than ever permeating all areas of the life of modern people. Smart Home is a familiar concept for everyone, ranging from the smart coffee machine to the smart door lock. But also industry sectors, including critical infrastructures, like agriculture, become more complex and interconnected through digitalization (Koenig & Schauer, 2019) . In order to make agricultural systems intelligent, techniques from the fields of 'machine learning' (Lottes et al., 2017) and 'big data' are also used to further support farmers and autonomous systems (Wolfert et al., 2017). The objective of smart farming is to emancipate from stationary control and monitoring systems of a farm. Control interfaces are now available on common end devices such as smartphones (Ryu et al., 2015) and tablets. This makes it possible to perform everyday tasks remotely. Also common to almost all processes and techniques, regardless of the type of application, is that they require a communication channel for the purpose of signal or data transmission. For regular operations in agriculture, communication with other actors is necessary, which, as described, increasingly takes place via digital channels (Linsner et al., 2021). A product research of different large manufacturers has shown that the available (relevant) possibilities are currently the following: mobile radio, LAN, WLAN, Bluetooth, satellite, proprietary radio solutions, USB, LoRaWAN, and NB-IoT.

'Narrowband Internet of Things (NB-IoT)' and 'Long Range Wide Area Network (LoRaWAN)' belong to the so-called 'Low Power Wide Area Networks (LPWAN)' (Farrell, 2018). LPWAN are different radio technologies that aim to work using as little energy and as cost-efficient as possible while at the same time trying to maximize the radio range. They are often used in the IoT sector (Bardyn et al., 2016), where it is important to connect the highest possible number of devices. The aforementioned characteristics also predestine LPWANs for agriculture, where large arable land, livestock pastures, or stables exist. This is particularly evident in countries with huge farming areas such as China, the USA, or Australia.

Despite all the benefits for humans, animals, and the environment, smart farming also brings challenges (Barreto & Amaral, 2018). Given the current dependence of agriculture on digitalization, an outage of technology can potentially cause great damage. For example, the barn climate has a direct influence on the health of the animals (Schüller & Heuwieser, 2016), so an outage of the air-conditioning system is considered critical. The 'Federal Ministry of the Interior, Germany (BMI)' in 2016 issued an ordinance (Bundesministerium des Inneren, 2016), which lists, among others, the sectors energy, water, information technology, and telecommunications as critical infrastructures. Of particular note is the inclusion of the food sector. This encompasses agricultural companies, which, according to the ordinance, are particularly worthy of protection. To an increasing degree, the focus it hence put on implementing interconnectedness along the food supply chain in a crisis-proof manner (Muenzberg et al., 2013). This is reflected in current research approaches (Reuter et al., 2019), which support the idea of making smart farming resilient.

However, crises do not have to have the scale of a war or a nationwide environmental disaster to cause damage to agriculture and industry. Scenarios such as the outage (of parts) of the Internet or local emergencies also have significant potential to cause major damage. After Egypt was cut off from the rest of the Internet for five days in 2011, the cost to Egypt's economy was estimated to be at least $90 million (Kathuria et al., 2018). For countries heavily dependent on the internet, the authors estimate the damage at $23.6 million per 10 million inhabitants. Because of its enormous impact, research is also engaged in illuminating the scenario of internet outages (Aceto et al., 2018). Also, sector-specific phenomena like 'Agro-Terrorism' (Rohn & Erez, 2012) pose a potential threat in the field.

The research question that arises and which is to be answered in the context of this work reads as follows: *In times of increasing digitalization in agriculture, how can reliable data transmission to minimize or partly avoid the effects of local crises (outages of the internet/mobile network, radio gaps) with regard to operational safety-relevant processes, be realized?*

In this work, a data link & network layer is to be evaluated for a selected physical layer. It is important that integration into the existing IT landscape with minimum effort, high interoperability, and compatibility is possible. For this purpose, the existing protocols for the physical layer are examined. Taking into account current research, trends, and the increasing demands and framework conditions developed, our own concept is presented.

12.2 Related Work and Comparisons of LPWAN Technologies

LPWAN technologies are closely linked to the IoT, which is also gaining importance in agriculture. Raza et al. (2017) give a comprehensive introduction to the topic of LPWAN technologies in general. Chaudhary et al. (2018) analyze LPWAN technologies specifically in the IoT context. Here, they consider NB-IoT, RPMA, SigFox as well as LoRaWAN. Among other things, the different approaches, advantages and disadvantages, bandwidth, range, as well as the type of applications for which the respective technology is best suited are highlighted. Civelek (2017) also deal with LPWAN technologies but in the agricultural context. The author describes IoT as particularly useful for agriculture and highlights the increasing importance of wireless technologies. He also attributes to LPWAN technologies the increasingly important characteristics of security, reliability, low installation, and operating costs. In addition to mobile communication, WiMAX and LoRaWAN with long-range, WiFi, Bluetooth, and RFID with short-range are also compared with regard to agricultural applications. They recommend LoRaWAN for large ranges and Bluetooth 4.0 for short ranges. Finally, the author develops an application example and uses LoRaWAN as a transmission technology for a tractor data acquisition system. An idea for using LoRa-based peer-to-peer communication in emergency scenarios is found in the work of Höchst et al. (2020). They propose a low-cost companion device, consisting of a LoRa transceiver including an onboard Bluetooth chip that is connected via Bluetooth to a self-developed messaging app on a smartphone, which allows for infrastructure-less text communication. A practical evaluation shows that their approach could allow peer-to-peer chats with a communication distance up to 2.89 km in an urban environment with low-cost LoRa hardware. R. Xu et al. (2016) design and implement a LPWAN network based on the LR(Low

Table 12.1: Overview - LPWAN Technologies and Sources

LPWAN Technology	*Sources*
Sigfox	IoT Analytics GmbH, 2018, Brown, 2016, Mekki et al., 2018, Mekki et al., 2019, Madhumitha and Singh, 2017, Jung, 2017, Shi et al., 2019, W. Wang et al., 2019, Herlich and von Tüllenburg, 2018
NB-IoT	IoT Analytics GmbH, 2018 Mekki et al., 2018, Mekki et al., 2019, Madhumitha and Singh, 2017, Shi et al., 2019, W. Wang et al., 2019, Herlich and von Tüllenburg, 2018
LoRa(WAN)	IoT Analytics GmbH, 2018, Brown, 2016, Mekki et al., 2018, Mekki et al., 2019, Madhumitha and Singh, 2017, Jung, 2017, Shi et al., 2019, W. Wang et al., 2019, Herlich and von Tüllenburg, 2018
RPMA	IoT Analytics GmbH, 2018 Brown, 2016, Madhumitha and Singh, 2017, Jung, 2017, W. Wang et al., 2019, Herlich and von Tüllenburg, 2018
D7AP	Brown, 2016, Madhumitha and Singh, 2017, W. Wang et al., 2019
*Weightless-**	Brown, 2016, Madhumitha and Singh, 2017, Jung, 2017, W. Wang et al., 2019, Herlich and von Tüllenburg, 2018
MIOTY	W. Wang et al., 2019, Herlich and von Tüllenburg, 2018
NB-Fi	Madhumitha and Singh, 2017, W. Wang et al., 2019, Herlich and von Tüllenburg, 2018

Rate) WPAN standard 'IEEE 802.15.4' for monitoring critical infrastructure and facilities in cities. A long range is cited as a critical requirement for such a network. In a test bed, it could be shown that the system works well within a radius of about 3 km. A similar paper to the aforementioned article using LPWAN technology but set in the context of agriculture and critical infrastructure was not found at the time of the search. This work intends to take this circumstance into account. In the following, a comparison of different LPWAN physical layers is conducted in order to evaluate the most suitable physical layer, taking into account the context and previously defined requirements.

Due to the ability to bridge long distances with low energy expenditure, there is now a multitude of different LPWAN technologies, so it is first necessary to identify them and thus create an overview. Therefore, various papers, journals, and market analyses were considered, and the previously mentioned product analysis was used to provide the broadest possible overview of technologies from research and industry. Table 12.1 lists the identified LPWAN technologies and their researched sources.

Eight relevant LPWAN technologies could be identified, with Sigfox, NB-IoT, and LoRa(WAN) being the most popular, more specifically, the most widespread ones. The presented technologies and physical layer, as well as the characteristics

Table 12.2: Comparison — LPWAN Technologies — Part 1/2

	SigFox	*NB-IoT*	*LoRa(WAN)*	*RPMA*	*D7AP*
Technology	UNB	LTE	WB/SS	SS	2-GFSK
Band	ISM	LTE/GSM	ISM	ISM	ISM
Network Operation	ISP	ISP	ISP/Private	ISP/Private	Private
Data Rate	↑: 100 bps ↓: 600 bps	250 kbps	50 kbps	↑: 78 kbps ↓: 19,5 kbps	166 kbps
Range	50 km	10 km	30 km	15 km	2 km
Link Budget	159 dB	164 dB	154 dB	177 dB	140 dB

Table 12.3: Comparison — LPWAN Technologies — Part 2/2

	Weightless-N	*Weightless-P*	*Weightless-W*	*MIOTY*	*NB-Fi*
Technology	UNB/ DBPSK	NB/GMSK+ OQPSK	WS/ Variabel	UNB/ TS	NB/ DBSK
Band	ISM	ISM	WS	ISM	ISM
Network Operation	ISP/ Private	ISP/ Private	ISP/ Private	Private	ISP/ Private
Data Rate	↑: 100 bps ↓: n/a	100 kbps	1 kbps – 10 Mbps	407 bps	100 bps
Range	5 km	2 km	10 km	15 km	50 km
Link Budget	n/a	147 dB	Variabel	154 dB	176 dB

relevant for this work, are summarized in the following Tables 12.2 and 12.3. The feasible maximum values are always referenced. Since LPWANs by definition have a low energy consumption, which may vary depending on the scenario and the higher layers used, this characteristic is not included in the tables.

One of the most important requirements for a communication channel during a local crisis is provider-independent network operation (Gul et al., 2018). This eliminates the technologies SigFox and NB-IoT as potential candidates in the selection since they can only be operated via an 'Internet Service Provider (ISP)'. As explained in the beginning, agricultural areas are very large, which is why the range plays an essential role. The Weightless-N, Weightless-P, and D7AP technologies are ruled out because their range is - comparatively - too short. Moreover, Weightless-N only intends an uplink so that messages can only be sent but never received. Even though LPWANs do not achieve high data rates due to their technical characteristics, it is still desirable to achieve the highest possible data throughput. From this point of view, the MIOTY and NB-Fi technologies are eliminated because, at 407 bps and 100 bps, respectively, they do not reach the kbps mark as the rest of the technologies.

It is now to decide between the last three technologies, LoRa, RPMA, and Weightless-W. Of these technologies, LoRa has the highest range and Weightless-W the lowest. Weightless-W, on the other hand, allows the highest data rates and RPMA the lowest. One of the issues with Weightless-W is the utilization of 'TV white spaces'. These frequencies are not available or approved in all countries. In addition, distribution and hardware availability seems to be very limited. No freely available hardware components or information about networks in use could be found at the time of the research. Due to this and its relatively short range compared to the remaining technologies, Weightless-W is eliminated as a candidate.

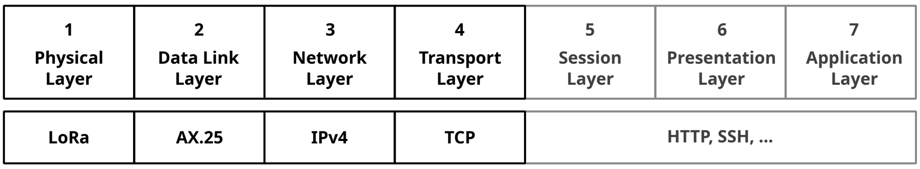
In direct comparison, LoRa has twice the range of RPMA. The data rates are, depending on the higher layer used, higher with LoRa (Symphony Link). Only in comparison with LoRaWAN (approx. 50 kbps), RPMA has an advantage in the uplink (78 kbps), but only a very low downlink (19.5 kbps). One advantage of RPMA is the use of the free 2.4 GHz band, where there is no duty cycle. In Rama and Özpmar (2018), the future safety of LoRa is predicted to be five times better than RPMA. This is also reflected in a product analysis, which has already identified LoRaWAN-capable products. The fact that there are two other productive LoRa-based protocols in addition to LoRaWAN, namely Symphony Link and DASH7, underscores this assessment. In the conference paper of Vangelista et al. (2015), LoRa is described as the most promising technology in the field of 'wide-area IoT'. Another advantage is the broad hardware availability from low-cost DevKits to complete gateways. Based on the arguments presented, LoRa is preferable to RPMA in direct comparison for the present scenario.

12.3 Concept: LoRa + AX.25 + IPv4 + TCP

In Nolan and Kelly (2018), a data link layer protocol - a variation of the X.25 protocol - is specially adapted for amateur radio and specifies, inter alia, the communication via frames (Beech et al., 1997). It is mainly used for 'Packet Radio', which is to be understood as the sending and/or receiving of digital data packets between two end devices via a radio channel. If more than one device participates, it is also called a 'packet radio network'. AX.25 performs typical data link layer tasks such as establishing a connection between two end devices or providing wireless channel access.

For packet radio communication using AX.25, a modem connected to a 'Terminal Node Controller (TNC)' is required. This serves as an interface between the terminal device and the modem by means of a serial connection. End devices in an AX.25 network either communicate directly with each other or can be arranged in any topology. If the radio signals of two terminals do not reach each other due to too great a distance, they can be forwarded to the destination by one or more digipeaters, which, however, requires a-priori knowledge of the topology. The 'Carrier Sense Multiple Access with Collision Resolution (CSMA/CR)' method is used to control access to the radio channel. To identify subscribers, a six-digit 'call sign' ID is specified as the MAC address. Correspondingly, an AX.25 frame contains at least one source/destination address for addressing and, in the case of source routing using digipeaters, the addresses of the respective intermediate stations.

Since the current specification follows the OSI model, it is possible to use a variety of higher layers. For example, this is utilized by the ‘AMateur Radio Network (AMPRNet)’, where TCP/IP is used as a transport and network layer together with AX.25 as a data link layer. Since 1981, an entire class-A network is available for the use of IP in amateur radio networks with the regulated 44.0.0.0/8 address block, of which some blocks have been sold so far. The reserved private class-C address block 44.128.0.0/16 is, however, open to any amateur radio operator. To send AX.25 frames to a TNC via serial interface, a protocol is required. Nowadays, the ’Keep It Simple, Stupid (KISS)’ protocol is most commonly used for this purpose, which was developed primarily for the use of IP over AX.25 (Chepponis & Karn, 1987). The flexibility of the OSI model for higher layers also applies to the physical layer in AX.25, as shown in Figure 12.1. Thus it would be possible to use a LoRa modem with suitable firmware for a TNC and hence enable TCP/IP communication via LoRa. Accordingly, only TCP/IP capable (legacy) systems would be available for direct integration into a network. This concept is to be implemented and carried out in the next step.



1 Physical Layer	2 Data Link Layer	3 Network Layer	4 Transport Layer	5 Session Layer	6 Presentation Layer	7 Application Layer
LoRa	AX.25	IPv4	TCP	HTTP, SSH, ...		

Figure 12.1: Concept of LoRa + AX.25 + TCP/IPv4 in the OSI Model

12.3.1 Test Bed: IP-Communication via LPWAN

For the purpose of evaluation, we implement the concept in the form of a test bed that should allow TCP/IP communication over LoRa. Regardless of the explicit test set-up, some components are needed to realize the test bed. First, the actual modem that supports the selected LoRa technology is required to establish a wireless connection. The modem, on the other hand, is typically embedded in a micro-controller platform. This platform can then be used to equip gateways with it so that they can establish a wireless connection via LoRa. Finally, two arbitrary terminal devices are needed that communicate with each other via TCP/IP.

Modem

LoRa is a technology patented by Semtech. Accordingly, LoRa modems are only available directly from Semtech or from licensed companies such as HopeRF. With the SX1260/1270/1300 chip family, Semtech has several LoRa modems that differ mainly in the supported bandwidth and frequency. In this work, a modem with the Semtech SX1276 chip is used (Semtech Corporation, 2020). This supports the frequencies released in Europe and offers a link budget of up to 168 dB with a low power consumption of 9.9mA during the reception.

Micro-controller

In order to use a LoRa modem, a micro-controller is needed to drive and control it. Generally, any platform can be used that allows an appropriate connection of the modem, for example, by means of UART pins. Further peripheral components complete the platform. This includes the SMA board for the connection of an antenna. For this work, the micro-controller ATmega1284P from Microchip is used. It offers 128 kB programmable flash and 1k kB RAM. As developer board, the RNode (see Figure 12.2) from unsigned.io is used (Qvist, 2018b), which offers a USB port for communication. The selection is justified by the fact that this board offers the most mature firmware for a required KISS-TNC.

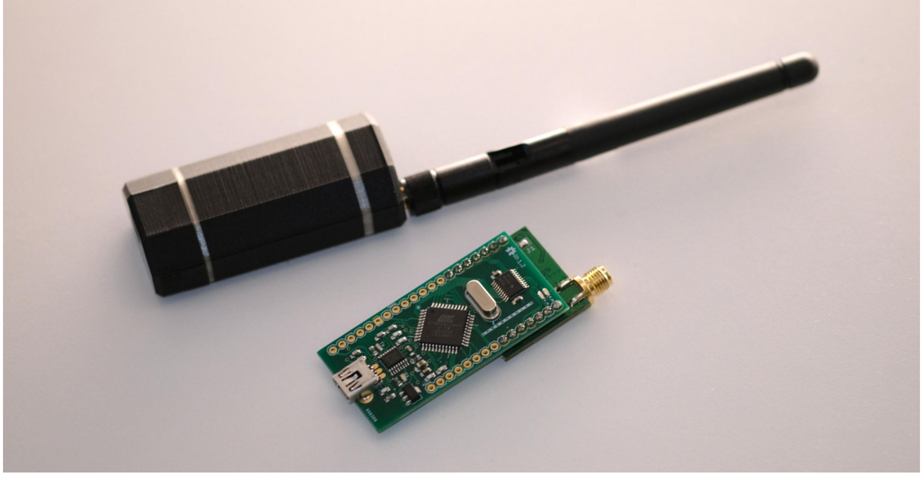


Figure 12.2: One RNode with case and the plain circuit board

Gateways

To communicate with two RNodes via TCP/IP, each node must be connected to a gateway. For the gateways, any hardware can be used that has a USB port, supports a Linux distribution, and offers an additional network interface such as LAN or WLAN. For portability reasons, a virtual machine (VM) is used for the first gateway. The resources of a VM can also be changed to runtime so that it is possible, among other things, to extend it with any network adapters and networks. Debian 10.3.0 is used as the operating system. For reasons of mobility, a laptop is used for the second gateway.

End Devices

To demonstrate and evaluate the concept, two end devices are needed that communicate with each other using TCP/IP. These are implemented as VMs for the same reasons as the first gateway. Here, the flexibility of the operating system and the associated software offer also play a major role.

12.4 Study Design

The utilized hardware has to be structured and arranged in a network topology. The following Figure 12.3 shows the individual components, required networks, and IP addresses of the test setup:

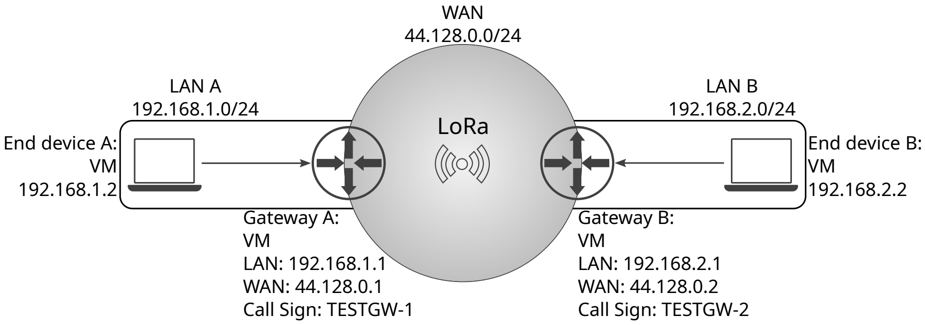


Figure 12.3: Schematic Illustration of Test Setup

If end device A wants to communicate with its counterpart B, the data is first sent to the local gateway A. The gateway knows a route to LAN B via gateway B and routes the data accordingly via the LoRa AX.25 WAN link. Gateway B finally forwards the data to end device B as the final destination. Vice versa, the same process applies to communication from B to A.

The described experimental setup is varied by the following parameters:

Distance

To test the range of the LoRa AX.25 WAN link in the existing hardware constellation, three different distances are to be covered in line-of-sight, resulting in three series of tests, as shown in Table 12.4:

LoRa Parameters

As already discussed, LoRa can be influenced by the parameters frequency, spreading factor, bandwidth, and coding rate (Augustin et al., 2016). The frequency used is 869.4 MHz for all settings. The frequency is not varied due

Table 12.4: Test Series

	Aim	*Distance [m]*
Series A	feasibility	10
Series B	medium range functionality	100
Series C	long range functionality	1,000

to radio regulation. The maximum duty cycle of 10% is possible in the bands between 869.4 and 869.65 MHz, so a frequency within this range was chosen. For the remaining parameters, three different constellations are described below, which, similar to the test series, are intended for short, medium, and long distances, respectively, as shown in Table 12.5:

Table 12.5: LoRa Settings

	Application Scenario	*Spreading Factor*	*Bandwidth [MHz]*	*Coding Rate*
Setting 1	short distance, high data rates	7	250	1
Setting 2	medium range, lower data rate	9	125	1
Setting 3	maximum range and reliability	12	125	1

This provides 9 combinations of test series and LoRa settings.

12.4.1 *Implementation*

Since the required AX.25 packages are not included by default in the Linux distributions being used, they must first be post-installed on both gateways:

```
# sudo apt install libax25 ax25-apps ax25-tools
```

The next step is to configure the AX.25 Data Link Layer. The following entry is added to the file /etc/ax25/axports:

```
ax0 TESTGW-X 115200 484 5 LoRa Gateway
```

Here, 'ax0' stands for the name of the AX.25 port and 'TESTGW-X' for the AX.25 call sign ID, the X having to be replaced correspondingly with gateway A by 1 or with B by 2. The number '115200' represents the baud rate, '484' represents the MTU, and '5' represents the window size. These values are specified by the platform firmware used, only the window size can be changed. However, since this is used by the platform developer, no changes are made. The last option serves as a free description text.

When the data link layer is ready for use, the network adapter can be configured. The file /etc/network/interfaces.d/ax0 is created for this purpose and provided with the following static IP settings:

```
iface ax0 inet static
    address 44.128.0.X
    netmask 255.255.255.0
    network 44.128.0.0
    broadcast 44.128.0.255
    pre-up kissattach /dev/ttyUSB0 ax0
    post-down pkill -9 kissattach ; rm -f \
        /var/lock/LCK..ttyUSB0
```

Here, in the same manner as further above, the 'X' must be replaced by 1 or 2 respectively.

Now it is necessary to connect the RNode platforms to one of the gateways via USB. Usually these are available under the file `/dev/ttyUSB0`. In order for an RNode to function as TNC, it is necessary to put it into TNC mode. For this, the 'RNode Configuration Utility' (Qvist, 2018c) can be used with the following command:

```
# sudo ./rnodeconf /dev/ttyUSB0 -T --txp 17 --freq \
  869400000 --bw 250 --sf 7 --cr 1
```

The parameter 'T' is required to place the RNode under `/dev/ttyUSB0` in TNC mode and 'txp' for setting the radio strength in dBm. Subsequently, the frequency is given through 'freq', followed by the setting 'bw' for the bandwidth. Finally, the spreading factor is determined with 'sf' and the chip rate is being set with 'cr'. Depending on the LoRa setting, the command must be adjusted accordingly.

It is then possible to make the Linux network interface available under the name ax0:

```
# sudo ifup ax0
```

The command in the pre-up operation causes the USB-connected RNode to be used as TNC and initialized from the 'axports' file with the previously defined setting named ax0.

From this stage on, it is possible for the two gateways to communicate with one another via their respective network interface ax0. Static ARP entries help to reduce network load. In order to enable terminals of the different networks which are also connected to LAN ports to communicate with one another, routes to the respective LAN network must be introduced to the gateways. To expand the ARP/routing table of Gateway A accordingly, the arp or ip configuration tool is being applied:

```
[root@GatewayA ~]# arp -s -H ax25 44.128.0.2 \
                   TESTGW-2
[root@GatewayA ~]# ip r add 192.168.2.0/24 via \
                   44.128.0.2
```

For gateway B, the command reads:

```
[root@GatewayB ~]# arp -s -H ax25 44.128.0.1 \
                   TESTGW-1
[root@GatewayB ~]# ip r add 192.168.1.0/24 via \
                   44.128.0.1
```

In order for the Linux Kernel to route the received IP packets, the associated functionality must finally be activated on both gateways:

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

At the very last, the static IP settings must still be made on the terminals in accordance with the mapping of the test setup. Since this is different, depending on the terminal and operating system used, and does not represent any challenge, it will not be discussed in detail.

12.5 RESULTS

In order to obtain unadulterated results, the measurements are carried out with the two gateways. The regular network parameters data rate, latency, and packet loss are measured for the combinations of test series/LoRa settings. This results in a total of 9 measuring points for each network parameter, providing a total of 27 measurements.

Data Rate

To determine the data rate, the frequently used open-source software iperf3 for network measurements is being applied. iperf3 is realized through a client / server application, so that a gateway displays the iperf3 server and the other combines to this as client.

First, iperf3 version 3.1.3 is launched in the verbosen TCP-server mode on gateway A and the report interval on two seconds is set:

```
[root@GatewayA ~]# iperf3 -s -V -i 2
```

To launch the measurement, the verbose iperf3 client mode is executed on Gateway B with the following command:

```
[root@GatewayB ~]# iperf3 -c 44.128.0.1 -V
```

Depending on the LoRa setting and distance, it is necessary to limit the number of bytes to be transmitted, otherwise the transit times become too long. This can be influenced with the parameter 'n', so instead of time-based transfer with the following command 10240 bytes data are transferred:

```
[root@GatewayB ~]# iperf3 -c 44.128.0.1 -V  -n 10240
```

Table 12.6: Measurements - Test Series A, 10 Meter

	Data Rate [kbps]	*Latency* [ms]	*Packet Losses* [#packets]
LoRa-Setting 1 (SF=7; BW=250 kHz; CR=1)	4,30	385,928	0
LoRa-Setting 2 (SF=9; BW=125 kHz; CR=1)	1,02	1322,451	0
LoRa-Setting 3 (SF=12; BW=125 kHz; CR=1)	0,0547	8471,749	0

Latency and Packet Loss

To determine the latency and the number of lost packets, the 'Internet Control Message Protocol (ICMP)' and the application 'ping' contained in the operating system are inserted. For TCP latency measurements, applications such as nuttcp or qperf are also available, which, however, cannot run with all LoRa settings. Instead of measuring the packet loss of the TCP protocol, it can already be determined at IP or ICMP level. The micro-controller platform offers relatively little RAM and buffer for the TCP protocol compared to fully developed gateway hardware, therefore a packet loss could be due to these circumstances. In order to measure the quality of the link and not to explore the hardware limits, the packet loss is therefore determined without the TCP.

To get an empirical average, the number of sent ICMP packets is increased to 100, and the operation is started with the following command:

```
[root@GatewayB ~]# ping −c 100 44.128.0.1
```

Thereafter, Gateway B begins sending sequential ICMP echo requests to Gateway A. After receiving the ICMP echo response from Gateway A, the complete circulation time of the ICMP packet pair is issued as the measurement result.

For higher transit times, it is necessary to adjust the default setting of the timeout and transmission interval, otherwise incorrect measurements will likely occur. For a timeout of 10 seconds using parameter 'W' and a transmit interval of 10 seconds with parameter 'i', the command reads:

```
[root@GatewayB ~]# ping −c 100 44.128.0.1 −W 10 −i 10
```

Results of the different test series measurements are shown in three Tables 12.6, 12.7 and 12.8. In the results of the data rate and latency, the measured values each reflect the mean value of the test.

As can be derived from the measurements, the LoRa radio connection is stable at 10 meters with all settings since no packet losses have occurred. The maximum data rate and minimum latency are achieved with LoRa-Setting 1. LoRa-Setting 3, which is explicitly intended for large distances, provides the lowest data rate and highest latency values. The measurement results show that even at 100

Table 12.7: Measurements - Test Series B, 100 Meter

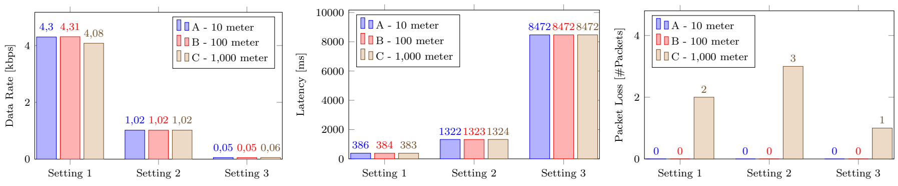
	Data Rate [kbps]	*Latency* [ms]	*Packet Losses* [#packets]
LoRa-Setting 1 (SF=7; BW=250 kHz; CR=1)	4,31	384,037	0
LoRa-Setting 2 (SF=9; BW=125 kHz; CR=1)	1,02	1322,658	0
LoRa-Setting 3 (SF=12; BW=125 kHz; CR=1)	0,0543	8471,936	0

Table 12.8: Measurements - Test Series C, 1,000 Meter

	Data Rate [kbps]	*Latency* [ms]	*Packet Losses* [#packets]
LoRa-Setting 1 (SF=7; BW=250 kHz; CR=1)	4,08	382,778	2
LoRa-Setting 2 (SF=9; BW=125 kHz; CR=1)	1,02	1323,771	3
LoRa-Setting 3 (SF=12; BW=125 kHz; CR=1)	0,0552	8472,444	1

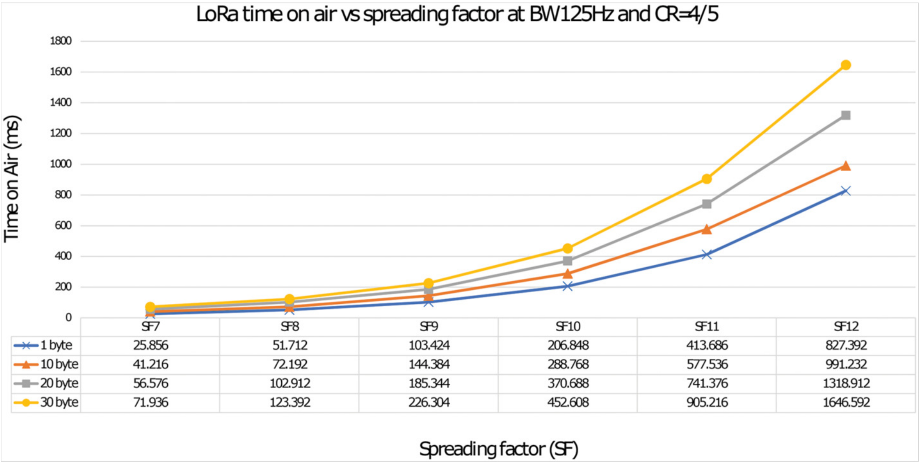
meters the radio connection is stable for all settings since no packet loss has occurred. From the results of the 1,000 meter test series, it can be deduced that the radio connection has some packet losses. However, these are so small that the radio connection can be regarded as fairly stable. The lowest packet loss is seen in LoRa-Setting 3, which, however, provides the worst data rate and latency.

As can be followed from the measurements, the LoRa-Settings have a decisive influence on data rate, latency, and packet loss. The settings differ in the spreading factor and partly in bandwidth, with a constant coding rate of 1. The LoRa-Settings 2 and 3, which differ only in the spreading factor, indicates that changes on these level have an impact on the measured data rate and latency. The Figures 12.4a, 12.4b, and 12.4c illustrate the relationship of the individually measured parameters to the respective LoRa settings for each test series.



(a) Data Rate (b) Latency (c) Packet Loss

Figure 12.4: Measured parameters of the three LoRa settings (1, 2, 3) for each range series (10 m, 100 m, 1000 m).



	SF7	SF8	SF9	SF10	SF11	SF12
1 byte	25.856	51.712	103.424	206.848	413.686	827.392
10 byte	41.216	72.192	144.384	288.768	577.536	991.232
20 byte	56.576	102.912	185.344	370.688	741.376	1318.912
30 byte	71.936	123.392	226.304	452.608	905.216	1646.592

Figure 12.5: Calculated LoRa Airtime vs. Spreading Factor, Source: Durand et al. (2019)

The correlation between transmission time and different packet sizes is illustrated in Figure 12.5. The bandwidth and coding rate are the same as LoRa-Settings 2 and 3. The figure reveals that an increase in the spreading factor is accompanied by a reduction in the data rate or, conversely, an increase in the transmission time required. The calculated values can be derived directly from the LoRa technology. The document 'LoRa Modulation Basics' from Semtech is available for this purpose, which contains a detailed derivation (Semtech Corporation, 2020).

12.6 Discussion

The selection of measurement applications showed that, for example, `nuttcp` or `qperf`, especially with low throughput and high latency as given with LPWAN technologies, do not work reliably and could be optimized for these. Operating system standard tools such as ping or netcat, on the other hand, prove to be fully functional even under these conditions with certain parameters. Special measurement applications for LPWAN and similar technologies would be desirable.

The slight variations in the measured values from different test series and one LoRa setting in particular illustrate the long-range character of the technology and the potential for bridging long ranges. In general, the fluctuations are within normal measurement tolerances, although at 1,000 meters, the somewhat larger deviations could be attributed to interference factors in the measurement path. In general, LoRa-Setting 1 delivers the best-measured values in all test series. Since even at the largest tested distance of 1,000 meters, the measured values are similar or equal to those of the previously tested distances, it can be concluded that much larger ones could be bridged. This is also consistent with the researched ranges of the physical layer comparison from Section 12.2.

The successfully tested functionality of TCP and application protocols such as HTTP and SSH enables a whole range of different scenarios for monitoring or operating IT systems relevant to operational security in the event of a local crisis. In the case of HTTP, it is particularly noticeable that it remains functional in principle even with the low data rate and high latency of LoRa-Setting 3. In principle, the data rates achieved should also be sufficient for other application protocols based on TCP, such as the text-based protocols Telnet or SMTP/IMAP. Database connections or file transfers via FTP are also possible scenarios.

The limits of the test bed can be seen in the hardware used, among other things. The RNode developer platform has only very limited capacities and buffers, which are particularly important for the TCP protocol due to the connection orientation. Since the associated firmware is mainly developed by a single person and is intended for test purposes, it also has its limits when dealing with TCP. Whether a special application is ultimately functional with the concept or with technologies that have a low throughput and high latency depends on the protocol used and the individual application behavior, such as hard-coded timeouts. Another limitation is the SMA antenna with dimensions of only L105 × W10 × H10 mm. Especially at very large distances, an exchange is necessary in order to continue to exploit the range advantage of LoRa technology and to ensure a more stable connection (Qvist, 2018a). Height positioning also plays an important role. For the same reasons, the height used in the test bed for positioning the antenna should be further increased by approx. two meters for large distances.

The tested application protocols, hardware components, and the test bed itself consequently hold potential for optimization. For HTTP, it is advisable to utilize the cache mechanisms contained in the protocol. If the requested data has not changed, this saves having to retransmit data when pages or functions are called, so that applications respond faster or better overall. Besides, the use of the SSH protocol can also be optimized. Continuous performance could be further increased by appropriate hardware. A platform with sufficient computing power and memory for buffers, as well as improved firmware optimized for TCP, could additionally increase the data rate. For long distances, as is common in agricultural fields, the range can be optimized by appropriately dimensioned and height-positioned antennas. However, even with the small antenna used, an increase is still achievable at 1,000 meters, as the technical evaluation shows.

12.7 Conclusion and Future Work

The research question that we posed in Section 12.1 is as follows: *In times of increasing digitalization in agriculture, how can reliable data transmission to minimize or partly avoid the effects of local crises (outages of the internet/mobile network, radio gaps) with regard to operational safety-relevant processes, be realized?* To give an answer to this question, we firstly developed a concept based on our assessment of requirements and available (technical) options. Our concept allows the usage of *classic* IP-based communication protocols via a LoRa communication channel. This could be useful, e. g., to create redundant data transmission for critical information, like error messages of cattle shed air-ventilation systems, or to connect multiple stakeholders in cases of an Internet outage. Both examples of use could be mission-critical for the food production of an agricultural company. An implementation in the form of a test bed was able to confirm the general feasibility of our concept for different application protocols, distances, and settings.

Of interest would be further investigations of LoRa technology in the context of TCP. This includes the optimization potential of the test bed mentioned in the discussion. Since the full range potential of LoRa technology is not yet exhausted in the test bed, it would be of further interest to explore the limits with the given hardware. Also the AX.25 protocol supports more features, like so-called 'digipeaters', that allow packet forwarding over several hops, so even greater distances could be bridged than possible with a point-to-point connection. The development of a KISS/TNC firmware for more powerful hardware platforms would also be desirable, thus allowing more test scenarios to be evaluated that do not fail due to hardware or firmware limitations. Last but not least, the point of IT security could also be considered specifically for the scenario of critical infrastructures and their communication channels. In the future, it can be assumed that research will look at other IP-based solutions for LPWAN technologies and focus more on TCP since marketable solutions already exist for UDP. Thus, similar to the SCHC technology designed for UDP, which is currently still being standardized at the IETF, a variant for TCP would be conceivable. It remains uncertain which of the LPWAN technologies will prevail in the future within agriculture and in which protocol composition. However, it has been shown that LoRa technology is a promising candidate for this.

13

RURAL COMMUNICATION IN OUTAGE SCENARIOS: DISRUPTION-TOLERANT NETWORKING VIA LORAWAN SETUPS

Abstract Since communications infrastructure is subject to many impacts, e.g., destructive natural events, it can potentially collapse at any time. Especially in rural areas, the recovery of public network infrastructure can take some time, so a dedicated communication channel would be advantageous. We explore the possibility of transforming commodity LoRaWAN gateways into meshed network nodes for a digital emergency communication channel. In order to obtain the required parameters, we collected farm locations in Germany with OpenStreetMap. Based on the assumptions of LoRa communication range and considering our use case requirements, connecting farm communities seems theoretically feasible in many areas of our data set. To further analyze our idea, we ran simulations of two common DTN routing protocols with different scenarios. A proof-of-concept implementation allows smaller messages to be transmitted using real hardware and demonstrates that a decentralized communications infrastructure based on commodity hardware is possible.

Original Publication *Kuntke, F., Baumgärtner, L., & Reuter, C. (2023). Rural Communication in Outage Scenarios: Disruption-Tolerant Networking via LoRaWAN Setups.* Proceedings of Information Systems for Crisis Response and Management (ISCRAM)*, 1–13. http://dx.doi.org/10.59297/WZMQ1124*

Acknowledgments This work was supported by funds of the German Government's Special Purpose Fund held at Landwirtschaftliche Rentenbank in the projects Geobox-II and AgriRegio, as well as by the funds of the LOEWE initiative (Hesse, Germany) within the emergenCITY centre and the German Research Foundation (DFG) in the Collaborative Research Center (SFB) 1053 MAKI.

13.1 Introduction

The ability to communicate over long distances using technical devices is of great importance to modern society. In agriculture, communication plays a critical role when multiple farmers rely on shared labor and equipment to harvest cropland within tight time windows. Although easy to overlook, it should be noted that agriculture is generally considered a critical infrastructure with the responsibility to produce the required amount of food to sustain people's basic livelihoods. Serious efforts should be made to strengthen technology for this sector in many ways, as the technologies used in this sector are said to have comparatively poor resilience capacities (Kuntke, Linsner, et al., 2022).

Currently, the terms Agriculture 4.0 and Smart Farming are used to highlight several developments towards automated data generation and exchange between different stakeholders in the entire food production chain, by incorporating current trends in Information Technology (IT), such as the Internet of Things (IoT) and Cloud Computing (Rose & Chilvers, 2018). As a logical consequence, the continuation of the vision of field robots also results in an increased need for communication between devices, such as autonomous vehicles, weather stations, sensors, and actuators. In order to meet the increasing demand for data exchange, while at the same time ensuring energy efficiency, so-called Low Power Wide Area Networks (LPWANs) have been established in certain areas of application, e.g., to connect a large number of sensors. A prominent representative of this technology category is the Long Range Wide Area Network (LoRaWAN), which allows the development of autarkic IoT networks. As already described, not only machinery depends on communication, but also farmers require reliable line communication between each other. An exemplary use case is the bundling of labor and machinery of neighboring actors during harvest. This use case is particularly important for efficient agriculture in small-structured agricultural regions, as e.g. in Germany.

In the event of major internet outages – which are not unlikely (Grandhi et al., 2020), although their duration and extent cannot be predicted – basic data exchange would still be possible in self-established LoRaWAN networks. This leads to the idea of using this technology in crisis situations – especially when the general communications infrastructure is broken. The possibility to change the usual LoRaWAN star-of-star topology to build multi-hop networks has already been investigated in various works (Centelles et al., 2021). Promising approaches utilize Disruption-Tolerant Networking (DTN) to increase the success rate of delivering messages in crisis situations with rather unpredictable networking resources (Baumgärtner et al., 2020a). Two downsides, however, to the approaches most commonly described in literature are (1) the incompatibility with default LoRaWAN networks, leading to devices that only have the single-purpose of crisis-communication, and (2) the requirement of custom firmware for most developer devices, making the approaches hard to use for IT-laypeople. But as the distribution of LoRaWAN hardware increases, especially in the domain of agriculture, we can see the benefit of enhancing the software stack behind a commodity LoRaWAN gateway to allow messages to be exchanged between neighboring farms up to several kilometers apart. This approach would connect rural communities that have LoRaWAN hardware for common IoT applications in the event of a crisis. Since no *expert* hardware will be needed, the approach can be made to work with just installation of our software addition - which at best is already running in the background before a crisis event - and can thus be more inclusive than other approaches.

This core question of this work is therefore: *How can LoRaWAN-based IoT setups be utilized to allow DTN-based peer-to-peer communication?* As part of our work, we make the following contributions:

- A novel tool[1] for calculating geographic statistics for wireless network planning based on OpenStreetMap data
- A concept that allows to send/receive payloads in a LoRaWAN-conform manner via commodity LoRaWAN gateways, along with a prototypical implementation
- An evaluation of the concept through simulations of 40 farm neighborhoods in two scenarios, comparing performance of two DTN routing mechanisms
- A novel software library `chirpstack_gwb_integration`[2] as a companion to ChirpStack LoRaWAN Network Server, working with commodity hardware allowing to send/receive arbitrary payloads in a LoRaWAN-conform manner
- A novel software `spatz`[3] that builds a DTN routing, utilizing `chirpstack_gwb_integration`

The developed tools and evaluations were conducted with the application area of agriculture in mind, but can also be transferred to other areas – especially where IoT technology is already being used.

13.2 Background

In this section, a brief overview of LoRa, LoRaWAN, DTN and the DTN Bundle Protocol are given and related work in the field of adapting LPWAN technologies is presented.

13.2.1 *LoRaWAN and LoRa*

LoRaWAN was standardized by the LoRa Alliance, 2015. LoRaWAN is a popular LPWAN technology that adjusts and modulates signals using an exclusive proprietary spread spectrum technology in the sub-GHz-ISM band. The physical layer of LoRaWAN is LoRa, which stands for *Long Range*. LoRa operates in the unlicensed ISM band (e.g., in Europe 433/868 MHz, in North America 915 MHz). Depending on the region, a duty cycle regulation may apply, for example 1% in Europe for 868 MHz. As shown by Vejlgaard et al., 2017, interference issues are possible when the unlicensed bands are widely used in an area. The level of such interference issues is expected to grow with the deployment of more wireless IoT solutions. However, this problem mainly concerns urban deployments, while in this work we focus on rural areas, especially agricultural areas.

[1] https://github.com/PEASEC/distance-statistics
[2] https://github.com/PEASEC/LoRaWAN-DTN/tree/main/chirpstack_gwb_integration
[3] https://github.com/PEASEC/LoRaWAN-DTN/tree/main/spatz

LoRa works with Chirp Spread Spectrum (CSS) as a modulation type. A coding rate indicates the rate of the Forward Error Correction (FEC), whereby the value 4/5 is used for standard LoRa frames. LoRa allows for six different spreading factors (SF7 to SF12) to balance the signal scattering factor (and thus the range), the data rate, and the energy consumption. The spreading factors define the number of symbols. A sinusoidal signal sequence or transmission pulse is referred to as a symbol. The number of bits that can be represented by a symbol corresponds to the SF. The maximum payload (`MACPayload`) capacity is 250 bytes (LoRa Alliance Technical Committee Regional Parameters Workgroup, 2021).

The LoRaWAN standard uses LoRa as a transmission technology (with predefined settings on code rate, SF, bandwidth) and defines the used architecture, as well as LoRaWAN-compliant devices. A LoRaWAN setup is a stars-of-stars topology, with $1..n$ end-devices transmitting data (encapsulated into LoRa frames) to $1..m$ gateways, which itself are connected (via IP) to a single network server. For different regions, different specific transmission preferences exist, which are allowed and respect the local free ISM bands. LoRaWAN itself allows for different data rate configurations, that are a combination of SF and bandwidth, depending on the regional parameters (LoRa Alliance Technical Committee Regional Parameters Workgroup, 2021). For Europe (SRD860, 863-870MHz), data rate 0 is the long range configuration with SF 12 and 125 kHz bandwidth, and data rate 6 is the fastest LoRa transmission configuration, with SF 7 and 250 kHz bandwidth. Of course, a wireless data transmission technology is also subject for security attacks, and despite the fact that LoRaWAN also takes into account several security aspects in the protocol design, there is still a known attack surface that should be taken into account when developing and deploying IoT systems based on this technology (Kuntke, Romanenko, et al., 2022).

13.2.2 *Disruption-Tolerant Networking*

Disruption-Tolerant Networking (DTN), also called Delay-Tolerant Networking, receives increasing attention for various applications, as it allows for a resilient and flexible data exchange in challenging network conditions. DTN solutions are commonly based on a *store, carry, and forward*-approach. Here, network participants act as *data-mules* and physically carry around and opportunistically exchange data with other nodes encountered. Therefore, it is not suitable for real-time applications such as video conferencing or other applications that require a stable end-to-end connection, but provides robustness and fault tolerance for applications that can tolerate delays in data dissemination, e.g., messaging, sensor data, or file sharing. Here, one area of application is disaster communication, in case of network infrastructure outages, e.g. after natural disasters (Setianingsih et al., 2018; Zobel et al., 2022). The Bundle Protocol Version 7 (BP7) is the most recent Internet Engineering Task Force (IETF) standard (Burleigh et al., 2022) for such a DTN architecture. Additionally, different routing algorithms, e.g., epidemic routing or Probabilistic Routing Protocol using History of Encounters and Transitivity (PRoPHET) (Lindgren et al., 2012) can be used for distributing the bundles. This enables optimization for various properties such as fast/reliable bundle delivery or a minimum number of duplicates in the network. Besides advanced routing decisions that take into account, for example, geographic locations (Baumgärtner et al., 2020a; P.-C. Cheng et al., 2010; Sánchez-Carmona et al., 2016), there also exist other metrics which affect data dissemination across different convergence layers, e.g., duty-cycle restrictions when using LoRa (Msaad et al., 2021) or the workload of the involved nodes (W. Wang et al., 2021; S. Zhang et al., 2013).

13.3 Related Work: Adapting LPWAN

Previous research approaches have already investigated multi-hop networks using LPWANs. For example, Abrardo and Pozzebon, 2019 describe a LoRa network where the network topology is changed to bridge the route to the gateway through other nodes. The resulting sensor network based on LoRa was used to perform measurements in an underground environment that only allows for a maximum range of 200m. Zguira et al., 2018 utilize a 802.11p-based multi hop network to transmit sensor data of shared bikes to base stations.

Other publications, such as Abrardo et al., 2019 or Dias and Grilo, 2018 are concerned with increasing the range of the network while simultaneously saving the energy of the end devices by reducing the necessary transmission power by shortening the distance to the receiver, as the receiver is the closest sensor. To realize this, they rely on multi-hop networks. Furthermore, other contributions, such as the work of Ebi et al., 2019, describe using multi-hop LoRa-networks in other range-critical situations. Instead of a star or linear topology, they are based on a mesh network topology. Further studies such as H.-C. Lee and Ke, 2018 and Huh and Kim, 2019 describe the extension of the network's coverage through a mesh network. However, the data from sensor nodes is always forwarded to the base station (gateway) via other sensor nodes in order to expand large sensor networks.

Other work is investigating the use of LPWAN-based networking technologies to increase resiliency, e.g., in the form of a long-range wireless data channel for TCP/IP-based network hardware (Kuntke, Sinn, & Reuter, 2021). Vigil-Hayes et al., 2022 describe a system that combines high bandwidth networks with LPWAN to extend internet coverage. *"The key idea behind this paradigm is that a useful set of service calls can be partially completed with limited data rate transfers and then fully completed when high bandwidth access is available."* (Vigil-Hayes et al., 2022, p.196). The transmission range of their test setup was only 400m with line-of-sight in an urban region, which could be due to the fact that rather small chips were used for LoRa transmission.. The aspect of addressed communication between two end nodes or end node and gateway is also addressed in some other works, but communication between two gateways is not intended. The protocol on the data link layer (OSI-layer 2) is modified and extended in some studies. A communication system cannot be implemented using the procedures described above. Such a system would be based on the physical layer and would require a replacement of the previously used protocol on the data link layer.

A related approach for bidirectional communication is the Serval Project (Gardner-Stephen, 2011). The underlying purposes of Serval Mesh are crisis communication and the provision of basic mobile communication for low-income or isolated communities (Gardner-Stephen & Palaniswamy, 2011). While being independent of further hardware, the Serval Mesh application utilizes the WiFi function of Android-driven smartphones. It features a *store, carry and forward*-architecture through which text messages, calls, and data transmissions are made available. Therefore, an advantage of this approach is that a cost-effective physical layer is created that is detached from local providers. However, the use of WiFi technology in the Serval Project entails the disadvantages of incompatibility issues and reduced range compared to LoRa (Gardner-Stephen & Palaniswamy, 2011). To resolve the range limitation, inexpensive and weatherproof extenders which use UHF to allow for long-distance connections have been designed (Gardner-Stephen et al., 2017).

Höchst et al., 2020 connect smartphones via Bluetooth with LoRa capable microcontroller boards. A specific chat application allows the smartphone user to send SMS-like messages as LoRa signals to other users. The developed system allows for device-to-device communication with an experimentally evaluated range of up to 2.89 km.

Baumgärtner et al., 2020a describe a similar application that differs from our approach in several ways. Firstly, it is based on the scenario of immediate crisis communication in environments without any ICT, while our goal is to build a communication network that can serve as a substitute for internet-based communication also in the medium and long term, where previous existing ICT is damaged. Secondly, a major difference lies in the choice of hardware needed for the implementation, which is also rooted in the scenario choice: While Baumgärtner et al., 2020a have developed additional battery-powered, low-cost relay nodes and pager devices, our project aims at utilizing only already installed commodity LoRaWAN gateways for communication purposes. By this way, our system does not need specific actions regarding crisis prevention, but is just available for all farms that use LoRaWAN IoT technologies.

Therefore, the aim of our work is to design and implement a concept that enables addressed communication between LoRaWAN gateway hardware in a multi-hop network without internet access. In doing so, the advantages offered by the physical layer of LPWAN technologies are to be utilized. This concept is intended to ensure the resilient transmission of messages and to develop a communication system. The use case and exemplary scenario are presented in the following section.

13.4 Use Case and Scenario: Emergency Communication for Agricultural Areas

Farmers in developed countries are increasingly adopting smart farming technologies involving IoT solutions. To our understanding, LoRaWAN has a high standing in this domain, probably due to low-cost sensors and low sequential costs. To build up resilience capacities regarding communication infrastructure in this domain, we see an opportunity to leverage the increasing adoption of LoRaWAN setups for a self-operated communication network. Such a communication network could be used for emergency communication over long distances when the landline and cellular network is broken. It could also help to organize the farmers' workforce in situations of prolonged internet connectivity outages, or allow neighborhoods surrounding of these farms to communicate with other nearby communities. We have three kinds of possible messages in mind that could be exchanged in crisis scenarios and that differ in their time priority:

TIME-CRITICAL COMMUNICATION There are numerous reasons for a need for time-critical communication, e.g. a medical emergency. In the farming context, there is often a need to coordinate multiple neighboring actors that are required to combine their workforce during harvest within ideal time windows. Such messages are short, but should arrive in seconds rather than minutes.

TIME-RELAXED COMMUNICATION In emergency situations, there is also a need for regular communication between people in a local community. This involves transmission of small-sized data like messages, medium-sized data like photos or small audio-files, or large-sized data like videos. This data exchange is not considered to be highly time-sensitive, but should, of course, be transmitted as fast as possible.

SENSOR-RELATED COMMUNICATION For technology-driven farming that enables optimal use of resources like water, fertilizer, fuel, and electric energy, the analysis of recent environmental data is of great importance. However, typically not every farm has all kinds of sensor stations. This applies particularly to small, family-driven businesses, which are predominant in Europe. Therefore, such small farms in particular have a specific need for sensor data exchange, as this could provide necessary data without the financial burden of having to invest in multiple sensor stations. Especially for weather analyses, aggregated data from multiple neighboring regions, in the best case high-quality data from meteorological services, could be of high importance to improve a farm's overall efficiency. Such data is likely to be extensive, but not as time-sensitive as the other communication.

In the next section, we elaborate on the possibility of connecting farms via LoRaWAN, that has a reliable coverage of several kilometers, using Germany as an example.

13.5 FARM-TO-FARM DISTANCES

To have a first estimate about the feasibility of connecting neighboring farms via wireless communication technologies, we evaluated distances between farms. As we have no access to a farm address database (perhaps there is no such database), we have chosen to evaluate available data provided by the OpenStreetMap project and developed a tool for this purpose.

13.5.1 *Querying and Processing OpenStreetMap Data*

The objective is to determine whether the given distances that a wireless setup has to bridge between individual farms can be achieved by LoRaWAN. For this purpose, we developed a tool in python[4]. The tool's jobs can be roughly grouped into three parts:

1. retrieving: query and filter OpenStreetMap data
2. processing: calculate distance matrix
3. presenting: generate statistics and graphs

To retrieve farms, we were faced with the problem that OpenStreetMap has an inconsistent level of detail in the mapped data, especially when comparing rural and urban areas. Next to large cities, farms are often tagged very accurately (`building=farm`), even with the company name. In such cases, a query for farm buildings retrieved a superset of current farm businesses' buildings. In rural areas, however, farms are not often tagged as such, resulting in low recall performance, i.e., there are many non-retrieved farms. We chose to use the tag `landuse=farmyard`: *"Area of land with farm buildings (farmhouse, sheds, stables, barns, etc.)"*[5] and to filter empty areas. Using this tag provides a better approximation of current farm business areas (more relevant elements), but requires additional filtering of the retrieved data (also more false positives). Filtering is done based on the child elements of the farmyards. In case there is no building inside a farmyard, we omit this area as we are only looking for buildings. As some neighboring farmyards were obviously part of the same farm business – sometimes as a result of a complex polygon that was split, sometimes because a street splits an area – we decided to merge nearby (up to 300m distance from geometric center to center) areas. Even in case this merges multiple farm businesses, they might share their communication link in case of an emergency situation. In the last step of the retrieving part, we selected a random building on each of the remaining areas as a representative farmhouse that may contain IT equipment, including a LoRaWAN gateway.

The processing is a much more straightforward task. Based on the filtered farmhouses, we calculated center points for each farm. These centers allowed us to compile a distance matrix that takes into account the curvature of the earth by using `geopy.distance`. We embedded comfort functions to store intermediate results to continue a distance matrix creation, which can take several hours depending on the node count and computational resources. Based on the

[4] https://github.com/PEASEC/distance-statistics

[5] https://wiki.openstreetmap.org/wiki/Item:Q4877

Table 13.1: Count of retrieved farms ($N = 117{,}744$) that have at least n neighboring farms in a specific range.

range [km]	1	2	3	4	5
$n = 1$	96,229	112,662	116,419	117,301	117,580
$n = 2$	72,758	104,620	113,455	116,288	117,192
$n = 3$	52,974	95,979	109,450	114,550	116,438
$n = 4$	37,084	87,739	104,914	112,405	115,429
$n = 5$	25,263	80,133	100,247	109,826	114,093

distance matrix, we evaluated two properties: (1) minimum distances between farms, and (2) count of neighboring farms in a range of $[1, 2, 3, 4, 5]$ km. We took these ranges as assumptions for typical real-world coverage of LoRaWAN hardware, respecting our experience for typical deployment ranges, as well as literature (El Chall et al., 2019).

Presentation of the statistics is done by using `geopandas`, `folium`, and `matplotlib`. Embedded in an jupyter notebook file, the statistics allow for further data analysis.

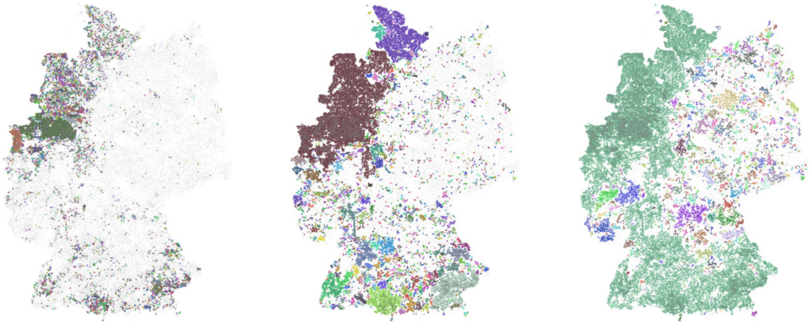
13.5.2 *Analysis of Retrieved Data*

We ran the tool for all federal states of Germany as an example for a large industrialized European country. Contacting colleagues from different parts of Germany allowed us to verify retrieved data on a random basis and check the data quality for their local neighborhood. Comparing the data with the statistics of the agricultural sector in Germany, we find that the number of buildings we retrieved ($N = 117{,}744$) is only 45% of the registered agricultural businesses in 2021 ($N = 259{,}200$) (Statistisches Bundesamt (Destatis), 2021b). To our understanding, this is mainly due the incompleteness of OpenStreetMap data, being a voluntary tool without the claim for 100% correct data. Taking this into consideration, our data represent a rather lower bound of possible application. Nonetheless, our data evaluation shows that the principal idea can work for some areas: As shown in Table 13.1, most of the detected farms ($N = 80{,}133$; 68%) have five or more neighboring farms within a 2 km radius, which is supposed to be a feasible range for LoRaWAN devices with good antennas in rural areas (El Chall et al., 2019).

We also clustered the buildings using DBSCAN (Ester et al., 1996), which creates groups such that each member of a group has at least one neighboring member in the same group with the maximum distance set. In Table 13.2 clustering results are presented for the parameter combinations ϵ with 1000m, 2000m, and 3000m, and $\mathtt{minPts}$ with 3, 5, and 7. Figure 13.1 shows three plotted configurations with colored clusters. As can be seen, there are very large differences in the mean size of the clusters in our data set, ranging from 10.68 to 143.87. As expected,

Table 13.2: Results of different clustering parameters.

ϵ	1000 m			2000 m			3000 m		
minPts	3	5	7	3	5	7	3	5	7
count	7881	3462	1743	3345	1910	1401	1076	916	745
mean	10.68	16.35	19.69	32.73	52.12	63.83	107.71	122.79	143.87
std	163.76	188.38	68.78	836.33	1045.44	1059.23	2904.94	3058.33	2034.03
median	4	7	10	5	8	11	6	8	11
max	14,028	10,768	1863	46,643	44,396	38,674	95,328	92,615	50,657
noise	33,545	61,143	83,427	8252	18,199	28,318	1848	5265	10,563



(a) ϵ = 1000 m

(b) ϵ = 2000 m

(c) ϵ = 3000 m

Figure 13.1: Clustering results with maximum distance ϵ and at least five elements per cluster (*minPts* = 5). Each element of a cluster is assigned a random color. All (including non-clustered) buildings are displayed as gray dots overlaid. With a point-to-point communication range of 2000 m or more, large parts of south and west of Germany could be covered.

increasing the maximum Euclidean distance between two points (ϵ) reduces the noise points, i.e., the coverage of the data set by all clusters is higher.

13.6 Simulation

Based on the results from the previous Section Farm-to-Farm Distances, we see the opportunity of building networks that connect neighboring farms via LPWAN networks that could be used for small data exchange, e.g., messaging. In this section, we evaluate two DTN routing approaches by simulation using gathered real-world data from OpenStreetMap.

13.6.1 *Setup*

For simulation of the network approach we use the `ONE` (Keränen et al., 2009) DTN simulation software. We test two scenarios (Kuntke & Baumgärtner, 2023):

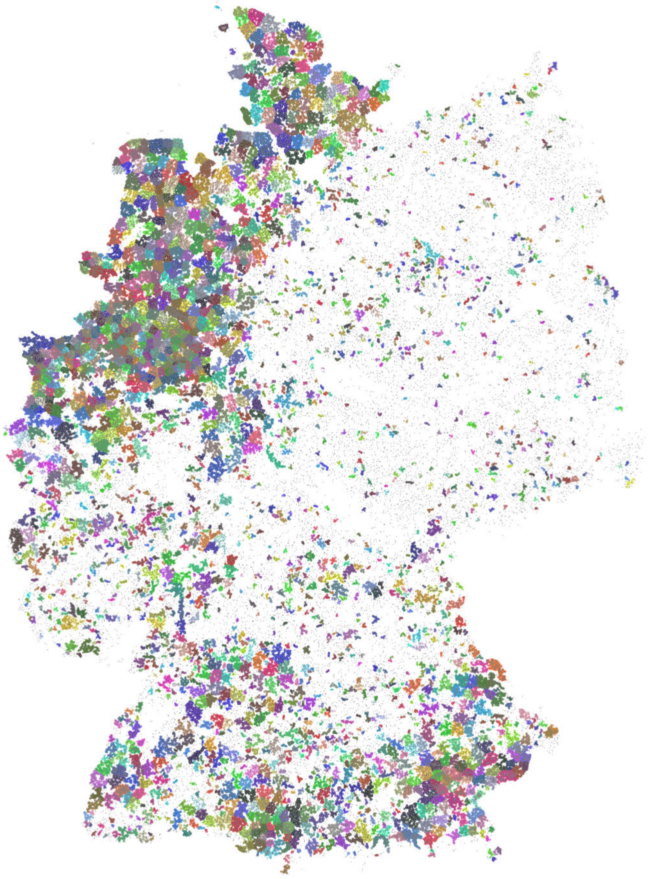


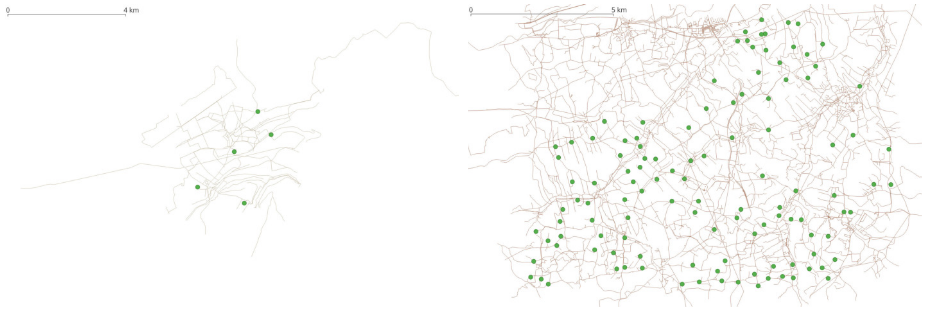
Figure 13.2: As we investigate on neighborhood communication, we reduced large clusters of our data set by k-Means to get more community-sized clusters for simulation.

(1) complete static nodes using only LoRaWAN as a transmission channel, and (2) a mixed-mode with additional WiFi ad-hoc data exchange of mobile nodes.

The simulation is based on real geographic data extracted from the data generated as described in Section Farm-to-Farm Distances. For further processing we decided to use one of the previously described DBSCAN clusterings results with a moderate setting, i.e. ϵ = 2000m and $\mathtt{minPts}$ = 5. The largest cluster of this data set has a size of 44,396 elements. As the scope of our work is the connection of farms and people inside a local community, we decided to further reduce the size of large clusters to better approximate the size of local communities. For this reason, we reduce each cluster c with $|c| > 100$ by using k-Means with $k = \lceil \frac{|c|}{100} \rceil$ to receive rather community-sized clusters. Figure 13.2 visualizes the resulting data set (base data set without k-Means visualized via Figure 13.1b), and Table 13.3 presents the statistics. Based on the 95% confidence interval (35.74, 39.10), we decided to simulate 40 randomly chosen clusters, which should give us a good approximation of the complete data set.

Table 13.3: Statistics of the k-Means *post-processed* data set, used for picking simulation areas.

count	mean	std	median	max
2660	37.42	37.42	11	224



(a) Cluster 7, one of the smallest clusters with 5 elements.

(b) Cluster 1, largest cluster with 116 elements.

Figure 13.3: Static nodes (farms) overlaid on extracted OpenStreetMap paths, used for simulation of pedestrians.

The 40 selected clusters have an average size of 37.95 ($\mathtt{std} = 37.29$). The largest chosen cluster includes 116 elements, and there are three clusters with the smallest size of 5 elements. For the mixed-mode scenario, we took mobile nodes into consideration. To have a more realistic simulation, we exported additional path geometries from OpenStreetMap to let our simulated pedestrians (mobile nodes) move on streets and ways. Figure 13.3 shows two exemplary clusters with their corresponding paths.

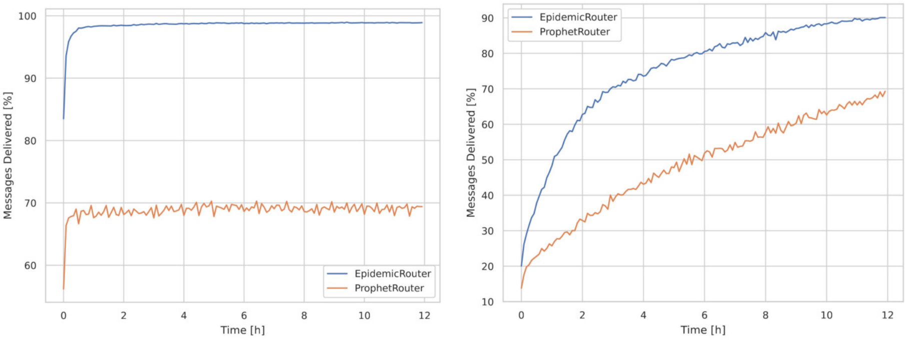
General Simulation Configuration

Both scenarios are simulated for all 40 clusters. The simulated time duration is 12 hours (43,200 seconds), with 0.05 second update intervals. Each cluster element is considered to be a static node, representing a farm. To evaluate the performance of two common DTN routing protocols for our scenario, we ran all configurations with both *PRoPHET* and *Epidemic* routing.

Scenario Related Configuration

We used the following settings for our two scenarios:

STATIC A random static node sends a message to a random target within $\lfloor \frac{1800s}{|\mathtt{node}|} \rfloor$. The message size is also random, between 80 and 500 Bytes. The



(a) *static*

(b) *mobile*

Figure 13.4: Message delivery rates of both scenarios. Mean over all 40 runs.

LoRaWAN communication range is set to a maximum of 2000m, and the transmission speed is set to 7 kbps, which is between 5470 bps (data rate 5) and 11 kbps (data rate 6). These static nodes also have a WiFi interface; however, with a limited range of 100m, they are not used in the static scenario at all.

MOBILE Scenario *mobile* uses the same static nodes as scenario *static*, but adds mobile nodes representing pedestrians. We add as many mobile nodes as static nodes, i.e. one moving person is simulated per farm, traveling during the day. A random node (static or mobile) sends a message to a random target within $\lfloor \frac{3600s}{|node|} \rfloor$. The message size is also random, between 80 and 500 Bytes. These mobile nodes only have WiFi interfaces (smartphones) to exchange messages when in a range of 100m with another mobile node or with a static node. Each WiFi interface is set up with a transmission speed of 54 MBit/s.

13.6.2 *Results*

Statistics of the messages sent are presented in Table 13.4 and Table 13.5. The evaluation shows that in both scenarios, the flooding-based *Epidemic* routing achieves a higher delivery probability, at the cost of more routed messages. Figure 13.4 plots the message delivery rate over time for both scenarios. In *static*, *Epidemic* routing could deliver about 99% of the created messages. Both *PRoPHET* and *Epidemic* routing have an almost constant delivery probability

Table 13.4: Message statistics of *static*. Mean over all 40 runs.

	created	started	relayed	delivered	delivery	latency
					_prob	_avg [s]
Epidemic	927.75	66,411.25	66,410.63	917.03	0.99	0.29
PRoPHET	927.75	10,211.43	10,210.90	614.78	0.81	0.18

Table 13.5: Message statistics of *mobile*. Mean over all 40 runs.

	created	started	relayed	delivered	delivery _prob	latency _avg [s]
Epidemic	927.75	123,095.88	123,095.40	835.18	0.88	3863.13
PRoPHET	927.75	54,895.90	54,895.55	631.78	0.72	7326.52

after a few minutes. From the second hour, however, a gap builds up between *PRoPHET* and *Epidemic* routing. Interestingly, *static* with LoRaWAN-only communication achieves an overall higher delivery performance compared to *mobile*. From a technical point of view, this is obvious, since the mobile nodes must first come within WiFi reception range of another node. However, this could have practical implications: With regard to successful message delivery, it may make more sense to nudge users to rely less on mobile ad hoc connections via WiFi, and instead rely on static but connected LoRaWAN gateways.

13.7 Concept and Implementation

Based on the results from previous Section Simulation, we see the opportunity of building networks that connect neighboring farms via LPWAN networks, that could be used for small data exchange, e.g., messaging. LoRaWAN itself offers a range of multiple km depending on the settings, hardware and geographic circumstances. In this section, we describe our concept and the proof-of-concept implementation.

13.7.1 *Concept*

We assume a farm building contains a small server for the purpose of running management software, as well its own LoRaWAN network server, to be able to collect and process the data without limitations and running expenses. When considering the challenges of using LoRaWAN for our goal, we are faced with high airtime of up to nearly three seconds per frame, a duty cycle restriction for most region/band combinations (e.g., 1% in the EU within the 868 MHz band), low payload and potentially unavailable network nodes (e.g., powered-down gateways), and additionally also the typical wireless problem that transmissions can fail in practice for various reasons (e.g., high noise in the used frequency band). Then again, we achieved a potentially high transmission range of up to several km by extending an existing software ecosystem.

Communication via LoRaWAN Gateways

Our goal is to use neighboring LoRaWAN gateways to communicate with each other. A proxy is supposed to intercept the communication between the

LoRaWAN Network Server and a gateway and forward our own frames to another processing pipeline. In this way we do not interrupt the IoT setup in its regular operations, but add our emergency communication layer on top. In our concept, the LoRaWAN network server software and our proxy are located on a physical mini server next to the gateway.

LoRaWAN Frames According to ISO/OSI

On the *Physical Layer*, we are bound to LoRa transmission, as we use off-the-shelf LoRaWAN gateways. On the *Data Link* and *Network Layer*, we differ from the plain LoRaWAN standard (LoRa Alliance Technical Committee, 2020) in that we use our own frames. However, we only differ in the fields `MACPayload` and `MIC` for our goal. In this way, we could be compatible with future LoRaWAN repeaters (LoRa Alliance Technical Committee, 2020), which may enhance the usefulness of our approach. On the upper layers (*Transport, Session, Presentation*), we use BP7 (Burleigh et al., 2022) for message delivery allowing applications to send and receive bundles.

Routing Between End-Devices

The ability to send frames via a gateway with our proxy software, as well as receive and process frames sent by other gateways, allows us to integrate this into the bigger picture of creating a disruption-tolerant multi-hop communication network. For this purpose, we need a routing logic that processes bundles. In case of a received bundle there are two options: (1) the current gateway is the destination, meaning the bundle must be forwarded internally to an application/end-device; or (2) the bundle must be forwarded externally, meaning it has to be sent out by the gateway. By using the bundle protocol standard, we allow applications to exchange data through additional ways, e.g., via a smartphones' Bluetooth or WiFi. One important aspect is the address scheme. For this purpose, we use the phone number (E.123 notation) as the interplanetary network (IPN) endpoint identifier, as every user is expected to possess one main mobile device and a unique phone number. As we have a very limited payload, we use 4 bytes for the address by calculating the CRC-32 checksum of the phone number. The bundle itself is encoded as Concise Binary Object Representation (CBOR) (Bormann & Hoffman, 2020), according to the standard.

13.7.2 *Implementation*

When inspecting the ChirpStack[6] (the de-facto standard open-source LoRaWAN network server), we saw that all necessary communication from and to gateways had already been converted into a message queuing protocol (MQTT), which we

[6] https://chirpstack.io

could use to read LoRa frames received by a gateway, as well as send messages via a LoRaWAN gateway. By sending commands to a gateway, we can specify the payload in our own way, respecting the limitations on maximum payload size depending on the set up data rate (SF and bandwidth). By doing this, we do not have to intercept the packet forwarder, as described in our concept, but we can do the same by just implementing a specific MQTT client, which reduces the complexity.

Due to the modular design, we separated the two functions: (1) being an MQTT client, reading LoRaWAN frames, and sending commands towards a gateway, and (2) parsing LoRaWAN frames into DTN bundles, containing routing logic, and connecting them with applications like our concept messenger app. We implemented[7] this (1) in Rust as a library, called `chirpstack_gwb_integration`, and (2) also in Rust as our convergence layer application `spatz` that uses DTN7-RS[8] as BP7 implementation. Additionally, we created a simple browser-based messaging client with VueJS that connects to a `spatz` instance via TCP/IP and allows us to send messages as an end-user. Figure 13.5 depicts the components of our proof-of-concept implementation.

CHIRPSTACK_GWB_INTEGRATION The library's[9] main purpose is to be a Rust interface for directly interacting with a gateway, which is registered on a Chirpstack instance. The goal is not to interfere with the usual IoT setup of a LoRaWAN instance, but being able to independently send and receive LoRa frames via one or more connected LoRaWAN gateways. The library acts as a MQTT client and allows the creation of callbacks for incoming messages, as well as triggering `downlink` commands as outgoing LoRaWAN frames with specific transmission parameters like frequency and data rate, and payload.

SPATZ The main application[10] implements the bundle protocol convergence layer and the routing logic. It allows external user interfaces to connect to it by using websocket connections. `spatz` also handles the packet fragmentation, in cases a retrieved bundle could not be transmitted in one LoRaWAN frame. Due to the higher delivery probability in our simulation results, we decided to implement epidemic routing. For configuration settings, e.g. adding and deleting associated phone numbers (IPN endpoint identifier), `spatz` has a REST API.

Real World Setup

For our real world tests we use a Raspberry Pi 4, 4GB and three different LoRaWAN gateways: Dragino LPS8, Dragino DLOS8N, and RAK 7268-N. One node setup consists of a Linux server (e.g. Raspberry Pi 4) and one LoRaWAN

[7] https://github.com/PEASEC/LoRaWAN-DTN

[8] https://github.com/dtn7/dtn7-rs

[9] https://github.com/PEASEC/LoRaWAN-DTN/tree/main/chirpstack_gwb_integration

[10] https://github.com/PEASEC/LoRaWAN-DTN/tree/main/spatz

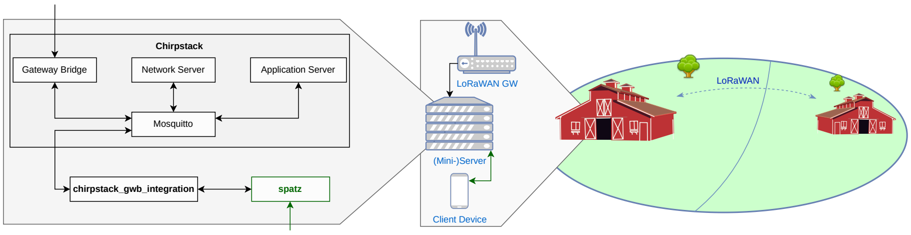


Figure 13.5: Technical concept: Regular LoRaWAN setup is extended by a LoRaWAN Packet Forwarder AddOn that allows to send and receive arbitrary LoRa(WAN) frames. The concept allows message exchange during network infrastructure outages.

Table 13.6: List of exemplary system component options with current prices (retrieved in January 2023).

Component Type	Name	Price
Mini-Server	Raspberry Pi 4 Computer Modell B, 4GB RAM	~€70
	Accessories (case, heat sink, power supply, 64 GB SDCard)	~€26
Mini-Server	Intel NUC 8 Rugged Kit 4GB RAM, 64GB SSD	~€200
LoRaWAN Gateway (indoor)	Dragino LPS8N-868	~€160
LoRaWAN Gateway (indoor)	RAK 7268-N	~€180
LoRaWAN Gateway (outdoor)	Dragino DLOS8-868	~€320

Gateway (e.g. Dragino LPS8). Table 13.6 lists exemplary hardware costs. The cost of our evaluation setup hardware for one node starts at €256 (Raspberry Pi 4 + required accessories and a Dragino LPS8N-868). However, it should be kept in mind that these hardware requirements — at least a LoRaWAN gateway — are also necessary for regular LoRaWAN IoT setups, especially for farms that require long range and cost-effective wireless transmission of sensor data. We use Debian 12 as Raspberry Pi operating system, and Chirpstack v4 is installed according to the official *Quickstart Docker Compose* guide [11]. Our own software (`chirpstack_gwb_integration` and `spatz`) is compiled and executed directly on the Raspberry Pi. The browser-based messaging client is served by its own Docker container on the Raspberry Pi and allows it to be opened from a browser on a device (e.g. smartphone or laptop) on the same network. With this setup we were able to confirm the proper operation of our development with three nodes. As a limitation, we have not carried out a large-n scale test with real hardware, which will be part of follow-up research.

[11] https://www.chirpstack.io/project/guides/docker-compose/

13.8 Conclusion

This work presents a novel approach for transforming commercial off-the-shelf LoRaWAN setups into DTN base stations for long range communication and looks into the feasibility of building communication networks in rural areas by leveraging these LoRa-DTN base stations located on farms. Current research has already shown how multi-hop networks based on LPWAN technology can be used to increase coverage (Abrardo & Pozzebon, 2019; Ebi et al., 2019). Until now, the focus has mainly been on the data flow between the end device (e.g. the sensor) and the base station. We differ from the existing body of work on multi-hop communication and LPWAN improvements through our use case and design to provide support in crisis scenarios by DTN based message transmission. The existing approaches for extending IoT-communication described in the literature are not suitable for the design of a communication system that we focused on. We also differ by using commodity hardware from the existing works of LPWAN-based emergency communication technologies, as those rely on specific devices like self-made pagers or smartphone companion boards that might not being available in times of crisis event. By analyzing data from OpenStreetMap, we have obtained an approximation of positions of real farms in Germany. Even though the database is not complete, it gives a good indication of how well our idea could work in the European area if farms might enrich already existing LoRaWAN installations with our approach to be able to communicate across farms without external infrastructure in case of a crisis. Our simulation results have shown the feasibility, even if only LoRaWAN is in charge of message transmission. One possible application scenario for our development is to ensure the exchange of short messages during times of communication infrastructure failure in rural communities. Future work should identify the feasibility of concrete application cases under realistic conditions in order to prepare the technology for real crisis scenarios.

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

ABP	Activation By Personalization
ADR	adjusting adaptive data rate
AES	Advanced Encryption Standard
AFR	autonomous field robot
AI	artificial intelligence
AS	application server
BP7	Bundle Protocol Version 7
CSCW	Computer-Supported Cooperative Work
DoS	Denial-of-Service
DSR	design science research
DTN	disruption-tolerant networking
ED	end device
FMIS	Farm Management Information System
GPS	Global Positioning System
GW	gateway
HCI	Human-Computer Interaction
ICT	Information and Communications Technology
IETF	Internet Engineering Task Force
IT	information technology
ITU	International Telecommunication Union
IoT	Internet of Things
JS	join server
LoRaWAN	Long Range Wide Area Network
LoS	line of sight
LPWAN	Low Power Wide Area Network
MANET	Mobile Ad Hoc Network
MIC	message integrity code
NAS	network-attached storage
NS	network server
OTAA	Over-The-Air Activation
OSI	Open Systems Interconnection
PWA	Progressive Web App
RQ	research question

RSSI	received signal strength indicator
SLR	Systematic Literature Review
SME	small and medium-sized farms and enterprises
SNR	Signal-to-Noise-Ratio
SUS	System Usability Scale
UAV	unmanned aerial vehicle
UI	User Interface
WSN	Wireless Sensor Network

BIBLIOGRAPHY

Abrardo, A., Fort, A., Landi, E., Mugnaini, M., Panzardi, E., & Pozzebon, A. (2019). Black Powder Flow Monitoring in Pipelines by Means of Multi-Hop LoRa Networks. *Proceedings of the Workshop on Metrology for Industry 4.0 and IoT*.

Abrardo, A., & Pozzebon, A. (2019). A multi-hop LoRa linear sensor network for the monitoring of underground environments: the case of the Medieval Aqueducts in Siena, Italy. *Sensors*, *19*(2).

Aceto, G., Botta, A., Marchetta, P., Persico, V., & Pescapé, A. (2018). A Comprehensive Survey on Internet Outages. *Journal of Network and Computer Applications*, *113*, 36–63. https://doi.org/10.1016/j.jnca.2018.03.026

Adeel, A., Gogate, M., Farooq, S., Ieracitano, C., Dashtipour, K., Larijani, H., & Hussain, A. (2019). A survey on the role of wireless sensor networks and iot in disaster management. In T. S. Durrani, W. Wang, & S. M. Forbes (Eds.), *Geological disaster monitoring based on sensor networks* (pp. 57–66). Springer Singapore. https://doi.org/10.1007/978-981-13-0992-2_5

Aldehoff, L., Dankenbring, M., & Reuter, C. (2019). Renouncing privacy in crisis management? people's view on social media monitoring and surveillance. *Proceedings of the Information Systems for Crisis Response and Management (ISCRAM)*, 1184–1197.

American Heritage Dictionary of the English Language. (2021). Agriculture. Retrieved February 4, 2021, from https://www.ahdictionary.com/word/search.html?q=agriculture

Ammann, J., Walter, A., & El Benni, N. (2022). Adoption and perception of farm management information systems by future Swiss farm managers – An online study. *Journal of Rural Studies*, *89*, 298–305. https://doi.org/10.1016/j.jrurstud.2021.12.008

Annosi, M. C., Brunetta, F., Monti, A., & Nati, F. (2019). Is the trend your friend? An analysis of technology 4.0 investment decisions in agricultural SMEs. *Computers in Industry*, *109*, 59–71. https://doi.org/10.1016/j.compind.2019.04.003

Aras, E., Ramachandran, G. S., Lawrence, P., & Hughes, D. (2017). Exploring the security vulnerabilities of lora, 1–6. https://doi.org/10.1109/CYBConf.2017.7985777

Aras, E., Small, N., Ramachandran, G. S., Delbruel, S., Joosen, W., & Hughes, D. (2017). Selective jamming of lorawan using commodity hardware, 363–372. https://doi.org/10.1145/3144457.3144478

Atik, C. (2022). Towards comprehensive european agricultural data governance: Moving beyond the "data ownership" debate. *IIC-International Review of Intellectual Property and Competition Law*, 1–42. https://doi.org/10.1007/s40319-022-01191-w

Augustin, A., Yi, J., Clausen, T., & Townsley, W. (2016). A study of lora: Long range & low power networks for the internet of things. *Sensors*, *16*(9), 1466.

Bacco, M., Berton, A., Ferro, E., Gennaro, C., Gotta, A., Matteoli, S., Paonessa, F., Ruggeri, M., Virone, G., & Zanella, A. (2018). Smart farming: Opportunities, challenges and technology enablers. *2018 IoT Vertical and Topical Summit on Agriculture - Tuscany (IOT Tuscany)*, 1–6. https://doi.org/10.1109/IOT-TUSCANY.2018.8373043

Backman, S. (2021). Conceptualizing cyber crises. *Journal of Contingencies and Crisis Management*, *29*(4), 429–438. https://doi.org/10.1111/1468-5973.12347

Bala, S., Barthel, D., & Gharout, S. (2019). Separate session key generation approach for network and application flows in lorawan, 870–879. https://doi.org/10.1145/3297280.3297366

Balafoutis, A. T., Evert, F. K. V., & Fountas, S. (2020). Smart Farming Technology Trends: Economic and Environmental Effects, Labor Impact, and Adoption Readiness. *Agronomy*, *10*(5), 743. https://doi.org/10.3390/agronomy10050743

Ballani, H., Francis, P., & Zhang, X. (2007). A Study of Prefix Hijacking and Interception in the Internet. *Proceedings of the 2007 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, 265–276. https://doi.org/10.1145/1282380.1282411

Bangor, A., Staff, T., Kortum, P., Miller, J., & Staff, T. (2009). Determining What Individual SUS Scores Mean: Adding an Adjective Rating Scale. *Journal of Usability Studies*, *4*(3), 114–123.

Bardram, A. V. T., Delbo Larsen, M., Malarski, K. M., Petersen, M. N., & Ruepp, S. (2018). LoRaWan capacity simulation and field test in a harbour environment. *2018 Third International Conference on Fog and Mobile Edge Computing (FMEC)*, 193–198. https://doi.org/10.1109/FMEC.2018.8364064

Bardyn, J., Melly, T., Seller, O., & Sornin, N. (2016). Iot: The era of lpwan is starting now. *ESSCIRC Conference 2016: 42nd European Solid-State Circuits Conference*, 25–30. https://doi.org/10.1109/ESSCIRC.2016.7598235

Barreto, L., & Amaral, A. (2018). Smart Farming: Cyber Security Challenges. *International Conference on Intelligent Systems (IS)*, 870–876. https://doi.org/10.1109/IS.2018.8710531

Baumgärtner, L., Lieser, P., Zobel, J., Bloessl, B., Steinmetz, R., & Mezini, M. (2020a). LoRAgent: A DTN-based Location-aware Communication System using LoRa. *Proceedings of the Global Humanitarian Technology Conference*. https://doi.org/10.1109/GHTC46280.2020.9342886

Baumgärtner, L., Lieser, P., Zobel, J., Bloessl, B., Steinmetz, R., & Mezini, M. (2020b). LoRAgent: A DTN-based Location-aware Communication System using LoRa. *Proceedings of the Global Humanitarian Technology Conference*.

Beech, W. A., Nielsen, D. E., Noo, J. T., & Ncuu, L. K. (1997). Ax. 25 link access protocol for amateur packet radio, version: 2.2 rev. *Tucson Amateur Packet Radio Corp*.

Benkahla, N., Belgacem, B., & Frikha, M. (2018). Security analysis in enhanced lorawan duty cycle, 1–7. https://doi.org/10.1109/COMNET.2018.8622296

Bermeo-Almeida, O., Cardenas-Rodriguez, M., Samaniego-Cobo, T., Ferruzola-Gómez, E., Cabezas-Cabezas, R., & Bazán-Vera, W. (2018). Blockchain in agriculture: A systematic literature review. *International Conference on*

Technologies and Innovation, 44–56. https://doi.org/https://doi.org/10.1007/978-3-030-00940-3_4

Bernardi, A., Reuter, C., Schneider, W., Linsner, S., & Kaufhold, M.-A. (2019). Hybride Dienstleistungen in digitalisierten Kooperationen in der Landwirtschaft. In A. Meyer-Aurich (Ed.), *39. GIL-Jahrestagung: Informatik in der Land-, Forst- und Ernährungswirtschaft Fokus; Digitalisierung für landwirtschaftliche Betriebe in kleinstrukturierten Regionen – ein Widerspruch in sich?, Lecture Notes in Informatics (LNI)* (pp. 25–30). Gesellschaft für Informatik. http://gil-net.de/Publikationen/139_25-30.pdf

Berni, A. J., & Gregg, W. D. (1973). On the utility of chirp modulation for digital signaling. *IEEE Transactions on Communications*, *21*(6), 748–751. https://doi.org/10.1109/TCOM.1973.1091721

Birner, R., Daum, T., & Pray, C. (2021). Who drives the digital revolution in agriculture? A review of supply-side trends, players and challenges. *Applied Economic Perspectives and Policy*, *43*(4), 1260–1285. https://doi.org/10.1002/aepp.13145

Biselli, T., & Reuter, C. (2021). On the relationship between it privacy and security behavior: A survey among German private users. *Wirtschaftsinformatik 2021 Proceedings*, 1–17.

Bökle, S., Paraforos, D. S., Reiser, D., & Griepentrog, H. W. (2022). Conceptual framework of a decentral digital farming system for resilient and safe data management. *Smart Agricultural Technology*, *2*, 100039. https://doi.org/10.1016/j.atech.2022.100039

Bokusheva, R., & Kimura, S. (2016). Cross-Country Comparison of Farm Size Distribution. *OECD Food, Agriculture and Fisheries Papers*, (94). https://doi.org/10.1787/5jlv81sclr35-en

Bonke, V., Fecke, W., Michels, M., & Musshoff, O. (2018). Willingness to pay for smartphone apps facilitating sustainable crop protection. *Agronomy for Sustainable Development*, *38*(5), 1–10. https://doi.org/10.1007/s13593-018-0532-4

Bormann, C., & Hoffman, P. E. (2020). *Concise Binary Object Representation (CBOR)* (Request for Comments No. 8949). https://doi.org/10.17487/RFC8949

Braun, A. T., Colangelo, E., & Steckel, T. (2018). Farming in the Era of Industrie 4.0. *Procedia CIRP*, *72*, 979–984. https://doi.org/10.1016/j.procir.2018.03.176

Brooke, J. (1996). SUS - A quick and dirty usability scale. *Usability evaluation in industry*, 189.

Brown, I. (2016). *A detailed breakdown of lpwan technologies and providers*. Retrieved November 3, 2019, from http://web.luxresearchinc.com/hubfs/Insight_Breakdown_of_LPWAN_Technologies.pdf

Bucci, G., Bentivoglio, D., & Finco, A. (2018). Precision agriculture as a driver for sustainable farming systems: State of art in litterature and research. *Quality - Access to Success*, *19*(S1), 114–121.

Buhleier, L., Gantner, P., Frey, T., Boers, M., Kaufhold, M.-A., & Reuter, C. (2022). Effizienz und Nachhaltigkeit durch Green-IT: Ein systematischer Literaturüberblick im Kontext der Klimakrise. *INFORMATIK 2022: 52. Jahrestagung der Gesellschaft für Informatik*.

Bundesanstalt für Landwirtschaft und Ernährung. (2023). *Statistisches Jahrbuch für Ernährung, Landwirtschaft und Forsten 2022* (Vol. 66). Bundesministerium für Ernährung und Landwirtschaft.

Bundesministerium des Inneren. (2016). Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung–BSI-KritisV); Bundesgesetzblatt Jahrgang 2016 Teil I Nr. 20.

Bundesministerium für Ernährung und Landwirtschaft. (2018). Daten und Fakten: Land-, Forst- und Ernährungswirtschaft mit Fischerei und Wein- und Gartenbau. Retrieved April 23, 2021, from https://www.bmel.de/SharedDocs/Downloads/DE/Broschueren/Daten-und-Fakten-Landwirtschaft.html

Bundesministerium für Ernährung und Landwirtschaft. (2020, July). Arbeitsmarkt Landwirtschaft in Deutschland. https://www.bmel.de/SharedDocs/Downloads/DE/Broschueren/studie-arbeitsmarkt-landwirtschaft-in-deutschland.pdf

Bundesministerium für Ernährung und Landwirtschaft. (2021). Klassifizierungssystem für landwirtschaftliche Betriebe. https://www.bmel-statistik.de/fileadmin/daten/SJT-3010210-2021.xlsx

Burleigh, S., Fall, K., & Birrane, E. J. (2022). *Bundle Protocol Version 7* (Request for Comments No. 9171). https://doi.org/10.17487/RFC9171

Butun, I., Pereira, N., & Gidlund, M. (2018a). Analysis of lorawan v1.1 security: Research paper. https://doi.org/10.1145/3213299.3213304

Butun, I., Pereira, N., & Gidlund, M. (2018b). Security risk analysis of LoRaWAN and future directions. *Future Internet*, *11*(1), 1–22. https://doi.org/10.3390/fi11010003

Cajander, Å., Lárusdóttir, M. K., Lind, T., & Nauwerck, G. (2021). Walking in the jungle with a machete: ICT leaders' perspectives on user-Centred systems design. *Behaviour and Information Technology*, 1–15. https://doi.org/10.1080/0144929X.2020.1864776

Cambra, C., Sendra, S., Lloret, J., & Garcia, L. (2017). An IoT service-oriented system for agriculture monitoring. *IEEE International Conference on Communications*. https://doi.org/10.1109/ICC.2017.7996640

Carbonell, I. (2016). The ethics of big data in big agriculture. *Internet Policy Review*, *5*(1).

Carli, G., Xhakollari, V., & Tagliaventi, M. R. (2017). How to model the adoption and perception of precision agriculture technologies. In *Precision agriculture: Technology and economic perspectives* (pp. 223–249). Springer.

Cascio, M. A., Lee, E., Vaudrin, N., & Freedman, D. A. (2019). A Team-based Approach to Open Coding: Considerations for Creating Intercoder Consensus. *Field Methods*, *31*(2), 116–130. https://doi.org/10.1177/1525822X19838237

Cattani, M., Boano, C. A., & Römer, K. (2017). An Experimental Evaluation of the Reliability of LoRa Long-Range Low-Power Wireless Communication [Number: 2 Publisher: Multidisciplinary Digital Publishing Institute]. *Journal of Sensor and Actuator Networks*, *6*(2), 7. https://doi.org/10.3390/jsan6020007

Cavallo, E., Ferrari, E., Bollani, L., & Coccia, M. (2014). Attitudes and behaviour of adopters of technological innovations in agricultural tractors: A case study in Italian agricultural system. *Agricultural Systems*, *130*, 44–54. https://doi.org/https://doi.org/10.1016/j.agsy.2014.05.012

Centelles, R. P., Freitag, F., Meseguer, R., & Navarro, L. (2021). Beyond the Star of Stars: An Introduction to Multihop and Mesh for LoRa and LoRaWAN.

Pervasive Computing, *20*(2). https://doi.org/10.1109/MPRV.2021.3063443

Chacko, S., & Job, M. D. (2018). Security mechanisms and Vulnerabilities in LPWAN. *IOP Conference Series: Materials Science and Engineering*, *396*(1). https://doi.org/10.1088/1757-899X/396/1/012027

Chandra, R., & Collis, S. (2021). Digital agriculture for small-scale producers: Challenges and opportunities. *Communications of the ACM*, *64*(12), 75–84. https://doi.org/10.1145/3454008

Chaudhary, H., Patel, H., & Tank, B. (2018). Comparative analysis of internet of things (iot) based low power wireless technologies. *International Journal of Engineering Research*, *7*(01).

Chen, X., Jiao, L., Li, W., & Fu, X. (2016). Efficient Multi-User Computation Offloading for Mobile-Edge Cloud Computing. *IEEE/ACM Transactions on Networking*, *24*(5), 2795–2808. https://doi.org/10.1109/TNET.2015.2487344

Cheng, P.-C., Lee, K. C., Gerla, M., & Härri, J. (2010). GeoDTN+ Nav: geographic DTN routing with navigator prediction for urban vehicular environments. *Mobile Networks and Applications*, *15*(1).

Cheng, Y., Saputra, H., Goh, L. M., & Wu, Y. (2018). Secure smart metering based on lora technology, 1–8. https://doi.org/10.1109/ISBA.2018.8311466

Chepponis, M., & Karn, P. (1987). The kiss tnc: A simple host-to-tnc communications protocol. *6th Computer Networking Conference*, *225*, 06111–1494.

Civelek, C. (2017). Low power wide area network (lpwan) and internet of things adaptation in agricultural machinery. *Scholars Journal of Agriculture and Veterinary Sciences*, *4*(1).

Coman, F. L., Malarski, K. M., Petersen, M. N., & Ruepp, S. (2019). Security issues in internet of things: Vulnerability analysis of lorawan, sigfox and nb-iot, 1–6. https://doi.org/10.1109/GIOTS.2019.8766430

Commission, E. (2015). User guide to the SME definition. *Luxembourg: Publications Office of the European Union*.

Coopamootoo, K. P., & Groß, T. (01 Oct. 2017). Why privacy is all but forgotten. *Proceedings on Privacy Enhancing Technologies*, *2017*(4), 97–118. https://doi.org/https://doi.org/10.1515/popets-2017-0040

Corbin, J. M., & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative sociology*, *13*(1), 3–21.

Cravotta, S., & Grottke, M. (2019). Digitalization in German family firms–some preliminary insights. *Journal of Evolutionary Studies in Business*, *4*(1), 1–25. https://doi.org/https://doi.org/10.1344/jesb2019.1.j051

Dainotti, A., Squarcella, C., Aben, E., Claffy, K. C., Chiesa, M., Russo, M., & Pescapé, A. (2011). Analysis of Country-Wide Internet Outages Caused by Censorship. *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference*, 1–18. https://doi.org/10.1145/2068816.2068818

Danish, S. M., Lestas, M., Qureshi, H. K., Zhang, K., Asif, W., & Rajarajan, M. (2020). Securing the LoRaWAN join procedure using blockchains. *Cluster Computing*, *8*. https://doi.org/10.1007/s10586-020-03064-8

Danish, S. M., Nasir, A., Qureshi, H. K., Ashfaq, A. B., Mumtaz, S., & Rodriguez, J. (2018). Network intrusion detection system for jamming attack in lorawan join procedure, 1–6. https://doi.org/10.1109/ICC.2018.8422721

Darnhofer, I. (2021). Resilience or how do we enable agricultural systems to ride the waves of unexpected change? *Agricultural Systems*, *187*, 102997. https://doi.org/10.1016/j.agsy.2020.102997

Davcev, D., Mitreski, K., Trajkovic, S., Nikolovski, V., & Koteli, N. (2018). IoT agriculture system based on LoRaWAN. *IEEE International Workshop on Factory Communication Systems - Proceedings, WFCS*, *2018-June*, 1–4. https://doi.org/10.1109/WFCS.2018.8402368

Demestichas, K., Peppes, N., & Alexakis, T. (2020). Survey on Security Threats in Agricultural IoT and Smart Farming. *Sensors*, *20*(22), 6458. https://doi.org/10.3390/s20226458

Dias, J., & Grilo, A. (2018). Lorawan multi-hop uplink extension. *Procedia Computer Science*, *130*.

Doll, H., Fasterding, F., & Klare, K. (2001). Auswirkungen des landwirtschaftlichen Erbrechts auf den agrarstrukturellen Wandel in Deutschland. *German Journal of Agricultural Economics*, (670-2016-45544), 5. https://doi.org/10.22004/ag.econ.98863

Dönmez, T. C., & Nigussie, E. (2018). Security of lorawan v1.1 in backward compatibility scenarios. *Procedia Computer Science*, *134*, 51–58. https://doi.org/10.1016/j.procs.2018.07.143

Dörr, J., & Nachtmann, M. (Eds.). (2022). *Handbook Digital Farming: Digital Transformation for Sustainable Agriculture*. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-64378-5

Durand, T., Visagie, L., & Booysen, M. ((2019). Evaluation of next-generation low-power communication technology to replace gsm in iot-applications. *IET Communications*, 1. https://doi.org/10.1049/iet-com.2019.0168

Eberz-Eder, D., Kuntke, F., Brill, G., Bernardi, A., Reuter, C., Wied, C., Nuderscher, P., & Reuter, C. (2023). Prototypische Entwicklungen zur Umsetzung des Resilient Smart Farming (RSF) mittels Edge Computing. *43. GIL-Jahrestagung: Informatik in der Land-, Forst- und Ernährungswirtschaft*. https://dl.gi.de/handle/20.500.12116/40264

Eberz-Eder, D., Kuntke, F., & Reuter, C. (2022). Sensibilität für Resilient Smart Farming (RSF) und seine Bedeutung in Krisenzeiten. *42. GIL-Jahrestagung: Informatik in der Land-, Forst- und Ernährungswirtschaft*. https://dl.gi.de/handle/20.500.12116/38375

Eberz-Eder, D., Kuntke, F., Schneider, W., & Reuter, C. (2021). Technologische Umsetzung des Resilient Smart Farming (RSF) durch den Einsatz von Edge-Computing. *41. GIL-Jahrestagung: Informatik in der Land-, Forst- und Ernährungswirtschaft*, 79–84. https://dl.gi.de/handle/20.500.12116/35651

Ebi, C., Schaltegger, F., Rüst, A., & Blumensaat, F. (2019). Synchronous lora mesh network to monitor processes in underground infrastructure. *IEEE Access*, *7*.

El Chall, R., Lahoud, S., & El Helou, M. (2019). LoRaWAN Network: Radio Propagation Models and Performance Evaluation in Various Environments in Lebanon. *Internet of Things Journal*, *6*(2). https://doi.org/10.1109/JIOT.2019.2906838

Eldefrawy, M., Butun, I., Pereira, N., & Gidlund, M. (2019). Formal security analysis of lorawan. *Computer Networks*, *148*, 328–339. https://doi.org/10.1016/j.comnet.2018.11.017

Elijah, O., Rahman, T. A., Orikumhi, I., Leow, C. Y., & Hindia, M. N. (2018). An Overview of Internet of Things (IoT) and Data Analytics in Agriculture: Benefits and Challenges. *IEEE Internet of Things Journal*, *5*(5), 3758–3773. https://doi.org/10.1109/JIOT.2018.2844296

Ester, M., Kriegel, H.-P., Sander, J., Xu, X., et al. (1996). A density-based algorithm for discovering clusters in large spatial databases with noise. *Proceedings of the 2nd International Conference on Knowledge Discovery and Data Mining*, *96*(34).

Eurostat. (2016). Agriculture: Labour force by sex, legal status of holding and working time. https://ec.europa.eu/eurostat/web/products-datasets/-/ef_lf_leg

Eurostat. (2018). Of the 10.3 million farms in the EU, two thirds are less than 5 ha in size. *Eurostat Newsrelease*, *2016*(105/2018), 5–9. https://ec.europa.eu/eurostat/documents/2995521/9028470/5-28062018-AP-EN.pdf

Farrell, S. (2018). Low-power wide area network (lpwan) overview. *Internet Engineering Task Force (IETF)*.

Fecke, W., Michels, M., von Hobe, C.-F., & Musshoff, O. (2018). Wie kommunizieren Landwirte in Zeiten der Digitalisierung? *Berichte über Landwirtschaft, Zeitschrift für Agrarpolitik und Landwirtschaft*, *96*(2), 1–29.

Ferris, J. L. (2017). Data privacy and protection in the agriculture industry: Is federal regulation necessary. *Minn. JL Sci. & Tech.*, *18*, 309. https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1422&context=mjlst

Finger, R., Swinton, S. M., El Benni, N., & Walter, A. (2019). Precision Farming at the Nexus of Agricultural Production and the Environment. *Annual Review of Resource Economics*, *11*, 313–335. https://doi.org/10.1146/annurev-resource-100518-093929

FIRST — Forum of Incident Response and Security Teams. (2019). CVSS version 3.1 Specification Document. https://www.first.org/cvss/specification-document

Fleisch, E., & Thiesse, F. (2007). On the management implications of ubiquitous computing: An is perspective. *ECIS 2007 Proceedings*, 71.

Fleming, A., Jakku, E., Lim-Camacho, L., Taylor, B., & Thorburn, P. (2018). Is big data for big farming or for everyone? perceptions in the Australian grains industry. *Agronomy for sustainable development*, *38*(3), 24.

Fountas, S., Carli, G., Sørensen, C., Tsiropoulos, Z., Cavalaris, C., Vatsanidou, A., Liakos, B., Canavari, M., Wiebensohn, J., & Tisserye, B. (2015). Farm management information systems: Current situation and future perspectives. *Computers and Electronics in Agriculture*, *115*, 40–50. https://doi.org/10.1016/j.compag.2015.05.011

Fountas, S., Blackmore, S., Ess, D., Hawkins, S., Blumhoff, G., Lowenberg-Deboer, J., & Sorensen, C. (2005). Farmer experience with precision agriculture in denmark and the us eastern corn belt. *Precision Agriculture*, *6*(2), 121–141.

Francis, R., & Bekera, B. (2014). A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliability Engineering & System Safety*, *121*, 90–103. https://doi.org/10.1016/j.ress.2013.07.004

Fraser, A. (2019). Land grab/data grab: Precision agriculture and its new horizons. *The Journal of Peasant Studies*, *46*(5), 893–912.

Friha, O., Ferrag, M. A., Shu, L., Maglaras, L. A., & Wang, X. (2021). Internet of things for the future of smart agriculture: A comprehensive survey of emerging technologies. *IEEE CAA J. Autom. Sinica*, *8*(4), 718–752.

Froelicher, D., Egger, P., Sousa, J. S., Raisaro, J. L., Huang, Z., Mouchet, C., Ford, B., & Hubaux, J.-P. (2017). UnLynx: A Decentralized System for Privacy-Conscious Data Sharing. *Proceedings on Privacy Enhancing Technologies*, *2017*(4), 232–250. https://doi.org/10.1515/popets-2017-0047

Gandorfer, M., Schleicher, S., Heuser, S., Pfeiffer, J., & Demmel, M. (2017). Landwirtschaft 4.0 – Digitalisierung und ihre Herausforderungen. In G. Wendl (Ed.), *Ackerbau-technische lösungen für die zukunft* (pp. 9–19). https://www.lfl.bayern.de/mam/cms07/ilt/dateien/digitalisierung_und_ihre_herausforderungen.pdf

Gardner, B., & Lerman, Z. (2006). Agricultural Cooperative Enterprise in the Transition from Socialist Collective Farming. *Journal of Rural Cooperation*, *34*(1). https://doi.org/10.22004/AG.ECON.7174

Gardner-Stephen, P., Farouque, S., Lloyd, M., Bate, A., & Cullen, A. (2017). Piloting the serval mesh and serval mesh extender 2.0 in Vanuatu: Preliminary results. *Proceedings of the Global Humanitarian Technology Conference*.

Gardner-Stephen, P. (2011). The Serval Project: Practical Wireless Ad-hoc Mobile Telecommunications. *Flinders University, Adelaide, Technical Report*.

Gardner-Stephen, P., & Palaniswamy, S. (2011). Serval Mesh Software-WiFi Multi Model Management. *Proceedings of the 1st International Conference on Wireless Technologies for Humanitarian Relief*. https://doi.org/10.1145/2185216.2185245

Gautam, R. S., Bhimavarapu, V. M., & Rastogi, S. (2021). Impact of Digitalization on the Farmers in India: Evidence using Panel Data Analysis. *International Journal of Management and Humanities*, *6*(1), 5–12. https://doi.org/10.35940/ijmh.L1372.0851221

Ge, L., Brewster, C., Spek, J., Smeenk, A., Top, J., van Diepen, F., Klaase, B., Graumans, C., & de Wildt, M. d. R. (2017). *Blockchain for agriculture and food: Findings from the pilot study*. Wageningen Economic Research. https://doi.org/10.18174/426747

Geil, A., Sagers, G., Spaulding, A. D., & Wolf, J. R. (2018). Cyber security on the farm: An assessment of cyber security practices in the United States agriculture industry. *International Food and Agribusiness Management Review*, *21*(3), 317–334. https://doi.org/10.22434/IFAMR2017.0045

Gerhold, L., Wahl, S., & Dombrowsky, W. R. (2019). Risk perception and emergency food preparedness in Germany. *International Journal of Disaster Risk Reduction*, *37*, 101183. https://doi.org/https://doi.org/10.1016/j.ijdrr.2019.101183

Gladisch, A., Rietschel, S., Mundt, T., Bauer, J., Goltz, J., & Wiedenmann, S. (2018). Securely connecting iot devices with lorawan, 220–229. https://doi.org/10.1109/WorldS4.2018.8611576

Grandhi, S. A., Plotnick, L., & Hiltz, S. R. (2020). An Internet-less World? Expected Impacts of a Complete Internet Outage with Implications for Preparedness and Design. *Proceedings of the ACM on Human-Computer Interaction*, *4*. https://doi.org/10.1145/3375183

Groher, T., Heitkämper, K., Walter, A., Liebisch, F., & Umstätter, C. (2020). Status quo of adoption of precision agriculture enabling technologies in swiss plant production. *Precision Agriculture*, *21*(6), 1327–1350.

Grosmann, M., & Ioannidis, C. (2020). Cloudless Computing - A Vision to Become Reality. *2020 International Conference on Information Networking (ICOIN)*, 372–377. https://doi.org/10.1109/ICOIN48656.2020.9016441

Grunwald, A., Schaarschmidt, M., & Westerkamp, C. (2020). LoRaWAN in a rural context: Use cases and opportunities for agricultural businesses. *24. ITG-Symposium on Mobile Communication - Technologies and Applications*, 134–139. https://ieeexplore.ieee.org/document/8731787

Gu, C., Jiang, L., Tan, R., Li, M., & Huang, J. (2020). Attack-aware data timestamping in low-power synchronization-free lorawan, 100–110. https://doi.org/10.1109/ICDCS47774.2020.00109

Gu, Y., & Jing, T. (2011). The IOT research in supply chain management of fresh agricultural products. *2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC)*, 7382–7385. https://doi.org/10.1109/AIMSEC.2011.6011477

Gul, S., Gutierrez, J., Sarkar, N. I., & Lai, E. (2018). Resilicomm: A framework for resilient communication system. *Proceedings of ISCRAM Asia Pacific*, 1–5.

Guntrum, L., Güldenring, B., Kuntke, F., & Reuter, C. (2022). Using Digitally Mediated Methods in Sensitive Contexts: A Threat Analysis and Critical Reflection on Security, Privacy, and Ethical Concerns in the Case of Afghanistan. *Zeitschrift für Friedens- und Konfliktforschung (ZeFKo)*, *11*(2), 95–128. https://doi.org/10.1007/s42597-022-00088-2

Gupta, M., Abdelsalam, M., Khorsandroo, S., & Mittal, S. (2020a). Security and Privacy in Smart Farming: Challenges and Opportunities. *IEEE Access*, *8*, 34564–34584. https://doi.org/10.1109/ACCESS.2020.2975142

Gupta, M., Abdelsalam, M., Khorsandroo, S., & Mittal, S. (2020b). Security and Privacy in Smart Farming: Challenges and Opportunities. *IEEE Access*, *8*, 34564–34584. https://doi.org/10.1109/ACCESS.2020.2975142

Gurschler, T., Großmann, J., Kotarski, D., Teichmann, C., Thim, C., Eichler, J., Göllner, J., Gronau, N., & Lechner, U. (2017). Risikobeurteilung in der IT-Sicherheit Kritischer Infrastrukturen – Eine Analyse der Risikobeurteilung im Förderschwerpunkt ITS|KRITIS. *Tagungsband zum 15. Deutscher IT-Sicherheitskongress*, 395–410.

Hamami, L., & Nassereddine, B. (2020). Application of wireless sensor networks in the field of irrigation: A review. *Computers and Electronics in Agriculture*, *179*(April), 105782. https://doi.org/10.1016/j.compag.2020.105782

Han, C., Reyes, I., Feal, Á., Reardon, J., Wijesekera, P., Vallina-Rodriguez, N., Elazari, A., Bamberger, K. A., & Egelman, S. (01 Jul. 2020). The price is (not) right: Comparing privacy in free and paid apps. *Proceedings on Privacy Enhancing Technologies*, *2020*(3), 222–242. https://doi.org/https://doi.org/10.2478/popets-2020-0050

Harris, M. (2018). Tech giants race to build orbital internet. *IEEE Spectrum*, *55*(6), 10–11. https://doi.org/10.1109/MSPEC.2018.8362213

Hassan, S. S., Reuter, C., & Bzhalava, L. (2020). Perception or capability? – an empirical investigation of the factors influencing the adoption of social media and public cloud in German SMEs. *International Journal of Innovation Management*, 1–29. https://doi.org/10.1142/S136391962150002X

Herlich, M., & von Tüllenburg, F. (2018). Introduction to narrowband communication. *Wireless Congress: Systems and Applications*, 1–15.

Hessel, F., Almon, L., & Álvarez, F. (2020). Chirpotle: A framework for practical lorawan security evaluation, 306–316. https://doi.org/10.1145/3395351.3399423

Hevner, A., & Chatterjee, S. (2010). *Design Research in Information Systems: Theory and Practice* (Vol. 22). Springer US. https://doi.org/10.1007/978-1-4419-5653-8

Hill, K., Gagneja, K. K., & Singh, N. (2019). Lora phy range tests and software decoding - physical layer security, 805–810. https://doi.org/10.1109/SPIN.2019.8711682

Hobe, C.-f. V., Michels, M., Fecke, W., Mußhoff, O., Johann, P., & Ahlefeld, W. V. (2019). Wie kommunizieren Landwirte in Zeiten der Digitalisierung ? Ergebnisse und Diskussion. *39. GIL-Jahrestagung, Digitalisierung für landwirtschaftliche Betriebe in kleinstrukturierten Regionen - ein Widerspruch in sich?*, 269–274.

Höchst, J., Baumgärtner, L., Kuntke, F., Penning, A., Sterz, A., & Freisleben, B. (2020). LoRa-based Device-to-Device Smartphone Communication for Crisis Scenarios. *Proceedings of Information Systems for Crisis Response and Management (ISCRAM)*, 996–1011. http://idl.iscram.org/files/jonashochst/2020/2291_JonasHochst_etal2020.pdf

Höchst, J., Baumgärtner, L., Kuntke, F., Penning, A., Sterz, A., Sommer, M., & Freisleben, B. (2023). Mobile Device-to-Device Communication for Crisis Scenarios Using Low-Cost LoRa Modems. In H. J. Scholl, E. E. Holdeman, & F. K. Boersma (Eds.), *Disaster Management and Information Technology* (pp. 235–268, Vol. 40). Springer International Publishing. https://doi.org/10.1007/978-3-031-20939-0_12

Hoeren, T., & Kolany-Raiser, B. (Eds.). (2018). *Big Data in Context*. Springer International Publishing. https://doi.org/10.1007/978-3-319-62461-7

Holling, C. S. (1973). Resilience and Stability of Ecological Systems. *Annual Review of Ecology and Systematics*, *4*(1), 1–23. https://doi.org/10.1146/annurev.es.04.110173.000245

Huh, H., & Kim, J. Y. (2019). LoRa-based Mesh Network for IoT Applications. *Proceedings of the 5th World Forum on Internet of Things*.

Huyeng, T.-J., Bittner, T., & Rüppel, U. (2022). Examining the Feasibility of LoRa-based Monitoring in Large-scale Disaster Response Scenarios. *Proceedings of the 19th International Conference on Information Systems for Crisis Response and Management (ISCRAM)*, 541–550.

IoT Analytics GmbH. (2018, September 1). *Lpwan market report 2018-2023* (Market Report). Retrieved November 1, 2019, from https://iot-analytics.com/product/lpwan-market-report-2018-2023/

Iova, O., Murphy, A. L., Picco, G. P., Ghiro, L., Molteni, D., Ossi, F., & Cagnacci, F. (2017). LoRa from the City to the Mountains: Exploration of Hardware and Environmental Factors. *Proceedings of the 2017 International Conference on Embedded Wireless Systems and Networks*. Retrieved July 8, 2022, from https://hal.archives-ouvertes.fr/hal-01647149

ITU. (2021). Y.4480. Low power protocol for wide area wireless networks. https://handle.itu.int/11.1002/1000/14818

Jawad, H., Nordin, R., Gharghan, S., Jawad, A., & Ismail, M. (2017). Energy-Efficient Wireless Sensor Networks for Precision Agriculture: A Review. *Sensors*, *17*(8), 1781. https://doi.org/10.3390/s17081781

Jenner, B., Flick, U., von Kardoff, E., & Steinke, I. (2004). *A companion to qualitative research*. Sage Publications.

Jerhamre, E., Carlberg, C. J. C., & Van Zoest, V. (2022). Exploring the susceptibility of smart farming: Identified opportunities and challenges. *Smart Agricultural Technology*, *2*, 100026. https://doi.org/10.1016/j.atech.2021.100026

Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed Methods Research: A Research Paradigm Whose Time Has Come. *Educational Researcher*, *33*(7), 14–26. https://doi.org/10.3102/0013189X033007014

Jung, T. M. (2017, July). *Vergleich aktueller lpwan-technologien im internet der dinge unter einbindung von energy-harvesting*. https://opus.hs-offenburg.de/frontdoor/deliver/index/docId/2297/file/TomJung_Bachelorthesis_final.pdf

Kalle, T., Kaufhold, M.-A., Kuntke, F., Reuter, C., Rizk, A., & Steinmetz, R. (2019). Resilience in Security and Crises through Adaptions and Transitions. In C. Draude, M. Lange, & B. Sick (Eds.), *INFORMATIK 2019: 50 Jahre Gesellschaft für Informatik – Informatik für Gesellschaft (Workshop-Beiträge), Lecture Notes in Informatics (LNI)* (pp. 571–584). Gesellschaft für Informatik e. V. https://doi.org/10.18420/inf2019_ws60

Kamath, R. (2018). Food Traceability on Blockchain: Walmart's Pork and Mango Pilots with IBM. *The Journal of the British Blockchain Association*, *1*(1), 1–12. https://doi.org/10.31585/jbba-1-1-(10)2018

Kamble, P., & Gawade, A. (2019). Digitalization of healthcare with iot and cryptographic encryption against dos attacks, 69–73. https://doi.org/10.1109/IC3I46837.2019.9055531

Karrer, K., Glaser, C., Clemens, C., & Bruder, C. (2009). Technikaffinität erfassen – der Fragebogen TA-EG. *Der Mensch im Mittelpunkt technischer Systeme*, *8*, 196–201.

Kathuria, R., Kedia, M., Varma, G., Bagchi, K., & Sekhani, R. (2018). *The anatomy of an internet blackout: Measuring the economic impact of internet shutdowns in india*. Indian Council for Research on International Economic Relations.

Kaufhold, M.-A. (2021). *Information Refinement Technologies for Crisis Informatics: User Expectations and Design Principles for Social Media and Mobile Apps*. Springer Vieweg. https://doi.org/10.1007/978-3-658-33341-6

Kaufhold, M.-A., Riebe, T., Reuter, C., Hester, J., Jeske, D., Knüver, L., & Richert, V. (2018). Business Continuity Management in Micro Enterprises: Perception, Strategies and Use of ICT. *International Journal of Information Systems for Crisis Response and Management (IJISCRAM)*, *10*(1), 1–19. https://doi.org/10.4018/IJISCRAM.2018010101

Kaup, F., Hacker, S., Mentzendorff, E., Meurisch, C., & Hausheer, D. (2018). The Progress of the Energy-Efficiency of Single-board Computers.

Kenny, U., & Regan, A. (2021). Co-designing a smartphone app for and with farmers: Empathising with end-users' values and needs. *Journal of Rural Studies*, *82*, 148–160.

Keränen, A., Ott, J., & Kärkkäinen, T. (2009). The ONE Simulator for DTN Protocol Evaluation. *Proceedings of the 2nd International Conference on Simulation Tools and Techniques*.

Kernecker, M., Knierim, A., Wurbs, A., Kraus, T., & Borges, F. (2020). Experience versus expectation: farmers' perceptions of smart farming technologies for cropping systems across Europe. *Precision Agriculture*, *21*(1), 34–50. https://doi.org/10.1007/s11119-019-09651-z

Khan, F. H., & Portmann, M. (2018). Experimental Evaluation of LoRaWAN in NS-3 [ISSN: 2474-154X]. *2018 28th International Telecommunication Networks and Applications Conference (ITNAC)*, 1–8. https://doi.org/10.1109/ATNAC.2018.8615313

Khutsoane, O., Isong, B., & Abu-Mahfouz, A. M. (2017). IoT devices and applications based on LoRa/LoRaWAN. *Proceedings IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society*, *2017-January*, 6107–6112. https://doi.org/10.1109/IECON.2017.8217061

Kim, J., & Song, J. (2017). A simple and efficient replay attack prevention scheme for lorawan. *Proceedings of the 2017 the 7th International Conference on Communication and Network Security*, 32–36. https://doi.org/10.1145/3163058.3163064

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing Systematic Literature Reviews in Software Engineering* (tech. rep. No. EBSE-2007-01). Keele University and University of Durham. Citeseer.

Kitzinger, J. (1995). Qualitative Research: Introducing focus groups. *BMJ*, *311*(7000), 299–302. https://doi.org/10.1136/bmj.311.7000.299

Kleppmann, M., Wiggins, A., Van Hardenberg, P., & McGranaghan, M. (2019). Local-First Software: You Own Your Data, in spite of the Cloud. *Proceedings of the 2019 ACM SIGPLAN International Symposium on New Ideas, New Paradigms, and Reflections on Programming and Software*, 154–178. https://doi.org/10.1145/3359591.3359737

Klerkx, L., Jakku, E., & Labarthe, P. (2019). A review of social science on digital agriculture, smart farming and agriculture 4.0: New contributions and a future research agenda. *NJAS - Wageningen Journal of Life Sciences*, *90-91*, 100315. https://doi.org/10.1016/j.njas.2019.100315

Koenig, S., & Schauer, S. (2019). Cascading threats in critical infrastructures with control systems. *Proceedings of the 16th ISCRAM Conference*, *16*, 1252–1259.

Koerhuis, R. (2020). John Deere: 'We believe in electric tractors. 100%'. Retrieved June 8, 2021, from https://www.futurefarming.com/Machinery/Articles/2020/3/John-Deere-We-believe-in-electric-tractors-100-552869E

Kontio, J., Lehtola, L., & Bragge, J. (2004). Using the focus group method in software engineering: obtaining practitioner and user experiences. *International Symposium on Empirical Software Engineering*, 271–280. https://doi.org/10.1109/ISESE.2004.1334914

Kuntke, F., & Baumgärtner, L. (2023). *Simulation of 40 Selected German Farm neighborhoods with LoRaWAN-based DTN*. https://doi.org/10.6084/m9.figshare.21082441.v1

Kuntke, F., Baumgärtner, L., & Reuter, C. (2023). Rural Communication in Outage Scenarios: Disruption-Tolerant Networking via LoRaWAN Setups.

Proceedings of Information Systems for Crisis Response and Management (ISCRAM), 1–13. http://dx.doi.org/10.59297/WZMQ1124

Kuntke, F., Bektas, M., Buhleier, L., Pohl, E., Schiller, R., & Reuter, C. (2022). *Lora signal loss in rural areas dataset*. https://doi.org/10.48328/tudatalib-975

Kuntke, F., Bektas, M., Buhleier, L., Pohl, E., Schiller, R., & Reuter, C. (2023). How Would Emergency Communication Based on LoRaWAN Perform? Empirical Findings of Signal Propagation in Rural Areas. *Proceedings of Information Systems for Crisis Response and Management (ISCRAM)*, 1–8. http://dx.doi.org/10.59297/QBHV2089

Kuntke, F., Eberz-Eder, D., Trapp, M., & Reuter, C. (2023). RSF-Lab'23: Konzepte und Anwendungen zur resilienten digitalen Landwirtschaft. *INFORMATIK 2023: 53. Jahrestagung der Gesellschaft für Informatik – Informatik für Gesellschaft (Workshop-Beiträge)*, 1–7. https://doi.org/10.18420/inf2023_156

Kuntke, F., Kaufhold, M.-A., Linsner, S., & Reuter, C. (2023). GeoBox: Design and Evaluation of a Tool for Resilient and Decentralized Data Management in Agriculture. *Behaviour & Information Technology*. https://doi.org/10.1080/0144929X.2023.2185747

Kuntke, F., Linsner, S., Steinbrink, E., Franken, J., & Reuter, C. (2022). Resilience in Agriculture: Communication and Energy Infrastructure Dependencies of German Farmers. *International Journal of Disaster Risk Science*, *13*(2), 214–229. https://doi.org/10.1007/s13753-022-00404-7

Kuntke, F., Reuter, C., Schneider, W., Eberz, D., & Bernardi, A. (2020). Die GeoBox-Vision: Resiliente Interaktion und Kooperation in der Landwirtschaft durch dezentrale Systeme. In C. Hansen, A. Nürnberger, & B. Preim (Eds.), *Mensch und Computer 2020 - Workshopband* (pp. 1–6). Gesellschaft für Informatik e.V. https://doi.org/10.18420/muc2020-ws117-407

Kuntke, F., Romanenko, V., Linsner, S., Steinbrink, E., & Reuter, C. (2022). LoRaWAN security issues and mitigation options by the example of agricultural IoT scenarios. *Transactions on Emerging Telecommunications Technologies*, 1–20. https://doi.org/10.1002/ett.4452

Kuntke, F., Sinn, M., Linsner, S., & Reuter, C. (2021). Low Power Wide Area Networks (LPWAN) für krisentaugliche Datenübertragung in landwirtschaftlichen Betrieben. In A. Meyer-Aurich, M. Gandorfer, C. Hoffmann, C. Weltzien, S. D. Bellingrath-Kimura, & H. Floto (Eds.), *41. GIL-Jahrestagung: Informatik in der Land-, Forst- und Ernährungswirtschaft* (pp. 193–198). Gesellschaft für Informatik. https://dl.gi.de/handle/20.500.12116/35671

Kuntke, F., Sinn, M., & Reuter, C. (2021). Reliable Data Transmission using Low Power Wide Area Networks (LPWAN) for Agricultural Applications. *Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES 2021)*, 1–9. https://doi.org/10.1145/3465481.3469191

Kurosh, R.-M., & Saeid, S. (2010). Agricultural specialists' intention toward precision agriculture technologies: Integrating innovation characteristics to technology acceptance model. *African Journal of Agricultural Research*, *5*(11), 1191–1199.

Lawson, L. G., Pedersen, S. M., Sørensen, C. G., Pesonen, L., Fountas, S., Werner, A., Oudshoorn, F. W., Herold, L., Chatzinikos, T., Kirketerp, I. M., &

Blackmore, S. (2011). A four nation survey of farm information management and advanced farming systems: A descriptive analysis of survey responses. *Computers and Electronics in Agriculture*, *77*(1), 7–20. https://doi.org/10.1016/j.compag.2011.03.002

Lazar, J., Feng, J. H., & Hochheiser, H. (2017). *Research Methods in Human-Computer Interaction*. Morgan Kaufmann.

Lee, H.-C., & Ke, K.-H. (2018). Monitoring of large-area IoT sensors using a LoRa wireless mesh network system: Design and evaluation. *Transactions on Instrumentation and Measurement*, *67*(9).

Lee, J., Hwang, D., Park, J., & Kim, K.-H. (2017). Risk analysis and countermeasure for bit-flipping attack in lorawan, 549–551. https://doi.org/10.1109/ICOIN.2017.7899554

Li, W., Clark, B., Taylor, J. A., Kendall, H., Jones, G., Li, Z., Jin, S., Zhao, C., Yang, G., Shuai, C., et al. (2020). A hybrid modelling approach to understanding adoption of precision agriculture technologies in chinese cropping systems. *Computers and Electronics in Agriculture*, *172*, 105305.

Lindgren, A., Doria, A., Davies, E., & Grasic, S. (2012). *Probabilistic Routing Protocol for Intermittently Connected Networks* (Request for Comments No. 6693). http://www.rfc-editor.org/rfc/rfc6693.txt

Linsner, S., Kuntke, F., Schmidbauer-Wolf, G. M., & Reuter, C. (2019). Blockchain in Agriculture 4.0 - An Empirical Study on Farmers Expectations towards Distributed Services based on Distributed Ledger Technology. In F. Alt, A. Bulling, & T. Döring (Eds.), *Mensch und Computer 2019* (pp. 103–113). ACM. https://doi.org/10.1145/3340764.3340799

Linsner, S., Kuntke, F., Steinbrink, E., Franken, J., & Reuter, C. (2021). The Role of Privacy in Digitalization – Analysing the German Farmers' Perspective. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, *2021*(3). https://doi.org/10.2478/popets-2021-0050

Linsner, S., Steinbrink, E., Kuntke, F., Franken, J., & Reuter, C. (2022). Supporting Users in Data Disclosure Scenarios in Agriculture through Transparency. *Behaviour & Information Technology (BIT)*, *41*(10), 2137–2159. https://doi.org/10.1080/0144929X.2022.2068070

Lioutas, E. D., Charatsari, C., & De Rosa, M. (2021). Digitalization of agriculture: A way to solve the food problem or a trolley dilemma? *Technology in Society*, *67*, 101744. https://doi.org/10.1016/j.techsoc.2021.101744

Liu, Y., Ma, X., Shu, L., Hancke, G. P., & Abu-Mahfouz, A. M. (2021). From Industry 4.0 to Agriculture 4.0: Current Status, Enabling Technologies, and Research Challenges. *IEEE Transactions on Industrial Informatics*, *17*(6), 4322–4334. https://doi.org/10.1109/TII.2020.3003910

Lokers, R., Knapen, R., Janssen, S., van Randen, Y., & Jansen, J. (2016). Analysis of Big Data technologies for use in agro-environmental science. *Environmental Modelling & Software*, *84*, 494–504. https://doi.org/10.1016/j.envsoft.2016.07.017

LoRa Alliance. (2015). Lorawan™ specification v1.0.

LoRa Alliance. (2017). LoRaWAN 1.1 Specification, 1–101. https://lora-alliance.org/wp-content/uploads/2020/11/lorawantm_specification_-v1.1.pdf

LoRa Alliance. (2018). LoRaWAN 1.0.3 Specification, 1–72. https://lora-alliance.org/wp-content/uploads/2020/11/lorawan1.0.3.pdf

LoRa Alliance Technical Committee. (2020). LoRaWAN® L2 1.0.4 Specification (TS001-1.0.4), 1–75. https://lora-alliance.org/wp-content/uploads/2021/11/LoRaWAN-Link-Layer-Specification-v1.0.4.pdf

LoRa Alliance Technical Committee Regional Parameters Workgroup. (2021). *RP002-1.0.3 LoRaWAN® Regional Parameters*. https://lora-alliance.org/resource_hub/rp2-1-0-3-lorawan-regional-parameters/

Lottes, P., Khanna, R., Pfeifer, J., Siegwart, R., & Stachniss, C. (2017). Uav-based crop and weed classification for smart farming. *2017 IEEE International Conference on Robotics and Automation (ICRA)*, 3024–3031.

Lucas, V., Gasselin, P., & Van Der Ploeg, J. D. (2019). Local inter-farm cooperation: A hidden potential for the agroecological transition in northern agricultures. *Agroecology and Sustainable Food Systems*, *43*(2), 145–179. https://doi.org/10.1080/21683565.2018.1509168

Lv, Z., Qiao, L., Kumar Singh, A., & Wang, Q. (2021). Ai-empowered iot security for smart cities. *ACM Trans. Internet Technol.*, *21*(4). https://doi.org/10.1145/3406115

Macaulay, L. A. (1996). *Requirements Engineering* (P. J. Thomas & R. J. Paul, Eds.). Springer London. https://doi.org/10.1007/978-1-4471-1005-7

Madhumitha, M., & Singh, B. P. (2017). A survey on lpwan technologies in content to iot applications. *ICT Express*, *3*(1), 14–21.

Mahdavian, F., Platt, S., Wiens, M., Klein, M., & Schultmann, F. (2020). Communication blackouts in power outages: Findings from scenario exercises in Germany and France. *International Journal of Disaster Risk Reduction*, *46*, 101628. https://doi.org/10.1016/j.ijdrr.2020.101628

Malkin, N., Deatrick, J., Tong, A., Wijesekera, P., Egelman, S., & Wagner, D. (01 Oct. 2019). Privacy attitudes of smart speaker users. *Proceedings on Privacy Enhancing Technologies*, *2019*(4), 250–271. https://doi.org/https://doi.org/10.2478/popets-2019-0068

Marfievici, R., Murphy, A. L., Picco, G. P., Ossi, F., & Cagnacci, F. (2013). How Environmental Factors Impact Outdoor Wireless Sensor Networks: A Case Study [ISSN: 2155-6814]. *2013 IEEE 10th International Conference on Mobile Ad-Hoc and Sensor Systems*, 565–573. https://doi.org/10.1109/MASS.2013.13

Marra, M., Pannell, D. J., & Abadi Ghadim, A. (2003). The economics of risk, uncertainty and learning in the adoption of new agricultural technologies: where are we on the learning curve? *Agricultural Systems*, *75*(2), 215–234. https://doi.org/10.1016/S0308-521X(02)00066-5

Martinez, I., Tanguy, P., & Nouvel, F. (2019). On the performance evaluation of LoRaWAN under Jamming, 141–145. https://doi.org/10.23919/WMNC.2019.8881830

Mdhaffar, A., Chaari, T., Larbi, K., Jmaiel, M., & Freisleben, B. (2017). IoT-based health monitoring via LoRaWAN. *IEEE EUROCON 2017 -17th International Conference on Smart Technologies*, 519–524. https://doi.org/10.1109/EUROCON.2017.8011165

Mekki, K., Bajic, E., Chaxel, F., & Meyer, F. (2018). Overview of cellular lpwan technologies for iot deployment: Sigfox, lorawan, and nb-iot. *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 197–202.

Mekki, K., Bajic, E., Chaxel, F., & Meyer, F. (2019). A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT Express*, *5*(1), 1–7. https://doi.org/10.1016/j.icte.2017.12.005

Melicher, W., Sharif, M., Tan, J., Bauer, L., Christodorescu, M., & Leon, P. G. (2016). (Do Not) Track Me Sometimes: Users' Contextual Preferences for Web Tracking. *Proceedings on Privacy Enhancing Technologies*, *2016*(2), 135–154. https://doi.org/https://doi.org/10.1515/popets-2016-0009

Meshtastic LLC. (2023). *Meshtastic*. Retrieved October 7, 2023, from https://meshtastic.org/docs/introduction

Meuwissen, M. P., Feindt, P. H., Spiegel, A., Termeer, C. J., Mathijs, E., de Mey, Y., Finger, R., Balmann, A., Wauters, E., Urquhart, J., Vigani, M., Zawalińska, K., Herrera, H., Nicholas-Davies, P., Hansson, H., Paas, W., Slijper, T., Coopmans, I., Vroege, W., . . . Reidsma, P. (2019). A framework to assess the resilience of farming systems. *Agricultural Systems*, *176*, 102656. https://doi.org/10.1016/j.agsy.2019.102656

Michels, M., Bonke, V., & Musshoff, O. (2020). Understanding the adoption of smartphone apps in crop protection. *Precision Agriculture*, *21*(6), 1209–1226.

Michels, M., & Mußhoff, O. (2020). An Empirical Study of Smartphone Use Intensity in German Agriculture. *German Journal of Agricultural Economics*, *69*(2), 127–142. https://doi.org/10.30430/69.2020.2.127-142

Michels, M., & Musshoff, O. (2021). The timing of smartphone adoption in german agriculture. In *Precision agriculture'21* (pp. 427–446). Wageningen Academic Publishers.

Michels, M., von Hobe, C.-F., & Musshoff, O. (2020). A trans-theoretical model for the adoption of drones by large-scale german farmers. *Journal of Rural Studies*, *75*, 80–88.

Michels, M., von Hobe, C.-F., Weller von Ahlefeld, P. J., & Musshoff, O. (2021). The adoption of drones in german agriculture: A structural equation model. *Precision Agriculture*, *22*(6), 1728–1748.

Mikhaylov, K., Fujdiak, R., Pouttu, A., Miroslav, V., Malina, L., & Mlynek, P. (2019). Energy attack in lorawan: Experimental validation. https://doi.org/10.1145/3339252.3340525

Mitchell, S., Weersink, A., & Erickson, B. (2018). Adoption of precision agriculture technologies in ontario crop production. *Canadian Journal of Plant Science*, *98*(6), 1384–1388.

Mohr, S., & Kühl, R. (2021). Acceptance of artificial intelligence in german agriculture: An application of the technology acceptance model and the theory of planned behavior. *Precision Agriculture*, *22*(6), 1816–1844.

Monteil, C., Barclay, J., & Hicks, A. (2020). Remembering, Forgetting, and Absencing Disasters in the Post-disaster Recovery Process. *International Journal of Disaster Risk Science*, *11*(3), 287–299. https://doi.org/10.1007/s13753-020-00277-8

Morgan, D. (1997). *Focus Groups as Qualitative Research* (Vol. 16). SAGE Publications, Inc. https://doi.org/10.4135/9781412984287

Moteff, J., Copeland, C., & Fischer, J. (2003). *Critical Infrastructures: What Makes an Infrastructure Critical?* (Tech. rep.). Library of Congress Washington DC Congressional Research Service. https://apps.dtic.mil/dtic/tr/fulltext/u2/a467306.pdf

Msaad, M., Waleed, M., & Kosta, S. (2021). Enabling LoRaWAN Communication with Out-of-coverage End Nodes in DTN Scenarios Through an Optimised Duty-cycle. *Proceedings of the 14th Critical ICT Infrastructures and Platforms International Conference*. https://doi.org/10.1109/CMI53512.2021.9663774

Muenzberg, T., Berbner, U., Comes, T., Friedrich, H., Gross, W., Pfohl, H.-C., & Schultmann, F. (2013). Decision support for critical infrastructure disruptions: An integrated approach to secure food supply. *Proceedings of the 10th International ISCRAM Conference*, *10*, 312–316.

Mundt, T., Gladisch, A., Rietschel, S., Bauer, J., Goltz, J., & Wiedenmann, S. (2018). General security considerations of lorawan version 1.1 infrastructures, 118–123. https://doi.org/10.1145/3265863.3265882

Munz, J., Gindele, N., & Doluschitz, R. (2020). Exploring the characteristics and utilisation of Farm Management Information Systems (FMIS) in Germany. *Computers and Electronics in Agriculture*, *170*, 105246. https://doi.org/10.1016/j.compag.2020.105246

Na, S., Hwang, D., Shin, W., & Kim, K.-H. (2017). Scenario and countermeasure for replay attack using join request messages in lorawan, 718–720. https://doi.org/10.1109/ICOIN.2017.7899580

Naeini, P. E., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L. F., & Sadeh, N. (2017). Privacy expectations and preferences in an iot world. *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 399–412. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/naeini

Navarro, E., Costa, N., & Pereira, A. (2020). A Systematic Review of IoT Solutions for Smart Farming. *Sensors*, *20*(15), 4231. https://doi.org/10.3390/s20154231

Nery, M., Santos, R., Santos, W., Lourenco, V., & Moreno, M. (2018). Facing digital agriculture challenges with knowledge engineering. *2018 First International Conference on Artificial Intelligence for Industries (AI4I)*, 118–119.

Nikander, J., Koistinen, M., Laajalahti, M., Pesonen, L., Ronkainen, A., & Suomi, P. (2015). Farm information management infrastructures in the future. *2015 26th International Workshop on Database and Expert Systems Applications (DEXA)*, 104–107. https://doi.org/10.1109/DEXA.2015.38

Nikander, J., Manninen, O., & Laajalahti, M. (2020a). Requirements for cybersecurity in agricultural communication networks. *Computers and Electronics in Agriculture*, *179*(October), 105776. https://doi.org/10.1016/j.compag.2020.105776

Nikander, J., Manninen, O., & Laajalahti, M. (2020b). Requirements for cybersecurity in agricultural communication networks. *Computers and Electronics in Agriculture*, *179*, 105776. https://doi.org/10.1016/j.compag.2020.105776

Nikkilä, R., Seilonen, I., & Koskinen, K. (2010). Software architecture for farm management information systems in precision agriculture [Special issue on Information and Communication Technologies in Bio and Earth Sciences]. *Computers and Electronics in Agriculture*, *70*(2), 328–336. https://doi.org/10.1016/j.compag.2009.08.013

Nolan, K., & Kelly, M. (2018). Ipv6 convergence for iot cyber–physical systems. *Information*, *9*(4), 70.

Noura, H., Hatoum, T., Salman, O., Yaacoub, J.-P., & Chehab, A. (2020). Lorawan security survey: Issues, threats and possible mitigation techniques. *Internet of Things*, *12*, 100303. https://doi.org/10.1016/j.iot.2020.100303

OECD. (2019, September). Digital innovations and the growing importance of agricultural data. In *Digital Opportunities for Better Agricultural Policies* (pp. 20–36). https://doi.org/10.1787/367ac383-en

Ojha, T., Misra, S., & Raghuwanshi, N. S. (2015). Wireless sensor networks for agriculture: The state-of-the-art in practice and future challenges. *Computers and Electronics in Agriculture*, *118*, 66–84. https://doi.org/10.1016/j.compag.2015.08.011

Ojo, M., Adami, D., & Giordano, S. (2021). Experimental Evaluation of a LoRa Wildlife Monitoring Network in a Forest Vegetation Area. *Future Internet*, *13*, 115. https://doi.org/10.3390/fi13050115

Onwuegbuzie, A. J., Dickinson, W. B., Leech, N. L., & Zoran, A. G. (2009). A Qualitative Framework for Collecting and Analyzing Data in Focus Group Research. *International Journal of Qualitative Methods*, *8*(3), 1–21. https://doi.org/10.1177/160940690900800301

Orlov, D., Kuntke, F., & Reuter, C. (2023). Optimierte Messenger-Applikation zur Notfallkommunikation via LoRaWAN-DTN. *INFORMATIK 2023: 53. Jahrestagung der Gesellschaft für Informatik – Informatik für Gesellschaft (Workshop-Beiträge)*, 1–6. https://doi.org/10.18420/inf2023_160

O'Rourke, T. D. (2007). Critical Infrastructure, Interdependencies, and Resilience. *BRIDGE-Washington-National Academy of Engineering-*, *37*(1), 22.

Panteli, M., & Mancarella, P. (2015). The Grid: Stronger, Bigger, Smarter? Presenting a Conceptual Framework of Power System Resilience. *IEEE Power and Energy Magazine*, *13*(3), 58–66. https://doi.org/10.1109/MPE.2015.2397334

Parker, C., & Sinclair, M. (2001). User-centred design does make a difference. The case of decision support systems in crop production. *Behaviour and Information Technology*, *20*(6), 449–460. https://doi.org/10.1080/01449290110089570

Paulus, M., Pfaff, S. A., Knierim, A., & Schüle, H. (2022). Landwirtschaftliche Digitalisierung im Vergleich von Haupt- und Nebenerwerb. *42. GIL-Jahrestagung, Künstliche Intelligenz in der Agrar- und Ernährungswirtschaft*, 213–218. https://dl.gi.de/handle/20.500.12116/38399

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Pelletier, N., Audsley, E., Brodt, S., Garnett, T., Henriksson, P., Kendall, A., Kramer, K. J., Murphy, D., Nemecek, T., & Troell, M. (2011). Energy Intensity of Agriculture and Food Systems. *Annual Review of Environment and Resources*, *36*(1), 223–246. https://doi.org/10.1146/annurev-environ-081710-161014

Perković, T., & Siriščević, D. (2020). Low-cost lorawan jammer, 1–6. https://doi.org/10.23919/SpliTech49282.2020.9243739

Perrin, A., & Martin, G. (2021). Resilience of French organic dairy cattle farms and supply chains to the Covid-19 pandemic. *Agricultural Systems*, *190*, 103082. https://doi.org/https://doi.org/10.1016/j.agsy.2021.103082

Petermann, T., Bradke, H., Lüllmann, A., Poetzsch, M., & Riehm, U. (2010). Gefährdung und Verletzbarkeit moderner Gesellschaften - am Beispiel eines großräumigen Ausfalls der Stromversorgung. Endbericht zum TA-Projekt.

Petit, C., Bressoud, F., & Aubry, C. (2010). The effects of transition towards short supply chains on liveability of farming systems: Initial findings and further research needs. *9. European IFSA Symposium*, 1138–1147.

Petrariu, A. I. (2021). A Study on LoRa Signal Propagation Models in Urban Environments for Large-scale Networks Deployment [Number: 4 Publisher: Stefan cel Mare University of Suceava]. *Advances in Electrical and Computer Engineering*, *21*(4), 61–68. https://doi.org/10.4316/AECE.2021.04007

Petrić, T., Goessens, M., Nuaymi, L., Toutain, L., & Pelov, A. (2016). Measurements, performance and analysis of LoRa FABIAN, a real-world implementation of LPWAN [ISSN: 2166-9589]. *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 1–7. https://doi.org/10.1109/PIMRC.2016.7794569

Pfaff, S. A., Paulus, M., Knierim, A., & Schüle, H. (2022). Welche spezifischen Anforderungen impliziert die klein- strukturierte Landwirtschaft für die Digitalisierung? *42. GIL-Jahrestagung, Künstliche Intelligenz in der Agrar- und Ernährungswirtschaft*, 219–224. https://dspace.gi.de/handle/20.500.12116/38400

Pfohl, T. N. (2014). *Katastrophenmanagement in Deutschland: Eine Governance-Analyse* (Vol. 197). LIT Verlag Münster.

Pham, A., Dacosta, I., Jacot-Guillarmod, B., Huguenin, K., Hajar, T., Tramèr, F., Gligor, V., & Hubaux, J.-P. (2017). PrivateRide: A Privacy-Enhanced Ride-Hailing Service. *Proceedings on Privacy Enhancing Technologies*, *2017*(2), 38–56. https://doi.org/https://doi.org/10.1515/popets-2017-0015

Philip, S. J., McQuillan, J. M., & Adegbite, O. (2020). Lorawan v1.1 security: Are we in the clear yet?, 112–118. https://doi.org/10.1109/DependSys51298.2020.00025

Pinaki, M., & Tewari, V. K. (2010). Present status of precision farming: A review. *International Journal of Agricultural Research*, *5*(12), 1124–1133. https://doi.org/https://doi.org/10.3923/ijar.2007.1.10

Pipek, V., & Wulf, V. (2009). Infrastructuring: Toward an Integrated Perspective on the Design and Use of Information Technology. *Journal of the Association for Information Systems*, *10*(5), 447–473. https://doi.org/10.17705/1jais.00195

Popescu, A., Alecu, I. N., Dinu, T. A., Stoian, E., Condei, R., & Ciocan, H. (2016). Farm Structure and Land Concentration in Romania and the European Union's Agriculture. *Agriculture and Agricultural Science Procedia*, *10*, 566–577. https://doi.org/10.1016/j.aaspro.2016.09.036

Porter, M. E., & Heppelmann, J. E. (2014). How smart, connected products are transforming competition. *Harvard business review*, *92*(11), 64–88.

Queralta, J. P., Gia, T., Zou, Z., Tenhunen, H., & Westerlund, T. (2019). Comparative Study of LPWAN Technologies on Unlicensed Bands for M2M Communication in the IoT: Beyond LoRa and LoRaWAN. *Procedia Computer Science*, *155*, 343–350. https://doi.org/10.1016/j.procs.2019.08.049

Qvist, M. (2018a). 15 kilometre lora ssh link with rnode. Retrieved January 8, 2020, from https://unsigned.io/15-kilometre-ssh-link-with-rnode/

Qvist, M. (2018b). Rnode. Retrieved January 8, 2020, from https://unsigned.io/projects/rnode/

Qvist, M. (2018c). Rnodeconfigutil. Retrieved January 8, 2020, from https://github.com/markqvist/rnodeconfigutil

Raad, N., Hasan, T., Chalak, A., & Waleed, J. (2019). Secure data in lorawan network by adaptive method of elliptic-curve cryptography, 1–6. https://doi.org/10.1109/ICCISTA.2019.8830653

Rademacher, Y. (2013). Community disaster management assets: A case study of the farm community in Sussex County, Delaware. *International Journal of Disaster Risk Science*, *4*, 33–47. https://doi.org/10.1007/s13753-013-0005-y

Rama, Y., & Özpmar, M. A. (2018). A comparison of long-range licensed and unlicensed lpwan technologies according to their geolocation services and commercial opportunities. *2018 18th Mediterranean Microwave Symposium (MMS)*, 398–403.

Rana, B., Singh, Y., & Singh, P. K. (2021). A systematic survey on internet of things: Energy efficiency and interoperability perspective. *Transactions on Emerging Telecommunications Technologies*, *32*(8). https://doi.org/10.1002/ett.4166

Raza, U., Kulkarni, P., & Sooriyabandara, M. (2017). Low power wide area networks: An overview. *IEEE Communications Surveys & Tutorials*, *19*(2), 855–873.

Regan, Á., Green, S., Maher, P., et al. (2018). Smart farming in ireland: Anticipating positive and negative impacts through a qualitative study of risk and benefit perceptions amongst expert actors in the irish agri-food sector. *Proceedings of the 13th European International Farm Systems Association Symposium, Chania, Greece*, 1–5. http://ifsa.boku.ac.at/cms/fileadmin/Proceeding2018/Theme4_Regan.pdf

Reuter, C. (2015). Towards Efficient Security: Business Continuity Management in Small and Medium Enterprises. *International Journal of Information Systems for Crisis Response and Management*, *7*(3), 69–79. https://doi.org/10.4018/IJISCRAM.2015070105

Reuter, C. (2019). *Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace* (C. Reuter, Ed.). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-25652-4

Reuter, C., Eberz-Eder, D., Kuntke, F., & Trapp, M. (2022). RSF-Lab'22: Resilient Smart Farming Laboratory: Für eine widerstandsfähige und intelligente Landwirtschaft. In D. Demmler, D. Krupka, & H. Federrath (Eds.), *INFORMATIK 2022: 52. Jahrestagung der Gesellschaft für Informatik – Informatik für Gesellschaft (Workshop-Beiträge), Lecture Notes in Informatics (LNI)* (pp. 931–934). Gesellschaft für Informatik e. V. https://doi.org/10.18420/inf2022_78

Reuter, C., Kuntke, F., Trapp, M., Wied, C., Brill, G., Müller, G., Steinbrink, E., Franken, J., Eberz-Eder, D., & Schneider, W. (2022). AgriRegio: Infrastruktur zur Förderung von digitaler Resilienz und Klimaresilienz im ländlichen Raum am Beispiel der Pilotregion Nahe-Donnersberg. In D. Demmler, D. Krupka, & H. Federrath (Eds.), *INFORMATIK 2022:*

52. Jahrestagung der Gesellschaft für Informatik – Informatik für Gesellschaft (Workshop-Beiträge), Lecture Notes in Informatics (LNI) (pp. 961–972). Gesellschaft für Informatik e. V. https://doi.org/10.18420/inf2022_81

Reuter, C., Ludwig, T., Kaufhold, M.-A., & Hupertz, J. (2017). Social Media Resilience during Infrastructure Breakdowns using Mobile Ad-Hoc Networks. In V. Wohlgemuth, F. Fuchs-Kittowski, & J. Wittmann (Eds.), *Advances and New Trends in Environmental Informatics - Proceedings of the 30th EnviroInfo Conference* (pp. 75–88). Springer. https://doi.org/10.1007/978-3-319-44711-7_7

Reuter, C., Schneider, W., & Eberz, D. (2019). Resilient Smart Farming (RSF) – Nutzung digitaler Technologien in krisensicherer Infrastruktur. In A. Meyer-Aurich (Ed.), *39. gil-jahrestagung: Informatik in der land-, forst- und ernährungswirtschaft fokus; digitalisierung für landwirtschaftliche betriebe in kleinstrukturierten regionen – ein widerspruch in sich?, lecture notes in informatics (lni)* (pp. 177–182). Gesellschaft für Informatik. http://gil-net.de/Publikationen/139_177.pdf

Riegel, N., & Dörr, J. (2015). A Systematic Literature Review of Requirements Prioritization Criteria. In S. A. Fricker & K. Schneider (Eds.), *Requirements Engineering: Foundation for Software Quality* (pp. 300–317, Vol. 9013). Springer International Publishing. https://doi.org/10.1007/978-3-319-16101-3_22

Rizzato, F. (2019). Parts of rural Germany see less than 50% 4G Availability. Retrieved April 21, 2021, from https://www.opensignal.com/2019/07/17/parts-of-rural-germany-see-less-than-50-4g-availability

Rocchetto, M., & Tippenhauer, N. O. (2016). On attacker models and profiles for cyber-physical systems. In I. Askoxylakis, S. Ioannidis, S. Katsikas, & C. Meadows (Eds.). Springer International Publishing.

Rohn, E., & Erez, G. (2012). Fighting agro-terrorism in cyberspace: A framework for intention detection using overt electronic data sources. *Proceedings of the 9th International ISCRAM Conference*, *9*, 1–5.

Rose, D. C., & Chilvers, J. (2018). Agriculture 4.0: Broadening Responsible Innovation in an Era of Smart Farming. *Frontiers in Sustainable Food Systems*, *2*. https://doi.org/10.3389/fsufs.2018.00087

Rosskopf, K., & Wagner, P. (2006). Vom Daten- zum Wissensmanagement : Wofür verwenden Landwirte einen Computer ? *GIL Jahrestagung*, 225–228.

Rübcke von Veltheim, F., & Heise, H. (2021). German farmers' attitudes on adopting autonomous field robots: An empirical survey. *Agriculture*, *11*(3), 216.

Ruotsalainen, H., & Grebeniuk, S. (2018). Towards wireless secret key agreement with lora physical layer. https://doi.org/10.1145/3230833.3232803

Ryu, M., Yun, J., Miao, T., Ahn, I.-Y., Choi, S.-C., & Kim, J. (2015). Design and implementation of a connected farm for smart farming system. *2015 IEEE SENSORS*, 1–4.

Salam, A. (2020). Internet of Things for Sustainability: Perspectives in Privacy, Cybersecurity, and Future Trends. In *Internet of Things for Sustainable Community Development* (pp. 299–327). Springer International Publishing. https://doi.org/10.1007/978-3-030-35291-2_10

Saleem, H., & Naveed, M. (2020). SoK: Anatomy of Data Breaches. *Proceedings on Privacy Enhancing Technologies*, *2020*(4), 153–174. https://doi.org/10.2478/popets-2020-0067

Sánchez-Carmona, A., Robles, S., & Borrego, C. (2016). PrivHab+: A secure geographic routing protocol for DTN. *Computer Communications*, *78*.

Sanjeevi, P., Prasanna, S., Siva Kumar, B., Gunasekaran, G., Alagiri, I., & Vijay Anand, R. (2020). Precision agriculture and farming using Internet of Things based on wireless sensor network. *Transactions on Emerging Telecommunications Technologies*, *31*(12). https://doi.org/10.1002/ett.3978

Saxena, S., Pandey, A., & Kumar, S. (2019). A multistage rssi-based scheme for node compromise detection in iot networks, 1–4. https://doi.org/10.1109/INDICON47234.2019.9029092

Schmid, D., Kuntke, F., Bauer, M., & Baumgärtner, L. (2023). BPoL: A Disruption-Tolerant LoRa Network for Disaster Communication. *2023 IEEE Global Humanitarian Technology Conference (GHTC)*, 440–447. https://doi.org/10.1109/GHTC56179.2023.10354717

Schröder, L., & Klaue, C. (2005). Eingeschneit: Schneechaos im Münsterland [[Documentary Film]]. https://www1.wdr.de/fernsehen/heimatflimmern/sendungen/schneechaos-im-muensterland-100.html

Schukat, S., & Heise, H. (2021a). Smart products in livestock farming—an empirical study on the attitudes of german farmers. *Animals*, *11*(4), 1055.

Schukat, S., & Heise, H. (2021b). Towards an understanding of the behavioral intentions and actual use of smart products among german farmers. *Sustainability*, *13*(12), 6666.

Schüller, L. K., & Heuwieser, W. (2016). Measurement of heat stress conditions at cow level and comparison to climate conditions at stationary locations inside a dairy barn. *Journal of Dairy Research*, *83*(3), 305–311. https://doi.org/10.1017/S0022029916000388

Schulze Schwering, D., & Lemken, D. (2020). Totally digital? adoption of digital farm management information systems. In M. Gandorfer, A. Meyer-Aurich, H. Bernhardt, F. X. Maidl, G. Fröhlich, & H. Floto (Eds.), *40. gil-jahrestagung, digitalisierung für mensch, umwelt und tier* (pp. 295–300). Gesellschaft für Informatik e.V.

Schwering, D. S., & Lemken, D. (2020). Totally Digital? Adoption of Digital Farm Management Information Systems. *40. GIL-Jahrestagung, Digitalisierung für Mensch, Umwelt und Tier*, 295–300.

Semtech Corporation. (2020). Semtech SX1276/77/78/79 Datasheet Rev. 7. Retrieved June 2, 2021, from https://www.semtech.com/products/wireless-rf/lora-core/sx1276

Setianingsih, C., Nurjanah, R. S., Devi Gunawan, A., Nurjanah, R., & Murti, M. A. (2018). ION-DTN based on UAV System for Emergency Communication During Natural Disaster. *Proceedings of the 21st International Symposium on Wireless Personal Multimedia Communications*. https://doi.org/10.1109/WPMC.2018.8713099

Shang, L., Heckelei, T., Gerullis, M. K., Börner, J., & Rasch, S. (2021). Adoption and diffusion of digital farming technologies - integrating farm-level evidence and system interaction. *Agricultural Systems*, *190*, 103074. https://doi.org/10.1016/j.agsy.2021.103074

Shepherd, M., Turner, J. A., Small, B., & Wheeler, D. (2018). Priorities for science to overcome hurdles thwarting the full promise of the 'digital agriculture'revolution. *Journal of the Science of Food and Agriculture*.

Shi, X., An, X., Zhao, Q., Liu, H., Xia, L., Sun, X., & Guo, Y. (2019). State-of-the-art internet of things in protected agriculture. *Sensors*, *19*(8), 1833.

Shin, Y., Im, C., Oh, H., & Kim, J. (2017). Design for experience innovation: understanding user experience in new product development. *Behaviour and Information Technology*, *36*(12), 1218–1234. https://doi.org/10.1080/0144929X.2017.1368709

Singh, R. K., Berkvens, R., & Weyn, M. (2020). Synchronization and efficient channel hopping for power efficiency in lora networks: A comprehensive study. *Internet of Things*, *11*, 100233. https://doi.org/10.1016/j.iot.2020.100233

Sinha, B. B., & Dhanalakshmi, R. (2021). Recent advancements and challenges of Internet of Things in smart agriculture: A survey. *Future Generation Computer Systems*, *126*, 169–184. https://doi.org/10.1016/j.future.2021.08.006

Sisinni, E., Carvalho, D. F., & Ferrari, P. (2020). Emergency communication in iot scenarios by means of a transparent lorawan enhancement. *IEEE Internet of Things Journal*, *7*(10), 10684–10694. https://doi.org/10.1109/JIOT.2020.3011262

Skorpil, V., Oujezsky, V., & Palenik, L. (2018). Internet of things security overview and practical demonstration, 1–7. https://doi.org/10.1109/ICUMT.2018.8631198

Slijper, T., de Mey, Y., Poortvliet, P. M., & Meuwissen, M. P. M. (2022). Quantifying the resilience of European farms using FADN. *European Review of Agricultural Economics*, *49*(1), 121–150. https://doi.org/10.1093/erae/jbab042

Smullen, D., Feng, Y., Zhang, S. A., & Sadeh, N. (01 Jan. 2020). The best of both worlds: Mitigating trade-offs between accuracy and user burden in capturing mobile app privacy preferences. *Proceedings on Privacy Enhancing Technologies*, *2020*(1), 195–215. https://doi.org/https://doi.org/10.2478/popets-2020-0011

Snow, V., Rodriguez, D., Dynes, R., Kaye-Blake, W., Mallawaarachchi, T., Zydenbos, S., Cong, L., Obadovic, I., Agnew, R., Amery, N., Bell, L., Benson, C., Clinton, P., Dreccer, M. F., Dunningham, A., Gleeson, M., Harrison, M., Hayward, A., Holzworth, D., ... Stevens, D. (2021). Resilience achieved via multiple compensating subsystems: The immediate impacts of COVID-19 control measures on the agri-food systems of Australia and New Zealand. *Agricultural Systems*, *187*, 103025. https://doi.org/10.1016/j.agsy.2020.103025

Soden, R., & Palen, L. (2018). Informating Crisis: Expanding Critical Perspectives in Crisis Informatics. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), 1–22. https://doi.org/10.1145/3274431

Sontowski, S., Gupta, M., Laya Chukkapalli, S. S., Abdelsalam, M., Mittal, S., Joshi, A., & Sandhu, R. (2020). Cyber Attacks on Smart Farming Infrastructure. *2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC)*, 135–143. https://doi.org/10.1109/CIC50333.2020.00025

Sørensen, C. G., Fountas, S., Nash, E., Pesonen, L., Bochtis, D. D., Pedersen, S. M., Basso, B. B., & Blackmore, S. (2010). Conceptual model of a future farm management information system. *Computers and Electronics in Agriculture*, *72*(1), 37–47. https://doi.org/10.1016/j.compag.2010.02.003

Spykman, O., Gabriel, A., Ptacek, M., & Gandorfer, M. (2021). Farmers' perspectives on field crop robots – Evidence from Bavaria, Germany. *Computers and Electronics in Agriculture*, *186*, 106176. https://doi.org/10.1016/j.compag.2021.106176

Statistisches Bundesamt. (2019). Land- und Forstwirtschaft. In *Statistisches jahrbuch 2019* (pp. 487–520). https://www.destatis.de/DE/Themen/Querschnitt/Jahrbuch/statistisches-jahrbuch-2019-dl.pdf?%7B%5C_%7D%7B%5C_%7Dblob=publicationFile

Statistisches Bundesamt (Destatis). (2021a). 2020 Census of Agriculture shows continuing decline in workforce [Accessed: 2022-08-18]. Retrieved August 18, 2022, from https://www.destatis.de/EN/Press/2021/09/PE21_N053_13.html

Statistisches Bundesamt (Destatis). (2021b). *Betriebsgrößenstruktur landwirtschaftlicher Betriebe nach Bundesländern*. Retrieved June 17, 2022, from https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Landwirtschaft-Forstwirtschaft-Fischerei/Landwirtschaftliche-Betriebe/Tabellen/betriebsgroessenstruktur-landwirtschaftliche-betriebe.html

Statistisches Bundesamt (Destatis). (2021c, July). Agricultural holdings and utilised agricultural area by size of the utilised agricultural area [Accessed: 2021-07-18]. https://www.destatis.de/EN/Themes/Economic-Sectors-Enterprises/Agriculture-Forestry-Fisheries/Agricultural-Holdings/Tables/agricultural-holdings-and-utilised-agricultural-areaby-size-of-the-utilised-agricultural-area.html

Strauss, A. L., & Corbin, J. (1998). *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage Publications.

SubCableWorld. (2015). Timeline for CNMI outage. https://www.subcableworld.com/scw-newsfeed/marine-services/timeline-for-cnmi-outage

Sundmaeker, H., Verdouw, C., Wolfert, S., & Pérez Freire, L. (2016). Internet of Food and Farm 2020. *Digitising the Industry Internet of Things Connecting the Physical, Digital and Virtual Worlds*, *49*(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

Sung, W.-J., Ahn, H.-G., Kim, J.-B., & Choi, S.-G. (2018). Protecting end-device from replay attack on lorawan, 167–171. https://doi.org/10.23919/ICACT.2018.8323684

Suryadevara, N. K., & Dutta, A. (2022). Meshtastic Infrastructure-less Networks for Reliable Data Transmission to Augment Internet of Things Applications. In Q. Guo, W. Meng, M. Jia, & X. Wang (Eds.), *Wireless and Satellite Systems* (pp. 622–640, Vol. 410). Springer International Publishing. https://doi.org/10.1007/978-3-030-93398-2_55

Sykuta, M. E. (2016). Big Data in Agriculture: Property Rights, Privacy and Competition in Ag Data Services. *International Food and Agribusiness Management Review*, (1030-2016-83141), 18. https://doi.org/10.22004/ag.econ.240696
The IFAMR is published quarterly my IFAMA. For more information visit: www.ifama.org.

Tendall, D., Joerin, J., Kopainsky, B., Edwards, P., Shreck, A., Le, Q., Kruetli, P., Grant, M., & Six, J. (2015). Food system resilience: Defining the concept. *Global Food Security*, *6*, 17–23. https://doi.org/10.1016/j.gfs.2015.08.001

Terence, S., & Purushothaman, G. (2020). Systematic review of Internet of Things in smart farming. *Transactions on Emerging Telecommunications Technologies*, *31*(6). https://doi.org/10.1002/ett.3958

Tey, Y. S., & Brindal, M. (2022). A meta-analysis of factors driving the adoption of precision agriculture. *Precision Agriculture*, *23*(2), 353–372.

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (2019). *Strategic importance of, and dependence on, undersea cables*. https://ccdcoe.org/library/publications/strategic-importance-of-and-dependence-on-undersea-cables/

Thiel, C. C., Thiel, C. C., Kmu, U., & Re-, F. (2010). Business Continuity Management für KMU. *Datenschutz und Datensicherheit - DuD*, *34*(6), 404–407. https://doi.org/10.1007/s11623-010-0114-3

Thomas, J., Cherian, S., Chandran, S., & Pavithran, V. (2020). Man in the middle attack mitigation in lorawan, 353–358. https://doi.org/10.1109/ICICT48043.2020.9112391

Tomasin, S., Zulian, S., & Vangelista, L. (2017). Security analysis of lorawan join procedure for internet of things networks, 1–6. https://doi.org/10.1109/WCNCW.2017.7919091

Twidale, M., Randall, D., & Bentley, R. (1994). Situated evaluation for cooperative systems. *Proceedings of the Conference on Computer Supported Cooperative Work (CSCW)*, 441–452.

Tzounis, A., Katsoulas, N., Bartzanas, T., & Kittas, C. (2017). Internet of Things in agriculture, recent advances and future challenges. *Biosystems Engineering*, *164*, 31–48. https://doi.org/10.1016/j.biosystemseng.2017.09.007

UN General Assembly. (1948). Universal Declaration of Human Rights.

van Es, E., Vranken, H., & Hommersom, A. (2018). Denial-of-service attacks on lorawan. https://doi.org/10.1145/3230833.3232804

Vangelista, L., Zanella, A., & Zorzi, M. (2015). Long-range iot technologies: The dawn of lora™. *Future Access Enablers of Ubiquitous and Intelligent Infrastructures*, 51–58.

Vejlgaard, B., Lauridsen, M., Nguyen, H., Kovacs, I. Z., Mogensen, P., & Sorensen, M. (2017). Interference impact on coverage and capacity for low power wide area iot networks. *Proceedings of the Wireless Communications and Networking Conference*. https://doi.org/10.1109/WCNC.2017.7925510

Vigil-Hayes, M., Hossain, M. N., Elliott, A. K., Belding, E. M., & Zegura, E. (2022). LoRaX: Repurposing LoRa as a Low Data Rate Messaging System to Extend Internet Boundaries. *Proceedings of the Conference on Computing and Sustainable Societies*. https://doi.org/10.1145/3530190.3534807

vom Brocke, J., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R., & Cleven, A. (2015). Standing on the Shoulders of Giants: Challenges and Recommendations of Literature Search in Information Systems Research. *Communications of the Association for Information Systems*, *37*. https://doi.org/10.17705/1CAIS.03709

Wachenheim, C., Fan, L., & Zheng, S. (2021). Adoption of unmanned aerial vehicles for pesticide application: Role of social network, resource endowment, and perceptions. *Technology in Society*, *64*, 101470.

Wadatkar, P. V., Chaudhari, B. S., & Zennaro, M. (2019). Impact of interference on lorawan link performance, 1–5. https://doi.org/10.1109/ICCUBEA47591.2019.9128417

Wallach, D., & Scholz, S. C. (2012). User-Centered Design: Why and How to Put Users First in Software Development [Series Title: Management for Professionals]. In A. Maedche, A. Botzenhardt, & L. Neer (Eds.), *Software for People* (pp. 11–38). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-31371-4_2

Walter, A., Finger, R., Huber, R., & Buchmann, N. (2017). Opinion: Smart farming is key to developing sustainable agriculture. *Proceedings of the National Academy of Sciences*, *114*(24), 6148–6150. https://doi.org/10.1073/pnas.1707462114

Wang, W., Bai, Y., Feng, P., Huang, J., Sha, M., & Tantai, J. (2021). DTN-Balance: A Forwarding-Capacity and Forwarding-Queue Aware Routing for Self-organizing DTNs. *Wireless Personal Communications*, *118*(1).

Wang, W., Capitaneanu, S. L., Marinca, D., & Lohan, E.-S. (2019). Comparative analysis of channel models for industrial iot wireless communication. *IEEE Access*, *7*, 91627–91640.

Wang, X., Kong, L., Wu, Z., Cheng, L., Xu, C., & Chen, G. (2020). Slora: Towards secure lora communications with fine-grained physical layer features, 258–270. https://doi.org/10.1145/3384419.3430770

Wedawatta, G., Ingirige, B., & Jones, K. (2010). Coping strategies against extreme weather events: A survey of SMEs in the UK. *COBRA 2010 - Construction, Building and Real Estate Research Conference of the Royal Institution of Chartered Surveyors*, (January).

Weltzien, C. (2016). Digital agriculture - or why agriculture 4.0 still offers only modest returns. *Landtechnik*, *71*(2), 66–68. https://doi.org/10.15150/lt.2015.3123

West, J. (2018). A Prediction Model Framework for Cyber-Attacks to Precision Agriculture Technologies. *Journal of Agricultural and Food Information*, *19*(4), 307–330. https://doi.org/10.1080/10496505.2017.1417859

Wobbrock, J. O., & Kientz, J. A. (2016). Research contribution in human-computer interaction. *Interactions*, *23*(3), 38–44. https://doi.org/10.1145/2907069

Wolfert, S., Ge, L., Verdouw, C., & Bogaardt, M.-J. (2017). Big Data in Smart Farming – A review. *Agricultural Systems*, *153*, 69–80. https://doi.org/10.1016/j.agsy.2017.01.023

Xu, J., Tang, Y., Wang, Y., & Wang, X. (2019). A practical side-channel attack of a lorawan module using deep learning, 17–21. https://doi.org/10.1109/ICASID.2019.8925203

Xu, R., Xiong, X., Zheng, K., & Wang, X. (2016). Design and prototyping of low power wide area networks for critical infrastructure monitoring. *IET Communications*, *11*. https://doi.org/10.1049/iet-com.2016.0853

Yalcin, H. (2017). Plant phenology recognition using deep learning: Deep-Pheno. *2017 6th International Conference on Agro-Geoinformatics*, 1–5. https://doi.org/10.1109/Agro-Geoinformatics.2017.8046996

Yang, X. (2017). LoRaWAN: Vulnerability Analysis and Practical Exploitation. *M.Sc. Thesis. Delft University of Technology*. https://pdfs.semanticscholar.org/a1e3/9d0f249a1afa2f5ade9d5473b3e64a0e84fe.pdf

Yang, X., Karampatzakis, E., Doerr, C., & Kuipers, F. (2018). Security vulnerabilities in lorawan. *IEEE International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 129–140. https://doi.org/10.1109/IoTDI.2018.00022

Zave, P. (1997). Classification of research efforts in requirements engineering. *ACM Computing Surveys*, *29*(4), 315–321. https://doi.org/10.1145/267580.267581
211 citations (Crossref) [2023-08-02].

Zguira, Y., Rivano, H., & Meddeb, A. (2018). IoB-DTN: A lightweight DTN protocol for mobile IoT applications to smart bike sharing systems. *Wireless Days*. https://doi.org/10.1109/WD.2018.8361708

Zhang, A., Jakku, E., Llewellyn, R., & Bake, E. (2018). Surveying the needs and drivers for digital agriculture in Australia. *Farm Policy Journal*, *15*(1), 25–39.

Zhang, S., Wu, J., & Lu, S. (2013). Minimum Makespan Workload Dissemination in DTNs: Making Full Utilization of Computational Surplus Around. *Proceedings of the Fourteenth ACM International Symposium on Mobile Ad Hoc Networking and Computing*. https://doi.org/10.1145/2491288.2491327

Zheng, S., Wang, Z., & Wachenheim, C. J. (2019). Technology adoption among farmers in jilin province, china: The case of aerial pesticide application. *China Agricultural Economic Review*, *11*(1), 206–216. https://doi.org/10.1108/CAER-11-2017-0216

Zimmermann, V., Gerber, P., Marky, K., Böck, L., & Kirchbuchner, F. (2019). Assessing users' privacy and security concerns of smart home technologies. *i-com*, *18*(3), 197–216.

Zobel, J., Kundel, R., & Steinmetz, R. (2022). CAMON: Aerial-Ground Cooperation System for Disaster Network Detection. *Proceedings of the 19th International Conference on Information Systems for Crisis Response and Management*.

Zscheischler, J., Brunsch, R., Rogga, S., & Scholz, R. W. (2022). Perceived risks and vulnerabilities of employing digitalization and digital data in agriculture – Socially robust orientations from a transdisciplinary process. *Journal of Cleaner Production*, *358*, 132034. https://doi.org/10.1016/j.jclepro.2022.132034

III

APPENDIX

A SUPPLEMENTARY MATERIAL

A.1 Supplementary Material for Chapter 7

The following supplementary material for Chapter 7 (*Resilience in Agriculture: Communication and Energy Infrastructure Dependencies of German Farmers*) is presented, consisting of material used to conduct and evaluate the focus groups (qualitative analysis), as well as the items of the questionnaire (quantitative analysis).

A.1.1 *Focus Group Guideline*

Aim: Determining attitudes, expectations, fears, and opportunities for resilience capacity determination.

Method: Free discussion with the focus group. The topics will be outlined, and possible introductory questions will be posed. Participants should report as freely as possible about their experiences and expectations. The discussion is somewhat guided by the instructors. The following topics and keywords serve this purpose (roughly sorted by order, deviation possible):

Thematic sheet:

- Digitalization
  - Opinion (current status is included in the questionnaire)
  - Self-reflection (Am I a person who is familiar with digitalization?)
  - Desire for promotion offers/expertise creation
  - Digitalization for the businesses: own network, own server, own information structure (What do you imagine a digitized business to look like?)
- Resilience
  - Discussion of which incidents and events are known to interfere with the operating schedule. These do not have to be catastrophes. Other keywords for the discussion: Outage of infrastructures (short-term, long-term, how long until critical), power failure, water supply, fuel supply, network failure (also mobile communication), if applicable: environmental influences (weather (e.g., storm), climate (e.g., drought), pest and diseases),

  - Discussion about possible solutions (realistic and desirable). Keywords to drop: aggregates, wells, diesel tanks, emergency supplies, animal food, other materials.
  - Role of insurance coverage
  - Emphasizing that other actors are not available in the event of an incident -> bridge to find out which players/actors are relevant.

For each incident:

1. What impact does this incident have on your business? (in your own words)
   (a) How could the incident be identified in advance? (forecasts by sensors or warning services, experiences)
2. Which emergency measures do you take in this specific emergency situation?
   (a) Do you think that you can cope with this situation with these measures? (assessment whether "enough" is done in the farmers' own perceptions)
   (b) Are you able to continue the operation normally after the end of the emergency situation?
   (c) Communication with public authorities (obligation to register, emergency contacts)
   (d) What else would you support? What tools and services facilitate dealing with the situation?
   (identify individual perceptions of farms)
3. Are there any experiences in dealing with such situations? Were there circumstances that disturbed the regular operation?

A.1.2 *Codes and Categories Used for Open Coding*

- digitalization in agriculture
  - digitalization/understanding
  - digitalization/examples and experiences
  - digitalization/personal opinion
  - digitalization/concerns
- infrastructure on farms
  - hardware
    - * hardware/pc

    - hardware/tablet
    - hardware/smartphone
    - hardware/drone
    - hardware/tractor
    - hardware/robot
  - software
    - software/field record
    - software/other software

- processes
  - processes/communication with other stakeholders
  - processes/stakeholders
- privacy
  - privacy/fears, risks
  - privacy/solutions
- resilience
  - IT
    - IT/ risks
    - IT/ precautionary measures
    - IT/ insurances
  - electricity
    - electricity/ risks
    - electricity/ precautionary measures
    - electricity/ insurances
  - water
    - water/ risks
    - water/ precautionary measures
    - water/ insurances
  - roads
    - roads/ risks
    - roads/ precautionary measures
    - roads/ insurances
  - internet, mobile network
    - internet, mobile network/ risks
    - internet, mobile network/ precautionary measures
    - internet, mobile network/ insurances
  - other
    - other/risks
    - other/precautionary measures
    - other/insurances

A.1.3 *Questionnaire Items*

Table A.1: Questions included in our online survey, translated from German into English

Personal and business data

- What is your age range? [*21-30* | *31-40* | *41-50* | *51-60* | *61-70* | *over 70* | *Not specified*]
- In which federated state do you work? (when several please decide for the one with the largest share)
- Do you work on a farm? [*Yes* | *No* | *Not specified*]
- In which employment relationship are you working in the farm? [*Temporary employed* | *Employed* | *Self-employed* | *Manager* | *Not specified*]
- Which agricultural sectors does your business serve? (multiple choice) [*Crops* | *Permanent crops* | *livestock*]
- How many people work in the company where you are employed?
- What is the size of the agricultural area of your farm? [*Up to 20ha* | *Up to 50ha* | *Up to 100ha* | *Up to 200ha* | *Up to 500ha* | *Not specified*]
- Do you perform any other activity in addition to your agricultural activity?
- In which (non-agricultural) field are you active?

Critical infrastructure

- How important do you consider the following infrastructures to your operation: (Gas/Fuel | Electricity | Water | Transport | Mobile network | Mobile internet (UMTS, LTE, 5G) | House phone | Fixed-line internet (DSL, internet via cable connection)) [*Not* | *A little* | *Medium* | *Quite* | *Very* | *Not specified*]
- How often have the following infrastructures experienced outages in the past 12 months? (Gas/Fuel | Electricity | Water | Transport | Mobile network | Mobile internet (UMTS, LTE, 5G) | House phone | Fixed-line internet (DSL, internet via cable connection)) [*Never* | *1x* | *2x* | *3x* | *More than 3x* | *Not specified*]
- How much have the outages of the last 12 months limited their operations: [*Not at all* | *Little stress / hardly any intervention necessary* | *Moderately stressful / interventions necessary* | *Quite stressful / laborious interventions necessary* | *Very strongly stressing / Hardly or not at all possible to compensate the failure*]
- What precautions against infrastructure failures do you have in place and have you already been able to help with incidents? (Power generator | Well | Fuel supply | Feed supply | Other supply | Radio link | Other (free text)) [*Not owned* | *Owned but not yet used* | *Owned and used, but did not help* | *Owned and used and has helped*]
- Please estimate the duration of your operational capability in case of infrastructure failure . . . (Feed supplier | Land trade | Dairy | Agricultural technician workshop | Veterinarian | Other) [*under 4 hours* | *4 hours or more* | *12 hours or more* | *24 hours or more* | *2 days or more* | *4 days or more* | *1 week or more* | *2 week or more* | *4 week or more* | *Not specified*]

Resilience of digital systems

- When do you think the use of digital systems will make up the majority (i.e. at least 50% of working time) of agricultural activities? [*This is already the case* | *In 1 year* | *In 2 years* | *In 5 years* | *In 10 years* | *Later* | *Never* | *Not specified*]
- Which of the following (digital) tools do you use? (Farm management information systems (e.g. Farmnet) | Digital automatic milking systems | Herd management systems | Machinery with ISOBUS | Digital communication platforms | Calculation aid | Others) [*Yes* | *No* | *Not specified*]
- Please estimate how much the technology you use for outdoor and indoor work is generally dependent on the Internet [*Not* | *A little* | *Medium* | *Quite* | *Very* | *Not specified*]
- Which of your digital tools would continue to function exactly the same even without an Internet connection (e.g., due to a communication network disruption), i.e., they would also function in offline mode? (Farm management information systems (e.g. Farmnet) | Digital automatic milking systems | Herd management systems | Machinery with ISOBUS | Digital communication platforms | Calculation aid | Others) [*Does not work offline* | *Works partially offline* | *Works completely offline* | *Cannot say*]
- Is your digital tools data in a cloud? (Farm management information systems (e.g. Farmnet) | Digital automatic milking systems | Herd management systems | Machinery with ISOBUS | Digital communication platforms | Calculation aid | Others) [*Yes* | *No* | *Not Specified*]
- Is your data secured by regular local backups? [*Yes* | *No* | *Not specified*]
- Do you see the possibility to establish direct contact with all involved actors, e.g. via travel to the involved company? [Yes | *No* | *Not specified*]
- How important is digital communication to your operations? [*Not* | *A little* | *Medium* | *Quite* | *Very* | *Not specified*]

A.2 Supplementary Material for Chapter 10

The following supplementary material for Chapter 10 (*GeoBox: Design and Evaluation of a Tool for Resilient and Decentralized Data Management in Agriculture*) is presented, consisting of material used to conduct and evaluate the usability evaluation (qualitative analysis).

A.2.1 *Evaluation Schedule Summary*

1. Introduction
    (a) Consent about processing of recorded data
    (b) Questionnaire: demographics and job (4 - 9 questions) + technical affinity Karrer et al., 2009 (19 questions)
2. Main part: Tasks with software based on a given scenario (Remote Usability Test)
    (a) Import (available) backup files (from hypothetical other application)
    (b) Update field details on map (changes since imported backup was created)
    (c) Place an order for a soil sample examination
    (d) Record a conducted fertilization
3. Concluding part
    (a) Questionnaire: SUS Brooke, 1996 (10 questions)
    (b) Conclusion (interview with 2 lead questions)

A.2.2 *Evaluation Guideline*

Introduction/Explanation

Aim of the evaluation: Evaluation of the current state of development with regard to user interfaces and planned functionalities.

Aim of the project: Decentralized data storage and regional networking for agricultural businesses. This includes storing the data in open formats and possible compatibility with other products that may rely on the data. This is why the system is also called a data hub.

Important information: We will treat all data confidentially, but we ask you to provide us only with information that is not secret or internal to the company. If you are unsure about certain points, please let us know.

PROCEDURE: You will first get an online questionnaire with 8 questions about yourself, such as your age range and experience with computers. Then the recording of the system will be started. At this point, I will again specifically point this out and then ask for your permission. From then on, the recording will record images and sound and store them on servers of the German research network. Only we will have access to the file. Afterward, you will be given a scenario and tasks to be solved with the current state of development of the system. We ask you to express your thoughts and impressions directly so that we can also assess where there is potential for improvement, what may already be good, and where improvements are absolutely necessary. After each task, we would like you to answer a few questions, which we will ask you. At the end, there is another questionnaire with 7 questions, which refers to the usability of the system. We expect this to take about 30 to 60 minutes, including the introduction, which we are already in. You are welcome to ask questions about the process now, otherwise, I'd like to get right to it.

CONSENT TO RECORD AUDIO/VIDEO?

- Secure storage of data internally at the university
- Use of data only anonymized and for research purposes

Statistical classification of participants (questionnaire)

1. What age range are you in?
2. In which federal state do you work? (if more than one, please choose the one with the largest percentage)?
3. Do you work on a farm? (No: jump to the last question)
4. In which employment relationship do you work on the farm?
5. Which agricultural sectors does your farm serve?
6. Is your farm operated on a full-time or part-time basis? (Main occupation: end)
7. In which (non-agricultural) sector do you operate?
8. How confident do you feel in using computer technology?k?

Scenario-based tests (Remote-Usability-Test)

ROLE You manage a family business with one permanent employee and cultivate cereals, primarily wheat, on a farm area of approximately 60 hectares. As the role of the farm manager, you typically also handle the planning and ordering. Likewise, only you have full access to the operational data.

DESCRIPTION OF THE SCENARIO It is winter, and it is time to start planning for the coming business year. An important fiber optic cable was destroyed during construction work, and as a result, the distribution nodes experienced a technical defect, leaving the large area in which you operate without a functioning internet connection. According to the companies responsible, it will take up to several days to repair the damage.

TASK PART 1 - FAMILIARIZE You now want to load the farm data that you exported earlier into the new application since it has promised to be able to act offline as well. To do this, start the application and first familiarize yourself a bit with the interface by drawing in a newly leased field.

Script

1. Download operating data
2. Initial start of the app via the browser
3. Follow dialog to load data
4. Open partial app map editor
5. Draw in new field

CONCLUDING QUESTIONS FOR TASK PART 1

1. How do you feel about the interface after the first steps?
2. What suggestions do you have for improving the user interface?
3. How important would it be for you to be able to import data from other programs that previously stored your operational data? And, from your point of view, which programs should be paid special attention to?
4. Does the user interface give the impression of being expandable?

TASK PART 2 - SUBMITTING A SOIL SAMPLE ORDER (USABILITY-TEST). By now, you know that you have to place an order for a soil sample test to an appropriate laboratory. You have chosen the laboratory "PEASEC-Lab" located in your neighborhood. Fortunately, the soil sampling laboratory offers compatible forms for download. Unfortunately, the internet access is still not working at your company. Therefore, you now use the possibility to download the form file at a friend's in the neighboring town and then import it back to your company computer via USB stick. Therefore, download the form from the website as a file and import it into the application. Fill in the form and save the completed form as a file. If the file has been saved, the task has been completed. In this case, we assume that the file can be sent via USB stick either directly to the soil sampling laboratory, or it can be sent via a neighboring place again via e-mail or web form.

Script:

1. Find and download form via website
2. Open geo-forms sub-app
3. Import form in the third tab
4. Open and fill in form in first form
5. Save form
6. Export completed form

CONCLUDING QUESTIONS FOR TASK PART 2

1. Could the scenario occur like this, in your opinion?
2. Do you have any ideas on how to improve import and export?
3. How important is it to you to always be able to go back to the file level, i.e., to be able to export (and also import) smaller data sets (e.g. a single form) from a program as a file?
4. Do you feel that you have control over the data in the user interface, i.e., that they are not sent on without permission? How could this feeling be strengthened/supported in case of doubt?

TASK PART 3 - DOCUMENTATION After the soil sample has been taken, fertilizer has been applied successfully in the meantime. The applied amounts of fertilizer are now to be documented again by hand since the automatic transmission did not work. On the field with the name "field for winter wheat", the fertilizer Alzon 46 was applied with 2.7 dt/h and a total of 125 kg N/ha.

Please record the fertilizer quantities accordingly in the "Buchungsjournal" sub-app.

Script:

1. Sub-app Buchungsjournal
2. Open input mask for field measure "apply mineral fertilizer"
3. Enter values, given: "Field for winter wheat", "Alzon 46", "2.7 dt/h", "125 kg N/ha".

CONCLUDING QUESTIONS FOR TASK PART 3.

1. Would you have expected the input masks elsewhere, and if so: where?
2. How intuitive do you find the documentation option?
3. Which actions should be available by default (offline)?

Standardized usability evaluation (questionnaire)

SYSTEM USABILITY SCALE (SUS) Use of SUS Brooke, 1996 in German translation [1], whereby each question is answered on a scale from 1 (do not agree at all) to 5 (completely agree)

1. I think I would like to use the system frequently.
2. I found the system unnecessarily complex.
3. I found the system easy to use.
4. I think I would need the help of a technophile person to use the system. System benutzen zu können.
5. I thought the various functions in the system were well integrated.
6. I think the system contained too many inconsistencies.
7. I imagine that most people could learn to use this system very quickly.
8. I found the system very cumbersome to use.
9. I felt very confident using the system.
10. I had to learn a lot before I could start using the system.

[1] https://experience.sap.com/skillup/system-usability-scale-jetzt-auch-auf-deutsch/

Closing questions (interview)

1. According to your estimation, how long would it take you to be able to use the interface confidently?
2. What potentials and problems or challenges do you see in using this application for basic data management?
3. How important is the issue of offline capability to you? Or: How acute do you see the dangers of internet failures, and how dependent do you think companies are on applications that require the internet to function?
4. Topic GeoBox: Do you see fundamental problems and dangers with the offline-first approach (if necessary, this will be explained), e.g., impairment of usability?
5. Do you have any general comments on the test procedure or the tested functions, and if so, which ones?

Thank you for participating in our test!

> “DO. OR DO NOT.
> THERE IS NO TRY.”
>
> YODA