



Inverter and Controller for Highly Available Permanent Magnet Synchronous Drives

genehmigte
Dissertation

von
Rammohan Rao Errabelli, M.Tech.
aus Warangal/Indien

Referent:
Korreferent:
Tag der Einreichung:
Tag der mündlichen Prüfung:

Prof. Dr.-Ing. Peter Mutschler
Prof. Dr.-Ing. Friedrich W. Fuchs
25.10.2011
08.05.2012

Inverter and Controller for Highly Available Permanent Magnet Synchronous Drives

Vom Fachbereich Elektrotechnik und Informationstechnik
der Technischen Universität Darmstadt
zur Erlangung des akademischen Grades eines
Doktor-Ingenieurs (Dr.-Ing.)
genehmigte Dissertation

von

Rammohan Rao Errabelli, M.Tech.

Geboren am 08. August 1979 in Warangal, Indien

Referent:	Prof. Dr.-Ing. Peter Mutschler
Korreferent:	Prof. Dr.-Ing. Friedrich W. Fuchs
Tag der Einreichung:	25. Oktober 2011
Tag der mündlichen Prüfung:	08. Mai 2012

Acknowledgement

I am grateful to Prof. Dr.-Ing. P. Mutschler for accepting me as his student and providing me the opportunity to work in the institute for power electronics and control of drives. I am really indebted for the ample and rich lab facilities he provided me for performing hardware implementation of my thesis. I am also thankful to him for his valuable guidance during the course of my research work. I have learnt a lot about work ethics, professional behavior and meticulous approach to problem solving from him, which will inspire me for the rest of my life.

Many thanks to Prof. Dr.-Ing. F.W. Fuchs for his interest and time to be as my co-advisor. I thank the DFG Deutsche Forschungsgemeinschaft for financially supporting my projects MU 1109/17-1.

Many thanks go to all my colleagues at SRT, for the support and for creating such a pleasant working environment. I want to thank Dr. Roberto Leidhold for all his support and Marius Mihalachi for his numerous valuable advices during my PhD. A special thanks to Calin Purcarea for his constant support in keeping alive our network server and assembling and sorting the issues of institute computers. Besides, I want to thank Sorin Silaghiu, Phong Khong, Tobias Fernandes, Rodrigo Benavides and Emad Hussein, for our talks and for our good time.

I would like to acknowledge the work of the SRT secretary Frau zinnia for her support in administrative work and Laboratory staff Herr Herbig and Herr Maul for their meticulous and artful work in building my experimental setup.

I must acknowledge the cheerful and warm company of my all other friends (Chakrapani, Satya, Swamy...) who made my life in Darmstadt memorable. Much gratitude to Hans Kalawsky and Ludwig Bauer for their unforgettable support during my stay in Darmstadt. I am also very grateful to all the member of Badminton Verein Darmstadt (BVD) for such a good time and company all the days.

I have no formal words for my wife Jaya who is also my colleague all the days during my PhD has played an instrumental role in many aspects for this accomplishment. The kind of support and encouragement she gave me not only to my PhD but in every step that I put forward, cannot be described in words. Finally, I thank all my family members for their moral support during my PhD.

Stuttgart, 01.07.2012

Rammohan Errabelli

Abstract

A typical modern industrial drive consists of a power electronic converter, a digital controller, feedback sensors and a motor. Several faults can affect the motor drive and a fault in any of the above will stop the operation of the drive, or at least it affects the drive's performance. There are many safety critical applications like power plants, aerospace, pitch drives for wind-turbines, automobiles, *etc.* where the drive with high availability is very important. For interlinked production processes, as in modern industrial processing plants, a fault in a single drive can result in tremendous damages of materials and machines. Follow-up costs due to the faults with drives in modern production plants can amount to huge sums. So, the adjustable speed drives with high availability is an area of great interest for modern drive solutions.

In this research project, solutions to improve the availability of different components of the drive are systematically developed and experimentally verified. Solutions to the

- 1) The information processing (digital controller)
- 2) Power section (inverter)
- 3) Feedback sensors (position and current sensors)

are presented.

An improved availability of the digital controller is achieved based on the principles of triple modular redundancy. Three digital signal processors (DSPs) are used in parallel running the same control algorithm. The pulse width modulation (PWM) outputs of all the three DSPs are voted out using a simple majority voting logic which is by itself a fault tolerant. In order to keep all the three DSPs in time synchronism to each other, a serial communication is developed between the three processors, which will exchange the timer values between all the three processors. This communication is also used to exchange the control variables between the three processors such that there is a synchronism in the control variables which are finally used for the control computation. Connections between all the three processors are made such that there is no common point of failure in the system.

An improved availability of the inverter is achieved by adding a redundant leg to the standard two-level voltage source inverter (VSI). The faulted leg isolation and the redundant leg insertion is done by using independent back-to-back connected thyristors. The proposed inverter provides tolerance to the both short circuit and open circuit faults of the switching devices.

Fault detection algorithms are implemented for both the cases of position sensor failure and current sensors failure. Position sensorless control algorithm is used in case of a position sensor failure. Normally, for the field oriented control of a PMSM with isolated neutral, two current sensors are sufficient. In case of a failure in any of these two current sensors, a redundant current sensor which is measuring the third phase current is used in place of a faulty current sensor.

The whole system is developed based on the concept that only a single arbitrary fault occurs at any time. Field oriented control of the PMSM implemented to test all the above solutions to improve the availability. In all the fault cases, the post fault performance is same as the pre-fault performance and during the fault detection and compensation there is negligible disturbance to the machine operation.

Kurzfassung

Ein typischer moderner elektrischer Antrieb besteht aus einem Wechselrichter, einem digitalen Kontrollsystem, Feedback-Sensoren und der Maschine. Verschiedenste Fehler können den reibungslosen Betrieb gefährden oder seine Leistungsfähigkeit einschränken. In vielen sicherheitskritischen Bereichen (Kraftwerke, Luftfahrt, Fahrzeugen, u.s.w) können Systemausfälle nicht toleriert werden. Bei verketteten Produktionsprozessen, wie sie in modernen Be- und Verarbeitungsanlagen vorliegen, kann der Ausfall eines einzelnen Antriebes zu erheblichen Material- und Maschinenschäden führen. Die Folgekosten von Antriebsausfällen in modernen Produktionsanlagen können ganz erhebliche Größenordnungen annehmen, so dass fehlertolerante Antriebslösungen zur Erzeugung einer sehr hohen Anlagen-Verfügbarkeit ein zukünftig wesentliches Thema sein werden.

In diesem Forschungsprojekt wurden Lösungen zur Verbesserung der Verfügbarkeit von Komponenten des Antriebsstranges unter Wahrung technischer und wirtschaftlicher Randbedingungen systematisch entwickelt und experimentell verifiziert.

Im Einzelnen sind dies:

- 1) Signalverarbeitung (im digitalen Kontrollsystem)
- 2) Leistungsteil (Wechselrichter)
- 3) Feedback-Sensoren (Lage- und Stromsensoren)

Die Hochverfügbarkeit der Kontrolleinheit wird auf Basis einer dreifachen modularen Redundanz erreicht. Drei digitale Prozessoren (DSPs) laufen parallel und benutzen den gleichen Algorithmus. Die PWM Ausgangssignale werden mit einer einfachen Logik auf Basis von Mehrheitsentscheidungen, die in sich fehlertolerant ist, ausgewertet. Um alle drei DSP synchron zu halten, wurde eine serielle Kommunikation zwischen ihnen entwickelt, die die Ergebnisse des Zeitgebers übermittelt. Über diese Schnittstelle werden auch Kontrollparameter ausgetauscht um die Abstimmung zwischen allen DSPs zu gewährleisten. Die Verbindungen zwischen allen DSPs wurden so ausgelegt, dass es keinen „Single Point of Failure“ gibt.

Die verbesserte Verfügbarkeit des Wechselrichters wird dadurch erreicht, dass den Standard- Zweistufen-Wechselrichtern eine weitere, redundante Halb-Brücke hinzugefügt wird. Die Isolation der fehlerhaften und die Einfügung der redundanten Halb-Brücke werden durch Anwendung zweier antiparallel geschalteter Thyristoren erreicht. Die hier entwickelte Lösung beherrscht den Kurzschluss und die Unterbrechung der Leistungshalbleiter im gesamten Wechselrichter.

Algorithmen zur Fehlererkennung wurden sowohl für Fehler der Lage- als auch der Stromsensoren entwickelt. Bei einem Ausfall des Lagesensors wird ein sensorloser Algorithmus angewendet. Im Normalfall sind zwei Stromsensoren für die feldorientierte Regelung eines PMSM (Permanent-Magnet-Synchron-Maschine) mit isoliertem Sternpunkt ausreichend. Beim Ausfall eines der beiden Stromsensoren wird er durch einen redundanten Sensor, der die dritte Phase misst, ersetzt.

Das Gesamtsystem wurde auf der Grundannahme entwickelt, dass nur ein einzelner Fehler zu einer gegebenen Zeit auftritt. Um alle oben genannten Fehlerzustände testen zu können, wurde eine feldorientierte Regelung des PMSM entwickelt. Es wurde dargestellt, dass das Verhalten des Systems vor und nach dem Fehlerfall nahezu identisch ist, mit vernachlässigbaren Beeinträchtigungen während der Fehlererkennungs- und Korrekturphase.

Table of Contents

Abstract	i
Kurzfassung.....	iii
Table of Contents	v
List of Abbreviations and Symbols	vii
1 Introduction	1
1.1 Motivation	1
1.2 Definitions and principles of fault tolerance	3
1.3 Problem definition	9
1.4 Contribution.....	9
1.5 Outline of the Thesis.....	10
2 Digital Controller with Increased Availability	12
2.1 Introduction	12
2.2 Classification and comparison of redundant controllers	12
2.2.1 Dynamic redundancy based controllers	12
2.2.1.1 Standby redundancy.....	12
2.2.1.2 Synchronization of dynamic redundant controllers	15
2.2.1.3 Fault detection in dynamic redundant controllers.....	15
2.2.2 Static redundancy based fault tolerant controller.....	17
2.2.2.1 N-modular redundancy	17
2.2.2.2 Triple Modular Redundancy (TMR) controllers.....	17
2.2.3 MTTF evaluation and comparison of redundant controllers.....	19
2.2.3.1 MTTF of hot standby redundant system –assuming perfect fault detection.....	19
2.2.3.2 MTTF of the hot standby redundant system – for an imperfect fault detection ...	21
2.2.3.3 MTTF of the TMR system.....	21
2.2.3.4 MTTF comparison of redundant systems:	22
2.2.4 Choosing of redundant controller topology for fault tolerant applications.....	23
2.3 Digital controller with increased availability	23
2.3.1 Synchronization.....	25
2.3.1.1 Timer synchronization	25
2.3.1.2 Control variables synchronization	29
2.3.2 Fault identification and compensation	29
2.3.3 Fault tolerant majority voter.....	36
2.4 Experimental setup description	37
2.5 Experimental results	39
2.6 Conclusions	39
3 Power Converter with Increased Availability	42
3.1 Introduction	42
3.2 Comparison of topologies for power converters with increased availability	45
3.2.1 Four leg inverter topology.....	45
3.2.2 Switch redundant topology.....	46
3.2.3 Double switch redundant topology	48

3.2.3.1	Double switch redundant topology with fault leg isolating fuses	49
3.2.3.2	Double switch redundant topology with fault leg isolating switches.....	49
3.2.4	Phase redundant topology	50
3.2.5	H-bridge inverter topology	52
3.2.6	Cascaded inverter topology with isolated DC links	53
3.2.7	Phase redundant topology with isolating switches (New Proposal).....	54
3.3	Conclusions of the comparison of converter topologies with increased availability.....	58
3.4	System description of the proposed inverter with increased availability.....	60
3.4.1	High dv/dt tolerance testing of the redundant leg inserting thyristors.....	60
3.4.2	Efficiencies comparison of standard inverter and inverter with increased availability.....	64
3.4.3	Inverter operation and fault compensation for single IGBT open circuit fault	66
3.4.4	Inverter operation and fault compensation for single IGBT short circuit fault	67
3.5	Simulation results.....	71
3.5.1	Uncompensated IGBT short circuit fault.....	71
3.5.2	Compensated IGBT short circuit fault.....	75
3.5.3	Compensated IGBT short circuit fault in case of low speed operation	79
3.6	Experimental results.....	81
3.6.1	Experimental setup description.....	81
3.6.2	Experimental results-IGBT open circuit fault	82
3.6.2.1	Uncompensated IGBT open circuit fault.....	82
3.6.2.2	Compensated IGBT open circuit fault.....	83
3.6.3	Experimental results-IGBT short circuit fault	84
3.6.3.1	Uncompensated IGBT short circuit fault	84
3.6.3.2	Compensated IGBT short circuit fault	88
3.7	Conclusions.....	91
4	Feedback Sensors with Increased Availability	92
4.1	Introduction.....	92
4.2	Position sensorless control of PMSM to increase the drive availability.....	93
4.3	Experimental results – tolerance to position sensor fault	96
4.4	Current sensors with increased availability	97
4.5	Experimental results - current sensor with increased availability.....	99
4.6	Conclusions.....	99
5	PMSM Drive with Improved Availability of Controller, Converter and Feedback System ...	100
5.1	Introduction.....	100
5.2	System description of PMSM drive with increased availability.....	100
5.3	Control algorithm of the PMSM drive with increased availability.....	101
5.4	Experimental results.....	104
6	Conclusions and Future Scope.....	107
6.1	General conclusions	107
6.2	Future scope of the work.....	109
	Bibliography	110
	Appendix A.....	115
A1.	Datasheet for IGBT module SK30GB123	115
A2.	Datasheet for thyristor module SK25UT	119

List of Abbreviations and Symbols

AC	Alternating Current
ADC	Analogue to Digital Converter
DC	Direct Current
DSP	Digital Signal Processor
EMF	Electro Motive Force
FDI	Fault Detection and Isolation
FOC	Field Oriented Control
FWD	Free Wheeling Diode
IGBT	Insulated Gate Bipolar Transistor
IPM	Intelligent Power Module
McBSP	Multi-channel Buffered Serial Port
MTBF	Mean Time Before Fault
MTTF	Mean Time To Fault
MTTR	Mean Time To Repair
PMSM	Permanent Magnet Synchronous Machine
pu	Per Unit
PWM	Pulse Width Modulation
QEP	Quadrature Encoder Pulse
r.p.m.	Revolutions per minute
SPI	Serial Peripheral Interface
SRS	Slave Ready Signal
SVM	Space Vector Modulation
TMR	Triple Modular Redundancy
VSI	Voltage Source Inverter
G_ψ, G_e	gains of the EMF observer
L	PMSM phase inductance
P_x	System states, where $x = 0, 1, 2, \dots$
R	PMSM phase resistance
V_x	Variables of DSP _x , where $x = 1, 2$ or 3
λ	Failure rate
μ	Repair rate
c	Coverage factor

1 Introduction

This chapter starts with introducing the motivation behind this research work. After this, some basic definitions and classification of fault tolerant systems are presented. Next, the problem and the purpose statement are defined with the corresponding contribution to the proposed problem.

1.1 Motivation

The advent of semiconductor technology drastically changed the industrial and commercial applications. In growing number of applications, mechanical and pneumatic systems are replaced with the electric drives because of the improved efficiency, ease of control and reduced maintenance. Few such applications are electric vehicles, concept of more electric aircraft, medical and industrial applications. Invention of digital controllers such as computers, microprocessors, micro controllers, digital signal processors (DSP), field programmable gate arrays (FPGA), *etc.* revolutionized the industrial automation and commercial equipment control without much human intervention. The invention of power semiconductor devices changed the drive control strategy and control methods. Along with the semiconductor's technology, advancement in the sensor technology provided efficient and robust control solutions in day to day applications of the drives.

Along with the increase in flexibility, industrial applications also demand the availability and safe operation of electric drives. For example, in case of availability, for interlinked production processes, as in modern industrial processing plants, a fault in a single drive can result in tremendous damages of materials and machines. Follow-up costs due to faults with drives in modern production plants can amount to huge sums. There are some critical applications like power plants, aerospace, railway locomotives, automobiles, *etc.* where a failure in a drive can be dangerous to the plant or humans working at the plant. In order to improve the availability and safety of the industrial drives fault-tolerant solutions can be implemented. Simply put, fault tolerance is a need in many applications because the consequences of fault or malfunction are more expensive than the cost of avoiding the faults. Accordingly, fault-tolerant solutions will entail the reduction in maintenance costs, downtimes, and more importantly the avoidance of unnecessary failures, with their potential costly or even perhaps catastrophic consequences.

A typical modern industry drive consists of a power electronic converter, a digital controller for implementing the control algorithms, feedback sensors for controller input and motor. Several faults can affect the motor drive and a fault in any of the above will stop the drive running, or at least it affects the drive's performance [KAS94]. So the fault tolerance of adjustable speed drives is an area of great interest for modern drive solutions. So far, a redundant or conservative design has been used such that drive continues to run even after the fault. In some cases, continuous operation of the drive is ensured even with the reduced performance or accepting short torque transients.

A survey is done by Thorsen and Dalva on the reliability of VSI for industrial drives [THO95]. According to the results of their survey, 50% of all failures are in the control circuits, 7.7% in the cooling fans and 37.9% are in the power circuits. So, after the control circuit faults, faults in power circuit share a large proportion of the total converter set. The large percentage of the inverter faults are the switch short circuit faults. However, according to Schwab *et al.* power switches poses more failure rates than any other component in an inverter [SCH03]. They evaluated the reliability of a PMSM drive for automotive applications. Their results show that, the failures of

the power transistors represent approximately, according to the RDF2000 [UTE00], 63% of the electronic parts failures for a three single phase inverter topology and 50% for a three phase full-bridge topology. For the failures in the field, this quotient becomes 56% and 40% respectively. The difference in the results can be attributed to application specific and insufficient field data available from the customers.

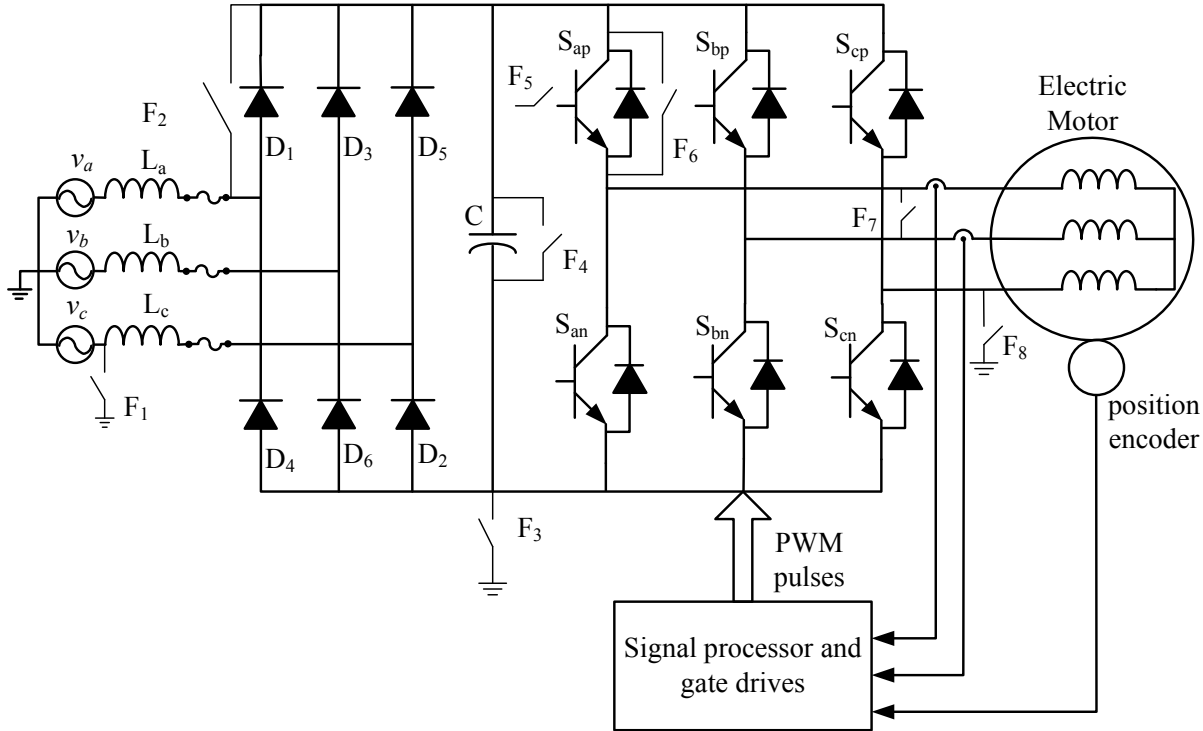


Figure 1.1: Voltage source inverter fed induction motor drive with possible fault modes (source [KAS94])

A voltage source inverter fed AC motor drive with different fault modes [KAS94] is shown in Figure 1.1. Different faults that can affect the motor performance are,

- Input supply single line fault (F_1)
- Rectifier diode short circuit fault (F_2)
- Earth fault on DC bus (F_3)
- DC link capacitor short circuit fault (F_4)
- Transistor base drive open fault or transistor open circuit fault (F_5)
- Transistor short circuit fault (F_6)
- Line to line short circuit fault at machine terminals (F_7)
- Single line to ground fault at machine terminals (F_8)
- Fault in the signal processing
- Fault in the position encoder
- Fault in the current sensors

The consequences of few of the above faults are described in [KAS94, FUC03]. In case of the fault F_1 , the diode bridge rectifier operates similar to a single phase diode bridge operation. This increases ripple voltage in the DC-link substantially. A pulsating torque is generated because of interaction between the fundamental frequency flux and the harmonic frequency currents. A short circuit fault in the rectifier diode (F_2) causes excessive stress on the line fuses. If the fuse in the fault phase blows then the diode bridge rectifier operates in the single phase mode. If the fuse in the

healthy phase blows first, then the fault will continue until the fuse in the faulted phase blows. This will cause total interruption to the DC-link.

A short circuit failure in the capacitor (F4) can be due to ageing of the capacitor. A short circuit fault in the DC-link capacitors causes the line fuses to blow and total interruption to the DC-link. An open circuit (F5) and short circuit (F6) fault in the IGBT may be due to the malfunctioning of the gate drive or permanent damage in the IGBT. An open-circuit fault in the IGBT causes pulsating torque in the motor and oscillations in the motor speed. A DC current offset is caused in the faulty phase and is equally divided between the healthy phases. A short circuit fault in the IGBT causes the corresponding phase permanently connected to the positive DC bus or negative bus, depending upon whether the upper IGBT or lower IGBT is short circuited. When a short circuit fault is detected in one of the IGBTs, inverter hardware protection disables the gate signals to all the IGBTs which bring the motor to stand still. Usually digital controllers are employed for drive control. A fault in the digital controller causes malfunction and erratic behavior of the drive. Feedback sensors (current, position, *etc.*) are used in case of closed-loop control of drives. If necessary control actions are not taken, any fault in the feedback sensors causes erratic and unpredictable behavior of the drive.

1.2 Definitions and principles of fault tolerance

Different terms and definitions related to the work are defined in this section. Most of the standard definitions are collected from the literature, to mention a few are [ISE06, KIR05 and DUB07]

Fault: “A fault is unpermitted deviation of at least one characteristic property (feature) of the system from an acceptable, usual, standard condition.”

Faults can be of different types such as design faults, hardware fault, software fault, components aging and wear faults, manufacturing and assembly fault, wrong operation fault (e. g. over load), operator fault, *etc.* Fault is an abnormal condition which causes a reduction in, or loss of, the capability of a functional unit to perform its intended function. A fault may initiate failure or malfunction of the system. According to fault duration fault can be permanent or transient fault.

Error: “An error is a deviation from correctness or accuracy in computation, which occurs as a result of a fault.”

Errors are usually associated with incorrect values in the system state. Errors can be due to incorrect software algorithms or faults in the hardware components.

Failure: “A failure is an event which causes a permanent interruption of a system ability to perform a required function under specified condition.”

A failure is the results from one or more events. Usually failures arise after start of the operation or if the system is subject to excessive stress.

Malfunction: “A malfunction is an intermittent irregularity in the fulfillment of a system’s desired function.”

Malfunction is an event, which is a temporary interruption of systems desired function resulting from one or more faults.

Dependability: “dependability is the ability of a system to deliver its intended level of service to its users ”

The attributes of dependability express the properties which are expected from the system. Three important attributes of the systems are reliability, safety and availability. Depending on the application, one or more of the above attributes are required to appropriately evaluate the system behavior. Some systems demand more reliability such as a pace maker for a cardiac patient, some systems demand more availability such as ATM machines and some systems demand more safety such as control of nuclear power stations. Dependability impairments are usually defined in terms of faults, errors, malfunctions and failures.

Reliability: *“The probability that an item can perform a required function under given conditions for a given time interval.” (IEC 50, 1992)*

Reliability is a measure of the continuous delivery of correct service. High reliability is necessary in cases when a system is required to operate without interruptions, as in the case of a peacemaker, or maintenance cannot be performed as in case of spacecraft missions. The reliability can be affected by faults and malfunctions. Reliability is a function of time.

Safety: *“Ability of system not to cause danger to persons, equipment or the environment.”*

A system or plant can attain several states after the fault, some are safe to the plant and human and other are unsafe and danger to the plant and human. A plant can be brought back from unsafe state to safe state if the plant is reversible and if necessary control actions are taken. With regards to fault tolerance a plant can have several states; few of them are shown in Figure 1.2.

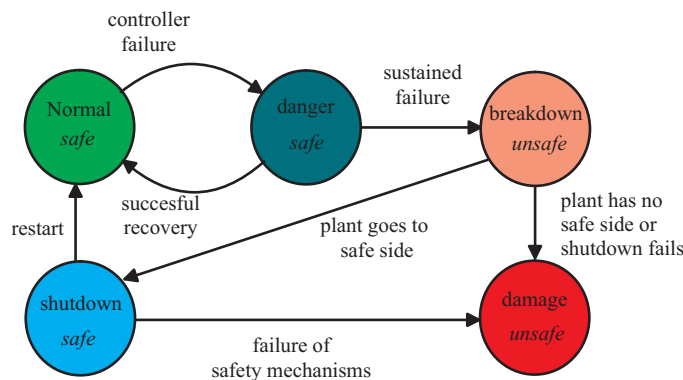


Figure 1.2: Plant states (source [KIR05])

Any fault in the normal state operation of system lead to a danger state but still the system is considered to safe and is not yet reached its critical point. The plant can be brought back to normal safe state, if necessary fault tolerance or automatic control action is taken to compensate the fault. If the fault is not compensated, the system may enter an unsafe or break down state. From this state depending on the system, system may lead either to a safety shutdown (if a safety mechanism is intervened) or damage state after certain time. After the system attained a safe shutdown, the fault can be repaired and the system can be restarted. In the meantime, if the safety mechanism of the system fails, the system can attain an unsafe and damaged state which may affect both the system and human.

The safety is concerned with the dangerous effects of faults and failure of the system. Reliability of a system can be improved by avoiding the failures, faults and malfunctions, whereas safety can be improved by avoiding the dangerous effect of failure, faults and malfunctions. An improvement in the system reliability can improve the system safety. From reliability point of view,

all failures are equal. In case of safety, failures are partitioned into fail-safe, fail silent and fail-unsafe ones. A system that rather stops than output erroneous data is fail-stop or fail-silent.

Fail-Safe (FS): “After one (or several) failure(s), the component directly reaches a safe state (passive fail-safe, with external power) or is brought to a safe state by a special action (active fail-safe, with external power) ”

Fail-silent (FSIL): “After one (or several) failure(s), the component exhibits quiet behavior externally (i.e., stays passive by switching off) and therefore does not wrongly influence other components. ’

Availability: “probability that a system or equipment will operate satisfactorily and effectively at any period of time.”

Availability takes into account that failures and malfunctions happened and need some time to repair. A measure for availability is $A = MTTF/(MTTF+MTTR)$, where $MTTR$ is Mean Time to Repair. From the equation it is evident that in order to achieve high availability, Mean Time to Fault ($MTTF$) should be high and $MTTR$ should be as low as possible. A high $MTTF$ can be achieved by using highly reliable components and also improving the fault tolerance capability of the system by using redundant structures. A low $MTTR$ can be achieved by fast and reliable fault detection methods, Fast and effective fault compensation or repair methods.

Service life: “It is a concept related to reliability and availability. It answers the question of life expectancy of a component such as how long is a component expected to perform before it begins to wear out.”

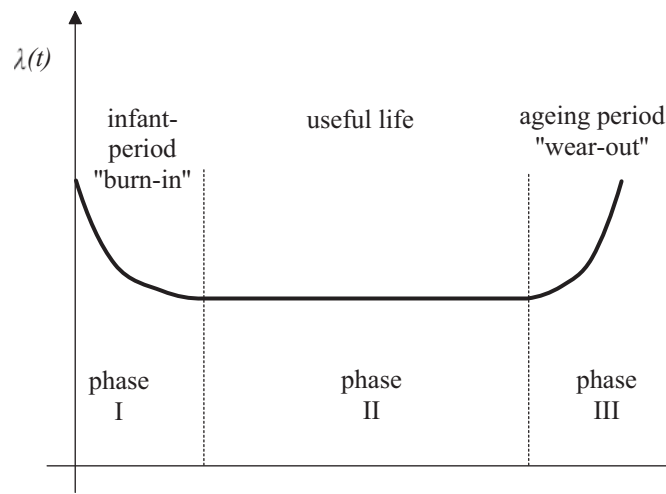


Figure 1.3: Relationship between component reliability over function of service-life

All electronic and electro mechanical systems have one or more wear out mechanisms which eventually lead to failures of the system. Figure 1.3 shows the relationship between components reliability with function of time. From the Figure 1.3 it is evident that components have a large failure rate at the commissioning, and then the failure rate decreases to become almost constant until the end useful service life. Finally, the failure rate of the components increases due to ageing of the components and wear of the mechanical parts.

The key concept to increase the system reliability and availability is by fault avoidance and fault tolerance. Even though the systems are designed and developed with a lot of care such as improvement of the component reliability, careful and generous design, applying reliability and safety analysis for improvement of design, exhaustive testing, quality control during the

manufacturing, regular maintenance and proper care to the equipment, the appearance of some faults cannot be avoided. Therefore, these unavoidable faults and failure in the system should be dealt with some design efforts. So where safety and availability are of prime importance, fault tolerance system should be employed.

Fault Tolerance (FT): ‘‘Fault-tolerance is the property that enables a system to continue operating properly in the event of one or more faults within some of its components.’’

That means, a system has either the property of fault tolerance (100%) or not (0%). To come closer to the technical reality, ‘‘Availability’’ can be used as a continuous measure. According to [WIKI1], the Harvard Research Group (HRG) defines in its ‘‘Availability Environment Classification (AEC)’’ six classes of availability, where fault tolerance is one of the highest classes, as shown in the Table 1.1 below.

Table 1.1: Harvard research group’s Availability Environment Classification (AEC)

HRG-Class	Denotation	Description
AEC-0	<i>Conventional</i>	Function can be interrupted, data integrity is not essential.
AEC-1	<i>Highly Reliable</i>	Function can be interrupted, however data integrity must be ensured
AEC-2	<i>High Availability</i>	Function may be minimum interrupted only within fixed times during the main operating hours.
AEC-3	<i>Fault Resilient</i>	Function must be maintained continuously, within fixed times or during the main operating hours.
AEC-4	<i>Fault Tolerant</i>	Function must be maintained continuously, i.e. 24x7 operation (24 hours, 7 days the week) must be ensured.
AEC-5	<i>Disaster tolerant</i>	Function must be available under all circumstances.

So in the electric drive applications, according to the definition of ‘‘fault tolerance’’, the operation of the drive must be possible for 24h at 7 days per week. But the definition contains no statement on the duration of uninterrupted period of operation which must be possible (how many weeks or years?). In this thesis, measures to increase availability of two major components of a drive are discussed: 1) Control equipment and 2) Inverter.

1) In the triple modular redundant (TMR) control system which will be discussed in section 2.3, a failed component (DSP) can be pinpointed and replaced by the service person without disturbing the operation of the healthy components (DSPs). With such a repair strategy, an extremely high availability class, i.e. AEC-4 ‘‘Fault tolerant’’ can certainly be achieved even for an extremely long uninterrupted period of operation.

2) A similar repair strategy for the inverter would necessitate two full size inverters and adequate switchgear (fuses, electronic or mechanical switches) for fast isolation of a failed inverter and/or transfer to a standby inverter. The very high cost of such an approach is not accepted for most applications. Therefore, in literature and in this thesis (section 3.4) a single voltage source inverter with a redundant fourth phase leg is used. In case of a failure, transfer to the redundant leg takes place without interrupting the operation of the drive. But the replacement of the faulted phase of the inverter by a service person while the inverter is in operation is only possible with a very modular and special mechanical construction. Such an unconventional construction increases the

costs. If this is not acceptable, then the replacement of a faulted inverter phase must be postponed until the next planned downtime of the drive. This can reduce the availability class to AEC-3 “Fault Resilient”. In this thesis, only single faults at a given time are considered.

In a broad sense, fault tolerance is associated with reliable operation without having any breakdowns. A fault-tolerant system should be able to tolerate faults in all the hardware and software components, power failures or any other external unexpected disasters and still meet its specifications. It is practically impossible to build a system without any faults. So an interim solution to the fault tolerance is redundancy. Redundancy is the technique of using additional resources in order to mask or compensate the fault. There are different redundant techniques, which improve the overall reliability or availability of the systems. Basically, there are two types of redundancy available: space redundancy and time redundancy. *Space redundancy* provides additional components, functions, or data items that are necessary for a fault-free operation. Space redundancy is further classified into hardware redundancy, software redundancy and information redundancy. In the hardware redundancy, in addition to the considered module, one or more modules are connected, usually in parallel. These redundant modules are either identical or diverse. A general classification of hardware redundant systems is shown in Figure 1.4. In case of static redundancy, redundant systems are always active and work in parallel with the active system. Static redundancy achieves increased availability by masking the faults that occur without requiring any action on the part of the system or an operator. In case of dynamic redundancy, redundant systems will replace the faulted active system. Dynamic redundancy requires a fault to be detected before it can be tolerated. Dynamic redundancy is further divided into duplication with comparison, standby redundancy (cold standby, hot standby), and pair and spare. In case of duplication and comparison, two identical modules perform the same function and the result of the two modules are compared in a comparator. Any deviation in the outputs of the two modules is an indication of fault in any of the modules. This method can only indicate that there is a fault in the system, but it is not possible to say which one is having the fault. This method is used mostly in cases of fail-stop systems. In case of the hot standby, redundant system is always powered up and in some cases it will be implementing the same function as the active system. In case of the cold standby, redundant system is used and powered up only if there is a fault in the active system. This way it improves the overall reliability of the system and reduces the power consumption. Pair-and-spare technique combines standby sparing and duplication and comparison approaches. The main idea of hybrid redundancy is to combine the active features of both static and dynamic redundancy. Fault masking is used to prevent the system from producing erroneous results and fault detection methods are used to detect and locate the fault such that recovery steps can be taken. One way to implement the information redundancy is by using error detection and correction codes, in order to increase the reliability of a computer system.

The use of redundancy does not immediately guarantee an improvement in the dependability of a system. A number of choices need to be examined to determine a best way to incorporate redundancy to the system. For example, weight increase can be reduced by applying redundancy to the lower-level components. Cost increase can be minimized if the expected improvement in dependability reduces the cost of preventive maintenance for the system.

For drive applications, dynamic redundancy is not suitable because, as “Fault tolerance is the property that enables a system to continue operating properly in the event of a fault”, dynamic

redundancy needs a 100% perfect Error Detection and a zero switch over time to avoid any breakdown. As in reality, in duplex systems, the probability of detecting all arbitrary errors immediately by the "Error detection" is far below 100%. For example, in drive applications, the probability of undefined output, i.e. gate signals for the IGBTs, is correspondingly high. In such a situation, the primary protection e.g. over current protection will stop the drive. Due to this, continuous operation for 24h at each day cannot be guaranteed.

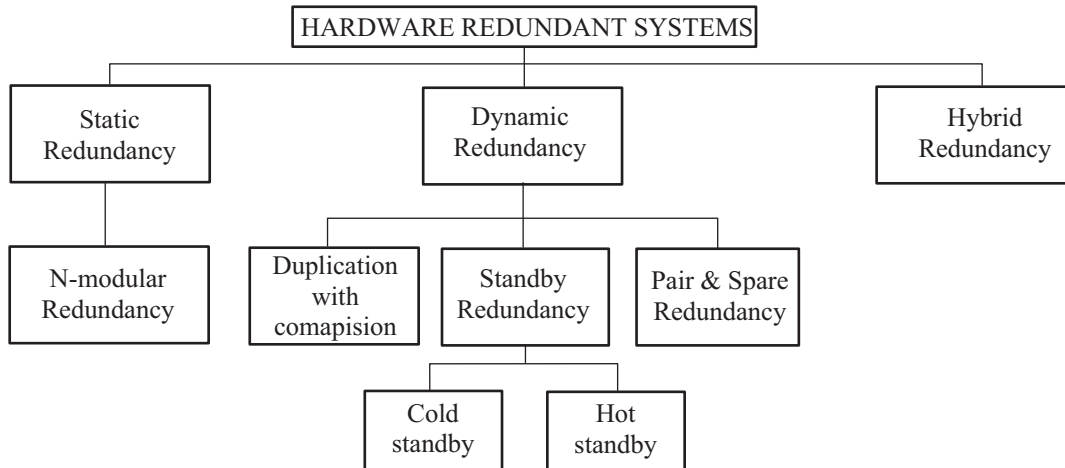


Figure 1.4: General classification of hardware redundant systems

Software redundancy is used to provide fault tolerance to errors and bugs in the control program. Software redundancy can be achieved by using diverse programs in the redundant controllers.

If a fault occurred on a system, the effect of the fault is visible after the grace time of the system. Grace time is the time that the system can tolerate a fault without affecting its performance. *Time redundancy* comes in the form of grace time during which the output of plant is not deviated from the expected output. Available time redundancy depends on the system or plant under fault. An optimum fault tolerant strategy depends on the amount of time redundancy available.

Mainly, because of cost, space, weight, availability and safety requirements, a suitable compromise should be made on which type of redundancy is used finally. In some redundant structure some suitable degrading steps are used where the system reaches a safe state which will not affect the safety requirements. Some fault tolerant systems are designed such that they will tolerate any arbitrary single fault. Such fault tolerant systems are called Fail-operational. The redundancy is allowed either to mask the fault or to detect the fault, with the following fault location, fault containment and recovery [DUB07].

Fault Masking is the process by which only correct values are allowed to output despite any failure in the system. This is done by preventing the system being affected by the faults, either by correcting the faults in time or compensating them by using remedial actions. By a fault masking method, faults are invisible to the operator and are automatically compensated. Static redundancy techniques are examples for the fault masking.

Fault detection is the process of finding out that a fault has occurred in a system. Different types of hardware and software techniques are used for the fault detection. In a broad sense, there are two methods of fault detection: Acceptance tests and comparison. In an acceptance test, the results of the process in combination with various feedback signals are subjected to test. There are different ways in which acceptance test can be implemented. Few of them are explained in [ISE06].

Different acceptance tests based fault detection methods are,

- Fault detection with limit checking
- Fault detection with signal models
- Fault detection with process-identification methods
- Fault detection parity equations
- Fault detection with state observers and state equations
- Fault detection with principle component analysis

Comparison is used for systems with duplicated components or modules. Outputs of functional identical systems are compared and any disagreement between them is an indication of a fault.

Fault location is the process of determining the location of a fault. Fault detection methods such as acceptance test and comparison will only indicate that there is a fault. Different fault diagnosis methods are used to find exactly which component of the system is failed. Different fault diagnosis methods using classification and inference methods are reported in [ISE06]

Fault containment is based on isolating the fault and preventing the propagation of the effect of the fault throughout the system. The idea is to stop the fault propagating from one area to other areas such that it will not affect the healthy part of the system. The result of fault detection and fault location are used further for fault containment.

Fault recovery is the process of isolating the faulted part of the system and taking necessary steps to resume its function. This is possible by replacing the faulted component, by making it off-line or using redundant techniques. In some cases, the system can continue to work without the faulted component or module but the performance may not be satisfactory. Such a process is known as graceful degradation.

1.3 Problem definition

In the research project, fault tolerant inverters for drives have to be systematically designed and analyzed. The inverter has to tolerate arbitrary single faults in

- the information processing,
- in the power section and
- in the sensors.

Different topologies and methods have to be compared and the most promising solution has to be realized in hard and software in an experimental setup. The ability to tolerate faults is to be proven by theory and by experiment.

1.4 Contribution

In this research project, solutions to increase the availability of different components of the drive are systematically developed and experimentally verified. Solutions to the

- 1) Failure in the information processing (digital controller)
- 2) Power section (PWM inverter)
- 3) Feedback sensors (position and current sensors)

are presented. The validity of the proposed solutions is verified using the field oriented control (FOC) of a permanent magnet synchronous machine (PMSM).

An improved availability of the digital controller is achieved based on the principles of triple modular redundancy. Three digital signal processors (DSPs) are used in parallel running the same

control algorithm. The PWM outputs of all the three DSPs are voted out using a simple majority voting logic which is by itself fault tolerant. In order to keep all the three DSPs in time synchronism to each other, a serial communication is developed between the three processors, which will exchange the timer values between all the three processors. This communication is also used to exchange the control variables between the three processors such that there is synchronism in the control variables finally used for the control computation. Connections between all the three processors are made such that there is no common point of failure in the system.

An improved availability of the inverter is achieved by adding a redundant leg along with standard three legs of two-level voltage source inverter (VSI). Faulted leg isolation and redundant leg insertion is done by using independent back-to-back connected thyristors. The proposed inverter provides tolerance to the both short circuit and open circuit faults of the switching devices. The post fault performance is same as the normal pre-fault operation and fault compensation is fast enough such that there is negligible disturbance in the drive operation.

Fault detection algorithms are implemented in both the cases of position sensor failure and current sensors failure. Position sensorless control algorithm is used in the case of position sensor failure. Normally, for FOC of the PMSM with isolated neutral, two current sensors are sufficient. In case of a failure in any of these two current sensors, a redundant current sensor measuring the third phase current is used in place of the faulty current sensor.

The whole system is developed based on the concept that only a single arbitrary fault occurs at any time. FOC of the PMSM is implemented to test all the above solutions to increase the availability. Faults at the DC-side of the inverter (mains, rectifier and DC-link) as well as faults in the machine are not part of this research project.

1.5 Outline of the Thesis

The content of this thesis is organized into six chapters. **Chapter 1** is an introduction chapter and presents the motivation behind this research works. The requirement of fault tolerant drives is explained briefly. Basic definitions and concepts of fault tolerance are presented in the next section. In the next sections, an exact problem definition and the contributions from the author to the proposed problem are presented.

Chapter 2 deals with fault tolerance of information processing (digital controller). It gives a brief comparison of different methods of redundant digital control systems. A MTTF analysis is done for selected methods of redundant digital controllers in the next section. A Triple Modular Redundancy (TMR) based fault-tolerant digital controller is selected for our application. The next sections present a single fault tolerant voter, synchronization, fault detection and compensation issues of the TMR based fault tolerant control system. A brief description about the experimental setup and relevant experimental results are presented in the subsequent sections.

Chapter 3 deals with the solutions to improve the availability of power section (Inverter) of a PMSM drive. A comprehensive survey and comparison of existing topologies is presented in the first section. In the next section, system description of the proposed voltage source inverter with increased availability is presented. The next two sections discuss the inverter operation and fault compensation during the IGBT open and short circuit faults. A brief description of hardware setup is given after this. Simulation and experimental results are shown for both IGBT open and short circuit fault cases (for both compensated and uncompensated) in the subsequent sections.

Chapter 4 deals with fault detection and compensation of the feedback system such as position sensor and current sensors. Principle of sensorless control for a PMSM is introduced first and then a method to detect the encoder failures is presented in first section. In the next section, method to detect the failure in the current sensor and compensation technique is presented. Finally, experimental results are shown for both position and current sensor failures.

Chapter 5 deals with a complete system with improved availability which can tolerate a fault in digital controller, inverter, position sensor and current sensor. System description is presented in the first section. Next section deals with the complete control algorithm in cases of faults in digital controller, inverter, position sensor and current sensor. In the last section, the experimental results are shown for faults in the digital controller, inverter IGBT short circuit fault, position sensor failure and current sensor failure.

Chapter 6 makes the general conclusion of the entire thesis and proposes some ideas for potential future research work.

2 Digital Controller with Increased Availability

2.1 Introduction

In an electric drive control, digital controllers play an important role of all the information processing of the feedback variables, control algorithm implementation and generating the corresponding control command to the inverter. Depending on the application requirements, for control of drives, different types of digital controllers are used, e.g. microprocessors, micro controllers, DSP, FPGA, computer with necessary interfacing cards, *etc.* As discussed in the chapter 1, any fault in the digital controller will cause malfunction of the drive or a complete shutdown. In order to provide fault tolerance to the digital controller or to improve the availability, different approaches and configurations are available in the literature which are briefly discussed in the following section.

Originally, hardware redundancy techniques are used for individual components to cope-up with the low reliable components. As providing the redundancy to individual components make a system more complex and with the decrease in the price of the silicon, in recent approaches, redundancies to the whole modules are employed. As reported in the chapter 1, hardware redundancy is classified into static redundancy, dynamic redundancy and hybrid redundancy. Static redundancy methods mask the fault rather than detect them. Special hardware or software techniques are used to detect the faults. Dynamic redundancy requires fault to be detected before it can be tolerated. Hybrid redundancy combines the features of both the static and dynamic redundancy. In the next few sections, a detailed explanation, advantages and disadvantages of selected redundancy types are presented, which are frequently employed in the real time applications.

2.2 Classification and comparison of redundant controllers

As reported in the chapter 1, hardware fault tolerant systems can be classified into: dynamic redundancy, static redundancy, and hybrid redundancy. In this section, among the aforementioned redundant controllers, only important types are compared.

2.2.1 Dynamic redundancy based controllers

Dynamic redundancy can be classified into duplication and comparison and standby redundancy. Duplication and comparison systems are mostly used in fail-safe systems. So they are neither considered fault tolerant nor do they improve the availability of the system. So they are not further considered here for comparison of redundant controllers.

2.2.1.1 Standby redundancy

In case of the standby redundancy, one redundant controller is used either in the cold standby or hot standby controller mode as shown in Figure 2.1 and Figure 2.2. Most of the times, the redundant controller hardware is the same as the main controller hardware because if the main controller fails, redundant controller takes over the control task and acts as the main controller. After the faulty controller is repaired, the repaired controller acts as a redundant controller to the active controller. That is the reason both the controllers are equipped with Error Detection blocks.

An extra hardware switch is required to transfer the control between the main controller and redundant controller. A communication link is necessary in order to either synchronize the two controllers or to exchange the control state before the fault. Fault detection can be part of the main controller or separate hardware can be used. Different fault detection techniques can be implemented in the main controller such as sanity check, watchdog timers and/or plausibility check. A brief description of different fault detection techniques is presented in the section 2.2.1.3.

Cold Standby:

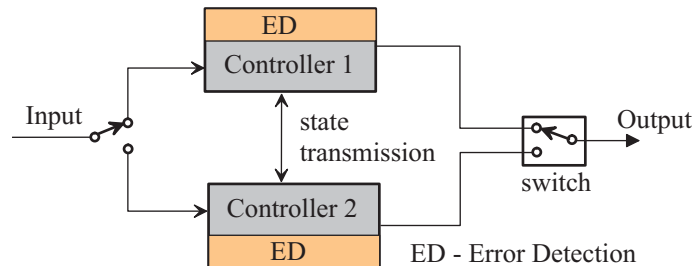


Figure 2.1: Architecture of cold standby controller

In case of the cold standby, main controller performs all the control tasks under the normal operating conditions. Redundant controller stays idle or powered OFF until it receives a takeover signal or fault signal either from the main controller or from the fault detection circuit (separate hardware). The main controller and redundant controllers are connected with an inter processor communication link. If any fault is detected in the main controller, the state of the control variables saved before the fault is communicated to the redundant controller and the input and output switch of the main controller is switched to the redundant controller. The transition time between the main controller and redundant controller depends on the fault detection duration and amount of the data to be transferred to the redundant controller. During the transition time, the output of the main controller is not defined and so is the plant behavior. The consequences of the fault depend on the type of the plant. In safety critical applications unpredictable behavior of the plant (e.g. drive of steer-by-wire systems) is not accepted. As there is a considerable delay in fault detection and redundant controller takeover, according to the definition of fault tolerance, such a system is not considered as a fault-tolerant system.

Advantages:

- As the backup or redundant controller is not in use in normal operation, power consumption of the whole system is less.
- As the redundant controller is not in use in the normal operating time, the reliability of the whole system increases.
- No synchronization between the controllers is necessary.
- As the main controller and redundant controller are not working at the same time, it is less likely that both the controllers are affected by a common mode fault.

Disadvantages:

- If the fault detection rate does not cover all the faults, it is possible that redundant controller will not take over the main controller in case of a fault.
- If the transition time between the main controller and redundant controller is high, then during this period, the plant behavior is unpredicted.
- If the main controller crashes completely, it is not possible to send the present control status of the main controller to the redundant controller.

Hot Stand by:

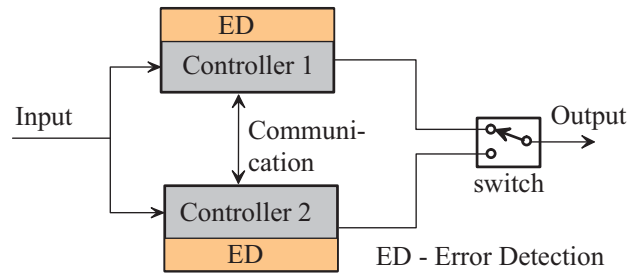


Figure 2.2: Architecture of hot standby controller

In the hot standby, redundant controller is powered ON and can also be used to monitor the plant behavior. It can also be additionally used to detect the fault in the main controller using a watchdog timer or any other suitable method. This eliminates the additional third party circuits to detect the faults in the main controller. Sometimes it is also possible to transfer the main controller status variables to the redundant controller such that in case of the main controller failure, the transition time is reduced. Indeed, the backup controller can also be used for other task and control functions.

Another variation of implementing the hot standby controller is based on the parallel operation of two functional identical controllers. If two controllers are running same type of control algorithm and fed with the same inputs and started at the same time, they should produce the same output. The outputs of the two controllers are constantly compared to detect the fault in one of the processors. However, this will not result in which controller is having a fault. Self-checkers in each controller such as coding techniques, plausibility check, sanity check and watchdog timers are used to detect some type faults in the controller.

If the two controllers are fed with different clocks, though started at the same time they deviate from each other because of the slight differences in the clock crystals. Though fed with the same inputs, slight variations in the A/D sampling and scaling & shifting circuits' cause variations in the input variables. If there are any integrators present in the control path, these errors will accumulate and eventually produce different results. So, inter processor communication is necessary to exchange the timer values and control variables. The two processors should be synchronized in time and also in control variables.

Advantages:

- As both the controllers are synchronized, switch over time to the redundant controller is very short and only depends on fault detection time.
- As the redundant controller is powered up and control status variables are exchanged within certain intervals, response to the external events is fast.
- If the plant cannot tolerate even short interruptions, a fail-safe controller can be implemented easily.

Disadvantages:

- As the redundant controller is also powered up always, whole system reliability is reduced and the power consumption is increased.
- If the fault detection rate does not cover all the faults, it is possible that the redundant controller will not take over the main controller in case of the fault.
- Additional hardware is required to synchronize the processors which ultimately decrease the reliability of the whole system.

2.2.1.2 Synchronization of dynamic redundant controllers

Synchronization is necessary in case of the parallel operation of the hot standby controllers. These duplex redundant controllers should have a common time reference otherwise they will have difficulty in agreeing on a common time frame for the inputs and outputs. Along with the common time reference, these duplex controllers should also be in synchronism at the input/output level, as any slight variations in these inputs will accumulate in the integrators and deliver an erroneous output. Usually systems are executed either in lockstep architecture or Master/Slave mode, or with a common fault-tolerant clock [POL96]. To achieve exactly the same internal state, all the replicated units should receive the same data at the same time, even if there are slight variations at the inputs of the units. In order to achieve the above criteria, all the input values to the controller should be exchanged and are matched such that finally all the inputs inside the controllers have the same values. The integrity of such synchronization can only be achieved with highly reliable fault detection methods, which are the bone of contention in duplex redundant systems [KIR05].

2.2.1.3 Fault detection in dynamic redundant controllers

Though different fault detection techniques are available for the dynamic redundancy, fault detection coverage depends on the effectiveness of the error detection circuits and algorithms. A close to 100% error detection or fault detection can only be achieved with complex error detection circuits and algorithms, which further decreases the reliability and increases the complexity of the whole system. Therefore, a tendency exists to reduce the coverage to save design efforts at the expense of the availability. At the end, the availability will depend entirely on the error detection coverage. Coverage is the probability that an error is discovered within a useful time [KIR05].

Watchdog timer:

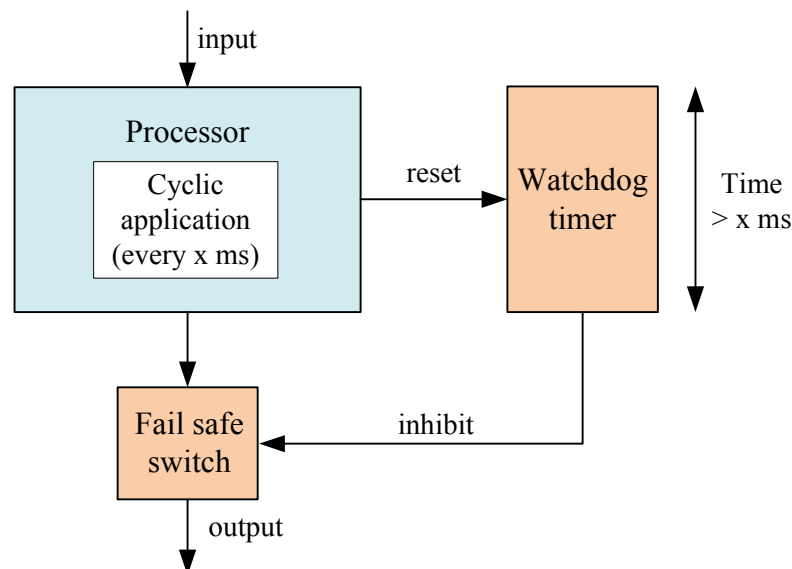


Figure 2.3: Fault detection using the watchdog timer

For keeping track of the proper program execution, watchdog timers are used. Figure 2.3 shows the watchdog timer, monitoring the status of a controller. The controller has to reset the watchdog timer after predefined time (x ms in Figure 2.3). If the controller fails to reset the watchdog timer, then the watchdog timer counter counts behind x ms and a fail-safe command is issued to the output switch as shown in Figure 2.3.

Error detection and correction by coding:

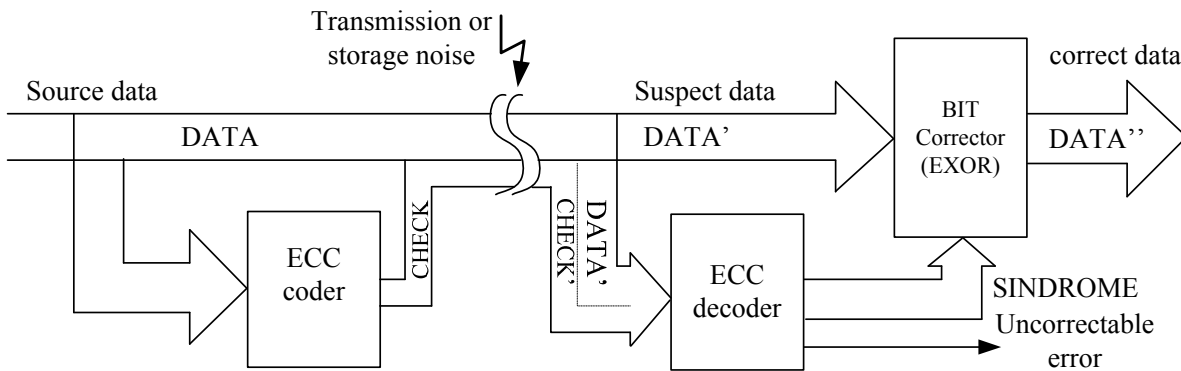


Figure 2.4: Error detection and correction by coding [KIR05]

Coding techniques are used for the error detection and correction in the digital systems, for example, Error Correction Codes (ECC) for all RAMs, parity on buses, Cyclic Redundancy Check (CRC) on serial transmissions and duplication and comparison for complex logic. In a coding technique, pieces of information are represented by code words or sequence of code words (parity, checksum, cyclic redundancy...). The basic principle of a coding is shown in Figure 2.4. The general idea for achieving the error detection and correction is to add some redundancy (i.e., some extra data) to a message (ECC coder), which the receiver can use to check consistency of the delivered message (ECC decoder), and to recover data determined to be erroneous (bit corrector). Some simple codes only perform error detection. Error correction is then done by some other mean, like retransmission. The largest application of the Error Correcting Codes is found in increasing the reliability of semiconductor memories, which suffer from spurious bit inversions. For example, in a 32-bit memory extended by a 7-bit Hamming Code for single error correction, double error detection. Similarly, coding schemes can also be applied for information transmission and also used to mask the errors in computing elements.

Fault detection by protocol checks:

The behavior of the most sequential logic circuits and systems can be described by the state machines and other protocols. Selected process states or module outputs can be compared to the predicted values, generated by alternative algorithms or off-line units. The data values can be checked for proper structure or consistency with previous or predicted values. To implement such fault detection methods, application-specific information is necessary, which might, in turn, depend on unpredictable inputs.

Fault detection by sanity monitoring:

A unit monitors the health of another unit by expecting periodic health messages. The unit that is being monitored should check its sanity and send the periodic health update to the monitoring unit. The monitoring unit will report a fault, if more than a specified number of successive health messages are lost.

Fault detection by plausibility and limit checking:

The simplest and frequently used method for the fault detection is limit checking of a directly measured variable. The absolute values of the measured variables are monitored and checked for their consistency and thresholds. If any of the variables exceed the defined thresholds, a fault is assumed in the process. A rough supervision of the measured variables is performed by

checking the plausibility of its indicated values. This means the measurements are evaluated with regards to credible, convincing values and their compatibility among each other. For example, a certain measurement is examined whether its sign is correct, and its values are within predefined limits.

Fault detection by sanity check:

A sanity test or sanity check is a basic test to evaluate quickly whether a claim or the result of a calculation is true or not. A rule-of-thumb may be checked to perform the test. For example, in electric drive applications, in a machine with isolated star connection, the sum of all the currents is zero (excluding measurement noise and offsets).

2.2.2 Static redundancy based fault tolerant controller

2.2.2.1 N-modular redundancy

N-modular redundancy is also called parallel redundancy, where multiple units are running in parallel. The same type of hardware in all the controllers can be used or in order to avoid common design faults, design diversity can also be employed. In the N-modular redundancy, the fault masking ensures that only correct values are passed to the system output in spite of the presence of a fault. Majority voters are used to mask the fault and produce the correct results finally at the output. The number N is usually selected to be odd, to make the majority voting possible. If any integrator present in the control path, along with the time synchronization control, the control variable's synchronization is also necessary. In order to achieve the fault tolerance, in N-modular redundancy, the faulted controller should be repaired online or replaced without disturbance to the operation of the plant. During this process, one should make sure that it will not disturb the existing controllers and steps should be taken to resynchronize the repaired controller.

2.2.2.2 Triple Modular Redundancy (TMR) controllers

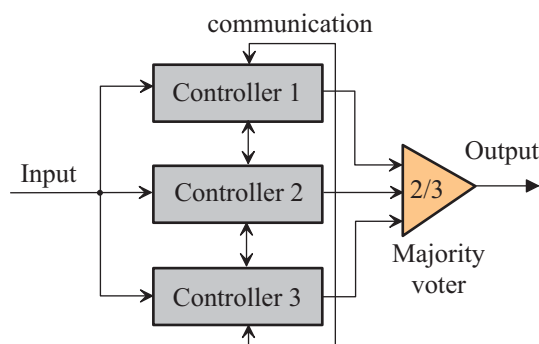


Figure 2.5: Triple modular redundant controller architecture

Though the dual modular redundancy increases the reliability by detecting and recovering the fault rapidly, some plants cannot tolerate even the short interruptions. In such a case, TMR controllers are used. Figure 2.5 shows the architecture of a TMR based fault tolerant controller.

According to [EMB], TMR is based on the assumption that the probability of a second error occurring before the failed part is replaced is very small. For systems where this assumption is invalid, TMR is sometimes extended to Quad Modular Redundancy (QMR), where four subsystems drive a voter circuit. In this instance, when a fault is detected in one of the four units, there is still a TMR fault-tolerant system in place. Further, should two errors occur, they are extremely unlikely to produce the same error condition. In this instance, the output of the two faulty subsystems will be

ignored and the voter will pass through the output of the two subsystems in agreement. The space shuttle uses a variation of QMR for its flight avionics. The primary system is a QMR implementation, with a fifth backup system in place. In the unlikely event that three of the four subsystems in the QMR group disagree, all four are shut down and control is transferred to the fifth system. [EMB]

In the TMR systems, three functionally identical controllers are used in parallel running the same control algorithm. A safe majority voter is used at the output of the controllers in order to select the final output for the control. A TMR system can mask only one controller fault. A failure in either of the remaining controllers would cause the voter to produce an erroneous result. The TMR controller differs to the dual modular redundancy in three ways:

- 1) In the healthy state all the controllers are active all the times
- 2) A fault in one controller will not affect the output
- 3) Majority voting is used to select the outputs of the controller

In TMR systems in order to avoid common mode failures, diversity in hardware and software can be employed. In such a system, functionally identical three independent controllers are used with software developed on three different platforms. Any fault in one of the controllers is masked by majority voting of the voter. Hence, a single fault in any controller is tolerated without any effort for specific fault detection. Though this system provides more availability than the dual modular redundant system, the cost of the system increases a lot. Strict time synchronization is required between all the modules such that output produced by all of them is same. An input variable or control variable synchronization is also necessary as small errors in input sampling will accumulate in the integrators of the controllers.

Advantages:

- The availability of the system is improved when compared to dual modular redundant system.
- For a single fault in any controller, no specific fault detection algorithms or circuits are necessary.
- Any fault in the controller is masked by the voter. So a bump less control of the plant is ensured

Disadvantages:

- Triplicated hardware, voter and synchronization hardware make the system more expensive.
- Additional communication link and computing power is required for synchronization.
- Extra software control algorithm is required for the synchronization and matching the inputs, but communication and synchronization is necessary for the standby systems too.
- The voter is the crucial part of the TMR system. If the reliability of the voter is insufficient, it must itself be replicated.

2.2.3 MTTF evaluation and comparison of redundant controllers

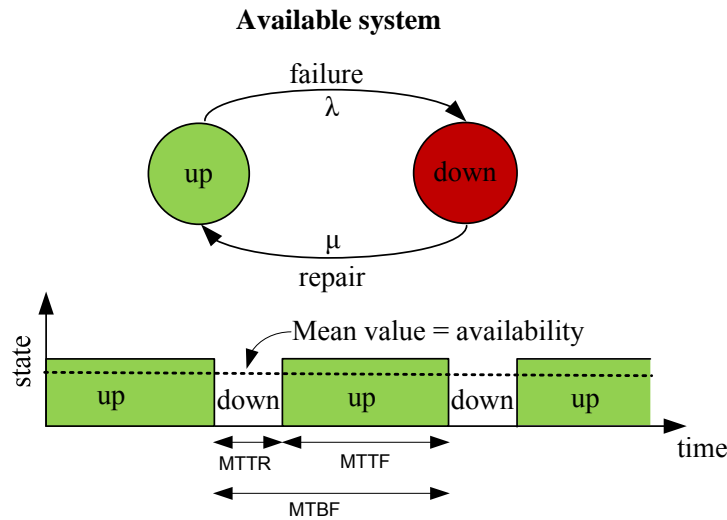


Figure 2.6: Life cycle of a repairable system [KIR05]

During the life phase of the system (phase 2 of Figure 1.3), failure rate function is assumed to have a constant value λ . Where, λ is the failure rate defined as the expected number failure per unit time. With the assumption of constant failure rate, the reliability of the system varies exponentially as a function of time [DUB07]:

$$R(t) = e^{-\lambda t} \quad (2.1)$$

To express the availability of an element, one often uses the Mean Time To Fail, or *MTTF* of that element, which is the average lifetime of the element. It is generally expressed in terms of reliability as:

$$MTTF = \int_0^{\infty} R(t) dt = \frac{1}{\lambda} \quad (2.2)$$

When a redundant controller can be repaired or replaced online without disturbing the system operation, the availability of the whole system increases drastically. So it makes sense for repairable system to define and calculate the availability. Markov models are used to calculate the availability of the repairable systems [KIR05].

Figure 2.6 shows the life cycle of a repairable element. The element can be in any of the two states, either working (up) or failed (down). A failure corresponds to the transition labeled λ and a repair corresponds to the transition labeled μ . The system oscillates between the two states up and down. As per the definition of the availability presented in the Section 1.2, the availability can be calculated as $A = MTTF / (MTTF + MTTR)$. In further availability evaluation, repair rate (μ) is assumed constant, with $\mu = 1/MTTR$. For repairable systems, it is easy to calculate *MTTF* of the system rather than availability. If the failure rate λ and the repair rate μ are assumed constant, then *MTTF* is an indirect measure of the availability [KIR05].

2.2.3.1 MTTF of hot standby redundant system –assuming perfect fault detection

Let us consider a repairable hot standby redundant system. As long as two controllers are healthy, the system is in the state 0. If one of the controllers fails, then the system reaches the state 1 and if all the two controllers fail, then the system reaches the state 2. The transition rate from the state 0 to the state 1 is 2λ , since there are two units that can fail. As defined before, the repair transition from the state 1 to the state 0 is μ . The transition rate from the state 1 to the state 2 is

only λ , since there is only one unit that remains to fail. State 0 and the state 1 are called non-absorbing states and the state 2 is called absorbing state.

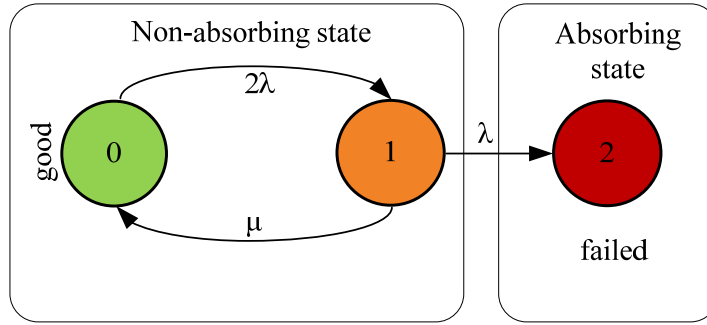


Figure 2.7: State transition diagram of repairable hot standby system

The Figure 2.7 can be represented in differential equation, which can be further solved by using the Laplace's transformations.

$$\frac{dP_0}{dt} = -2\lambda P_0 + \mu P_1 \quad (2.3)$$

$$\frac{dP_1}{dt} = 2\lambda P_0 - (\lambda + \mu) P_1 \quad (2.4)$$

$$\frac{dP_2}{dt} = \lambda P_1 \quad (2.5)$$

With initial conditions $P_0(0)=1$ (initially good), $P_1(0) = 0$ and $P_2(0)=0$. Where, P_0 , P_1 and P_2 are the system states.

Using the Laplace's transformations to solve the equations with the initial conditions,

$$sP_0(s) - P_0(t=0) = -2\lambda P_0(s) + \mu P_1(s) \quad (2.6)$$

$$sP_1(s) - 0 = 2\lambda P_0(s) - (\lambda + \mu) P_1(s) \quad (2.7)$$

$$sP_2(s) - 0 = \lambda P_1(s) \quad (2.8)$$

The MTTF can be calculated by using the boundary theorem such as,

$$MTTF = \int_0^{\infty} \sum P_i(t) dt \quad (2.9)$$

Where $\sum P_i(t)$ are non-absorbing states 0 and 1.

Applying the boundary theorem, $\lim_{t \rightarrow \infty} \int_0^{\infty} P(t) dt = \lim_{s \rightarrow 0} sP(s)$, and only including the non-absorbing states, equations (2.6)-(2.8) can be simplified as

$$-1 = -2\lambda P_0 + \mu P_1 \quad (2.10)$$

$$0 = 2\lambda P_0 - (\lambda + \mu) P_1 \quad (2.11)$$

Solution of the above two linear equations is,

$$MTTF_{HS-R} = P_0 + P_1 = \frac{\mu + \lambda}{2\lambda^2} + \frac{1}{\lambda} = \frac{\mu/\lambda + 3}{2\lambda} \quad (2.12)$$

In the equation (2.12), by inserting $\mu=0$, the result for the case of non-repairable system can be obtained as below,

$$MTTF_{HS-NR} = \frac{3}{2\lambda} \quad (2.13)$$

2.2.3.2 MTTF of the hot standby redundant system – for an imperfect fault detection

The above evaluation is done assuming that the fault detection is perfect, and if one of the controllers fails then the redundant controller takes over the control function. However, this is not always true as explained in the section 2.2.1.3. So in a dual system the probability of takeover to the redundant system is less than one. This probability is called coverage [KIR05]. It is extremely difficult and unconfident to predict a realistic value for the coverage. In drive applications, the controller has to generate the gate-pulses for the IGBTs. The useful time for detection of an arbitrary error in the controller by an algorithm executed on the possibly faulted controller itself is in the order of a millisecond or shorter. The reason is that, a wrong sequence of gate pulses can cause a high over-current and the over-current protection will shut down the drive. Therefore, error detection and coverage is crucial for the hot standby approach.

In the hot standby system, only one of the two controllers is used for control and the other remains hot standby. When an error occurs, it is detected with a certain probability and switchover takes place. The probability that the switchover successfully takes place is the coverage (c). The Markov diagram shown in Figure 2.7 can be modified to include the coverage factor as shown in Figure 2.8.

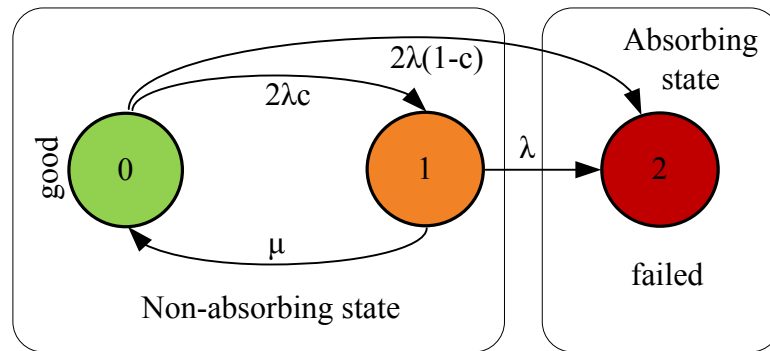


Figure 2.8: State transition diagram of repairable hot standby system with coverage

For an imperfect hot standby system based on the Markov model of Figure 2.8, equations (2.6)-(2.8) can be modified as,

$$-1 = -2\lambda P_0 + \mu P_1 \quad (2.14)$$

$$0 = 2\lambda c P_0 - (\lambda + \mu) P_1 \quad (2.15)$$

Solution of the above two linear equations is,

$$MTTF_{HS-R-c} = P_0 + P_1 = \frac{\mu/\lambda + (1 + 2c)}{2(\lambda + \mu(1 - c))} \quad (2.16)$$

2.2.3.3 MTTF of the TMR system

As described before, the TMR systems work based on the principle of masking. They are also called 2/3 voting systems, means at least 2 systems should be fault free for a correct output. These systems can tolerate only fault in any one of the modules. As long as the faulted module is repaired and replaced, the system is considered as fault-tolerant system. From the Figure 2.9 it is clear that, if the system is fault free then it is at the state 0, if one of the modules is failed, then is at the state 1, if one more module is failed, then is at the state 2. Here, the voter of the TMR system is assumed fault free (a single fault tolerant voter is presented in Section 2.3.3).

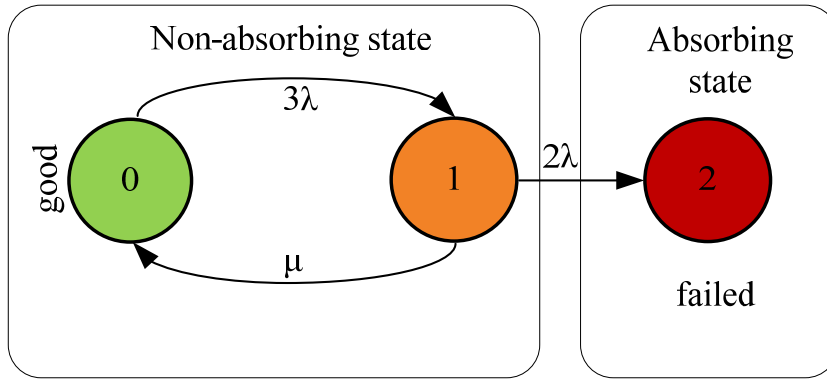


Figure 2.9: State transition diagram of repairable TMR system

Representing the Figure 2.9 in differential equations,

$$\frac{dP_0}{dt} = -3\lambda P_0 + \mu P_1 \tag{2.17}$$

$$\frac{dP_1}{dt} = 3\lambda P_0 - (2\lambda + \mu) P_1 \tag{2.18}$$

$$\frac{dP_2}{dt} = 2\lambda P_1 \tag{2.19}$$

Considering only non-absorbent states and applying the Laplace’s transformation and boundary theorem, equations (2.17)-(2.19) can be simplified as,

$$-1 = -3\lambda P_0 + \mu P_1 \tag{2.20}$$

$$0 = 3\lambda P_0 - (2\lambda + \mu) P_1 \tag{2.21}$$

Solution of the above two linear equations is,

$$MTTF_{TMR-R} = P_0 + P_1 = \frac{1}{\lambda} \left(\frac{5}{6} + \frac{\mu}{\lambda} \right) \tag{2.22}$$

In the equation (2.22), by inserting $\mu=0$, the result for the case of non-repairable system can be obtained as below,

$$MTTF_{TMR-NR} = \frac{5}{6\lambda} \tag{2.23}$$

2.2.3.4 MTTF comparison of redundant systems:

Table 2.1 shows the results of the MTTF evaluation of different redundant systems. Results are evaluated for both the repairable and non-repairable systems, including the coverage factors in case of duplex systems. In order to evaluation MTTF, it assumed that a simplex drive is expected to work at least for 3 years working 8 hours per day without any interruptions and also it assumed that it takes at least 24 hours to repair any fault in the drive. In this way the parameters considered for the MTTF evaluation are: failure rate $\lambda = 1.157e-4$, repair rate $\mu = 0.0417$ and coverage factor $c = 0.9$. As the TMR works based on the principle of fault masking, the coverage factor is assumed $c = 100\%$. From the results, it is evident that, the TMR systems with repair have the highest MTTF. Even, duplex systems with repair and 100% coverage factor have about half of MTTF compared to TMR systems. As, in reality, in duplex systems, the probability of detecting all arbitrary errors immediately by the “Error detection” is far below 100%. So in order to achieve fault tolerance, TMR based controllers are the best candidates.

Table 2.1: MTTF evaluation of redundant systems (for $\lambda = 1.157e-4$ and $\mu = 0.0417$)

Redundant system		MTTF equation	MTTF in hours	MTTF in years
Simplex		$\frac{1}{\lambda}$	8640	3
Duplex	Duplex without repair and $c = 100\%$	$\frac{3}{2\lambda}$	12960	4.5
	Duplex with repair and $c = 100\%$	$\frac{\mu/\lambda + 3}{2\lambda}$	1.5687e+06	544.5
	Duplex with repair and fault coverage $c = 90\%$	$\frac{\mu/\lambda + (1 + 2c)}{2(\lambda + \mu(1 - c))}$	4.2359e+04	14.7
TMR	TMR without repair	$\frac{5}{6\lambda}$	7200	2.5
	TMR with repair	$\frac{1}{\lambda} \left(\frac{5}{6} + \frac{\mu}{\lambda} \right)$	3.1176e+06	1082

2.2.4 Choosing of redundant controller topology for fault tolerant applications

After analyzing the different factors, TMR based controller is selected for fault tolerant drives application. Different factors that influenced the decision are,

- 1) Relatively high MTTF (or availability) when compared to the duplex systems.
- 2) Works based on the principle of fault masking. So a bumbles control output can be achieved even in the case of failure in one of the controllers.
- 3) Building a fault-tolerant majority voter in the TMR systems is easy when compared to building a fault-tolerant switch in the duplex systems.
- 4) Online repair or replacement of a faulted controller is possible (if the accessibility is available).
- 5) Implementing the fault detection algorithms are easy and require no additional hardware.

2.3 Digital controller with increased availability

In this research work, the availability of the digital controller is increased by using redundant digital controllers based on TMR. As explained in the section 2.2.2.2, TMR architecture needs three digital controllers. In order to synchronize (explained in the section 2.3.1) the three digital controllers, a high speed communication between all the processors is necessary. Even though the serial communication is slow when compared to parallel communication, it needs less hardware and wiring. So, the selected digital controller should be fitted with high speed serial communication ports. Modern DSPs and microcontrollers are equipped with different serial communication ports. Each digital controller should have at least two high speed serial communication ports such that it can communicate with other two controllers.

In this research work, three digital signal processors (DSP) based controllers are used in TMR architecture running the same control algorithm. The PWM outputs of all the three DSPs are voted out using a simple fault-tolerant majority voting logic (explained in the section 2.3.3). In order to keep all the three DSPs in the time synchronism to each other, a serial communication is developed

between the three processors, which will exchange the timer values between all the three processors for synchronization. This communication is also used to exchange the control variables between the three processors such that there is a synchronism in the control variables finally used for the control computation. Connections between all the three processors are made such that there is no common point of failure in the system. All the three DSPs are fed from separate power supplies. The only common point to the three DSPs is the voting logic, which is also fault-tolerant.

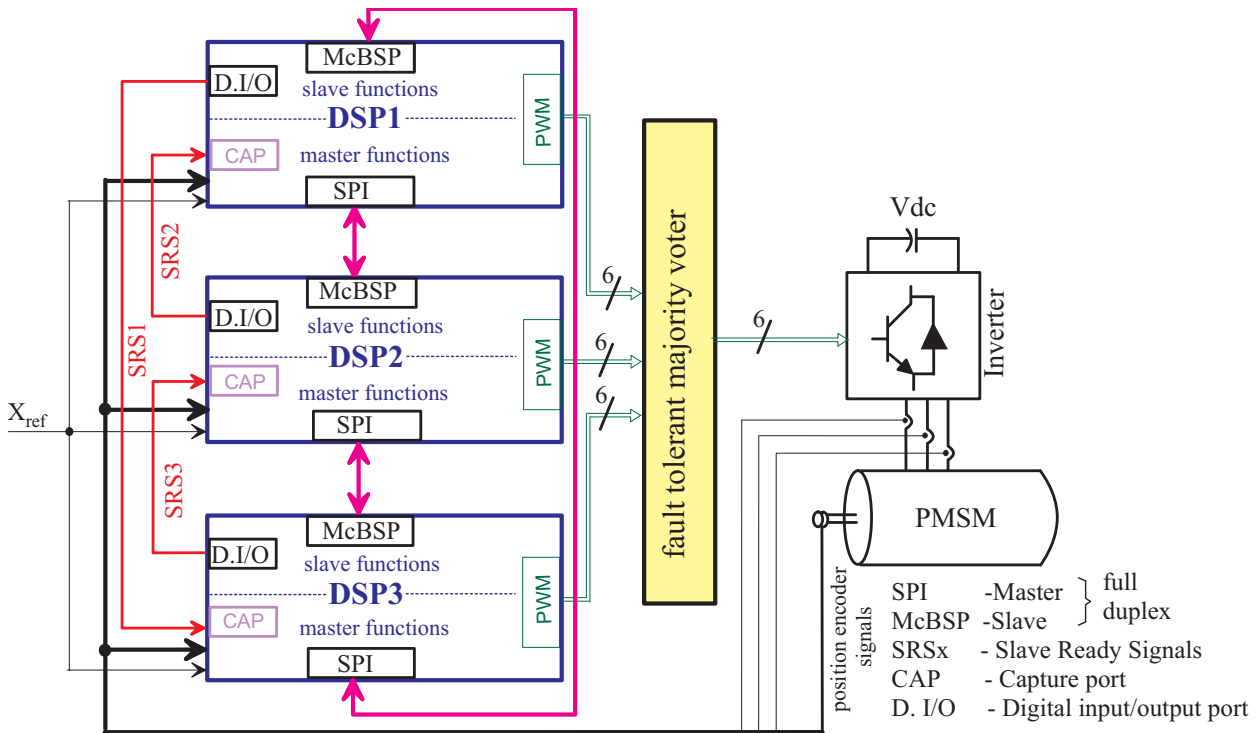


Figure 2.10: Fault tolerant digital controller architecture

Figure 2.10 shows the block diagram of the fault-tolerant digital controller architecture with three DSPs applied to a PMSM drive control. The main parts of the block diagram are three TMS320F2812 DSPs from Texas Instruments, one transistor based fault-tolerant majority voter board, IGBT IPM based 3-phase 2-level inverter, and a PMSM. Each DSP contains two synchronous serial communication ports: one is Serial Peripheral Interface (SPI) and the other one is Multi channel Buffered Serial Port (McBSP) [SPR61]. As indicated in Figure 2.10, in each DSP, master functions and slave functions can be found. The SPI is used as master and the McBSP is configured as the SPI slave. The communication between any two DSPs is in full duplex mode such that it can transfer and receive the data at the same time. In the SPI communication only the master will supply the clock. So a slave ready signal (SRS1...SRS3) is used in order to make sure that the slave device is ready to transfer the data when the master initiates the data transfer by clocking. Simultaneously, slave ready signals are also used to capture the timer values in the neighbor DSPs which are further used to synchronize the three DSPs in time. These SRS signals are used to trigger the capture port (CAP in Figure 2.10) to capture the timer values. In this communication architecture, each DSP has a master port and slave port. DSP1 will act as the master for DSP2, DSP2 will act as the master for DSP3 and DSP3 will act as the Master for DSP1. The physical communication connections between all the DSPs are developed such that there is no common point of failure.

2.3.1 Synchronization

Quartz crystals as the clock oscillator are used for providing the time base to the processors. No two crystals with the same specifications behave same because of the physical variations in crystal and temperature variations. These small variations in the crystals cause a drift in overall time. Though the drift is small, it adds up over the time. As the processor-clocks of three DSPs are generated by three independent crystals, it is quite possible that they will drift out of synchronism, even though they are started at the same instant of time. In order to keep three DSPs in time synchronism, timer values of the three DSPs are exchanged between all the DSPs and their timer counter are modified such that they will be in synchronism. The synchronization is done in each control cycle (100 μ s).

As the three processors have three independent A/D converters, it is quite possible that there will be some difference in the output of the A/D converter. They also use independent scaling and shifting circuits. Even though their offsets, scaling and shifting gains are finely tuned, there will be some minute differences, which will eventually accumulate in the integrators of the PI controllers. These differences in the integrators finally lead to erroneous output. In order to overcome above problem one has to exchange either the feedback variables or integrator values of the PI controllers such that finally all the same kind of integrators of all the DSPs has the same values.

For a fault-tolerant system, on-line replacement of a faulted component (e.g. DSP) without disturbing the healthy components (DSPs) is mandatory. After such a replacement, the state variables (integrators) in the control algorithm of the new (replaced) DSP must be set to the average of the corresponding state variables in the two healthy DSPs. For this reason, it makes sense to synchronize the state variables in the control algorithm of all DSPs during the whole operation time.

As the on-line replacement of a DSP was not experimentally investigated in this thesis, for convenience only the input variables have been synchronized, as can be seen in Figure 2.23.

If all the processors are in healthy condition then median value selection is used for final input variables selection. Fault detection and compensation algorithms will be implemented based on the information from exchanged variables (section 2.3.2).

All the algorithms in this document are developed with respect to DSP1, and similar algorithms are used in DSP2 and DSP3.

2.3.1.1 Timer synchronization

Normally, digital signal processors implement the code in sequential logic, so when the three processors are not synchronized and in order to sample the three processors timer counter values at the same time, we need to have a common time reference. As the three processors must be fault-tolerant, it is not recommended to have one master and the remaining slaves for timer synchronization. So a different approach is used, as explained below.

Each DSP has two neighbors: One is its master and the other is its slave. All DSPs execute the same code. The start of a control cycle in each DSP is triggered by an interrupt, which is generated when the value of the local timer (triangle waveform) is zero. By this, the execution of the control program in each DSP is synchronized to the local timer. At a specific point of the control program, the value of the local timer is read and stored locally. Quasi simultaneously a hardware output signal is generated, which causes the timer value of the neighboring master-DSP to be read and stored there without delay. By this, a pair of consistent values which existed at the same

instant of time in the local timer and in the timer of the master is stored. However, this is not enough. Additionally, a pair of consistent values from the local timer and the timer of its slave must be stored.

When the control program of the neighboring slave arrives at the specific point, the value of the timer in the slave is read and stored there. Quasi simultaneously the slave generates a hardware output signal, which causes the timer value of its neighboring master-DSP to be read and stored without delay. By this, a pair of consistent values which existed at the same instant of time in the timer of the slave and in the local timer is stored. Subsequently, all DSPs transmit their stored timer values via serial communication to their neighbors. Within these serial communication cycles, in addition to the timer values also all input and state variables are exchanged between the DSPs. After this transfer, each DSP has two pairs of consistent timer values. The difference between the two values of a pair represents the distance between associated the timers. These differences are used to update the slowest timer to next faster one and to update the fastest to the next slower one.

Figure 2.11 shows the content of the three PWM timers of the three DSPs. In order to explain the timer synchronization, a case is assumed where all the three DSP timers are deviating from each other. The content of all the three DSP timers are plotted verses a common time axis, and then synchronization is explained in steps below.

- 1) At t_1 , the control cycle of DSP1 starts (typically each 100 μs) and DSP1 will start with ADC sampling, conversion and machine rotor position calculation. Similarly, at t_2 , t_3 DSP2 and DSP3 control cycle will begin, and they start with ADC sampling, conversion and machine rotor position calculation.

At t_4 , DSP1 finished its actions mentioned in 1) and stores its own timer counter value (T10) then loads it in to the slave transmit (McBSP) register along with the feedback variables (e.g. i_a , i_b , θ_e) and issues a slave ready signal (SRS1) to DSP3 (see Figure 2.10). This SRS1 signal will trigger the capture port (CAP) in DSP3 to capture its timer value (T3S1Ry–Timer 3 values when Slave 1 is ready). Additionally, at t_4 the “Synchronization Window” (SyWin1 in Figure 2.11) for DSP1 starts. The synchronization window is a fixed time where each DSP will be polling for the slave ready signal and check for the data transfer from the other DSP’s to be finished. During such a data transfer, not only the timer values will be exchanged, but also the variables from the control algorithm, especially the feedback variables (e.g. i_a , i_b , θ_e) are exchanged. The synchronization window is the time required for the data transmission and some more grace time (about 5 μs). If no slave ready signal is detected, or if the communication is not finished within the synchronization window, neither the timer values nor the feedback variables are exchanged. This situation is detected and handled by the algorithm explained in the section 2.3.2 (Fault Identification and Compensation). Figure 2.12 shows algorithm for the synchronous window loop execution (for DSP1). In the algorithm T10 is the timer value of DSP1 stored before the synchronous window loop starts and the variable loop_out is set to 1. T1 is the DSP1 own timer counter value, T_{tt} is the time required for the data transmission, T_g is the grace time, Flag_S2Ry is set when DSP1 receives a slave ready signal (SRS2) from DSP2, Flag_21 is the flag set when DSP1 receives required number of bytes from the DSP2 and Flag_31 is the flag set when DSP1 receives required number of bytes from DSP3. The while loop constantly checks if the SRS2 signal is arrived from DSP2 and if the data transmission with the DSP2 and DSP3 are finished. As soon as the SRS signal is arrived from DSP2, DSP1 loads its captured timer counter value T1S2Ry and feedback variables in the master

transmit register and enable the data transmission with DSP2. The while loop comes out once the SRS2 Signal is issued and required number of data bytes are received or once the Timer T1 counts beyond the specified condition.

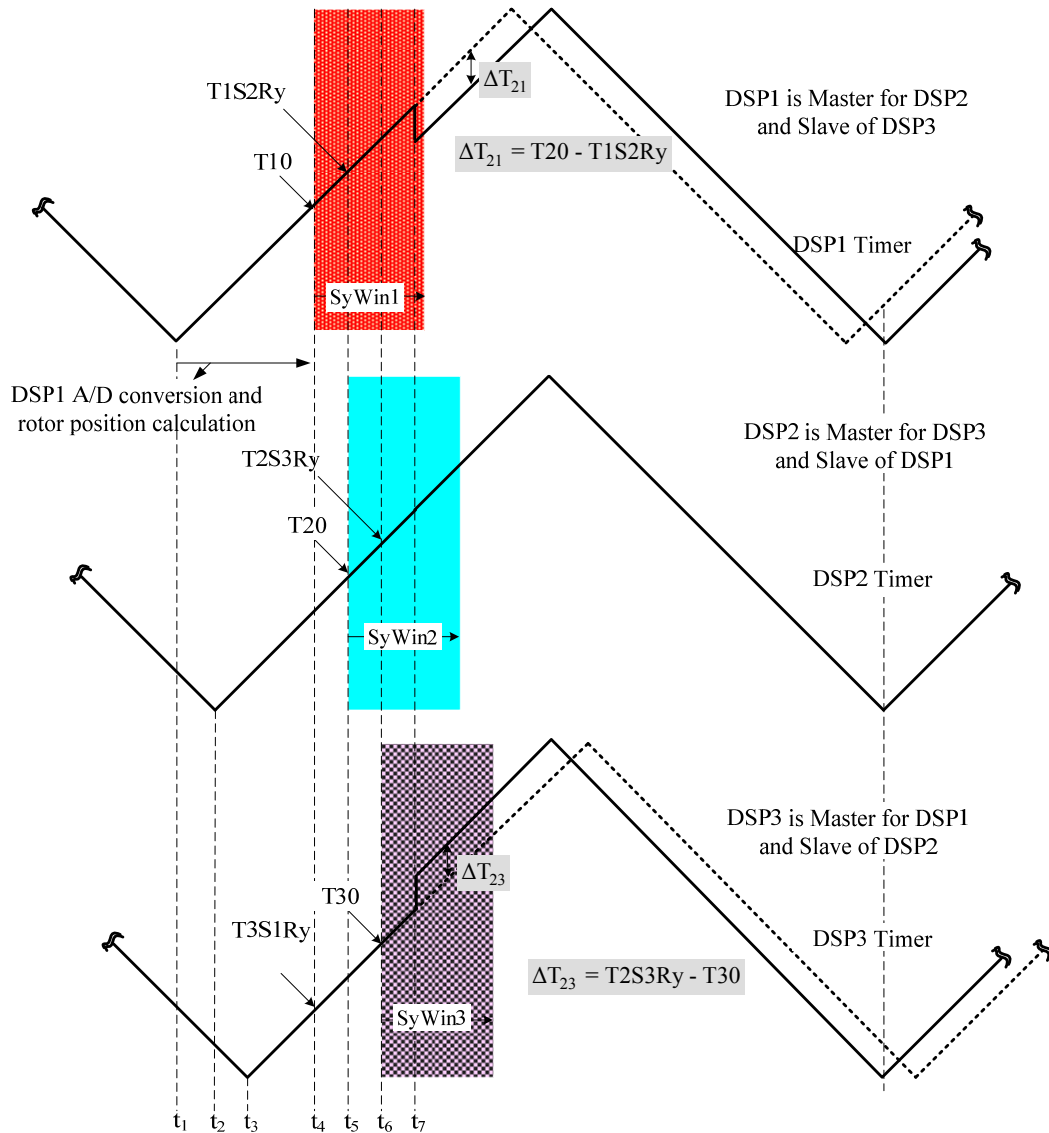


Figure 2.11: Timer synchronization of three DSPs'

- 2) At t_5 , DSP2 will store its timer value (T_{20}) and loads T_{20} into its McBSP transmit register along with the feedback variables, from where it will be sent later to DSP1 when DSP1 has received the SRS2 signal. After loading the McBSP transmit register, it issues a slave ready signal (SRS2) to DSP1. This SRS2 signal will trigger the capture port (CAP) in DSP1 to capture its timer value (T_{1S2Ry} –Timer 1 values when Slave 2 is ready). As DSP1 is the master for DSP2, as soon as the slave ready signal is received from DSP2, it will load its master transmit registers (with T_{1S2Ry} and feedback variables) and initiates the communication between DSP1 and DSP2. In this communication, T_{20} and the feedback variables of DSP2 are transmitted from DSP2 to DSP1 and T_{1S2Ry} and the feedback variables of DSP1 are transmitted from DSP1 to DSP2. At t_5 starts the synchronization window (SyWin2) of DSP2.
- 3) At t_6 , DSP3 will store its timer value (T_{30}) and loads T_{30} into its McBSP transmit register along with the feedback variables, from where it will be sent later to DSP2 when DSP2 initiates

the data transmission with DSP3. After loading its timer values (T30) and feedback variables, DSP3 issues a slave ready signal (SRS3) to DSP2. This SRS3 signal will trigger the capture port (CAP) in DSP2 to capture its timer values (T2S3Ry–Timer 2 values when Slave 3 is ready). As DSP2 is the master for DSP3, as soon as the slave ready signal is received from DSP3, it will load its master transmit (SPI) register with T2S3Ry and feedback variables and initiates the communication between DSP2 and DSP3. In this communication, T30 and feedback variables of DSP3 are transmitted from DSP3 to DSP2 and T2S3Ry and feedback variables of DSP2 are transmitted from DSP2 to DSP3. At t_6 starts the synchronization window (SyWin3) for DSP3.

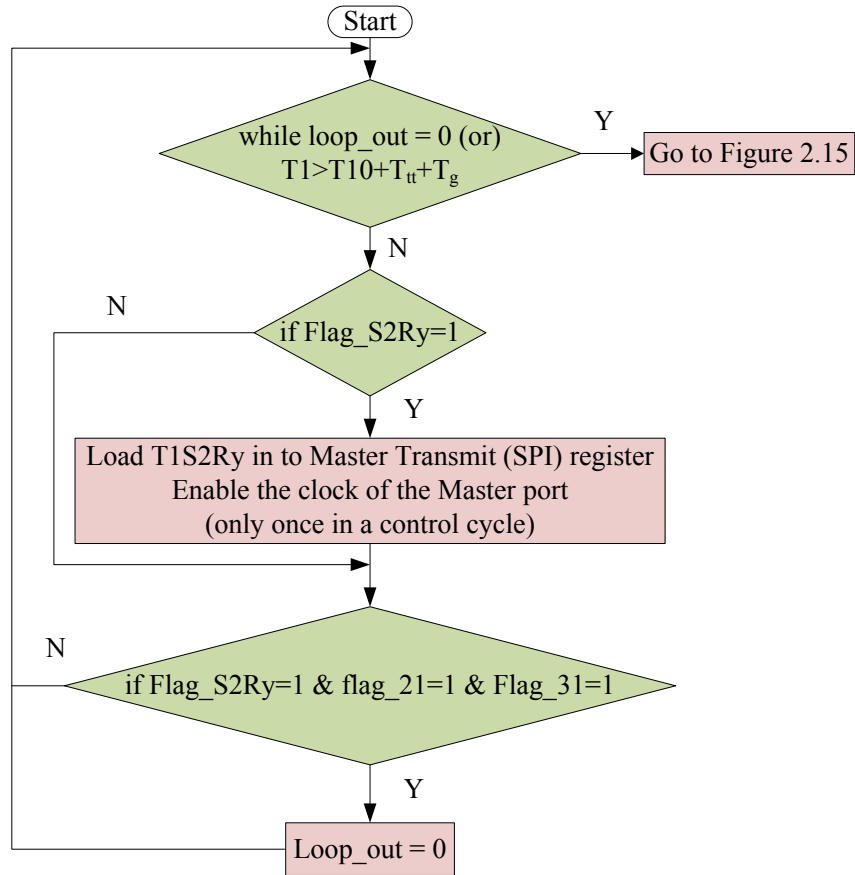


Figure 2.12: Synchronous window loop

- 4) At t_6 , as DSP3 is the master for DSP1 and DSP1 is ready since t_4 with its slave transmit register (McBSP) loaded with T10 and the feedback variables, DSP3 will also initiate the data transmission between DSP3 and DSP1. In this communication, T10 and the feedback variables of DSP1 are transmitted from DSP1 to DSP3 and T3S1Ry and the feedback variables of DSP3 are transmitted from DSP3 to DSP1.
- 5) Under the condition, that all slaves set their “Slave Ready Signals” not later than the synchronization window of their dedicated master ends, the data exchanges between all the DSP’s are finished at t_7 . Then all the DSP’s have the timer values from their neighbors. So it is possible to calculate the time difference between any DSP. For e.g. DSP1 finds T1S2Ry in its capture register, T10 was saved in 1), T20 was received in 2) and T3S1Ry was received in 4). Using this values, DSP1 calculates $D21 = T20 - T1S2Ry$ and $D31 = T3S1Ry - T10$. After calculating the timer difference, the slowest DSP timer counter value is updated to next faster and the fastest DSP timer counter values are updated to the next slower one. This means the timer counter values of the fastest and slowest DSPs are updated to the medium slower/ medium

faster DSP timer counter. If the timer difference is high then the update is done in steps instead of in one step. A detailed algorithm for the timer synchronization under no fault condition is shown in Figure 2.14. Figure 2.13 shows the six possible cases where the timer of DSP1 deviates from timers of DSP2 and DSP3. In Figure 2.13, T1, T2 and T3 are the timer values of DSP1, DSP2 and DSP3 respectively. In the case (a) and case (d), the time counter values of DSP1 are updated to T2 and in the case (b) and case (c) to T3. In the case of case (e) and case (f), the timer values of DSP1 are not modified.

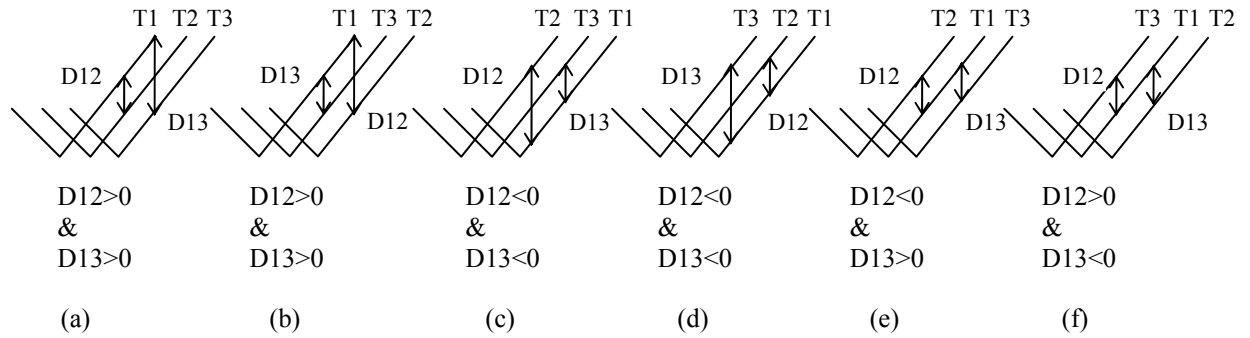


Figure 2.13: Possible combinations of DSP 1 timer deviation with respect to DSP2 and DSP3 timers

- 6) In Figure 2.11, DSP1 is faster compared to the DSP2 and DSP3 is slower compared to the DSP2 timer. So DSP1 will decrease its timer counter value by $\Delta T_{21} = T20 - T1S2Ry$ and DSP3 will increase its timer counter value by $\Delta T_{23} = T2S3Ry - T30$. If the data transmission between all the DSP's is accomplished within the synchronization window then the DSPs will come out of the synchronization window loop and continue with the remaining control algorithm.
- 7) If any particular DSP is not able to receive the data from any other DSP within the synchronization window time, neither the timer values nor the feedback variables are exchanged. This situation is detected and handled by the algorithm explained in the section 2.3.2 (Fault Identification and Compensation)

2.3.1.2 Control variables synchronization

Along with the timer values, data variables are exchanged between all the processors. These data variables can be either the feedback variables (current and rotor position) or PI controller integrator values.

Figure 2.23 shows the functional block diagram of the fault tolerant digital controller based FOC implementation of PMSM. The feedback input variables (i_a , i_b and θ_e) are exchanged between all the DSPs, as indicated in Figure 2.23. Once the variables exchange is finished, they are checked for $\pm 5\%$ tolerance variation between the variables as shown in Figure 2.19. If any variable is beyond $\pm 5\%$ tolerance then that variable is ignored as shown in Figure 2.19. In Figure 2.19, V_1 , V_2 and V_3 represent any particular variable (e.g. i_a , i_b or θ_e) of DSP1, DSP2 and DSP3 respectively. They are exchanged between all processors for the control variable synchronization.

2.3.2 Fault identification and compensation

The principle of the fault detection is as follows.

Though the TMR systems works based on the principle of fault masking, in order to keep the healthy controllers in synchronism, fault identification and compensation is necessary. The fault identification is done based on the information from the exchanged variables. Based on the

information exchanged it is possible to distinguish between the different faults such as fault in the neighboring controllers or faults in the communication system. When said fault in the controller, it can be any components of the controller board such as A/D converter, interfacing electronics, processor power supply or processors itself.

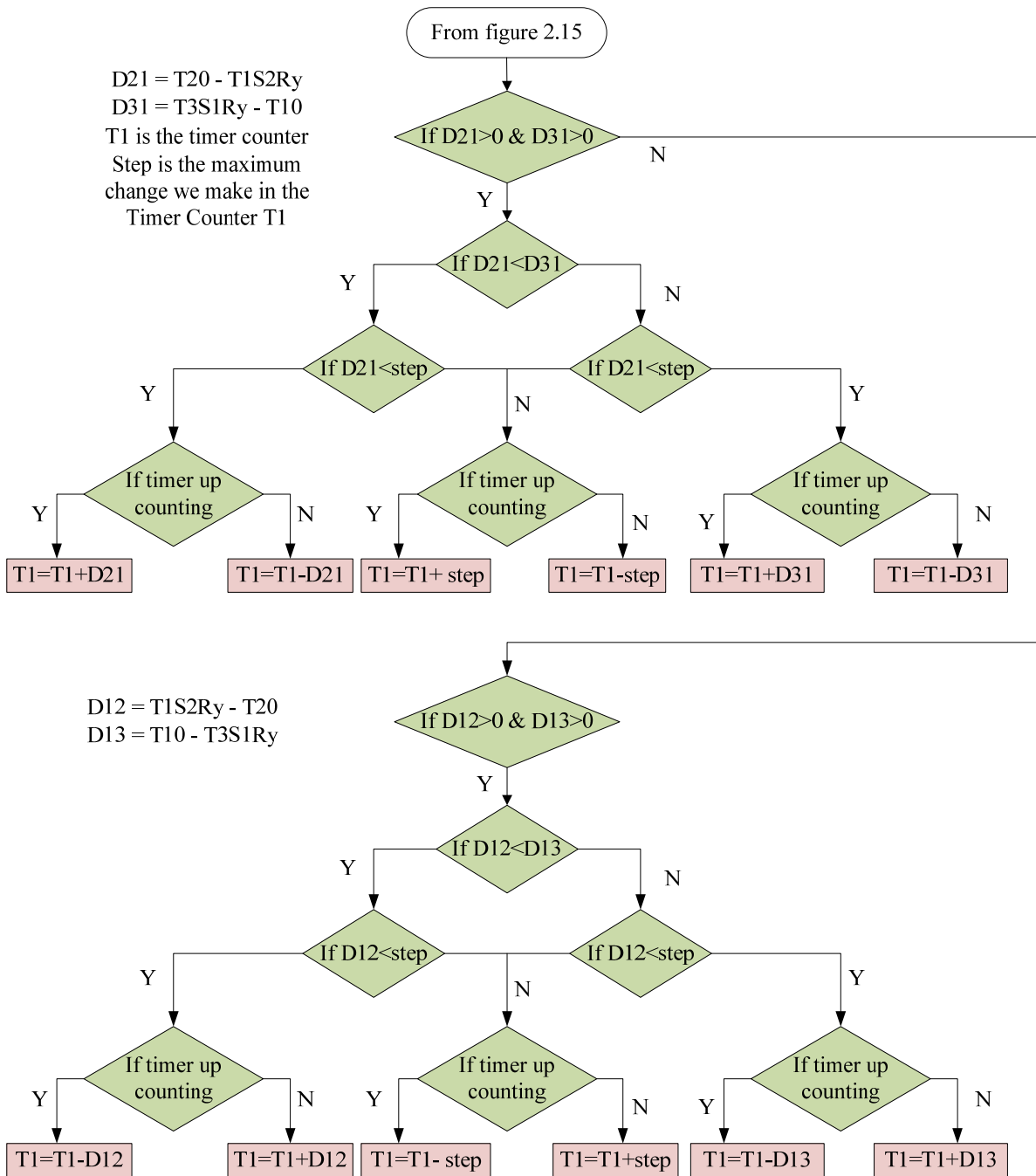


Figure 2.14: Timer synchronization in healthy case

All the inputs to the controllers are triplicated in the signal triplication board, means same inputs are fed to all the controllers. If there is no fault in any of the controller or communication system, then all the corresponding input values in all the controllers should be same. Slight variations in the input values can be expected because of the minute differences in the signal scaling and shifting circuits. After information exchange, all the variables are checked for 5% tolerance band. If any of the variables from any of the controllers is not within the 5% tolerance band, it is an

indication of fault in the system. In order to locate and localize the fault, different flags are used, which are set when the communication between any of the two controllers is successful.

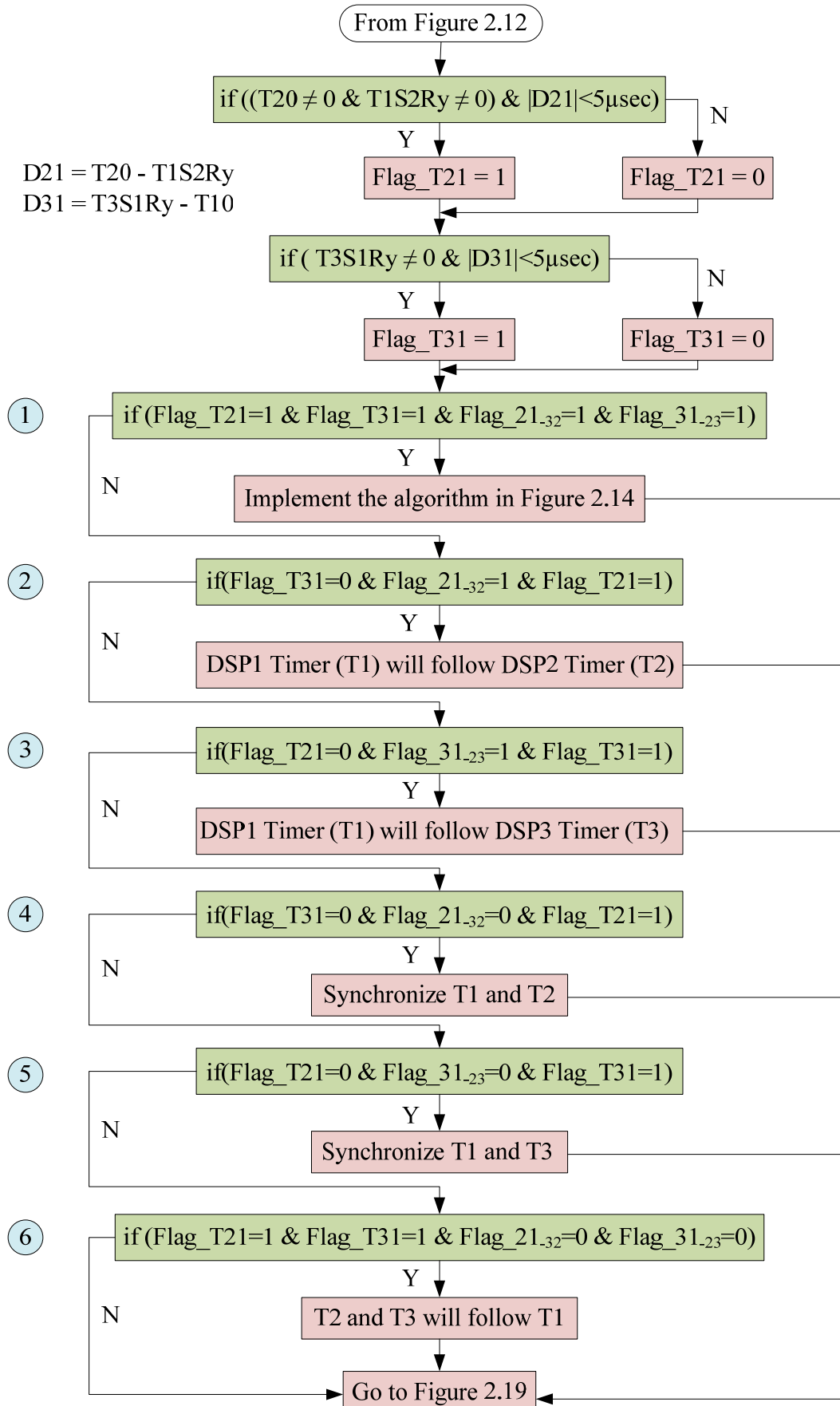


Figure 2.15: Timer synchronization in fault case

As the timer values are not the fixed inputs to the DSP, a different approach is followed to detect the fault in the controller or communication system. As explained in the section 2.3.1.1, the timer values are captured after the ADC sampling and the rotor position acquisition. So, unless there is a fault in the controller, the timer values should not have zero values. When all the controllers are healthy with proper communication between them, they are strictly synchronized with a maximum time deviation of 100 ns. So the time difference between the controllers is checked as the next condition to locate the fault in the controllers or communication system. In this work, a worst case of 5 μ s time deviation between all the controllers is considered, which is also the grace time allowed to finish the communication between all the controllers.

Figure 2.15 shows the algorithm for timer variables and Figure 2.19 shows the algorithm for data variables. In Figure 2.15, two flags are defined, which are further used to detect which DSP is having fault or going out of synchronism.

Flag_T21 is set to '1' when DSP1 and DSP2 are within the 5 μ sec band and Flag_T31 is set to '1' when DSP1 and DSP3 are within 5 μ sec band. They are set to zero, if they are not within the range of 5 μ sec. Here, 5 μ sec is the time used as grace time (t_g) in the synchronous window.

DSP1 has no information about the status of communication between DSP2 and DSP3. In order to get knowledge of status of the communication between DSP2 and DSP3, two status-flags are sent to DSP1:

Flag_21_32=1 is sent from DSP2 to DSP1, if the communication between DSP3 and DSP2 are in time synchronism.

Flag_31_23=1 is sent from DSP3 to DSP1, if the communication between DSP2 and DSP3 are in time synchronism.

At the beginning of each control cycle (100 μ s), all the flags are reset.

Additionally, DSP1 has to distinguish between two cases:

- 1) DSP2 is not in time synchronism with DSP3 (for example, communication between DSP2 and DSP3 is failed)
- 2) DSP2 is not in time synchronism with DSP1 and DSP3 (for example, DSP2 is having a complete breakdown)

In case 1), DSP2 sends to its master DSP1 the status flags Flag_21_32= 0 and DSP3 sends to DSP1 the status flags Flag_31_23= 0, whereas in case 2) DSP3 sends to DSP1 the status flag Flag_31_23= 0 and Flag_T21 remain reset in DSP1.

Any failure in the Slave Ready Signals (SRS1...SRS3) ultimately leads to a failure in communication, as any master will initiate its communication only if it receives a slave ready signal from its slave. So a failure in the slave ready signal is finally dealt as a failure in the communication. Different steps in Figure 2.15 are elaborated here as per the sequence highlighted in Figure.

- 1) This is the healthy case where all the three DSPs are in time synchronism. Then in this case, the algorithm shown in Figure 2.14 is used for the synchronization where the fastest and slowest DSP timers are updated to the medium faster/slower DSP timer.
- 2) This is the case where there is a communication failure between DSP1 and DSP3. This case can be better understood from Figure 2.16. In Figure 2.16 it is assumed that communication between DSP1 and DSP3 is failed. Variables in bold font indicate that they are within the tolerance band and Flag_21_32 = 1 tells that DSP2 and DSP3 are in synchronism or the communication between

DSP2 and DSP3 is good. In this case as DSP1 and DSP3 have only information from DSP2, DSP1 and DSP3 timers will follow DSP2 timer.

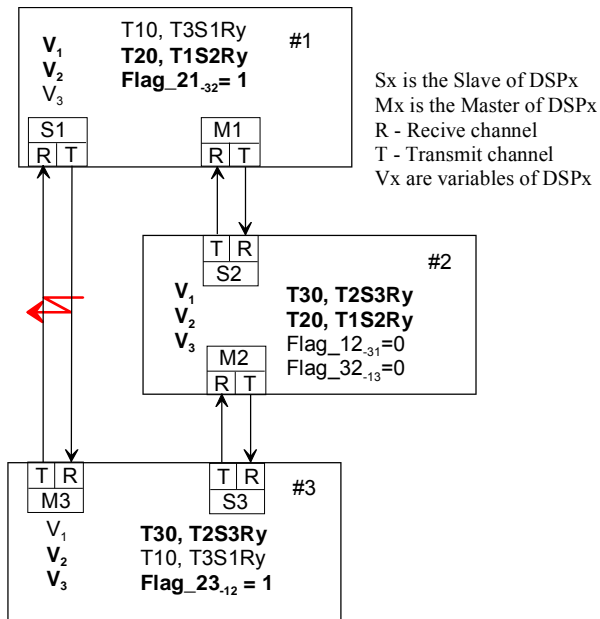


Figure 2.16: A case assuming communication between DSP1 and DSP3 is failed

3) This is the case where there is a communication failure between DSP1 and DSP2, which is similar to case 2). In this case, DSP1 and DSP2 timers will follow DSP3 timer.

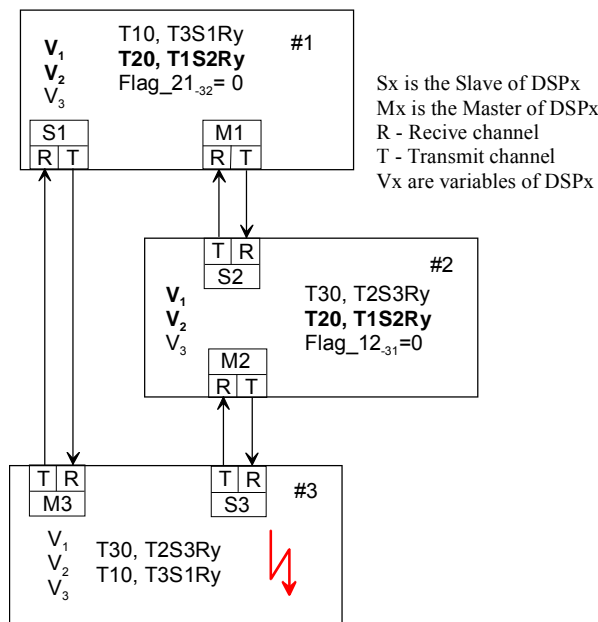


Figure 2.17: A case assuming DSP3 is failed

4) This is a case where the DSP3 communication is failed or DSP3 is not in synchronism with DSP1 and DSP2. In Figure 2.17, it is assumed that DSP3 is completely failed. Again here variables in the bold font indicate that they are in synchronism. In this case, we synchronize DSP1 and DSP2 timers in such a way that the slower DSP timer among the two is updated to the faster DSP timer.

5) This is a case where the DSP2 communication is failed or DSP2 is not in synchronism with DSP1 and DSP3, which is also similar to case 4). In this case, we synchronize DSP1 and DSP3

timers in such a way that the slower DSP timer among the two is updated to the faster DSP timer.

- 6) This is the case where the communication between DSP2 and DSP3 are failed or DSP2 and DSP3 are not in synchronism. In Figure 2.18, it is assumed that the communication between DSP2 and DSP3 is completely failed. In this case, only DSP1 contains all the information from DSP2 and DSP3, so DSP1 will not update its timer because DSP2 and DSP3 timers will follow DSP1 timer.

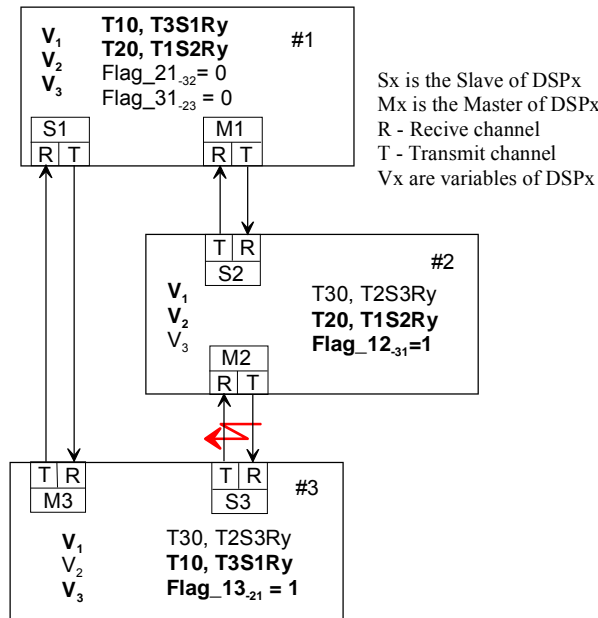


Figure 2.18: A case assuming communication between DSP2 and DSP3 is failed

Figure 2.19 shows variable synchronization under different fault conditions. The algorithm is shown for DSP1 for one variable and a similar algorithm is used for DSP2 and DSP3.

A brief description of the algorithm is provided below.

- 1) In case 1, the data exchanged between all the processors are within the 5% tolerance band. So we select median values of the variables V_1 , V_2 and V_3 .
- 2) In case 2, variable V_1 is not in the 5% tolerance band of V_2 and V_3 . So, here we select the average of V_2 and V_3 . Case 3 and case 4 are similar to case 2, where the variables V_2 and V_3 are not good. A similar approach is followed as in case 2.
- 3) In case 5, DSP2 is not communicating in time with DSP1 and DSP3. $Flag_{21} = 0$ says that communication between DSP2 and DSP1 is not in time and $Flag_{31-23} = 0$ says that the communication between DSP2 and DSP3 is not in time. In this case, we take the average of variables V_1 and V_3 . In this case, DSP2 is left out of service. Case 6 is similar to case 5, where DSP3 is not communicating in time with DSP1 and DSP2.
- 4) In case 7, the communication between DSP1 and DSP3 is not in time ($Flag_{31} = 0$), but communication between DSP1, DSP2 and DSP2, DSP3 is in time ($Flag_{21} = 1$ and $Flag_{21-32} = 1$). In this particular case if we look at the variables in three DSPs, DSP1 is having V_1 and V_2 , DSP2 is having V_1 , V_2 and V_3 and DSP3 is having V_2 and V_3 . The only common variables in all the three DSPs are V_2 , so variables V_2 are used in all the three DSPs. Case 8 is similar to case 7, where the communication between DSP1 and DSP2 is not in time. In this case, a similar approach is followed as explained before.

5) In case 9, the communication between DSP2 and DSP3 is not in time ($Flag_{21-32} = Flag_{31-23} = 0$) and communication between DSP1, DSP2 and DSP1 and DSP3 are in time ($Flag_{21} = Flag_{31} = 1$). In this case as explained before, DSP2 and DSP3 will use DSP1 variables, so DSP1 uses its own variables for the control. In case 10, DSP1 is not able to communicate with DSP2 and DSP3. In this case, it will do nothing but suspend its entire control program and set low all the PWM signals.

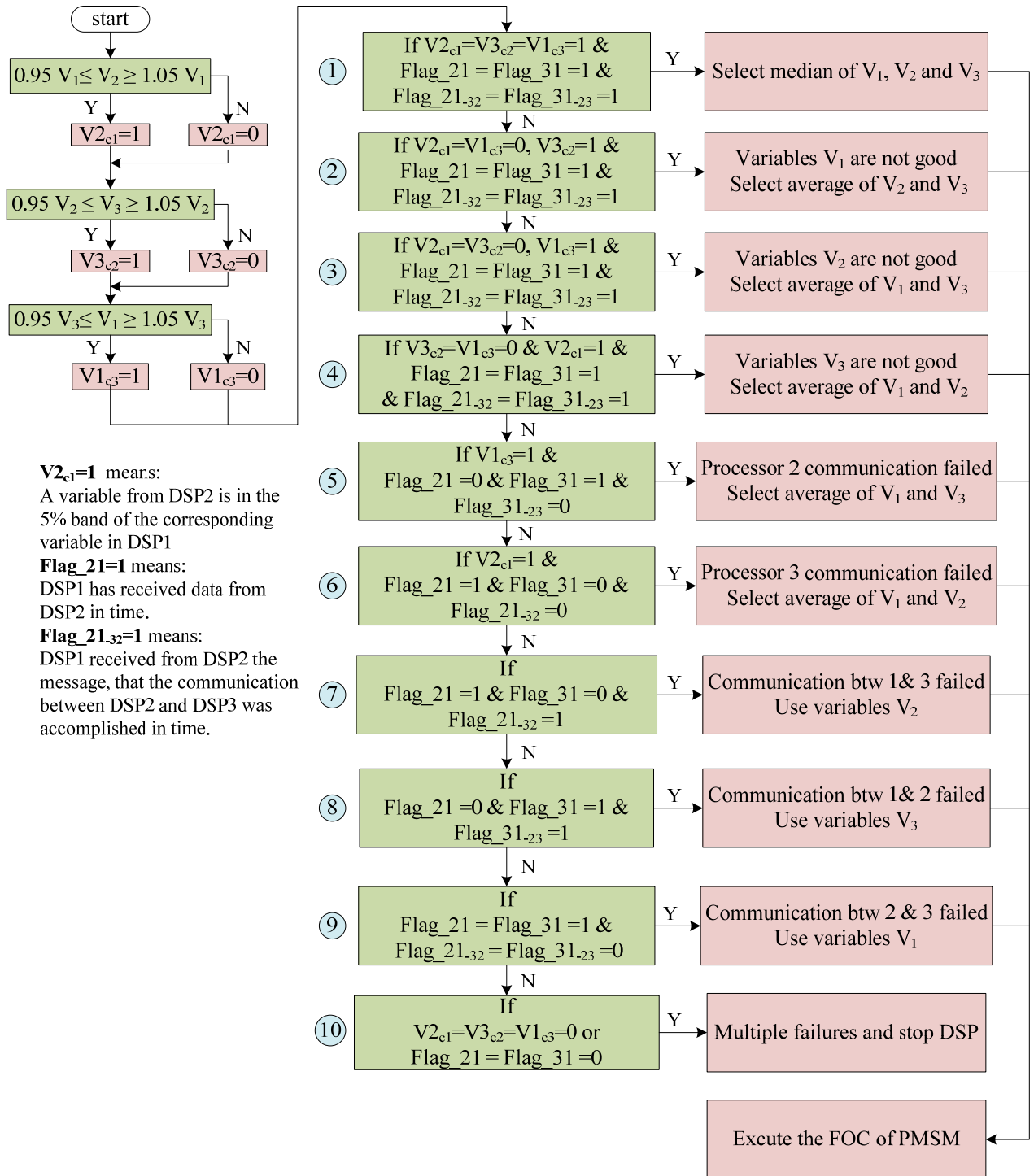


Figure 2.19: Variable synchronization in fault case

2.3.3 Fault tolerant majority voter

The voter is in series with the redundant modules, if it fails, the whole system fails. The availability of the voter must be very high in order to keep the overall availability of the TMR higher than the availability of the simplex system. The high availability of the TMR system is based on replacing a faulted part (e.g. DSP) without disturbing the operation of the other parts (e.g. DSPs). Any failure in the voter is regarded as a single point of failure and is considered as whole system failure. Figure 2.20 shows a simple fault-tolerant majority voter with transistors for a binary signal, e.g. one gate signal for one IGBT [WEN82] and Table 2.2 shows the corresponding truth table. The voter circuit has three PWM inputs A, B, C from the three processors and D is the PWM output to the inverter. The voter circuit further includes a resistive network (R1, R2) connected between output and ground. Two resistances are connected in parallel in order to provide the fault tolerance to the resistive network.

The operation of the voter circuit is as follows: When at least two input terminals are at logic high, then five volts will appear across the resistive network and output D is at logic high. When, at least two input terminals are at logic low, then no current flows through the transistors and $R_1 || R_2$. Thus the output is at ground potential. Even a single short circuit or single open circuit failure in one of the transistors or any fault in corresponding power supplies will not affect the voter operation. The voter can tolerate up to two transistor faults in different legs. Fault on the two transistors of the same leg is not considered here. But without additional measures, fault localization and on-line replacement or repair is not possible with the simple circuit of Figure 2.20.

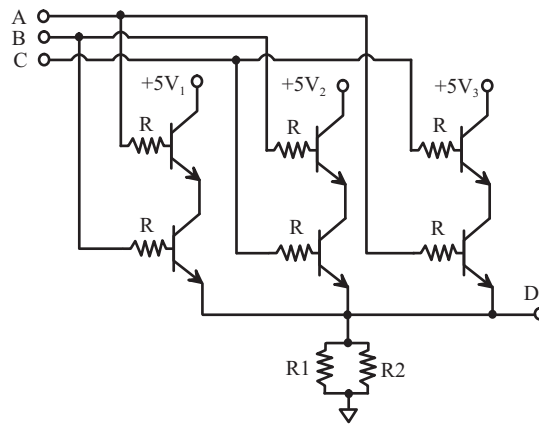


Figure 2.20: Fault tolerant majority voter (Source: [WEN82])

Table 2.2: Truth table of majority voting logic

A	B	C	D
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

2.4 Experimental setup description

A schematic diagram of the experimental setup is shown in Figure 2.21. It consists of three TMS320F2812 DSPs based evolution boards powered with single +5V power supply, transistor based majority voter board and signal triplication board, an IPM based 2-level voltage source inverter (VSI) and a PMSM. The 2-level VSI is of course not fault tolerant, but in Chapter 3, a VSI with one redundant leg will be investigated. All the feedback signals are fed to the signal triplication board. In the signal triplication board, all the signals are triplicated and further fed to interfacing boards of all the DSPs. The feedback signals shifting and gain adjustment is done on the ADC and Encoder interfacing board. In the ADC interfacing board current sensor's signals are further processed using the gain and shifting circuits. Position encoder connected to machine delivers sine/cosine signals. They are converted to rectangular signals in the encoder interfacing board which are then fed to the Quadrature-Encoder Pulse (QEP) unit of the DSP. All the signal transmission (serial communication and PWM signals) in the setup is done by using differential transmission (double ended signals). The single DSP power supply (+5V) is further used to supply all the corresponding ICs related to its interfacing board and differential signal ICs. Also the differential receivers of the PWM signals on the voter board is powered with their respective DSP power supplies (3.3V1, 3.3V2 and 3.3V3 in Figure 2.21) in order to avoid a common point of failure. FOC of PMSM is implemented in order to validate the proposed digital controller with increased availability. Figure 2.22 shows the experimental setup with three DSP boards, voter board, an IPM based 3-phase 2-level voltage source inverter and the PMSM with load machine. The load machine is also a PMSM and the stator terminals of the load machine are connected to a resistive load which provides the necessary load torque. The Voter and signal triplication board is sandwiched between DSP boards and inverter board. Figure 2.23 shows the functional block diagram of implementation of digital controller with increased availability for PMSM. In Figure 2.23, the details about the inter processor communication, timer and input variable synchronization, FOC implementation and PWM voting is clearly indicated. The output signals of the position encoder ($\sin\theta$, $\cos\theta$ and R) are fed to encoder interfacing board. In the interfacing board encoder signals are converted to rectangular pulses (QEP1, QEP2 and R) and are fed to Quadrature-Encoder Pulse unit of the DSP which will finally convert these signals in to position information of the rotor. The outputs of the current sensors are fed to the ADC of the DSP. With this all the necessary feedback variables information is available which are further fed to synchronization block. In this block all the tasks related to timer and feedback variable synchronization (section 2.3.1), fault detection and compensation (section 2.3.2) are implemented. The outputs of the synchronization block are synchronized feedback variables which, in healthy case, are same in all the three DSPs. These synchronized variables are used to implement the FOC of PMSM. If synchronized variables are used to implement the FOC and with PWM timers of all the DSPs are strictly synchronized then all the DSPs produce the same PWM output.

For a fault-tolerant system, on-line replacement of a faulted component (e.g. DSP) without disturbing the healthy components (DSPs) is mandatory. After such a replacement, the state variables (integrators) in the control algorithm of the new (replaced) DSP must be set to the average of the corresponding state variables in the two healthy DSPs. For this reason, it makes sense to synchronize the state variables in the control algorithm of all DSPs during the whole operation time. As the on-line replacement of a DSP was not experimentally investigated in this thesis, for convenience only the input variables have been synchronized, as can be seen in Figure 2.23.

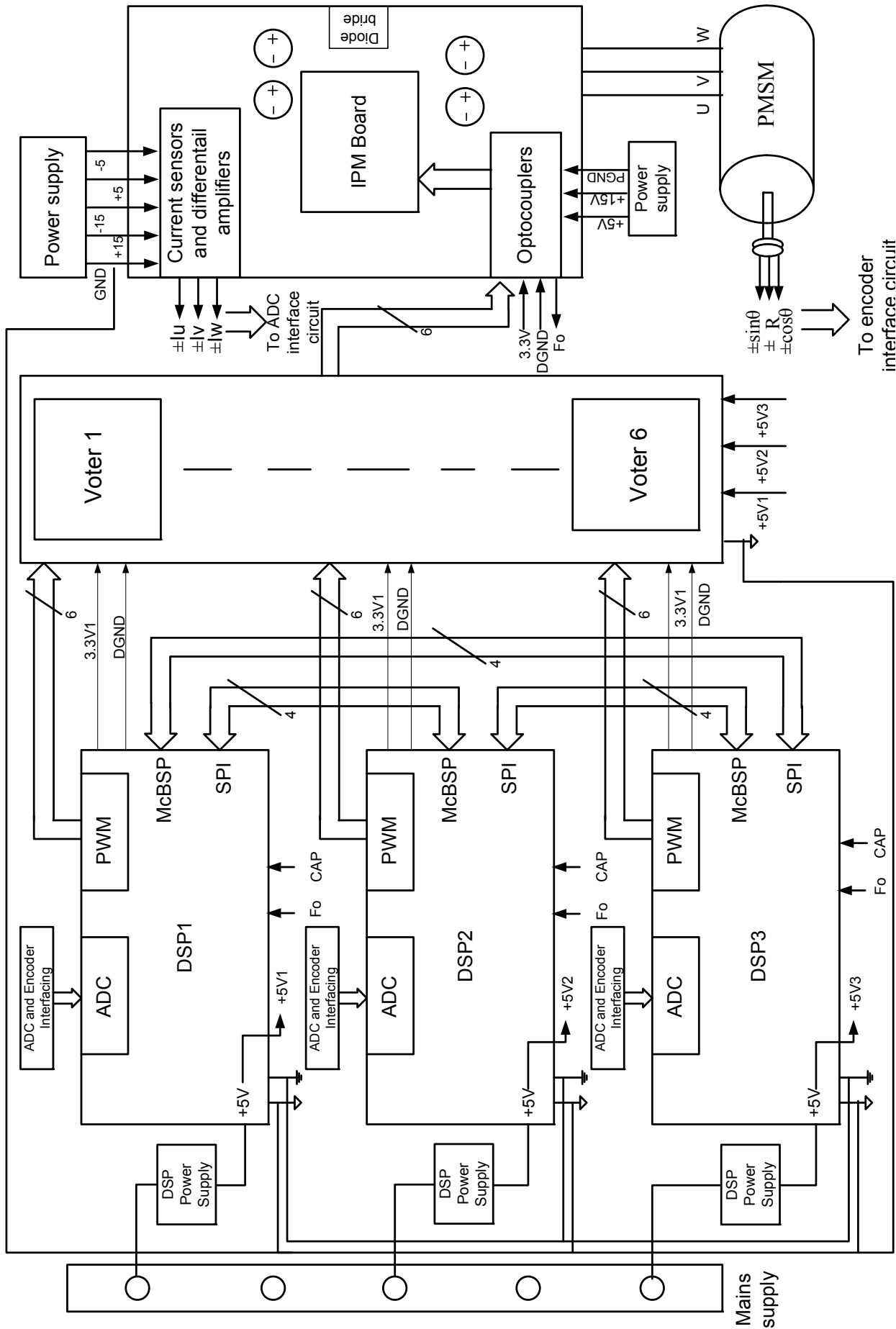


Figure 2.21: Schematic diagram of experimental setup

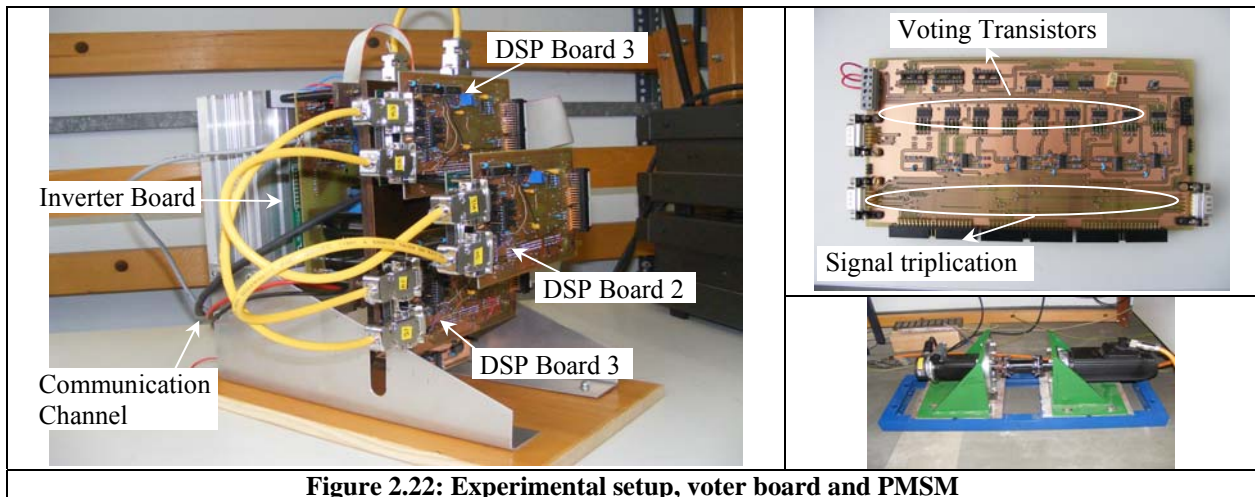


Figure 2.22: Experimental setup, voter board and PMSM

2.5 Experimental results

Figure 2.24 to Figure 2.26 show the different responses of three DSPs for a step change in speed reference when they are under no fault in any of the DSPs. Figure 2.24 is the speed response to a step change in the speed reference. Figure 2.25 is the q-axis current and its reference current which is output from speed controller. Figure 2.26 is the d-current response. Figure 2.24 to Figure 2.26 shows that there is strict synchronization in terms of time and variables so is the reason that the responses in three DSPs are exactly same. Physically, there exists of course just one speed. The three signals in Figure 2.24 are the internal measurement values in the three DSPs after synchronization. The experimental setup is tested for different fault conditions like complete failure of one of the processors or a failure in communication between any two processors or a failure in slave ready signal. In all the cases the PMSM is running as the control system was in healthy condition. Although in this work it is not implemented, the health status of all the controllers can be reported to the operator through CAN communication or simply by turning ON some LEDs such that failed component or controller can be repaired or replaced. Figure 2.27 to Figure 2.29 are the different responses when DSP2 is completely failed (in this case DSP2 is powered OFF). Figure 2.27 is the speed response in DSP1 and DSP3 for a step change in speed reference. Similarly, Figure 2.28 is the q-axis current and q-axis current reference and Figure 2.29 is the d-axis current response. From Figure 2.27 to Figure 2.29 it can be observed that even in the fault case there is no significant difference in the motor response. Figure 2.26 is the case when all the three DSPs are healthy, whereas in Figure 2.29 DSP1 is completely turned off. As in a fault case synchronism is maintained, the machine responses looks almost identical in both cases.

2.6 Conclusions

In this chapter, first, comparison, advantages and disadvantages of selected digital controllers with redundancy are presented. MTTF calculations for different cases of duplex and TMR systems are shown. From the results of MTTF calculations, it is clear that only TMR systems are better suitable for fault-tolerant applications where a system should have an availability of 24h at each day. So, a TMR based controller is selected to improve the availability of the PMSM drive. A single fault-tolerant majority voter is also introduced next, which is used along with the TMR based controllers. Suitable synchronization, fault detection and compensation algorithms are developed

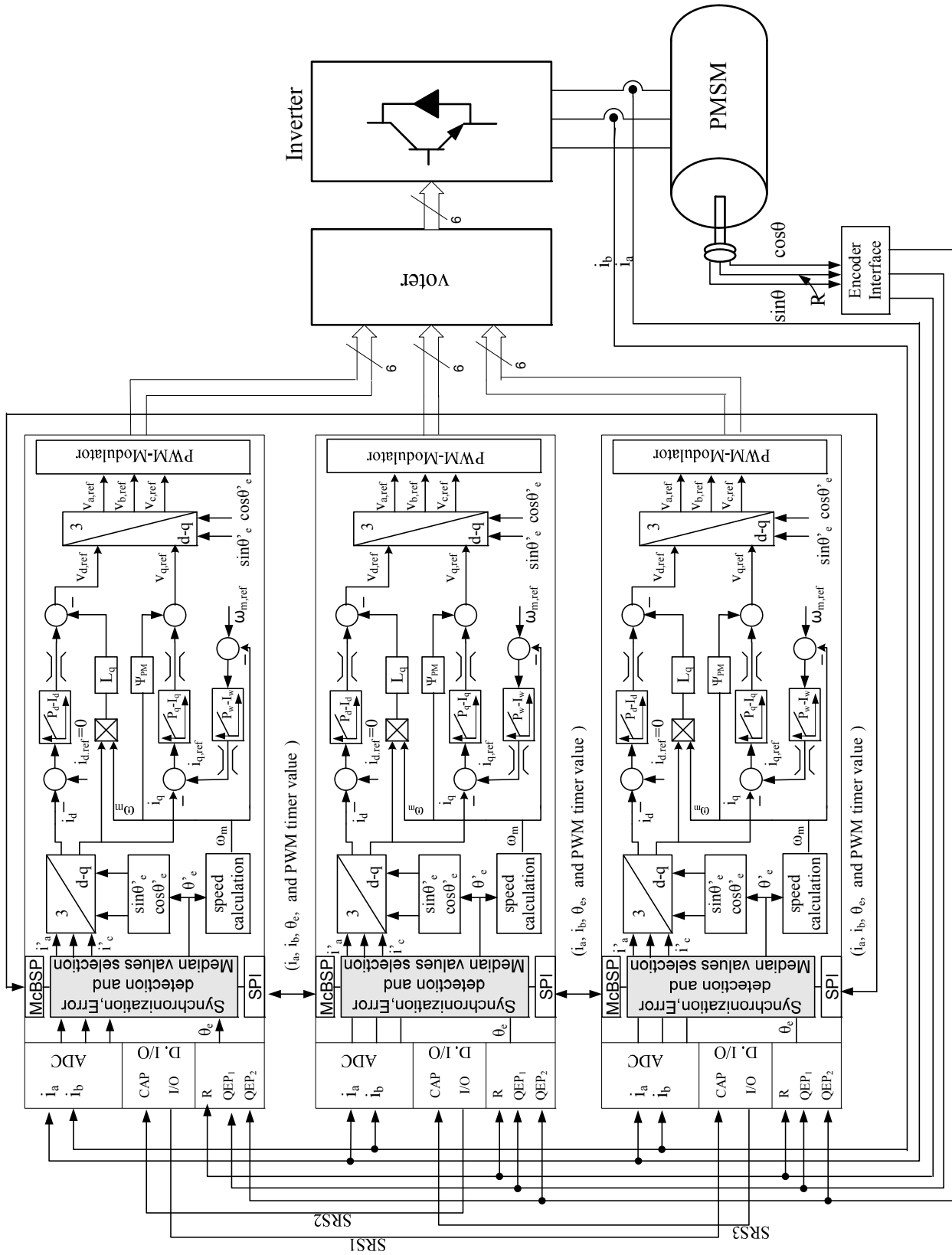


Figure 2.23: Functional block diagram for the FOC implementation of PMSM with fault tolerant digital controller

such that the remaining two controllers remain in synchronism, even if there is a fault in one of the controllers. FOC of PMSM is implemented in order to test the validity of proposed system with improved availability. System is tested for different faults on the controllers and results for the case of complete DSP failure are shown. In all the fault cases, a bump less control of the drive is observed without any disturbance to the drive operation.

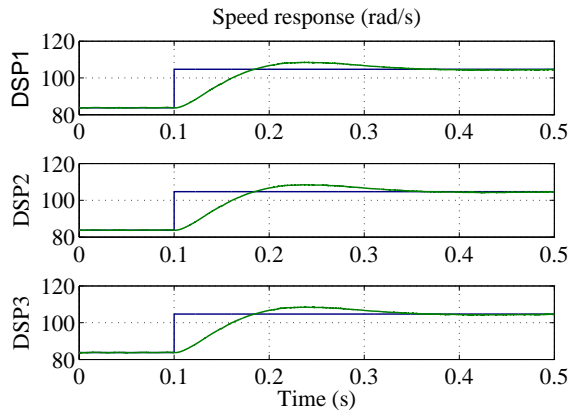


Figure 2.24: Speed response with three DSPs

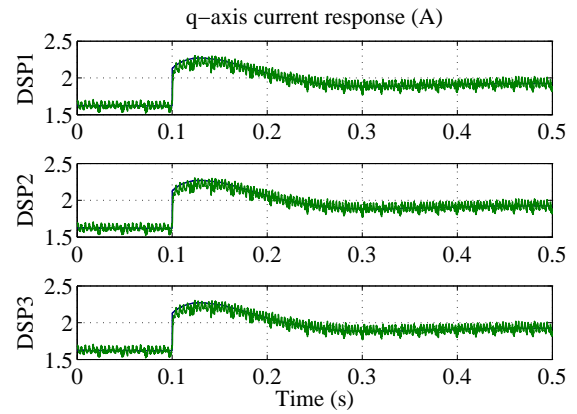


Figure 2.25: Q-axis current and q-axis current reference response with three DSPs

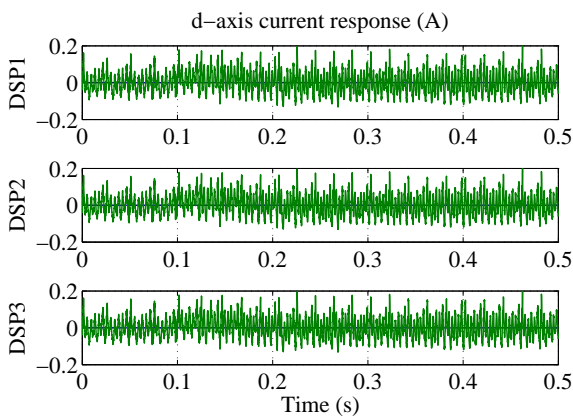


Figure 2.26: D-axis current response with three DSPs

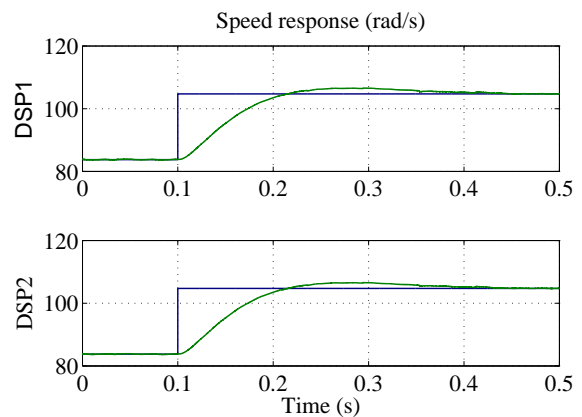


Figure 2.27: Speed response with two DSPs

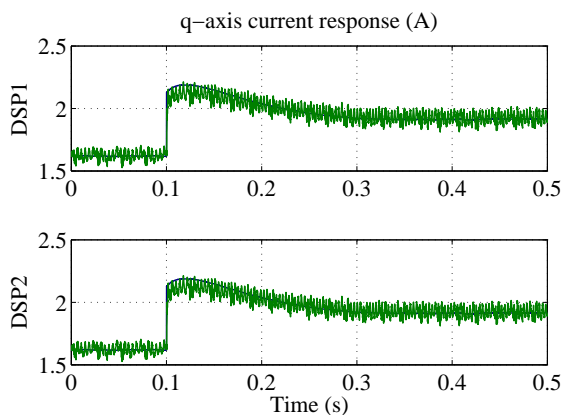


Figure 2.28: Q-axis current and q-axis current reference response with two DSPs

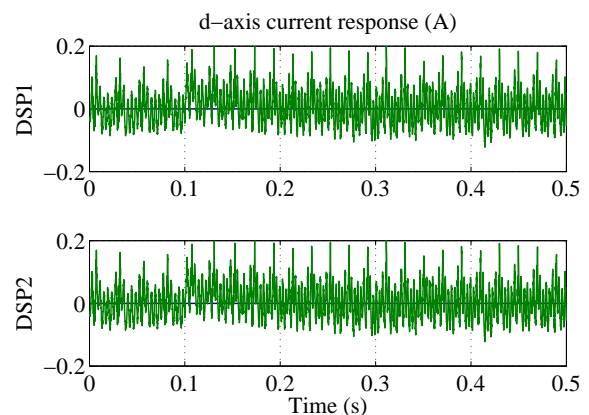


Figure 2.29: D-axis current response with two DSPs

3 Power Converter with Increased Availability

3.1 Introduction

The power converter is an integral part of an electric drive. Different types of power converters are used for drives. Voltage source inverters such as, two-level, multilevel (three level and above), H-bridge and matrix converters are some of the possibilities to feed a variable speed AC drive. A typical two-level converter driving an AC motor is shown in Figure 3.1. It mainly consists of a DC-link capacitor, six IGBTs with anti-parallel diodes and their corresponding IGBT drivers (not shown in Figure). Different faults in the inverter that can affect the drive performance are IGBT short circuit, IGBT open circuit, phase leg short circuit, phase leg open circuit, and DC-link capacitor short or open circuit.

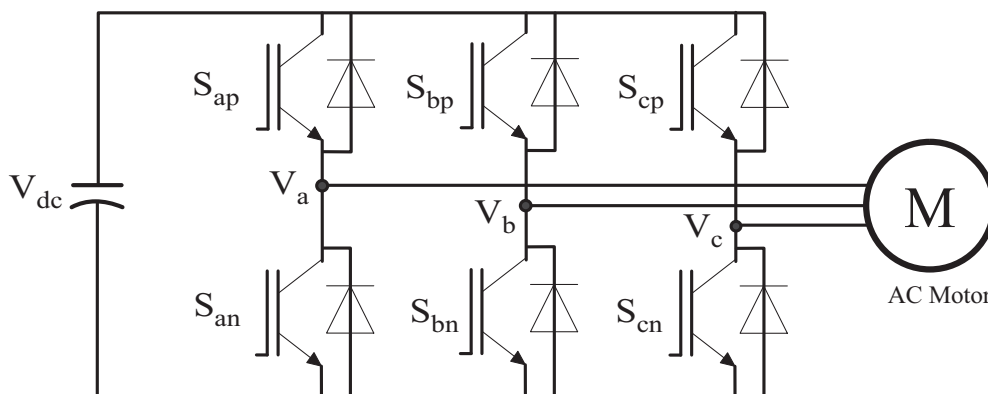


Figure 3.1: Standard three-phase 2-level inverter

As mentioned in chapter 1.2, due to high costs of class AEC-4 “Fault Tolerant” converters, also converters at class AEC-3 “Fault Resilient” are interesting solutions here.

Many of the inverter topologies in the literature suffer from a reduced power output in the post-fault operation. In a rigorous sense, they are neither fault-tolerant nor fault resilient. However, they are included here in the discussion, as in some applications reduced power may be accepted. Several topologies which aim to increase the availability are discussed in the literature [WEL04]. Some of them reconfigure the standard inverter topology and reformulate the current references so that the rotating MMF generated by the armature currents in the machine do not change, even if one phase is open circuited after fault occurrence. For proper operation with some topology, the neutral point of the motor or faulted phase of the machine (after isolating the fault leg) has to be connected to the midpoint of the DC-link, which is created by using the two capacitors [LIU93], see Figure 3.5. In this configuration, the inverter should be overrated to produce the rated torque output. A valid alternative that does not require the availability of the DC-link midpoint is proposed in [BOL00] (see Figure 3.7), at the cost of using additional components. This topology uses auxiliary capacitors and fast acting semiconductor fuses to isolate the faulted leg. The rating and size of the capacitors increases with the rating of the inverter. The presence of fuses increases the cost of the inverter and also DC-bus parasitic inductance. A simplified version of [BOL00] has been developed by [RIB01a], where only fast acting semiconductor fuses (connected between upper and lower IGBT) are used to isolate the fault leg. In case of an IGBT short, complementary IGBT is turned ON in order to blow the fuses connected in series with leg. But these fuses should have low i^2t rating

compared to the IGBTs and such fuses are very expensive. In this case also, the inverter should be overrated in order to avoid blowing the fuses for any over current. In some cases, it is also possible that only one of the fuses is blown and the faulted IGBT is still connected to the phase of the machine. An alternative configuration which increases the availability of the motor drive is developed in [QIN97, KRA99], where the three phases of the motor are fed by independent single phase converters, see Figure 3.10. In case of a fault in one converter or machine phase, the remaining devices can continue to operate. A reduction of the torque in case of a fault in one phase of the drive can be compensated by overrating the phases. A modular parallel redundant system has been proposed in [ERT02], where two complete sets of inverters and their control are arranged on a common shaft and all the motor phases are driven by independent single phase inverters. A fault in any set of the drive reduces the output power to 50%. An inverter topology which increases the availability similar to [BOL00] has been proposed in [RIC07] but using the back-to-back connected IGBTs for isolating the faulted leg, see Figure 3.8. These IGBTs increases the cost of the inverter and also the losses in the inverter are increased due to on-state resistance of the isolating devices. The redundant leg of this topology is connected to neutral point of the motor which means this topology necessitates the availability of neutral point in the machine, and also it cannot provide full rated output unless the inverter is overrated. The post fault control scheme is not the same as the pre-fault control scheme and is based on two-phase motor control. A topology similar to [BOL00] is proposed in [NAI10]. Electromechanical relays are used to isolate the faulted leg and connect the redundant leg. Post fault performance of this inverter is same as pre-fault but electromechanical relays have considerable amount of delay in opening or closing and by this time the motor may come to stop or in some cases may rotate in the reverse direction.

This work proposes some relevant modifications to the existing topologies such that there is no compromise between the cost and performance of the inverter (see Figure 3.13). Back-to-back connected thyristors are used in place of electromechanical relays used in [NAI10]. Adequate control measures are taken to bring the machine post fault current to zero in case of IGBT short circuit.

The next section of this chapter compares the different converter topologies available in the literature which increases the availability of the drive and discusses the advantages and disadvantages of each topology. A new topology is presented with few modifications to existing topologies available in the literature.

Different faults considered in comparison of converter topologies with increased availability are:

1. Switch short circuit
2. Switch open circuit
3. phase leg short circuit
4. single phase open circuit
5. DC-link capacitor short

In order to quantify the costs associated with each of the topologies studied and proposed, the output capacity and rating requirements of each topology is compared to a standard three-phase 2-level inverter [WEL04]. To quantify the post fault output capacity of each of the topology presented, a fault power rating factor (FPRF) is defined as,

$$FPRF = \frac{\text{Maximum kVA post fault output}}{\text{Maximum kVA output of standard unfaulted inverter}}$$

In order to compare the costs associated with extra silicon, semiconductor fuses and capacitors in the converter topologies, a silicon overrating & cost factor (SOCF) is defined as,

$$SOCF = \frac{\text{Cost of the all the devices in the converter with increased availability}}{\text{cost of the all the devices in standard inverter}}$$

By definition, the standard inverter would have SOCF of 1.0, meaning that it does not have any additional components. For this definition, it assumed that each switch can at least block the DC-link voltage of 1 pu and will carry a peak rated current of 1 pu. The cost of the device is assumed to be proportional to the kVA rating of the device. Now-a-days in low power and medium power standard inverters, IGBTs or MOSFETs are used as switching devices. In the converter topologies presented in next section, SCR and TRIAC (or back-to-back connected SCRs) are used to provide the necessary fault tolerance. Considering the cost of these SCRs, TRIACs, fast acting semiconductor fuses and capacitors, the factor used in SOCF comparison of these components, when compared with IGBT or MOSFET is assumed as below [WEL04],

- 1 SCR = 0.5 IGBT
- 1 TRIAC/back-to-back connected thyristor = 1.0 IGBT
- 1 Fuse = 0.5 IGBT
- 1 Capacitor = 0.5 IGBT

The rated fundamental peak voltage output of the standard inverter without over modulation is 0.577 pu (with the DC-link voltage as the base voltage) using space vector modulation (SVM) and rated peak phase current of 1 pu as shown in Figure 3.2. These parameters are used to compare the post-fault output of fault-tolerant inverter with standard un-faulted inverter.

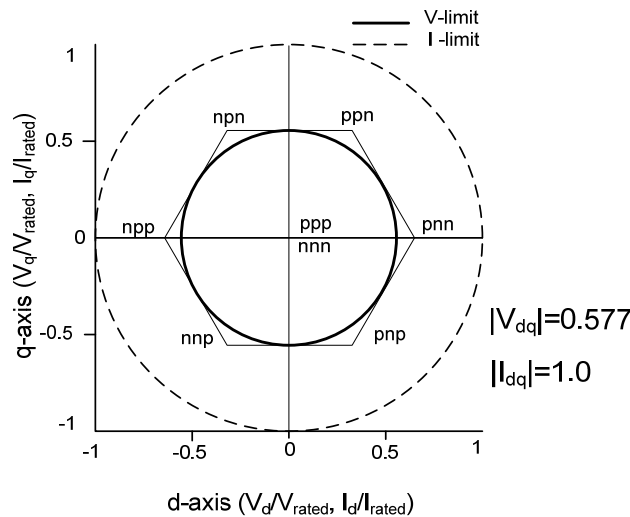


Figure 3.2: Phase fundamental voltage and current limit of a two-level three-phase inverter under no fault condition.

3.2 Comparison of topologies for power converters with increased availability

3.2.1 Four leg inverter topology

The basic approach to improve the availability of converter starts from the four leg inverter topology. A strategy to improve the availability of a variable speed AC motor drive is discussed in [COR01, RIB01a]. Figure 3.3 shows the four-leg converter topology applied to an AC machine. The mid points of three legs are connected to machine terminals and the midpoint of the fourth leg is connected to the star point of the machine. So this topology necessitates the availability of star point of the machine. This topology only works for the open-circuit fault of IGBT and open phase fault of the machine. This topology accommodates up to three simultaneous IGBT open circuit faults, as far as the fault is in upper switch or lower switch of the three legs. A failure in the combination of upper and lower switches is not accepted. A failure in the fourth leg is not acceptable. In case of open phase fault, two-phase control method is used as explained in [COR01] and in case of open switch fault, the post-fault control is based on the principle of unipolar current's control method, which is explained in [WEL01].

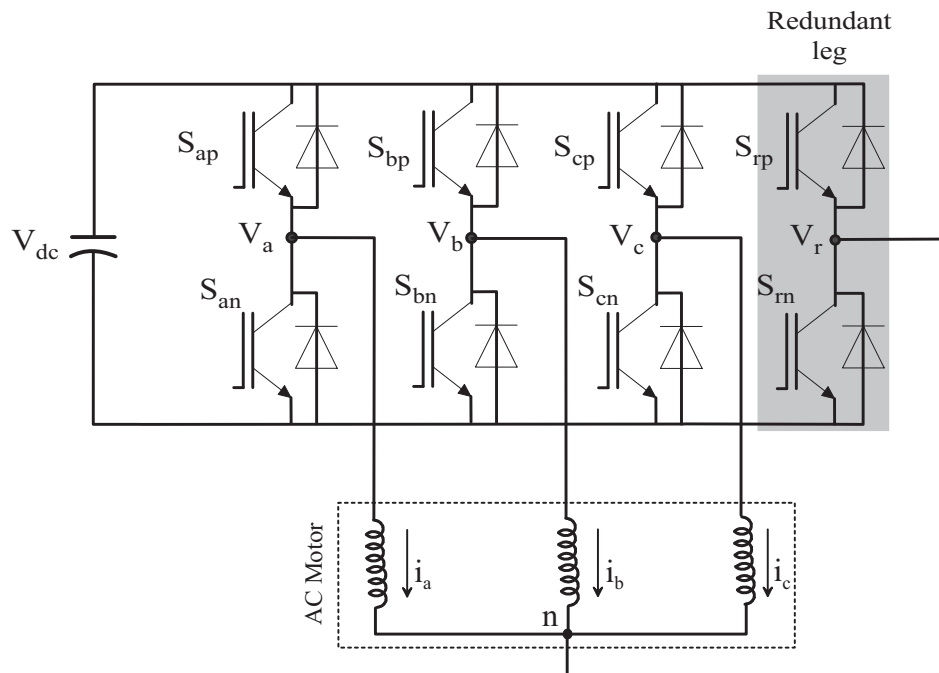


Figure 3.3: Four leg inverter topology

The unipolar current control method does not change the available voltage space, so the inverter can deliver peak fundamental voltage output, which is 0.577 pu with SVM. Due to the presence of zero sequence components in the current output, the torque producing dq currents are reduced to 0.577 pu as shown in Figure 3.4. The neutral leg, with this control scheme, carries 1.73 pu times the rated peak current. So the switching devices of neutral leg must be rated at least 1.73 times higher when compared to the switches controlling the phase currents. Considering all the extra components, the approximate SOCF of the system is 1.58 times the standard three-phase inverter.

Advantages:

- Simple in construction and control
- Silicon count is low (need only two extra IGBT's)

Disadvantages:

- Only works for switch open circuit fault and open phase fault
- Star point of the machine should be accessible
- Post fault output is only 0.58 times the rated output
- Fourth leg IGBTs must be rated at least 1.73 times the rated load current.
- Still Machine remains single point of failure in the drive system

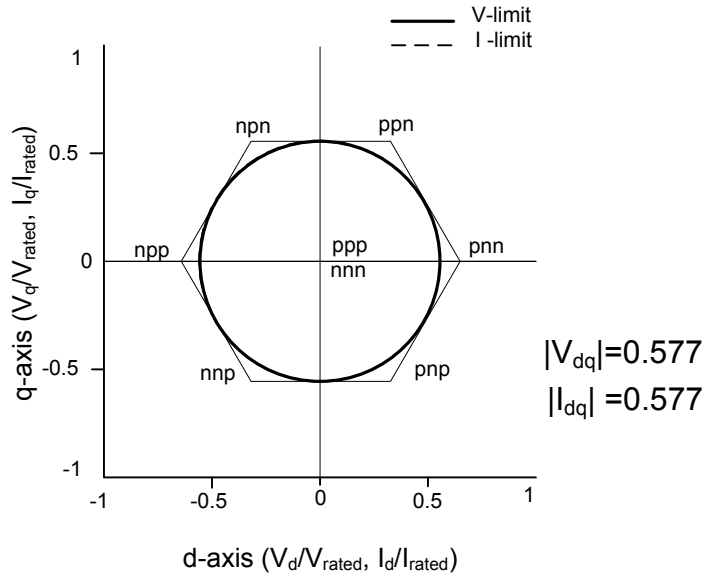


Figure 3.4: Phase fundamental voltage and current limits of four leg inverter after single switch open fault

3.2.2 Switch redundant topology

The concept of switch redundant topology was introduced in [LIU93, FU93]. Figure 3.5 shows the switch redundant topology applied to an AC machine. This topology is used for single switch open, single switch short circuit and open phase faults.

In case of a single switch short circuit fault, it is assumed that complementary IGBT is having a hardware protection to prevent the DC-bus shoot through fault. When there is a short circuit in any one of the IGBTs, then their corresponding phase TRIAC (TR_a , TR_b or TR_c) is turned ON to blow up the corresponding fuse (F_a , F_b or F_c). Once the fuse is blown up, the faulted phase is permanently connected to the midpoint of the DC bus through the corresponding TRIAC (TR_a , TR_b or TR_c). Now, the inverter structure is similar to four switch three phase inverter or B4 inverter topology as described in [VAN84]. In case of a single switch open circuit fault, same topology is applied without blowing the fuse but removing the gate pulses to the complementary IGBT. In the post fault operation, the inverter is able to impress the rated current with half the rated voltage. Under the rated conditions, the torque produced is same as before the fault but the machine runs at half the rated speed with machine entering the field weakening range.

In case of single phase open fault, the TRIAC, TR_n is turned ON to connect the star point of the machine to the midpoint of the DC bus. In order to maintain a constant flux trajectory, the phase currents of the un-faulted phase are increased in the magnitude by a factor of $\sqrt{3}$ and the phase is shifted 30° away from the faulted phase axis. As a result, the available torque producing current is reduced by a factor of $1/\sqrt{3}$, assuming a post-fault phase current of 1 pu. Since the star point of the

machine and midpoint of the DC bus are connected, the system still has the capacity to apply $\pm V_{dc}/2$ across the remaining two phases. This means, when compared to the original three-phase system, the space vector voltage capacity of the system is decreased from 0.577 pu to 0.5 pu. Due to the zero sequence currents, the TRIAC, TR_n should be rated $\sqrt{3}$ times the rated current of the machine.

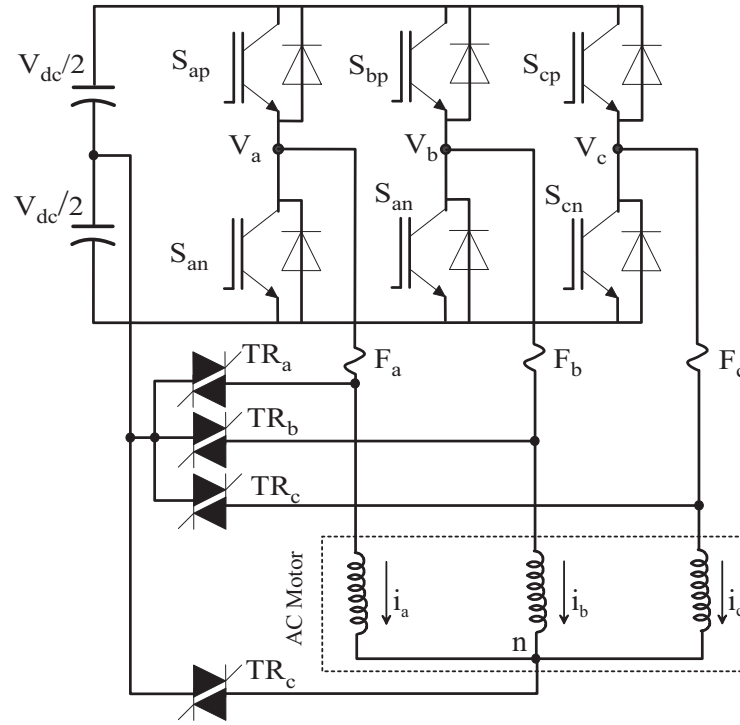


Figure 3.5: Switch redundant topology

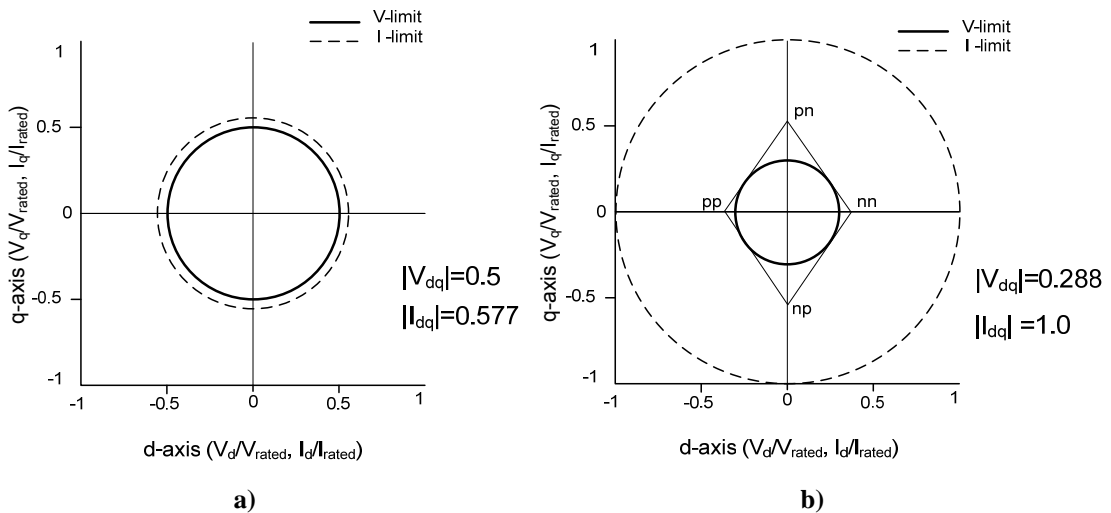


Figure 3.6: Phase fundamental voltage and current limits of switch redundant inverter after a) single phase open circuit fault, b) single switch short circuit fault

In case of open phase fault, the torque producing current is reduced by the factor of $1/\sqrt{3}$ and the space vector voltage capacity is decreased from 0.577 pu to 0.5 pu, so the overall FPRF is reduced to 0.5 times the pre-fault output rating as shown in Figure 3.6a. In case of an open switch fault or switch short fault, corresponding phase is always connected to the midpoint of the DC link through the TRIAC (TR_a , TR_b or TR_c) and the machine is controlled as a four-switch three-phase inverter or B4 topology. In this case, the inverter is capable of impressing one-half the rated phase

voltage of the standard un-faulted inverter and full rated current of the inverter as shown in Figure 3.6b. In this case also, the overall FPRF is reduced to 0.5 times the pre-fault output rating. Considering the above two cases together, this topology needs, three TRIACs (TR_a , TR_b and TR_c) with rated peak current rating, one TRIAC with 1.73 times rated peak current and three fast acting semiconductor fuses. Considering all the extra components, the approximate SOCF of the system is 2.0 times the standard three-phase inverter.

Advantages:

- Simple in construction and control
- Silicon count is low (need only four extra Triacs, three semiconductor fuses)

Disadvantages:

- Star point of the machine and midpoint of the DC-link should be accessible
- Post-fault output is only 0.5 times the rated output
- Does not work for a phase leg short circuit fault in the inverter
- Still, the machine remains single point of failure in the drive system
- DC-link capacitor failures are not addressed

3.2.3 Double switch redundant topology

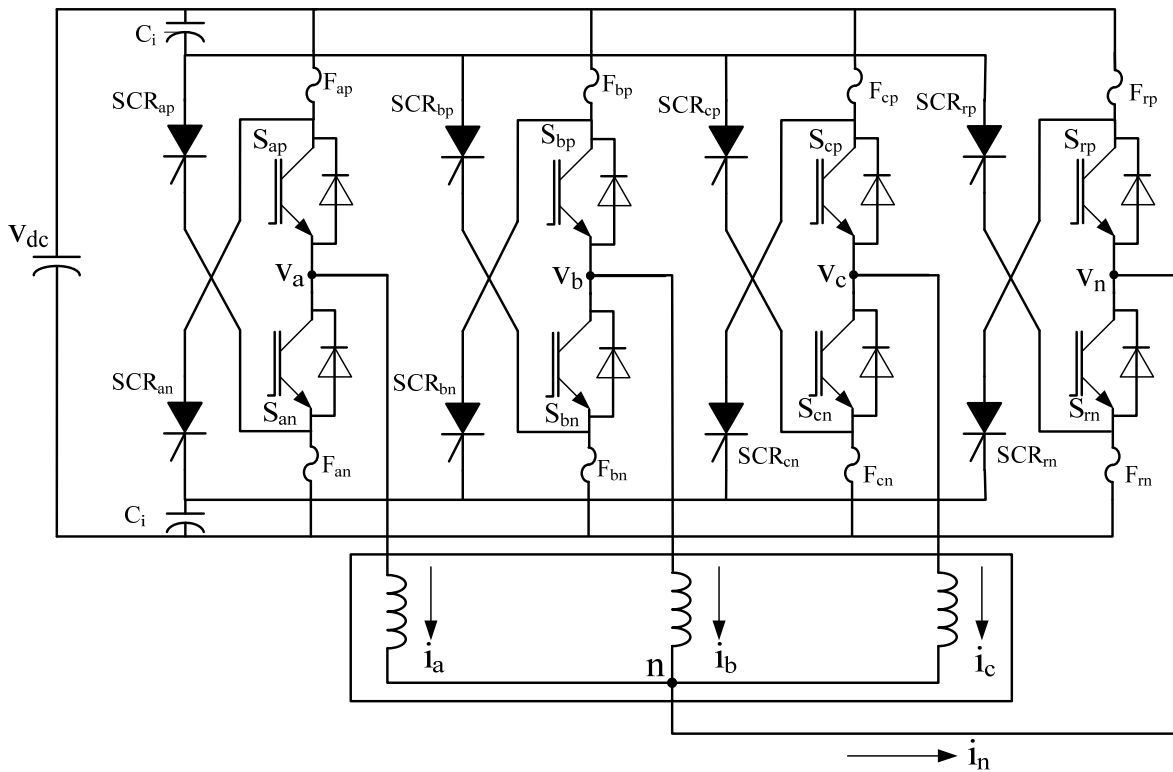


Figure 3.7: Double switch redundant topology with isolating fuses

This topology requires an inverter with four legs and a machine with four terminals (three phases and neutral). The fourth leg of the inverter is connected to the star point of the machine to control the neutral point voltage in case of fault in the inverter. In case of any fault in the inverter or machine open phase fault, the faulted leg (phase) is isolated and the machine is controlled with the remaining two phases. Depending on the faulted leg (phase) isolation techniques, there are two methods available as discussed below.

3.2.3.1 Double switch redundant topology with fault leg isolating fuses

The concept of double switch redundant topology with faulted leg isolating fuses was introduced in [BOL00]. Figure 3.7 shows the double switch redundant inverter topology. This topology needs eight fuses (F_{xp} and F_{xn} , where x is a, b, c or r), eight SCRs and two capacitors in order to isolate the faulted leg of the inverter.

In case of a short circuit fault in any of the IGBT, that particular leg is removed by turning ON the corresponding SCRs, which will eventually blow the fuses to isolate the leg. Two capacitors (C_i) are necessary in order to avoid a DC-bus shoot-through fault, when the SCRs are turned ON to blow the fuses and also they serve to create a means for the current in the SCRs to decay so that they can be turned OFF. After isolating the faulted leg, the machine is controlled in a two-phase manner with the neutral voltage being controlled. In case of winding open circuit fault, the same approach is followed without isolating corresponding inverter leg.

As described before in the four leg inverter topology, this topology also has a FPRF of 0.58 times pre-fault output. With 8 SCRs, 8 semiconductor fuses, two IGBTs (1.73 times peak rated current) and with the two extra capacitors, this topology has a SOCF of approximately 3 times the standard three-phase inverter.

Advantages:

- Works for all the faults such as IGBT short circuit, IGBT open circuit, machine winding open circuit and phase leg open and short circuit.
- Access to mid-point of the DC bus in not required

Disadvantages:

- Silicon count is high
- Two extra capacitors are required to remove the fault leg. The rating / size / cost of the capacitor increases with the rating of the inverter
- Fuses add additional inductance to the inverter, which ultimately causes more EMI and noise problems.
- Fuses causes more losses in the inverter
- DC-link capacitor failures are not addressed

3.2.3.2 Double switch redundant topology with fault leg isolating switches

The concept of using semiconductor switches to isolate the faulted leg is presented in [RIC07]. The use of semiconductor switches or solid-state relays avoid the use of big capacitors (C_i), SCRs and semiconductor fuses (F_{xp} and F_{xn} , where x can be a, b, c or r), which was necessary in Figure 3.7 in order to isolate the faulted leg of the inverter. The use of the semiconductor switches to isolate the faulted leg increases the losses in the system as the load current flows through the IGBT and diode.

As described before in four leg inverter topology, this topology also has a FPRF of 0.58 times the pre-fault output. With 8 IGBTs (6 x 1, 2 x 1.73 times peak rated current), this topology has a SOCF of approximately 2.57 times the standard three-phase inverter

Advantages:

- Semiconductor fuses and bulky capacitors are avoided
- Access to the midpoint of the DC-bus in not required
- Easy to control

Disadvantages:

- Post-fault output is not rated value
- Silicon count is high
- Increased losses in the system
- Does not work for the phase leg short circuit fault
- DC-link capacitor faults are not addressed

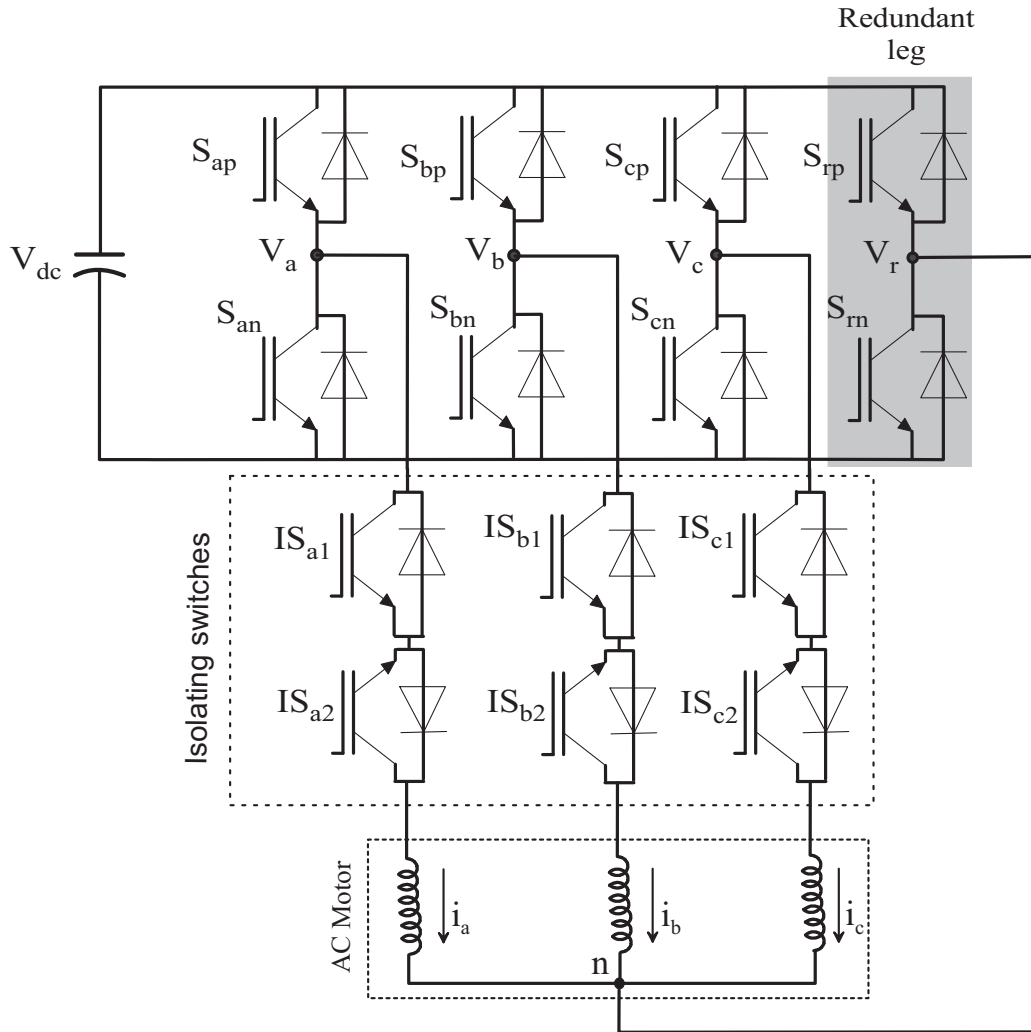


Figure 3.8: Double switch redundant topology with isolating switches

3.2.4 Phase redundant topology

The concept of phase redundant topology was introduced in [RIB01b] and the concept of removing the faulted inverter leg is explained in [BOL00]. Figure 3.9 shows the inverter with phase redundant topology. The inverter phase legs which are connected to the machine phases are equipped with two fuses as shown in Figure 3.9. In order to provide the fault tolerance to the inverter, a redundant leg is used as shown in Figure 3.9. In case of any fault, the faulty leg is removed by blowing-up the fuses (F_{xp} and F_{xn} , where x can be a, b or c) using SCRs (SCR_{xp} and SCR_{xn} where x can be a, b or c) and capacitors (C_i). The redundant leg is connected in place of the faulted leg using the TRIACs or anti parallel SCRs (TR_a , TR_b , or TR_c). The gate signals are transferred from the fault leg to the redundant leg.

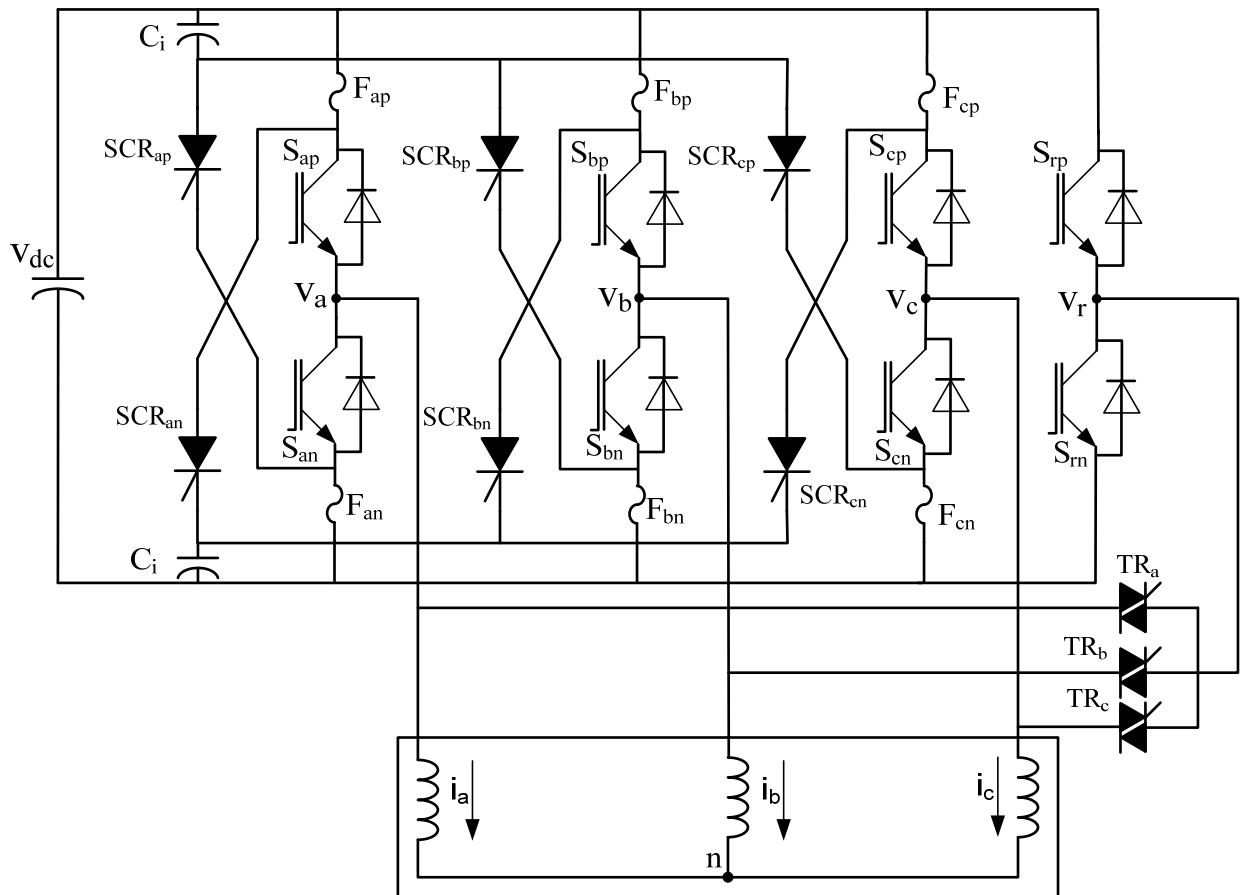


Figure 3.9: Phase redundant topology with isolating fuses

This topology also has a FPRF of 1.0 that means the post-fault output is same as the pre-fault output. With 6 SCRs, 6 semiconductor fuses, 2 IGBTs, 3 TRIACs and two extra capacitors this topology has a SOCF of approximately 3 times the standard three-phase inverter.

Advantages:

- Post-fault output is same as pre-fault rated
- Access to the star point of the machine and to the midpoint of the DC-bus is not required
- Works for all the faults such as open phase (only phase open between inverter terminals and machine terminals), phase leg short, IGBT short and IGBT open

Disadvantages:

- Silicon count is high
- Two extra capacitors are required to remove the fault leg. The rating / size / cost of the capacitor increases with rating of the inverter
- Fuses add additional inductance to the inverter which ultimately causes more EMI and noise problems.
- Fuses causes more losses in the inverter
- Still, the machine remains a single point of failure in the drive system
- DC-link capacitor failures are not addressed

3.2.5 H-bridge inverter topology

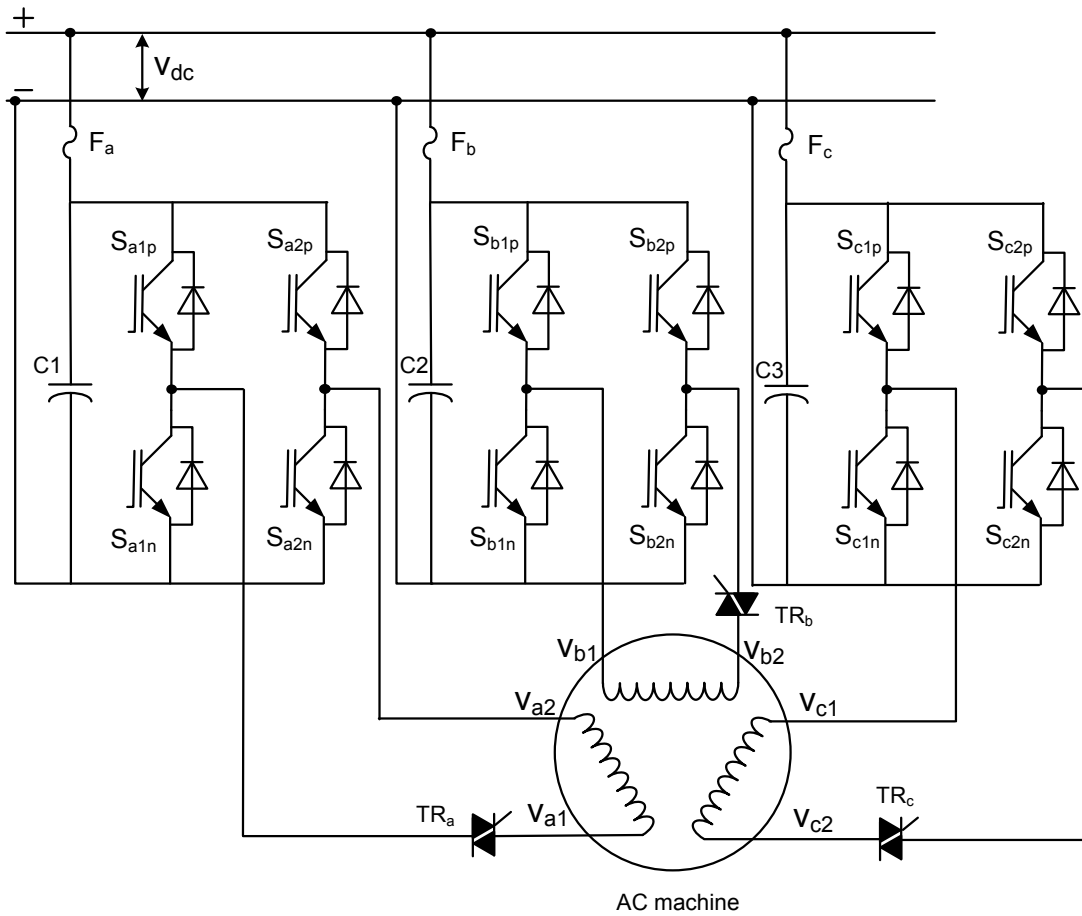


Figure 3.10: H-bridge inverter topology

The concept of using single-phase inverters for each phase of an AC machine was introduced in [QIN97] and is applied to a steer-by-wire system in [KRA99] and to a flight actuator in [BEN04]. For PMSMs and reluctance motors, the use of a single inverter for each phase provides the more flexibility and redundancy when compared with the three-phase six switch inverter. Figure 3.10 shows the H-bridge inverters controlling an AC machine. For this particular topology, the six terminals of the motor should be available and each phase of the machine is independently controlled with a separate H-bridge inverter.

Without thyristors (TR_a , TR_b and TR_c) the fault tolerance capability of the drive is limited to only open-phase faults. In case of a short circuit of any IGBT, though all the remaining IGBTs are turned OFF a circulating path for current exists through the shorted IGBT and freewheeling diode. These circulating currents produce a pulsating torque output. An open-circuit fault in any of the IGBT causes the circulating current to flow through the freewheeling diodes, DC-link and machine winding when the induced voltage in the machine windings is more than the DC-link voltage. In this way, the speed is limited in case of the IGBT open circuit fault. In order to overcome the above two problems, TRIACs or solid state relays (TR_a , TR_b and TR_c) are used in order to isolate the faulted phase of the machine. In order to address DC-link capacitor short circuit failure, fuses (F_a , F_b and F_c) can be included as shown in Figure 3.10. In case of DC-link capacitor short circuit, the fuse will automatically blow, which separate that particular H-bridge inverter. With 6 IGBTs, 3 TRIACs, 3 semiconductor fuses and 2 extra DC-link capacitors, this topology has a SOCF of 2.92 times of the standard inverter.

Advantages:

- Works for all the faults such as open phase, phase leg short, IGBT short and IGBT open circuit
- Machine is no more a single point of failure.
- DC-link capacitor failures are also addressed

Disadvantages:

- Post-fault output is not rated value
- Silicon count is high
- Extra losses in the thyristors (TR_a , TR_b and TR_c)
- Needs a special six terminal machine

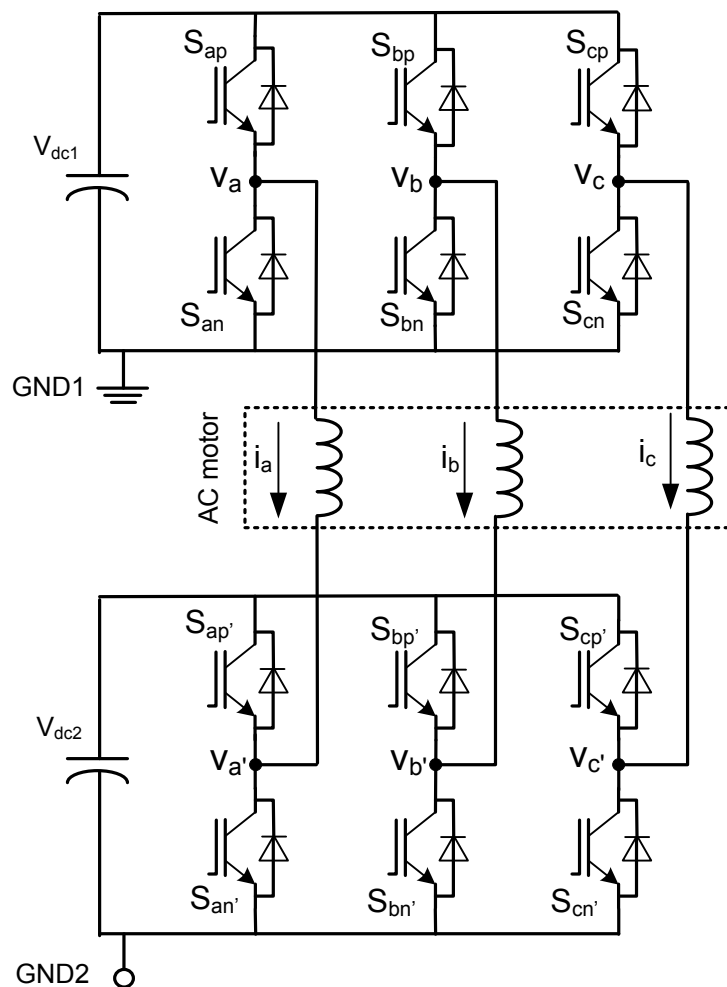
3.2.6 Cascaded inverter topology with isolated DC links**Figure 3.11: Cascaded inverter topology**

Figure 3.11 shows an AC machine driven by two three phase two-level inverters. The two DC-links of the two inverters are isolated and the machine should be an open winding machine. This configuration with isolated DC-links is sometimes used as an alternative implementation to a three-level inverter [STE93, KOR99]. As the two DC-links are isolated, the system can supply a three level waveform across each phase if $V_{dc1} = V_{dc2}$ is used. If different DC-link voltages are used ($V_{dc1} \neq V_{dc2}$) sophisticated waveforms with a higher number of levels are possible. In a standard two-level inverter, zero sequence current flows through the DC-link. However, in this topology, the

control algorithm should be modified in order to minimize the zero sequence currents in the inverters.

This topology can be modified to deliver rated output even under an IGBT open circuit fault or IGBT short circuit fault as explained below. If any of the IGBT in one of the inverters is short circuited, then all the corresponding IGBTs in the remaining legs are permanently turned ON in order to connect the machine in star connection. Then the machine is controlled with the remaining healthy inverter with standard two-level inverter control. If any of the IGBTs is open circuited, then the complementary IGBTs of all the legs are short circuited in order to connect the machine in star connection. The same procedure can also be used for DC-link capacitor short circuit. The main drawback of this topology is availability of two independent DC-link sources and an open winding machine. This topology is suitable for Electric Vehicles (EV) where DC source is the battery pack which can be divided into two parts with independent grounds.

This topology has a FPRF of 1.0 that means the post-fault output and pre-fault output is same (for switch open and switch short circuit fault). With 6 extra IGBTs and one DC-link capacitor, this topology has a SOCF of 2 times of the standard inverter.

Advantages:

- Works for open phase fault, IGBT short and IGBT open circuit fault
- DC-link capacitor failures are also addressed (with a fuse inserted between the DC source and DC-link capacitor)
- Machine faults are also addressed
- Post-fault output is rated value (in case of IGBT open and short circuit)

Disadvantages:

- Needs two independent DC-link sources
- Needs a special six terminal machine

3.2.7 Phase redundant topology with isolating switches (New Proposal)

Based on the criteria of rated post-fault output, a new converter topology is proposed and advantages and disadvantages are briefly discussed.

Figure 3.12 shows the phase redundant topology of fault tolerant converter with isolating switches. This topology is modified version of Figure 3.8 in order to facilitate post-fault rated output.

In case of an IGBT short circuit or open circuit fault, the corresponding phase leg isolating switches are turned OFF and redundant leg is inserted using the corresponding redundant leg inserting switches. In the healthy case, the isolating switches are always turned ON and in case of fault they are turned OFF to isolate the faulty leg. Three different possibilities of these isolating switches are: back-to-back connected IGBTs, or back-to-back connected thyristors, or electromagnetic relays.

Using electromagnetic relays is a cost-effective solution, but electromagnetic relays have considerable amount of delay in closing and opening their contacts. Some systems can tolerate such a delay but in other cases, machine may come to stand still or may rotate in the reverse direction, which is not acceptable in most applications. Electromagnetic relays as isolating switches were proposed for automotive steer-by-wire applications in [NAI10]. Instead of using six single pole single through (SPST) relays, three double pole single through (DPST) relays can be used. Special

relays should be selected, which are capable of interrupting the short circuit current flowing through the shorted IGBT in case of an IGBT short circuit fault.

This topology has FPRF of 1.0 that means post-fault output and pre-fault output is same. With 2 extra IGBTs and 3 DPST relays, this topology has SOCF of 1.83 times of the standard inverter.

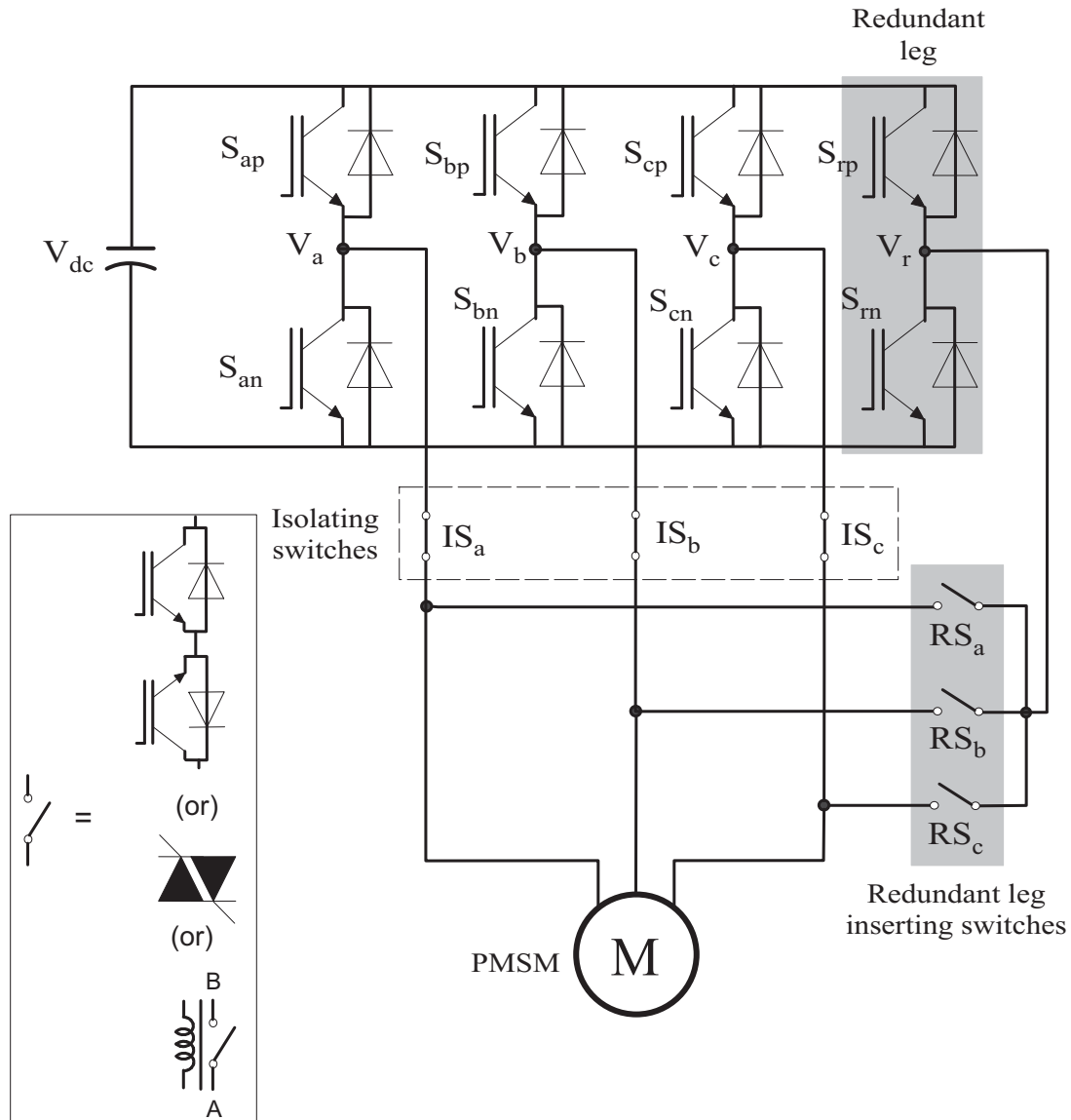


Figure 3.12: Phase redundant topology with isolating switches

In order to isolate the faulted leg fast, back-to-back connected IGBTs are proposed as isolating switches in [RIC07]. The main disadvantages of this topology are, firstly, the losses are increased as the load current is continuously flowing through the isolating IGBT and diode combination which will eventually increase the size of the heat sink. Secondly, the IGBT along with its gate drivers makes the system very expensive. Thirdly, if the current through device is not zero during turn OFF it may cause overvoltage causing the isolating switches to damage.

This topology has FPRF of 1.0 that means post-fault output and pre-fault output is same. With 8 IGBTs and 3 TRIACs (used to insert the redundant leg), this topology has a SOCF of 2.83 times of the standard inverter.

In order to overcome the disadvantage of continuous conduction losses in the topology with isolating back-to-back connected IGBTs, the isolating IGBT switches can be replaced with back-to-back connected thyristors. On-state resistance or conduction losses of the thyristors are considerably less when compared with the IGBTs [KRI10]. This topology also gives rated post fault output for IGBT open circuit and IGBT short circuit fault. If any of the IGBT is open circuited then its corresponding phase isolating thyristors are used to isolate the faulted leg. In case of an IGBT short circuit fault, sufficient care must be taken in order to make sure that IGBT short circuit fault current is brought to zero. The fault current flowing through the shorted IGBT phase should be brought to zero as fast as possible in order to isolate the faulted leg. After the fault leg is isolated, redundant leg is inserted using corresponding back-to-back connected redundant leg inserting thyristors. Gate signals of the faulted leg are transferred to the redundant leg.

This topology has FPRF of 1.0 that means post-fault output and pre-fault output is same. With 2 extra IGBTs and 6 back-to-back thyristors, this topology has a SOCF of 2.33 times of the standard inverter.

Advantages:

- Post-fault rated output is same as pre-fault
- Access to the star point of the machine and midpoint of the DC-bus is not required
- Post-fault control strategy is same as pre-fault control.

Disadvantages:

- Silicon count is high (for the case of back-to-back connected IGBT and thyristors)
- Increased losses in the system (for the case of back-to-back connected IGBT and thyristors)
- Does not work for the phase leg short circuit
- DC-link capacitor faults and machine faults are not addressed

Table 3.1: Comparison of power converters with increased availability

Topology	Split DC bus	Machine star point accessible	Open winding machine	Fuses	Extra Capacitors	Auxiliary Switches	I rating of Auxiliary switches (pu)	Fault Power Rating Factor (FPRF)	Silicon Overrating & Cost Factor (SOCF)	Fault Tolerant to					
										I switch short	Phase-leg short	I switch open	I phase open	DC-link capacitor short	
Standard (Figure 3.1)	N	N	N	0	0	0	N.A.	0	1						
Four leg converter (Figure 3.2)	N	Y	N	0	0	2 (IGBT)	1.73	0.58	1.58		X	X			
Switch redundant topology (Figure 3.5)	Y	Y	N	3	0	3 (TRIAC) 1 (TRIAC)	1.0 1.73	0.5	2.0		X	X			
Double switch redundant topology with isolating fuses (Figure 3.7)	N	Y	N	8	2	8 (SCR) 2 (IGBT)	1.0 1.73	0.58	3.0		X	X			
Double switch redundant topology with isolating switches (Figure 3.8)	N	Y	N	N	0	6 (IGBT) 2 (IGBT)	1.0 1.73	0.58	2.57		X	X			
Phase redundant topology with isolating fuses (Figure 3.9)	N	N	N	6	2	6 (SCR) 2 (IGBT) 3 (TRIAC)	1.0 1.0	1.0	3.0		X	X			
H-bridge inverter topology (Figure 3.10)	N	N	Y	3	2	6 (IGBT) 3 (TRIAC)	1.0	0.58	2.92		X	X	X	X	
Cascaded inverter topology (Figure 3.11)	N	N	Y	2	1	6 (IGBT)	1.0	1.0	2.0		X	X	X	X	
Phase redundant topology with isolating relays (Figure 3.12)	N	N	N	0	0	3 (DPST) 2 (IGBT)	1.0	1.0	1.83		X	X	X	X	
Phase redundant topology with isolating IGBTs (Figure 3.12)	N	N	N	0	0	8 (IGBT) 3 (TRIAC)	1.0	1.0	2.83		X	X	X	X	
Phase redundant topology with isolating thyristors (Figure 3.12)	N	N	N	0	0	2 (IGBT) 6 (TRIAC)	1.0	1.0	2.33		X	X	X	X	

3.3 Conclusions of the comparison of converter topologies with increased availability

In the previous section, different converter topologies with increased availability are discussed and a new topology is proposed with some modifications to the existing topologies. Table 3.1 shows the summary of all the topologies when compared with a standard three-phase inverter. Final selection of a topology depends on many parameters such as cost, complexity, post fault kVA output, tolerance to different faults, delay in detecting and compensating the faults and accessibility of the DC-link mid-point and the motor neutral point or an open winding motor. All the topologies for increased availability need extra semiconductor switches and some topologies need extra fuses and capacitors. Among the topologies considered, key results include the following,

- 1) Among all the topologies considered, four-leg inverter (Figure 3.3) is simple in construction and control, but this topology can provide tolerance to only open switch and open phase faults. The post fault output is only 0.58 times when compared with a standard inverter kVA output without any fault. This topology is not tolerant to the switch short faults. Considering all the extra components, the approximate SOCF of the system is 1.58 times of the standard three-phase inverter.
- 2) The switch redundant topology (Figure 3.5) provides tolerance to switch short, switch open and phase open faults of the power converter. In case of a switch short and switch open fault, the inverter is capable of impressing one-half the phase voltage of the standard unfaulted inverter and full rated current of the inverter. This means, in terms of motor capacity, the system will allow full rated torque output with the machine running in the field weakening range at approximately half the rated speed. In case of open phase fault, the dq components of the voltage are reduced from 0.577 to 0.5 and the magnitude of dq components of the torque producing currents is reduced by a factor of $1/\sqrt{3}$. This means the machine runs at almost the rated speed but with half the rated torque when compared to a standard inverter without fault. Considering all the extra components the approximate SOCF of the system is 2.0 times of the standard three-phase two-level inverter.
- 3) The double switch redundant topology (Figure 3.7) with isolating fuses is tolerant to all the four types of faults mentioned before, but its post fault kVA output is only 0.58 times the standard inverter kVA output without fault. The isolating fuses in this topology add extra stray inductance to the inverter DC-bus which causes more EMI and noise problems. It also needs two bulky capacitors to blow up the fuses, whose size and cost increases with the kVA rating of the inverter. In order to avoid the above disadvantage double switch redundant topology with isolating switches (Figure 3.8) are used. This topology is simple in construction and control but continuous conduction of current through isolating switches increases the losses in the inverter which ultimately decreases the efficiency of the inverter and increases the size of the heat sink. So, where, the size of the heat sink is not a constraint and in medium power or low power applications where the losses of the inverter are not an issue, the double switch redundant topology with isolating switches can be selected compared with double switch redundant topology with isolating fuses. Moreover, the double

switch redundant topology with isolating fuses has an SOCF of 3 when compared to 2.57 of the double switch redundant topology with isolating switches.

- 4) In order to increase the post-fault kVA output equal to pre-fault kVA output rating, phase redundant topology with isolating fuses (Figure 3.9) is used. This topology works for all the faults such as a switch open, switch short, phase leg short and phase open (phase open only between inverter terminals and motor terminals). As explained in 3), the phase redundant topology with isolating fuses have all the disadvantages of double switch redundant topology with isolating fuses. In order to overcome these limitations, phase redundant topology with isolating switches (Figure 3.12) is proposed.
- 5) The H-bridge topology (Figure 3.10) works for all the faults, including DC link capacitor failures, but this need special open winding machine. The post fault kVA output is 0.58 times the standard un-faulted inverter. Considering all the extra devices the SOCF of the inverter is 2.92 times of the standard inverter.
- 6) In case of cascaded inverter topology (Figure 3.11), this topology need open winding machine and independent DC buses. The main advantage of this topology is, in pre-fault operation the cascaded converter can be operated like a three-level converter and in post-fault operation like a two-level converter but with rated kVA output as per as any fault in the inverter is considered. Any fault in the machine causes that phase to be isolated and the machine works in the degraded mode. The SOCF of cascaded inverter topology is approximately 2 times standard three phase inverter. The main disadvantage of this topology is the need of having two isolated DC buses and an open winding machine.
- 7) In case of phase redundant topology with isolating switches (Figure 3.12), there are three possibilities of isolating switches: electromagnetic relays, back-to-back connected IGBTs and back-to-back connected thyristors. Electromagnetic relays can be a cost effective solution but needs a lot of time in closing and opening their contacts. So electromagnetic relays are suitable only to the systems where short interruptions in the drive are accepted. When it comes to the back-to-back connected IGBTs, they isolate the faulted phase leg fast enough such that there is a negligible disturbance in the drive operation. The main disadvantage of such a system is it's increased in losses and cost. In order to decrease the losses and cost, back-to-back connected IGBTs can be replaced by back-to-back connected thyristors. Thyristors have less on-state resistance compared to the IGBTs and doesn't need a sophisticated gate drive as in case of IGBTs. However, unlike IGBTs, thyristors cannot be turned OFF by a switching command. In order to turn the thyristor OFF, the load current must be reduced below its holding current for sufficient time to allow all the mobile charge carriers to vacate the junction. So in case of IGBT short fault, sufficient care must be taken to bring the short circuit fault current flowing through the faulted IGBT to zero.

After comparing the different topologies with increased availability, with the criteria of having rated post fault output with negligible disturbance to drive operation, phase redundant topology with back-to-back connected thyristors as the fault leg isolating switches is selected for further development. Extensive simulations are done to check the effectiveness of the converter in isolating the faulted leg in case of IGBT short circuit fault. Suitable control steps are proposed to isolate the faulted leg in case of IGBT short and IGBT open circuit faults such that there is negligible disturbance to the drive operation.

3.4 System description of the proposed inverter with increased availability

Figure 3.13 shows the proposed two-level voltage source inverter with increased availability. A standard two-level three-phase inverter consists of only three legs but, an inverter with increased availability of this topology consists of four legs, with one leg as redundant. The redundant leg is normally not used when the standard three legs are working without any fault. Back-to-back connected thyristors (IS_a , IS_b and IS_c) are connected between output terminals of the inverter (V_a , V_b and V_c) and corresponding motor phases. These thyristors are used as isolating switches of faulted leg. Additional three thyristors (TH_a , TH_b and TH_c) are connected between the output terminal of redundant leg (V_r) and motor phases as shown in Figure 3.13. These Thyristors are used for inserting the redundant leg in the place of faulted inverter leg. Instead of Back-to-back connected thyristors, TRIACs can do the same function but because of their poor dv/dt and di/dt ratings they are not suitable for this application.

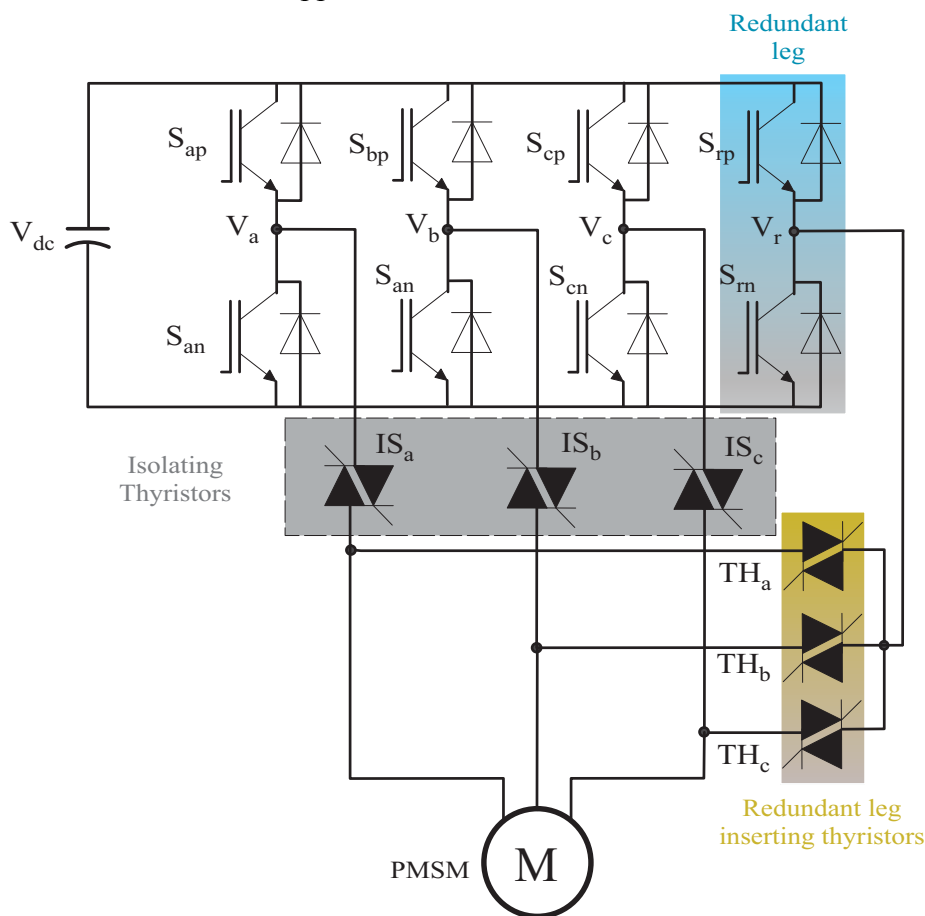


Figure 3.13: Proposed fault tolerant voltage source inverter

3.4.1 High dv/dt tolerance testing of the redundant leg inserting thyristors

As described in Figure 3.13, back-to-back connected thyristors are used to reconfigure the inverter in case of any fault in the existing inverter legs. However, the problem with the thyristors is they may not tolerate high dv/dt produced by the IGBTs. If they cannot tolerate the high dv/dt , they automatically turn ON without any gate pulse applied. But modern thyristors are produced with high dv/dt tolerance capability. In order to test the redundant leg inserting thyristors for dv/dt tolerance, a similar situation to the Figure 3.13 is tested experimentally as shown in Figure 3.14. The thyristor gate terminals are initially connected to the cathode using a resistance whose value is

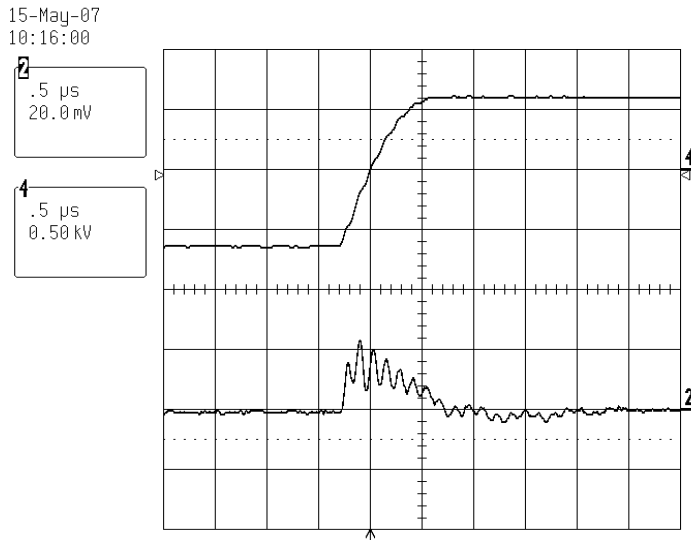


Figure 3.16: Voltage across and current through thyristor (turn off) (scale: ch2-200mA/div, ch4-500 V/div)

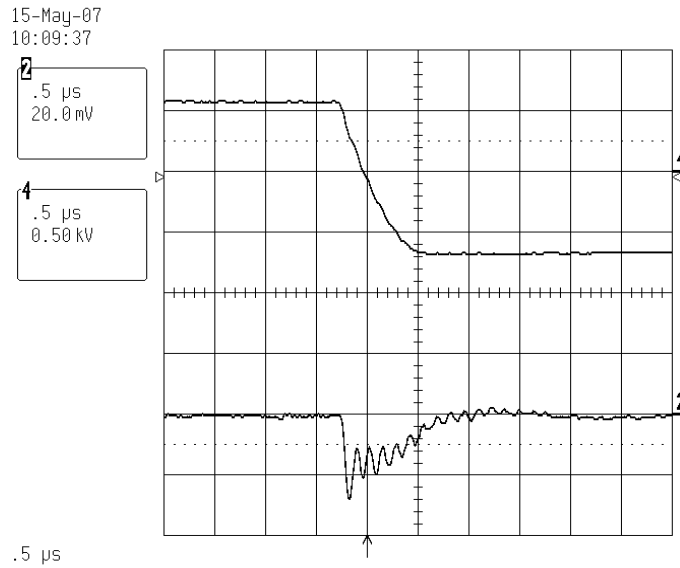


Figure 3.17: Voltage across and current through thyristor (turn on)
(Scale: ch2-200mA/div, ch4-500 V/div)

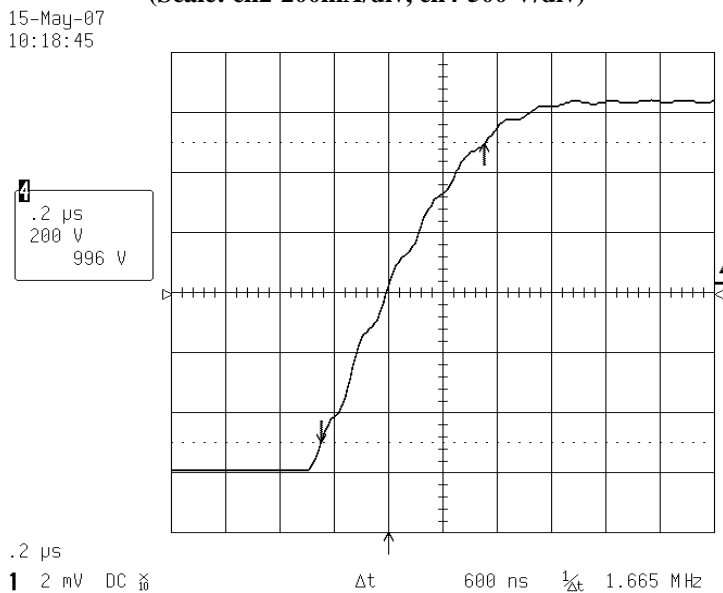


Figure 3.18: Voltage across thyristor (turn off dv/dt) (scale: ch4-200 V/div)

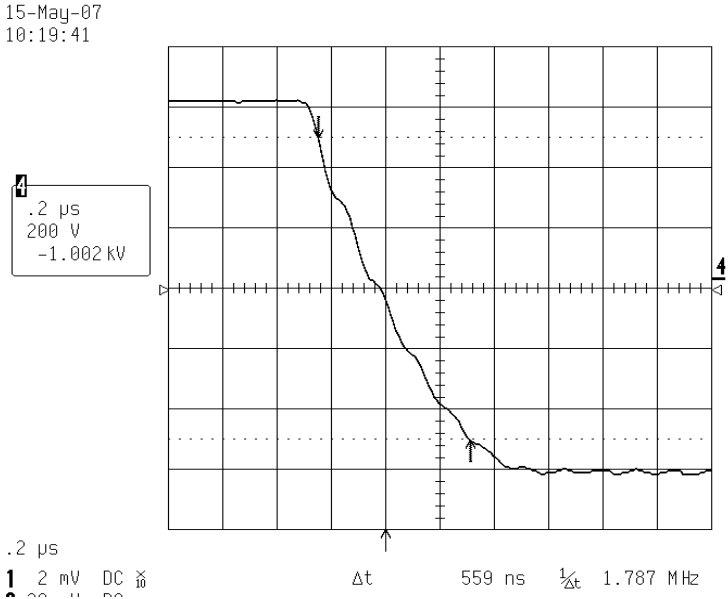


Figure 3.19: Voltage across thyristor (turn on dv/dt) (scale: ch4-200 V/div)

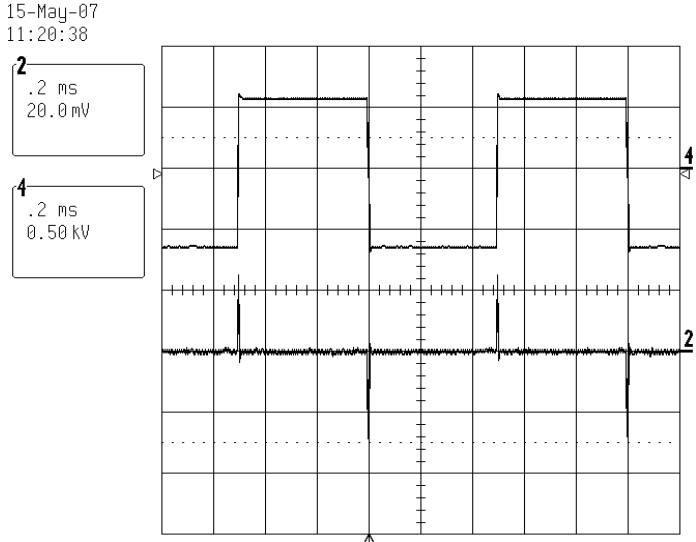


Figure 3.20: Voltage across thyristor and current through thyristor (with 75°C)
(Scale: ch2-200mA/div, ch4-500 V/div)

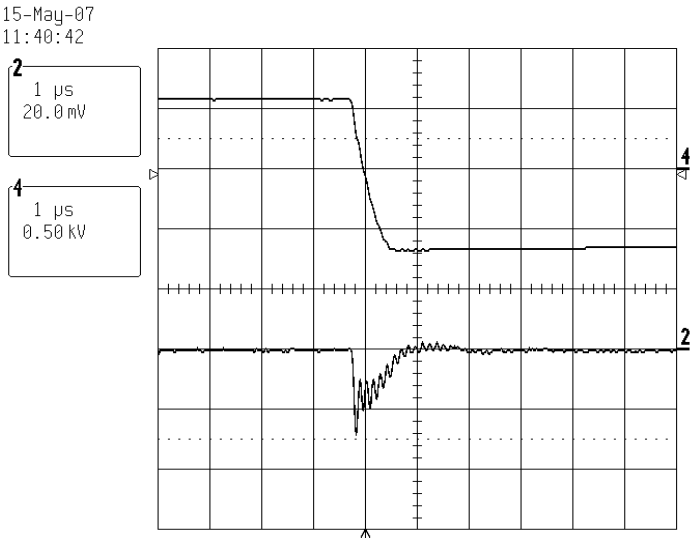


Figure 3.21: Voltage across thyristor and current through thyristor (turn on and 75°C)
(Scale: ch2-200mA/div, ch4-500 V/div)

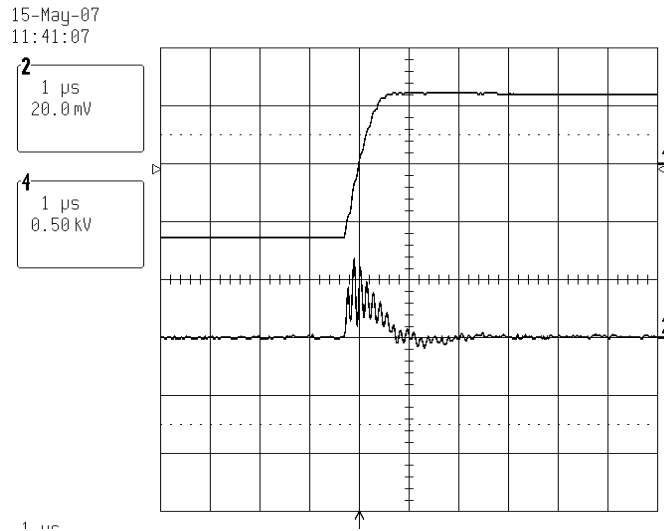


Figure 3.22: Voltage across thyristor and current through thyristor (turn off and 75°C)
(Scale: ch2-200mA/div, ch4-500 V/div)

3.4.2 Efficiencies comparison of standard inverter and inverter with increased availability

The rating of the thyristors is same as that of the IGBTs. During the normal operation, isolating thyristors (IS_a , IS_b and IS_c) are always turned ON which will cause undesired conduction losses. Usually thyristors have much lower on-state voltage drop compared to the IGBTs, so the reduction in efficiency is not significant when compared to the total losses of the inverter. For example, when considered of the almost equal rating of the IGBT (SK30GB123) and thyristor (SK25UT), the on-state voltage drop of the IGBT is, $V_{CE(sat)} = 3.7V$ max (@ $T_j = 125^\circ$, $I_{Cnom} = 25A$) and for the thyristor is $V_T = 1.62V$ max (@ $T_j = 125^\circ$ and $I_{nom} = 25A$).

The losses in the standard inverter are computed in the simulation by using ideal switches and diodes as explained in [MUN00]. Almost equal ratings of IGBT and thyristors are selected for loss comparison of standard inverter and inverter with increased availability. The data sheets of the selected IGBT (SK30GB123) and thyristor modules (SK25UT) are provided in the Appendix A. First, for all the devices, from the data sheets information, the relation between instantaneous on-state voltage $V_{ce-on-ds}$ vs. $i_{c-on-ds}$, $i_{c-on-ds}$ vs. E_{on-ds} , $i_{c-on-ds}$ vs. E_{off-ds} (in the nomenclature $-ds$ represents the values from the data sheets) are entered in to a lookup table (Junction temperature is assumed constant $T_j=125^\circ C$). The switching moments are detected using abrupt edges on voltage and current waveforms [MUN00]. The positive voltage edges occur at turn OFF moments and the negative voltage edges occurs at turn ON moments. The turn ON voltage, V_{ce-on} , is the first sample before the negative edge on the voltage waveform and the turn ON current, i_{c-on} , is the first sample after the positive edge on the current wave form. The turn OFF voltage, V_{ce-off} , is the first sample after the positive edge on the voltage waveform and the turn OFF current, i_{c-off} , is the first sample before the negative edge on the current wave form. Based on the lookup table and given V_{ce-on} and i_{ce-on} , the loss estimation program computes the turn ON energy loss E_{sw-on} using a linear interpolation. Similarly, the turn OFF energy loss E_{sw-off} is estimated. The turn ON and turn OFF energy losses are computed in the simulation by using the following equations:

$$E_{sw-on} = E_{on-ds} \frac{V_{ce-on}}{V_{ce-on-ds}} \frac{i_{c-on}}{i_{c-on-ds}} \tag{3.1}$$

$$E_{sw-off} = E_{off-ds} \frac{V_{ce-off}}{V_{ce-off-ds}} \frac{i_{c-off}}{i_{c-off-ds}} \quad (3.2)$$

Using the above two equations, the switching losses can be computed as below,

$$P_{sw-on} = \frac{1}{T} \sum E_{sw-on}, \quad P_{sw-off} = \frac{1}{T} \sum E_{sw-off} \quad (3.3)$$

The on-state voltage, V_{ce-on} , is computed using the lookup table and current (i_{c-on}) through the device.

$$V_{ce-on} = V_{ce-on-ds} \frac{i_{c-on}}{i_{c-on-ds}} \quad (3.4)$$

Then, the conduction losses are computed by averaging the equation (3.4) along an integration time T .

$$P_C = \frac{1}{T} \sum (V_{ce-on} \cdot i_{c-on} \cdot \Delta T) \quad (3.5)$$

where, ΔT is the simulation time step.

The total losses in the standard inverter are,

$$P_{HSI} = P_{sw-on} + P_{sw-off} + P_C \quad (3.6)$$

In case of the Inverter with increased availability, fault isolating back-to-back connected thyristors are connected in series with each phase and they are permanently tuned ON. So only conduction losses are occurred in these thyristors. V_{T-on} values of thyristors are extracted for different current values and the losses are computed as below:

$$P_{thy} = 6 \cdot V_{T-on} \cdot i_c \quad (3.7)$$

The total losses in the inverter with increased availability are,

$$P_{FTI} = P_{sw-on} + P_{sw-off} + P_C + P_{thy} \quad (3.8)$$

Figure 3.23 shows the efficiency comparison of a standard two-level inverter and inverter with increased availability for different load currents. From the figure, it is evident that the drop in efficiency for the proposed converter is not significant when compared to the standard inverter.

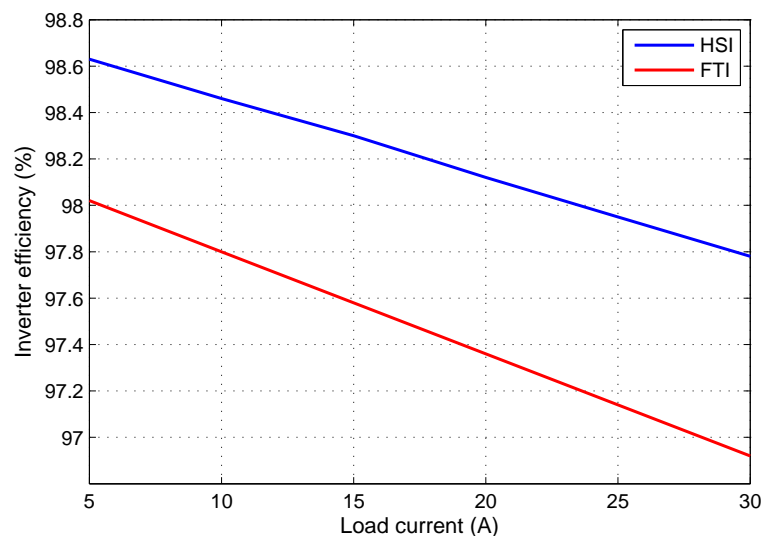


Figure 3.23: Efficiency comparison of standard two-level inverter (HSI) and inverter with increased availability (FTI)

3.4.3 Inverter operation and fault compensation for single IGBT open circuit fault

An open-circuit fault in the IGBT may be due to a fault in the gate drive or the break of bond wires in the IGBT. Figure 3.24 shows the standard three-phase two-level VSI with an open switch fault (S_{ap} open) controlling an AC machine. When one of the IGBT does not turn ON, in case of motor operation, current in that phase is zero for a half cycle, either positive half cycle or negative half depending on whether it is upper IGBT or lower IGBT. For example, in this case, IGBT ' S_{ap} ' is having a switch open fault. When the current is in the positive half cycle, the phase 'a' current is always zero. As a consequence of this, a DC current offset is caused in faulty phase and this offset is equally divided between the healthy phases. Moreover, the current DC component generates unequal current stress in the upper and lower transistors in the inverter, which may cause thermal defects in the transistors [KAS94].

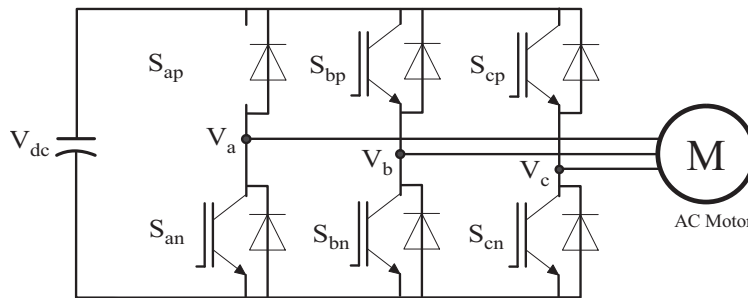


Figure 3.24: Three phase two-level inverter in the case of IGBT S_{ap} open fault

Different methods for detecting the open-circuit fault of the IGBTs are available in the literature [FUC03, RIB03, PEU98, and JUN09]. A detailed literature survey of different IGBT open circuit fault detection methods is presented in [BIN09]. Though, different methods exist in the literature, only selected methods are briefly explained here. Some methods are based on using the voltage sensors [RIB03] and some are based on software techniques without using any additional hardware [PEU98], [JUN09]. According to [RIB03], open circuit fault of the IGBT can be detected by inserting voltage sensors at desired locations. Depending on the location of the voltage sensor inserted, the fault detection techniques can be classified as,

- 1) Inverter pole voltage measurement
- 2) Machine phase voltage measurement
- 3) System line voltage measurement
- 4) Machine neutral voltage measurement

Though these methods have short fault detection time, they need extra voltage sensors for the fault detection. To overcome the above problem, in some papers, software-based techniques have been suggested. Peugeot *et al.* [PEU98] suggested the open switch fault detection by analyzing the current vector trajectory and instantaneous frequency in the faulty mode. With this method, it is easy to detect the fault, but it causes time delay for the fault detection while it needs to save the current vector trajectory of one cycle. As this method needs to save current vector trajectory of one cycle, a lot of memory is needed in the digital controller, and especially this is worse when the machine is working at low speed. Jung *et al.* [JUN09] proposed a different method for detecting an open switch fault based on comparing the estimated terminal voltage of the inverter and reference terminal voltage of the inverter. In case of open switch fault, there is a considerable difference between these two. This method of fault detection is fast but terminal voltage is estimated using machine

parameters. So any variation in the parameters should not affect the fault detection. In this work, no special fault detection method is adopted. In order to test the inverter performance, a worst case is assumed where it takes at least one current cycle to detect the fault.

As soon as the open-circuit fault in any IGBT is detected, gate signal to the corresponding leg and the corresponding isolating thyristors (IS_a , IS_b or IS_c) are blocked. The gate signals of the faulty leg are transferred to the redundant leg and its corresponding thyristors (TH_a , TH_b or TH_c) are turned ON as soon as the isolating thyristor is blocked. The same procedure can also be applied in the case of phase leg open circuit fault.

3.4.4 Inverter operation and fault compensation for single IGBT short circuit fault

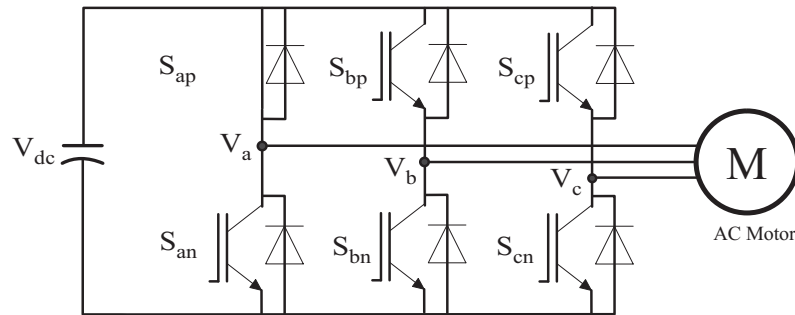


Figure 3.25: Three-phase two-level inverter in the case of IGBT S_{ap} short fault.

A short circuit fault in the IGBT may be due to the malfunctioning of the gate drive or permanent damage in the IGBT. Figure 3.25 shows the standard VSI with an IGBT short circuit fault (S_{ap} shorted). A standard V_{ce} desaturation based fault detection is used for the IGBT short circuit fault detection [BHA98].

As soon as IGBT short circuit fault is detected, all the IGBTs are turned OFF by hardware protection. Now for the case of IGBT permanent damage, corresponding phase is permanently connected to the DC-link positive bus or negative bus depending on upper IGBT or lower IGBT is damaged. As long as the machine is running, current flows through the shorted IGBT and remaining freewheeling diodes of the inverter. Figure 3.26 shows the standard VSI after the upper IGBT (S_{ap}) is short circuited and hardware protection turns OFF all the other IGBTs. Depending on the instance of fault in a current cycle, fault current in that corresponding phase may take a lot of time to reach zero crossing in order to isolate the faulted phase leg. Depending on the parameters of drive, load and operating point, sometimes this short circuit current could be unidirectional [BIA96]. However, for disturbance free operation or for negligible disturbance of drive operation, the isolation of faulted phase should be fast. In order to achieve the above requirement, the gate triggering signals of all the isolating thyristors (IS_a , IS_b and IS_c) are blocked, which facilitates in bringing the short circuit current to zero.

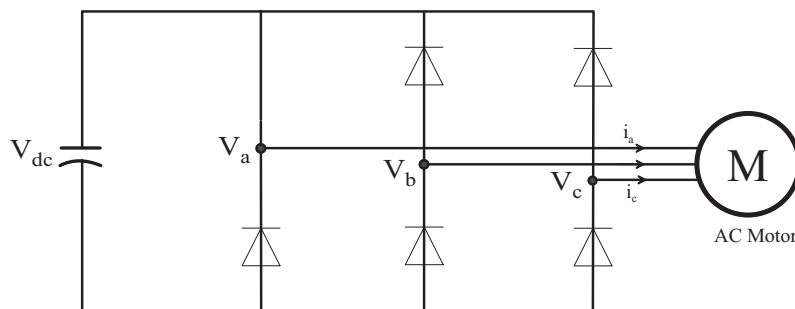


Figure 3.26: Post fault inverter topology in the case of IGBT S_{ap} short fault.

Below provided theoretical analysis shows that, removal of the gate triggering signals for all the isolating thyristors, current in the faulted phase reaches the zero crossing. With the short circuit fault on IGBT S_{ap} , Phase ‘a’ is permanently connected to DC-link positive bus. If the machine current ‘ i_a ’ is in the negative half cycle when the fault occurred, as the phase is permanently connected to the positive DC-bus after the fault, current tend to increase in the positive direction with certainly having a zero crossing. So, for the analysis, it is enough to consider only the positive half cycle of machine current ‘ i_a ’. Figure 3.27 shows the machine phase currents under the healthy condition. Positive half cycle of phase current ‘ i_a ’ is divided into three sections where the border of the sections is defined by the zero crossings of a machine’s phase current. Figure 3.28 shows the inverter configuration after the IGBT S_{ap} short circuit fault with simplified PMSM. In Figure 3.28, e_a, e_b and e_c are back- e.m.f of the machine and L is phase inductance of the PMSM. In order to analyze the machine behavior after the fault, the stator resistance of the machine is neglected and it is assumed that machine speed is constant. For a non-salient PMSM, the d-axis current in the pre-fault state is controlled to be zero and consequently, all current is in the q-axis. Therefore, when the fault occurs, the stator current is assumed to be in phase with the back-EMF.

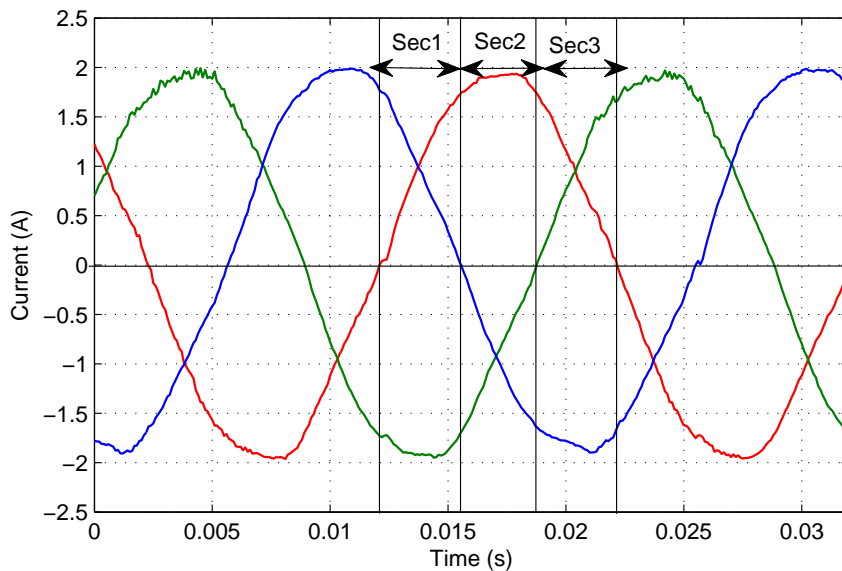


Figure 3.27: Three phase machine currents in healthy condition

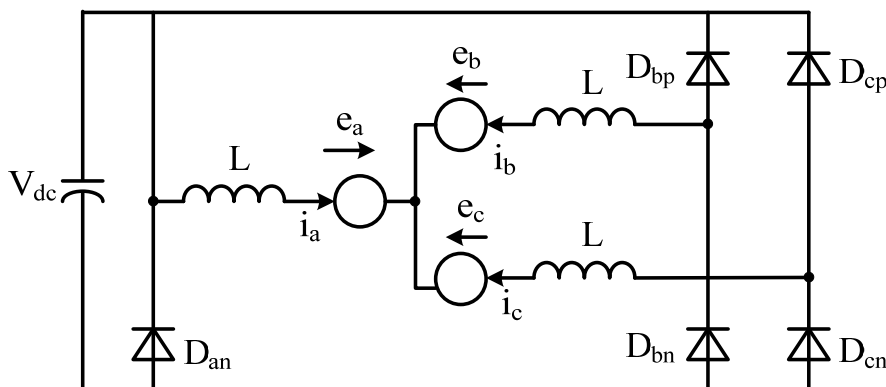


Figure 3.28: Post fault inverter topology in the case of IGBT S_{ap} short fault

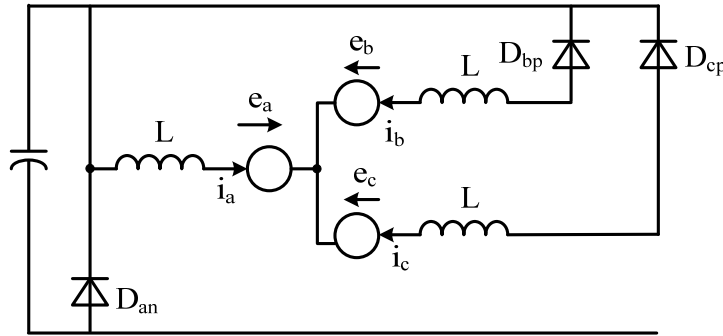


Figure 3.31: Post fault inverter topology in the case of IGBT S_{ap} short fault in Sec2

From (3.13) it clear that all back-EMFs oppose their currents which forces all the currents to reach zero. But for high current at low speed (standstill) with low or zero back-EMFs, the time to reach zero current will be long until the energy initially stored in the inductances is dissipated.

Sec3:

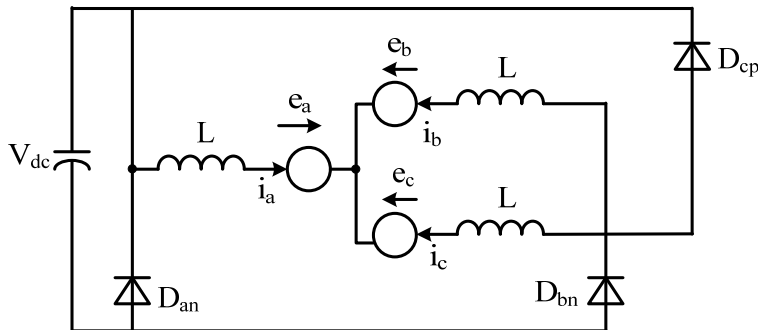


Figure 3.32: Post fault inverter topology in the case of IGBT S_{ap} short fault in Sec3

In Sec3, i_a, i_b are positive and i_c is negative. So Figure 3.28 can be further simplified as Figure 3.32 according to the direction of current flowing.

For a symmetrical machine, where the sum of all EMFs is always zero, the phases are decoupled. Using i_b and i_c as state variables, the differential equations for the general case with arbitrary induced voltages is:

$$L \frac{d}{dt} \begin{bmatrix} i_b \\ i_c \end{bmatrix} = \begin{bmatrix} -1 & 0 & -2/3 \\ 0 & -1 & 1/3 \end{bmatrix} \begin{bmatrix} e_b \\ e_c \\ V_{dc} \end{bmatrix} \tag{3.14}$$

The slope of i_b is strongly negative and i_b will reach zero fast. The thyristor ‘ IS_b ’ is blocking and the current remains at zero. With this condition, Figure 3.32 can be further simplified as Figure 3.33 and the equation for current i_a is

$$2 \cdot L \cdot di_a/dt = -e_a + e_c \tag{3.15}$$

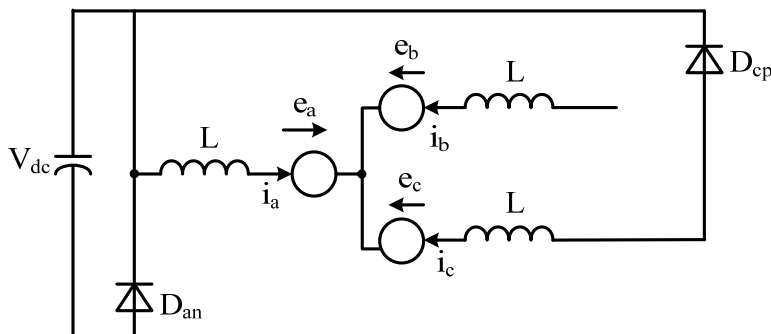


Figure 3.33: Post fault inverter topology in the case of IGBT S_{ap} short fault in Sec3 after current i_b becomes zero

As the back-EMF is assumed to be in phase with the current, in Sec3 of Figure 3.33, e_a is positive but e_c is negative so the resultant the slope of i_a is negative which brings i_a to zero. But for high current at low speed (standstill) with low or zero EMFs, the time to reach zero current will be long until the energy initially stored in the inductances is dissipated.

If we assume standstill and consider the winding resistances R in the phases of the machine, then we get

$$\frac{di_a}{dt} = -\frac{2R}{2L}i_a \quad (3.16)$$

with the solution $i_a = i_{a,t=0} \cdot e^{-\frac{R}{L}t}$ which does not reach zero in a finite time. Therefore, we assume the semiconductors in the current loop as a constant voltage source of 0.7V each. If the short circuit is ideal, there are the thyristors IS_a , IS_c (in Figure 3.13) and the Diode D_{cp} in the loop, forming a voltage source $V_{semi}=2.1V$. The differential equation is:

$$\frac{di_a}{dt} = -\frac{R}{L}i_a - V_{semi} \quad (3.17)$$

with the solution
$$i_a = \left(i_{a,t=0} + \frac{V_{semi}}{R} \right) e^{-\frac{R}{L}t} - \frac{V_{semi}}{R} \quad (3.18)$$

The current i_a will cross the holding current I_H at
$$t_{zero} = \frac{L}{R} \ln \left(\frac{R \cdot i_{a,t=0} + V_{semi}}{I_H \cdot R + V_{semi}} \right) \quad (3.19)$$

For the machine parameters given in Table 3.2 and $I_H=100mA$ with initial current $i_{a,t=0} = 5A$ results in $t_{zero} = 5.3$ ms

This is an optimistic approximation only, as the forward characteristic of the semiconductors will have zero voltage at zero current and not 0,7V. During this time interval, no useful torque is produced by the motor and external load torque may move the motor.

3.5 Simulation results

Simulations are carried out in MATLAB/Simulink® software. The machine parameters are presented in Table 3.2. Simulations are carried out for the case of uncompensated IGBT short circuit fault (standard inverter with IGBT short fault) and for the case of compensated IGBT short circuit fault (proposed inverter with IGBT short circuit fault). A FOC of the PMSM is implemented in order to test the behaviour of the machine for different faults. In the actual experimental setup presented in section 3.6.1, the PMSM is coupled with another PMSM, which is used as a load machine. A three phase variable resistance is connected at the output terminals of the load machine which provides a load torque proportional to the speed. A similar condition is assumed for simulations where the load torque is speed dependent and is zero at zero speed.

3.5.1 Uncompensated IGBT short circuit fault

Figure 3.34 to Figure 3.43 show the different responses of PMSM drive with IGBT short circuit fault on switch ‘ S_{ap} ’. In an inverter, as soon as the short circuit fault in any of the IGBT is detected, it is assumed that hardware protection blocks the gate signals to remaining IGBTs. A similar case is also assumed even in the simulations and as soon as a short circuit in any of the IGBTs is detected gate signals to all the IGBTs are blocked. In this way, the inverter structure after the short circuit fault is as shown in Figure 3.26. In Figure 3.34, when the instantaneous values of

the induced voltages are $e_b - e_a > 0$, then current is driven through the upper diode of phase ‘b’ (D_{bp}). This starts at $t = 17\text{ms}$ in Figure 3.34. Additionally, at $t = 20\text{ms}$ induced voltages become $e_c - e_a > 0$ and D_{cp} starts conducting. The transformation of the three phase currents shown in Figure 3.34 result in the negative q-axis current shown in Figure 3.35, which produces a braking torque. This braking torque reduces speed and induced voltages accordingly. The negative slope of the phase currents i_b and i_c change to a positive slope when the driving voltages $(e_b - e_a)$ and $(e_c - e_a)$ respectively change their sign. This brings i_b and i_c to zero at $t = 25\text{ms}$ and $t = 31\text{ms}$ respectively. At $t = 41\text{ms}$ again the condition $e_b - e_a > 0$ is fulfilled, but due to the low induced voltage only a small current is driven, which produces a braking torque and stalls the machine. In all the speed responses, it can be observed that after the speed reaches zero, it remains at zero because the load torque is assumed to be zero at zero speed. Switch S_{ap} short circuit fault is inserted at different instances of the PMSM current response of phase ‘a’. Three instances are in the positive half cycle (Sec1, Sec2 and Sec3 of Figure 3.27) and two instants in the negative half cycle with current is having positive and negative slope.

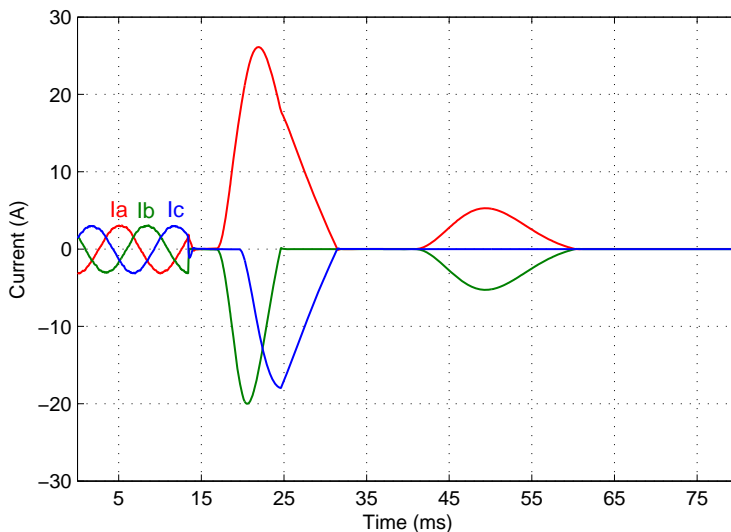


Figure 3.34: Simulated PMSM current response to an uncompensated IGBT S_{ap} short fault when the current is in Sec1 (see Figure 3.27)

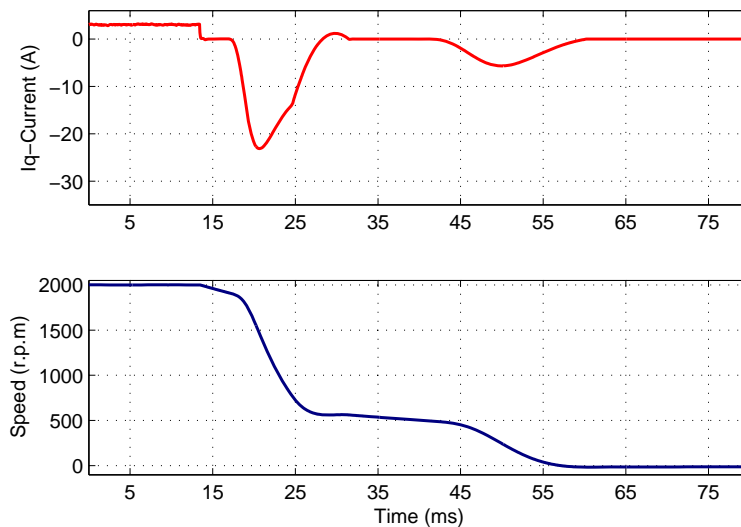


Figure 3.35: Simulated PMSM q-axis current and speed response to an uncompensated IGBT S_{ap} short fault when the current is in Sec1 (see Figure 3.27)

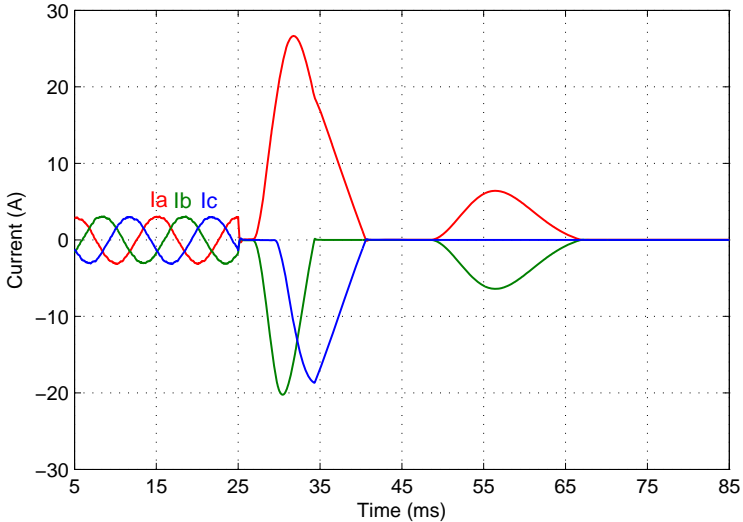


Figure 3.36: Simulated PMSM current response to an uncompensated IGBT S_{ap} short fault when the current is in Sec2 (see Figure 3.27)

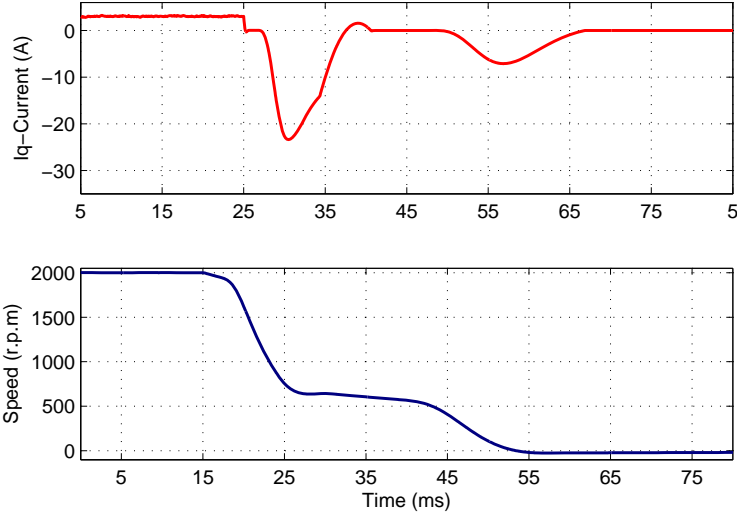


Figure 3.37: Simulated PMSM q-axis current and speed response to an uncompensated IGBT S_{ap} short fault when the current is in Sec2 (see Figure 3.27)

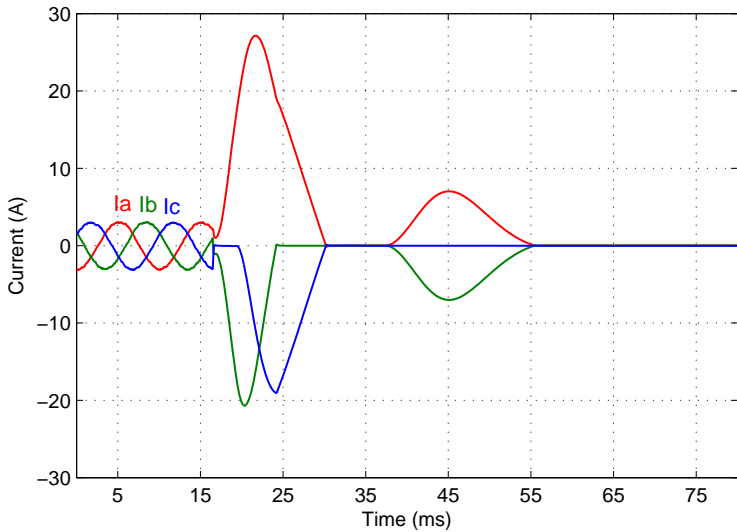


Figure 3.38: Simulated PMSM current response to an uncompensated IGBT S_{ap} short fault when the current is in Sec3 (see Figure 3.27)

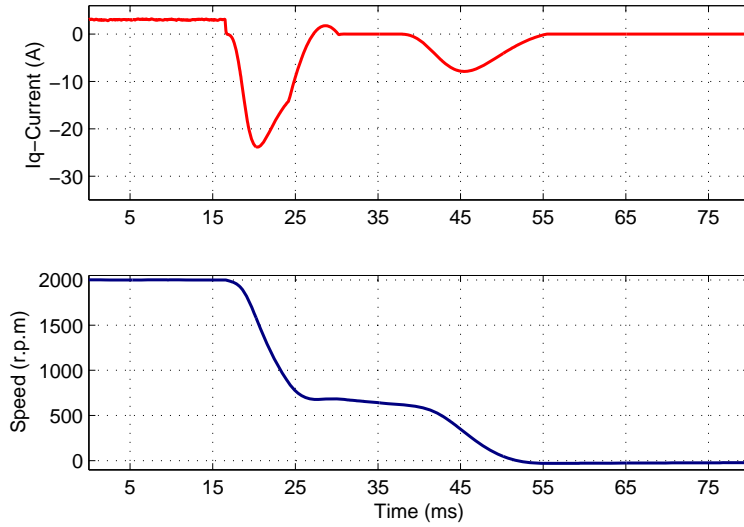


Figure 3.39: Simulated PMSM q-axis current and speed response to an uncompensated IGBT S_{ap} short fault when the current is in Sec3 (see Figure 3.27).

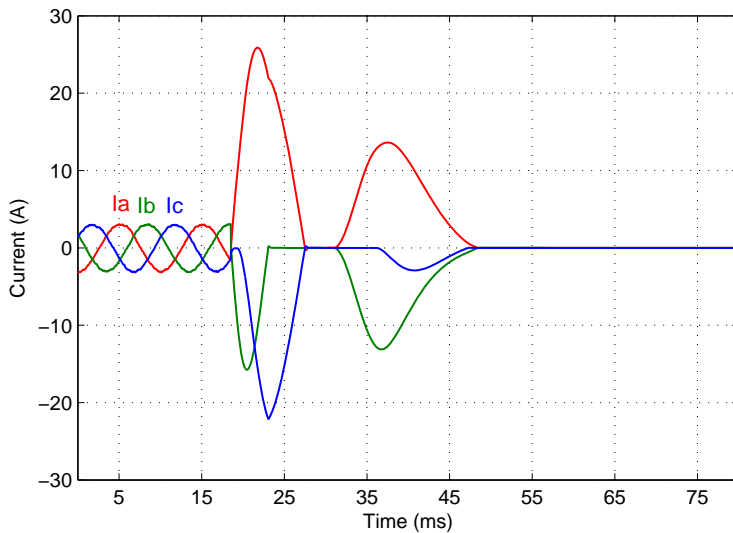


Figure 3.40: Simulated PMSM current response to an uncompensated IGBT S_{ap} short fault when the current is having a negative values and negative slope

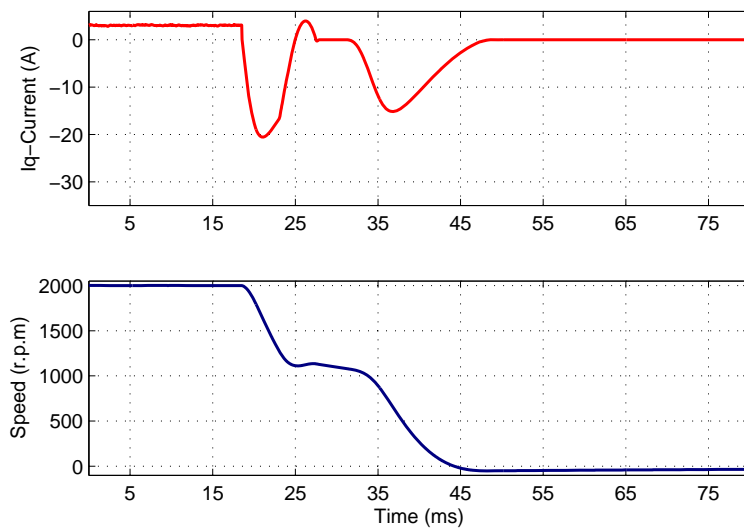


Figure 3.41: Simulated PMSM q-axis current and speed response to an uncompensated IGBT S_{ap} short fault when the current is having a negative values and negative slope

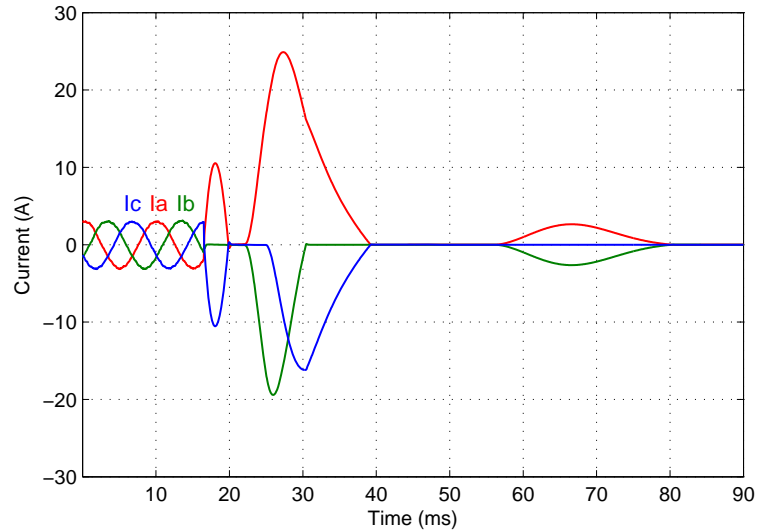


Figure 3.42: Simulated PMSM current response to an uncompensated IGBT S_{ap} short fault when the current is having a negative values and positive slope

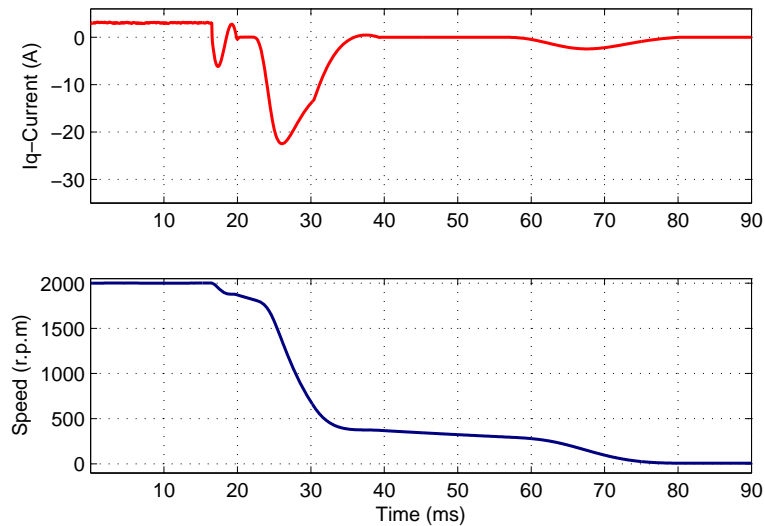


Figure 3.43: Simulated PMSM q-axis current and speed response to an uncompensated IGBT S_{ap} short fault when the current is having a negative values and positive slope

3.5.2 Compensated IGBT short circuit fault

As explained in the section 3.4.4, as soon as the short circuit fault is detected gate signals of all the IGBTs and isolating thyristors are blocked. Current in the faulted phase is monitored and whenever it comes to zero, around $500\mu\text{s}$ delay is provided in order to make sure that corresponding faulted phase isolating thyristors can block full voltage. After this, the redundant leg is inserted in place of faulted leg and gate signals of the faulted leg are transferred to the redundant leg. As soon as the fault is reported to the controller, the integrator values of the current and speed controllers are saved, and these integrators are stopped from further integrating. Figure 3.44 to Figure 3.53 show the different simulated responses of PMSM for the same instants of the faults mentioned in section 3.5.1. From the results in can be observed that the proposed control strategy can successfully isolate fault leg with negligible disturbance to the machine operation and the drive continue to run as in pre-fault case.

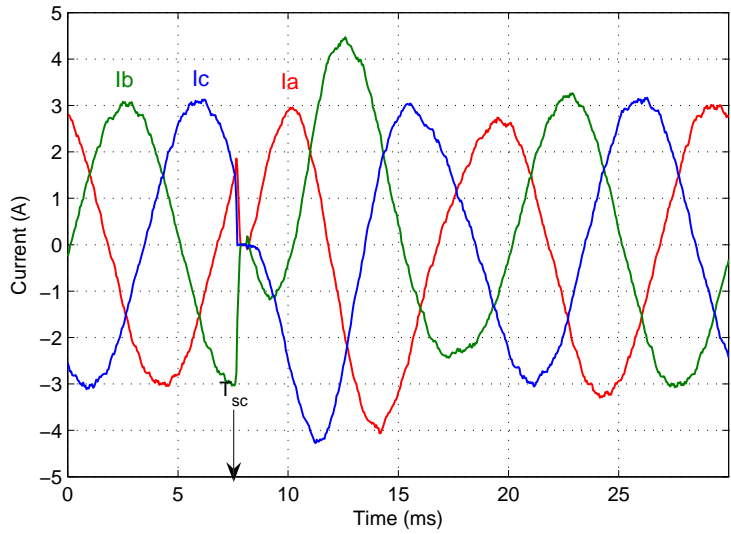


Figure 3.44: Simulated PMSM current response to a compensated IGBT S_{ap} short fault when the current is in Sec1

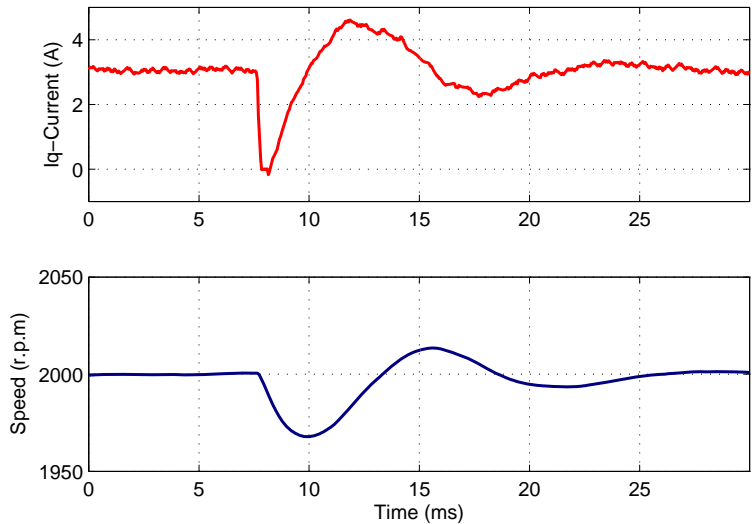


Figure 3.45: Simulated PMSM q-axis current and speed response to a compensated IGBT S_{ap} short fault when the current is in Sec1

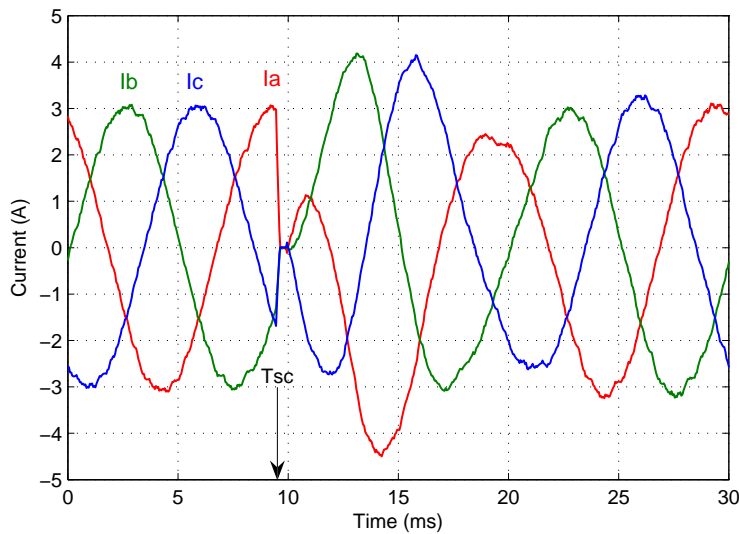


Figure 3.46: Simulated PMSM current response to a compensated IGBT S_{ap} short fault when the current is in Sec2

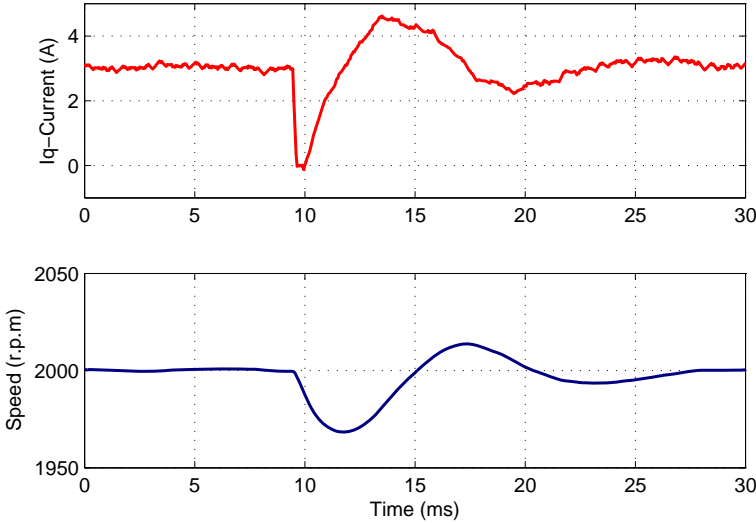


Figure 3.47: Simulated PMSM q-axis current and speed response to an uncompensated IGBT S_{ap} short fault when the current is in Sec2

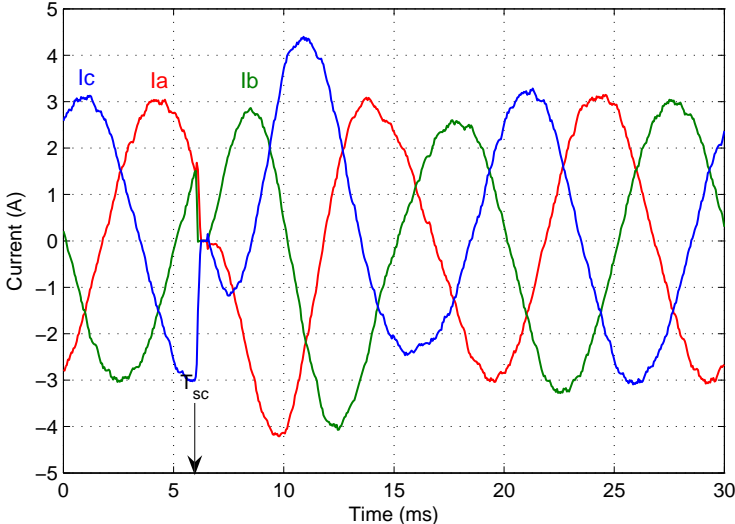


Figure 3.48: Simulated PMSM q-axis current and speed response to a compensated IGBT S_{ap} short fault when the current is in Sec3

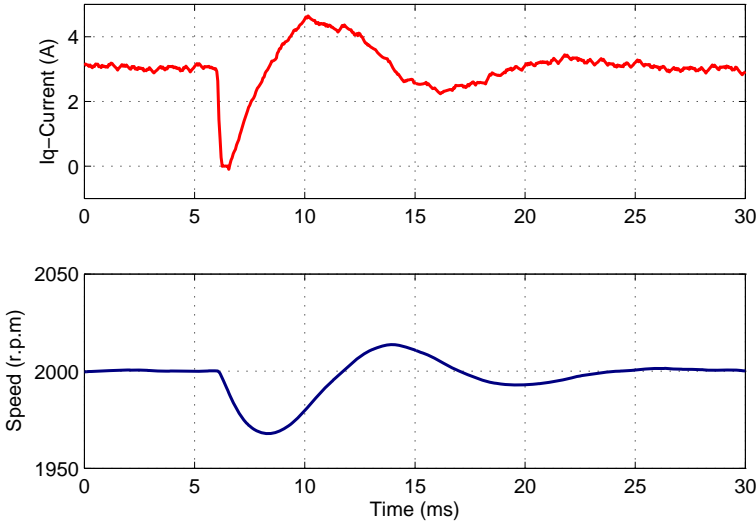


Figure 3.49: Simulated PMSM q-axis current and speed response to a compensated IGBT S_{ap} short fault when the current is in Sec3

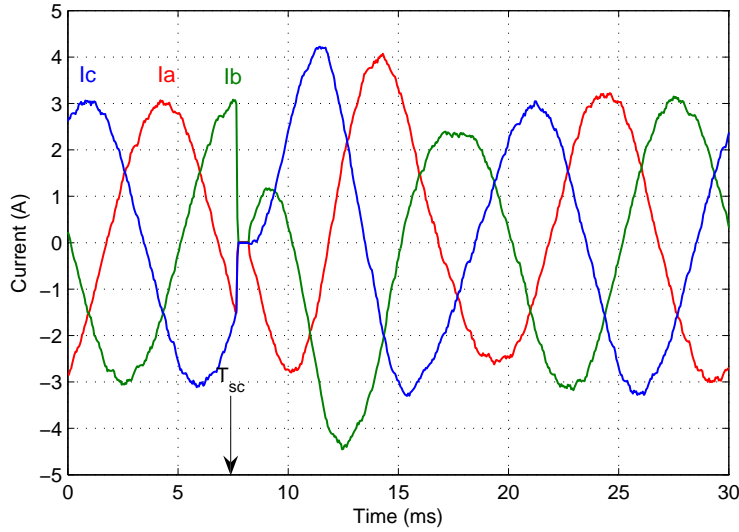


Figure 3.50: Simulated PMSM current response to a compensated IGBT S_{ap} short fault when the current is having a negative values and negative slope.

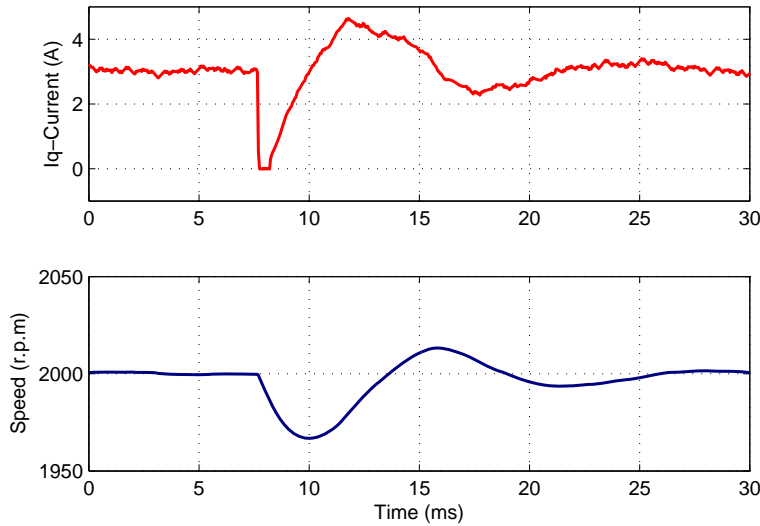


Figure 3.51: Simulated PMSM q-axis current and speed response to a compensated IGBT S_{ap} short fault when the current is having a negative values and negative slope

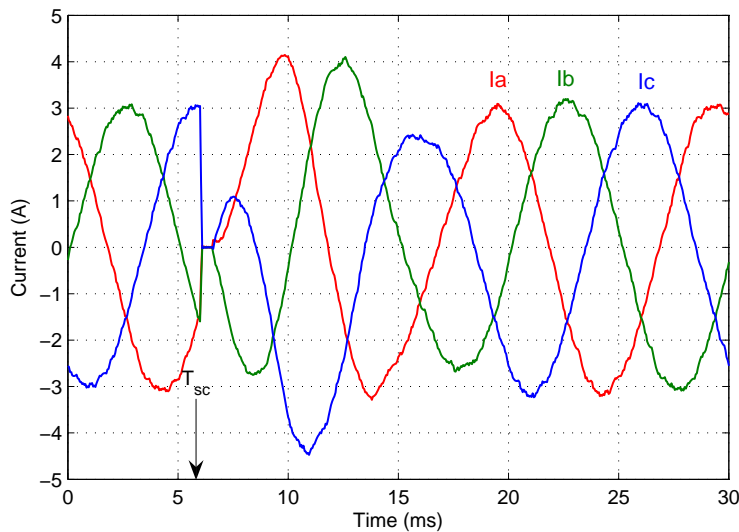


Figure 3.52: Simulated PMSM current response to a compensated IGBT S_{ap} short fault when the current is having a negative values and positive slope

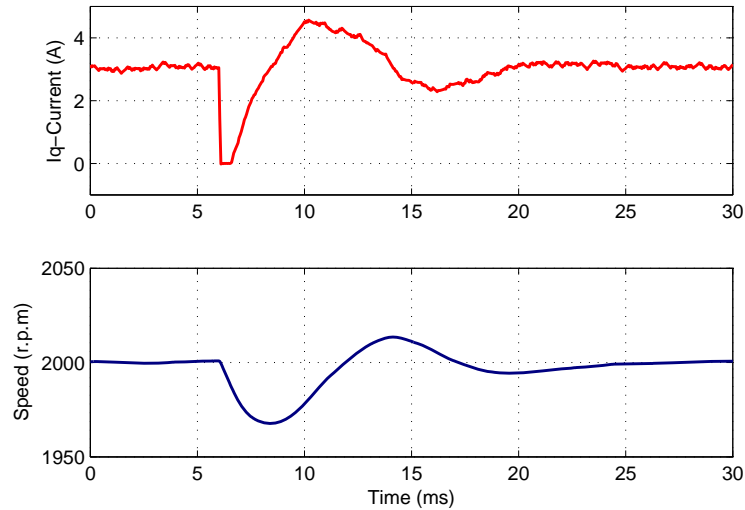


Figure 3.53: Simulated PMSM q-axis current and speed response to a compensated IGBT S_{ap} short fault when the current is having a negative values and positive slope

3.5.3 Compensated IGBT short circuit fault in case of low speed operation

In case of an IGBT short circuit fault, the fault current flowing through the corresponding isolating thyristor should be brought to zero as fast as possible such that there is a negligible disturbance for the drive operation. However, as mentioned in the section 3.4.4, for high current at low speed (standstill) with low or zero back-EMFs, the time to reach zero current will be long until the energy initially stored in the inductances is dissipated. As calculated in the section 3.4.4, for standstill operation and for a load current of 5A when the IGBT short fault is occurred on switch S_{ap} , the time to reach the current to zero is around 5.3ms. A similar case is simulated here but for a speed of 10 r.p.m. From the result it is observed that the time to reach the zero crossing is around 5ms and after that 500 μ s of time delay is inserted before switching to the redundant leg. From the result of the speed response it is clear that the speed goes almost to zero but attains the reference value as soon as the redundant leg is turned ON. Figure 3.54 and Figure 3.55 shows the response of the PMSM for an IGBT S_{ap} short circuit fault when the speed is at 10 r.p.m and current is at positive peak. Similarly, Figure 3.56 and Figure 3.57 are when the current is at negative peak.

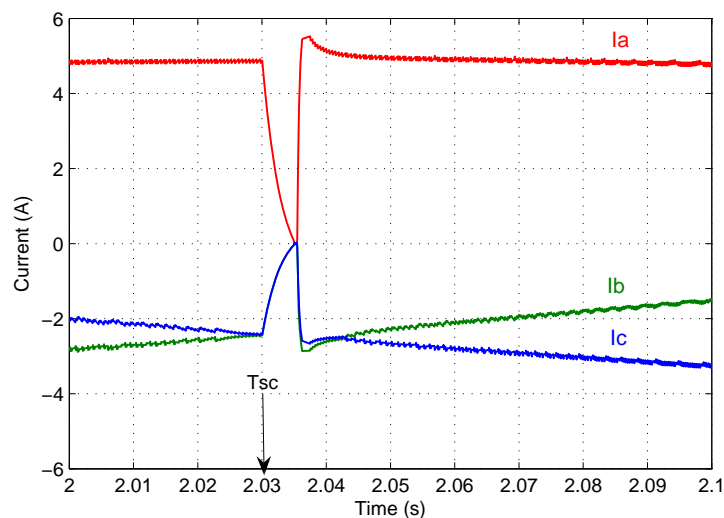


Figure 3.54: Simulated PMSM current response to a compensated IGBT S_{ap} short fault when the current is having a positive peak value of 5A and the machine is running at 10 rpm

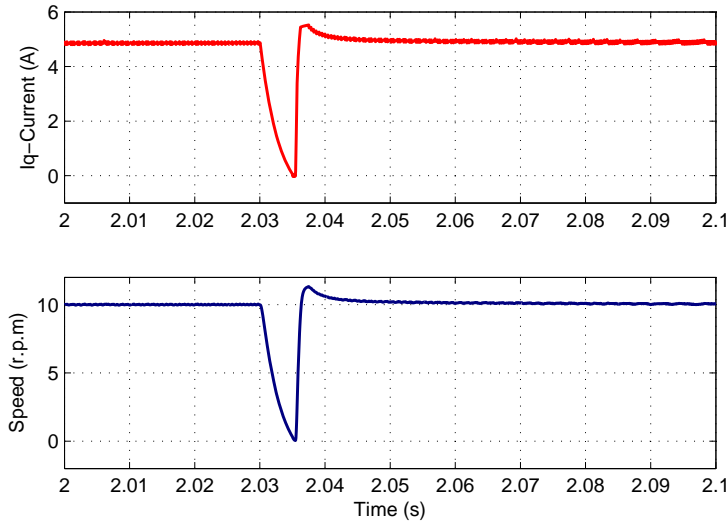


Figure 3.55: Simulated PMSM q-axis current and speed response to a compensated IGBT S_{ap} short fault when the current is having positive peak of 5A and machine is running at 10 rpm

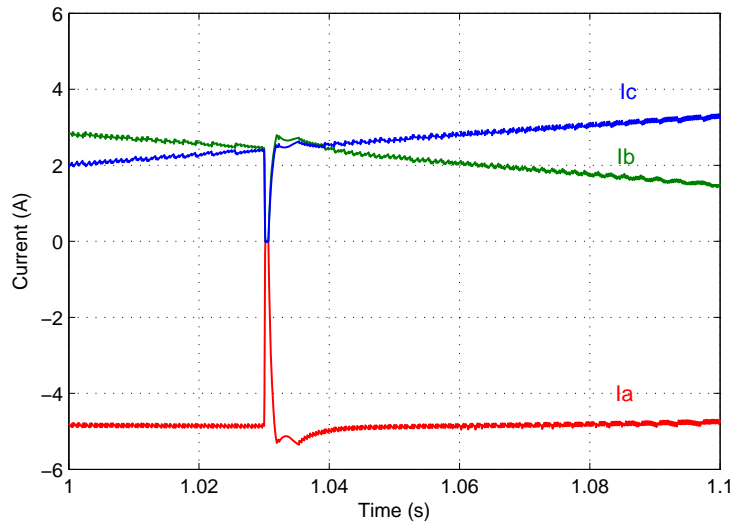


Figure 3.56: Simulated PMSM current response to a compensated IGBT S_{ap} short fault when the current is having a negative peak value of 5A and the machine is running at 10 rpm

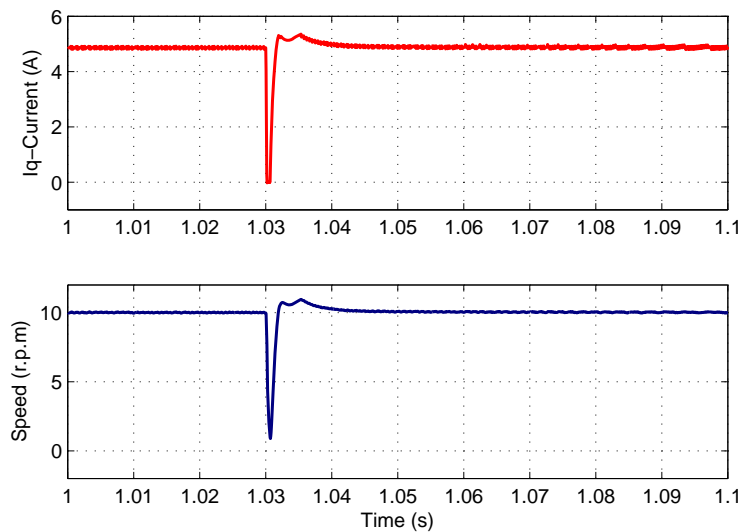


Figure 3.57: Simulated PMSM q-axis current and speed response to a compensated IGBT S_{ap} short fault when the current is having negative peak of 5A and machine is running at 10 rpm

3.6 Experimental results

3.6.1 Experimental setup description

A laboratory prototype has been built for testing the proposed inverter with increased availability, driving a field oriented controlled PMSM. Figure 3.58 shows the block diagram of the developed experimental setup. For the sake of testing the inverter for its fault tolerance capability, faults are always inserted only on the phase leg ‘a’ of the inverter. In this way, for the experiment, redundant leg inserting thyristors can be avoided. So the midpoint of redundant leg is directly connected to the phase terminal ‘a’ of the machine as shown in Figure 3.58. The PMSM is coupled with another PMSM which is used as a load machine. A three-phase variable resistance is connected at the output terminals of the load machine which provides a load torque proportional to the speed. The control algorithm is implemented in a Texas Instrument's F2812 fixed point digital signal processor (DSP) evaluation board. Generation of command signals for the converter, data acquisition, fault insertion, fault compensations are done through software written in ‘C’ language. All the necessary variables are stored in the external memory of the DSP during the control implementation and are later plotted using MATLAB[®]. IGBTs are used as main switching devices and thyristors are used for isolating the fault leg. Results are produced for both uncompensated fault and compensated fault case. To show the uncompensated fault currents, the IGBTs of this setup are heavily oversized (150A). Uncompensated fault case explains the behavior of the standard two-level inverter after the fault and compensated case is the proposed inverter's response to different faults. PMSM parameters are presented in Table 3.2 and a picture of experimental setup is included in Figure 3.59.

Table 3.2: PMSM parameters

Parameter	Quantity
Rated Power (P_N)	2.2 [kW]
Rated Torque (M_N)	5.2 [Nm]
Rated speed (n_N)	4100 [r.p.m]
Rated voltage (v_{l-l})	350 [V]
Rated Current (i_N)	3.5 [A]
Stator inductance per phase (L_s)	6.5 [mH]
Stator resistance per phase (R_s)	2.1 [Ω]
Torque constant (K_T)	1.1
Calculated Permanent Magnet flux from rated values (Ψ_{PM})	0.1739 [Wb]
Motor Inertia (J_m)	0.42×10^{-3} [kg.m ²]
Load Machine Inertia (J_L)	0.15×10^{-3} [kg.m ²]
Assumed coupling and encoder Inertia (J_c)	0.3×10^{-3} [kg.m ²]
Total Drive inertia :	0.87×10^{-3} [kg.m ²]

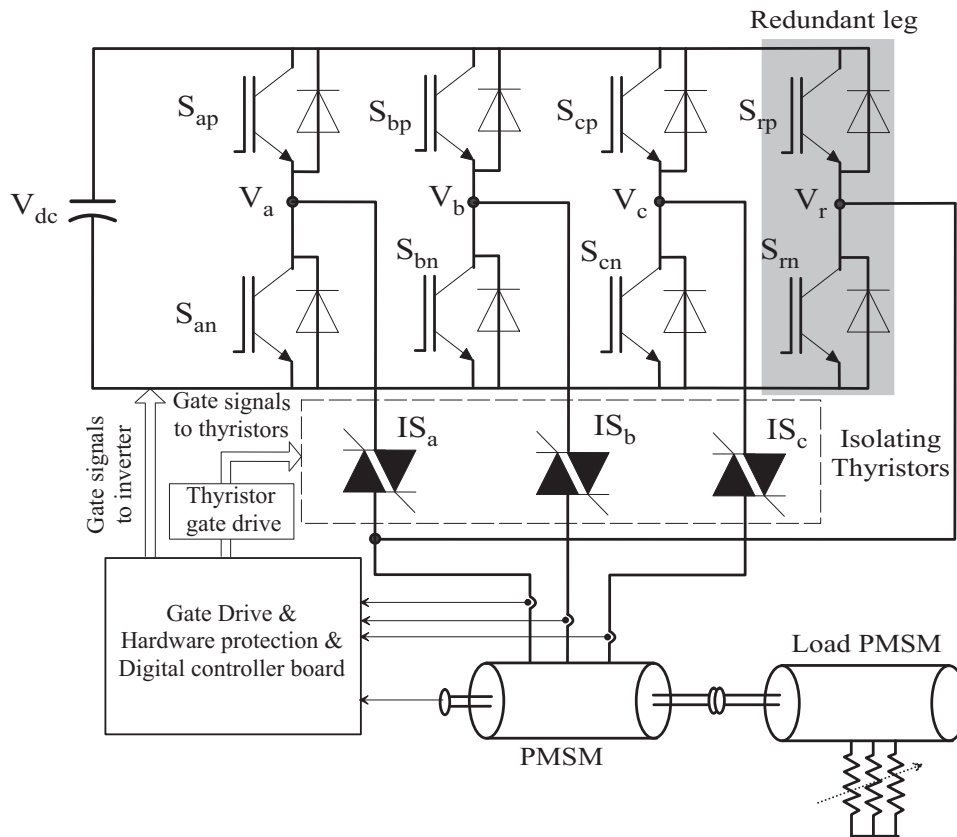


Figure 3.58: Schematic diagram of the experimental setup

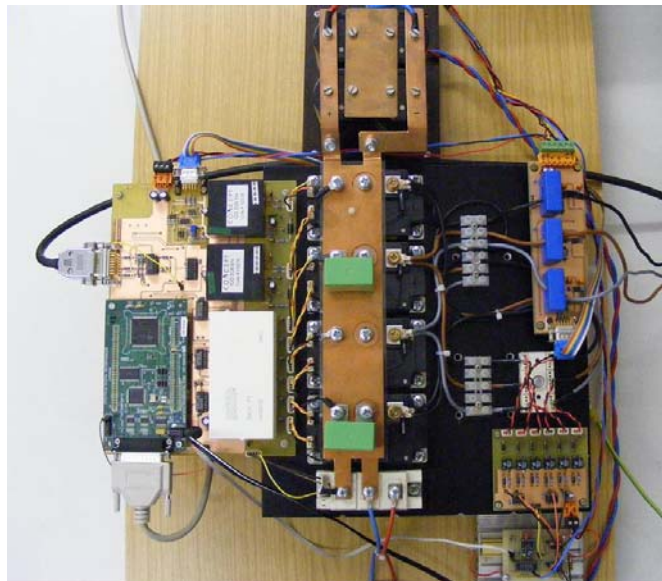


Figure 3.59: Experimental setup

3.6.2 Experimental results-IGBT open circuit fault

3.6.2.1 Uncompensated IGBT open circuit fault

An open-circuit fault is created by turning one of the IGBT gate signals permanently OFF. As explained before no separate fault detection method is used. A worst case of fault detecting time is assumed in order to verify the inverter performance. Figure 3.60 and Figure 3.61 show the current, torque producing q-axis current and speed response of the PMSM to an open-circuit fault in the upper IGBT of phase leg 'V_a'. Inverter structure in case of the upper IGBT open circuit fault, in

phase leg ' V_a ', is shown in Figure 3.24. In the case of upper IGBT (S_{ap}) open-circuit fault, the positive half of the corresponding phase current is zero. In case of the IGBT open circuit fault, the machine continues to rotate with oscillations as a consequence of the huge oscillations in the q-axis current which can be observed in Figure 3.61.

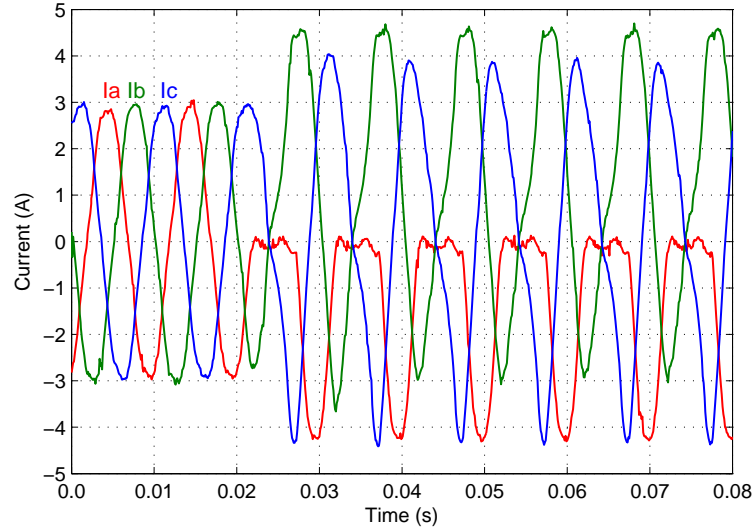


Figure 3.60: PMSM current response to an uncompensated IGBT S_{ap} open fault (Experimental result)

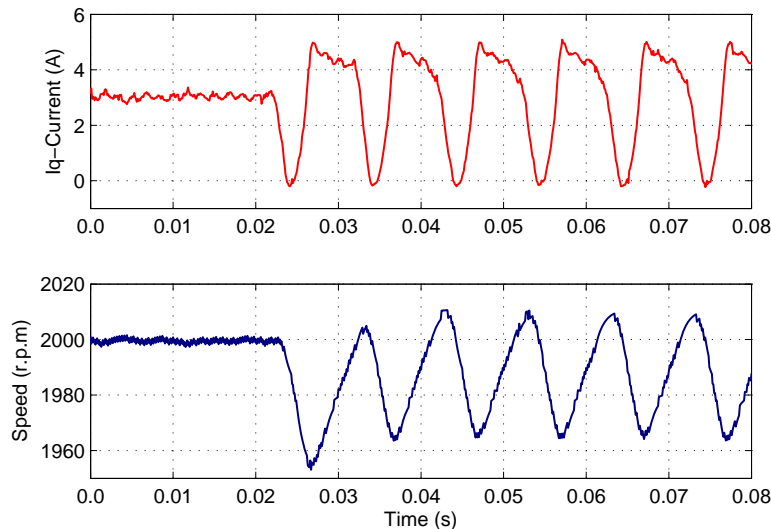


Figure 3.61: PMSM q-axis current and speed response to an uncompensated IGBT S_{ap} open fault (Experimental result)

3.6.2.2 Compensated IGBT open circuit fault

Figure 3.62 and Figure 3.63 shows the current, torque producing q-axis current and speed response of the PMSM to a compensated IGBT open circuit fault in the upper IGBT (S_{ap}) of the leg V_a . T_{oc} is the point in time where the fault is inserted and after one fundamental cycle of current, the gate signals to the complementary IGBT is stopped and also to the corresponding isolating thyristors. The gate signals of the faulted leg are transferred to the redundant leg and corresponding redundant leg inserting thyristors are turned ON. From the speed response of the machine it can be observed that, in the worst case, there is little disturbance in the machine speed and after that the machine continues to run same as in the pre-fault situation. The disturbance during the fault can be further reduced if the fault detection is fast, which is possible with methods mentioned before.

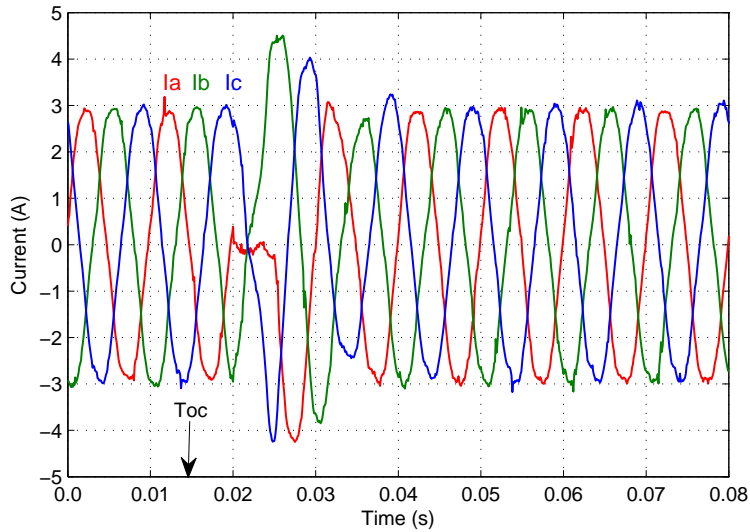


Figure 3.62: PMSM current response to a compensated IGBT S_{ap} open fault (Experimental result)

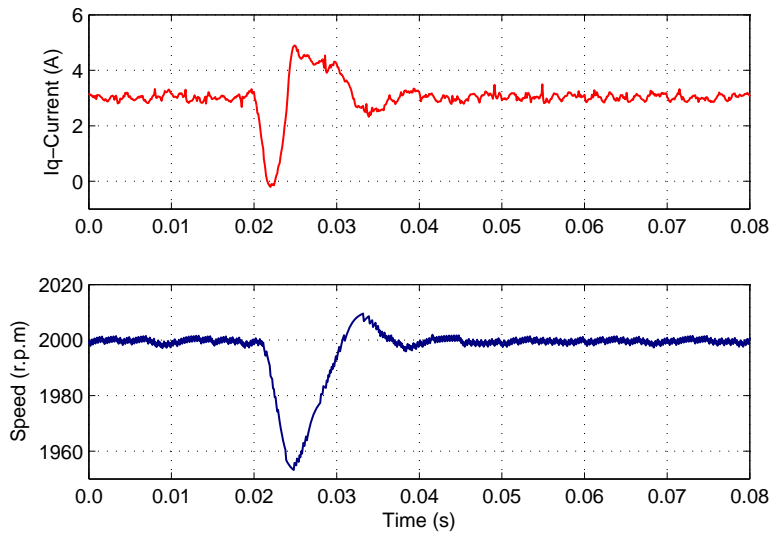


Figure 3.63: PMSM q-axis current and speed response to a compensated IGBT S_{ap} open fault (Experimental result)

3.6.3 Experimental results-IGBT short circuit fault

Short circuit faults are inserted by the DSP by turning the gate signal permanently ON. Special individual drivers are used for short circuit insertion. These drivers will not block their gate signals even in the case of short circuit but indicate the fault status.

3.6.3.1 Uncompensated IGBT short circuit fault

Figure 3.64 to Figure 3.71 shows the PMSM response to an upper IGBT fault of the leg ‘ V_a ’ in the case of the standard inverter. As soon as short circuit fault in one of the IGBT is detected, hardware protection disables the gate signals to all the remaining IGBTs. Now the inverter structure is as shown in Figure 3.26. The machine’s response depends on the current at the instant of failure, machine parameters and load. In order to analyze the machine response, short circuit fault is created at four instances of a fundamental current cycle. Two are in the positive half cycle and two are in the negative half cycle with the current is having the positive and negative slope. T_{sc} is the point in time where the short circuit occurred at the upper IGBT of phase leg ‘ V_a ’. As phase ‘ V_a ’ is always

connected to positive DC bus, phase current i_a increases in the positive direction till it is compensated by back-EMF of the machine. From the result of Figure 3.66 it can be observed that current takes at least one fundamental cycle of current to reach the zero crossing. For this case, it can be observed that by the time when current reaches its first zero crossing, speed almost fell down to one-third of its reference value which is 2000 r.p.m. In all the other cases, the zero crossing of the current is early compared to the case of Figure 3.66.

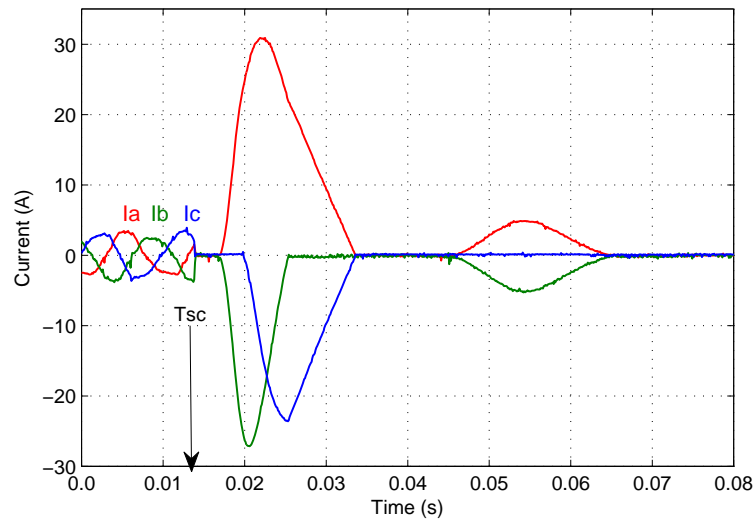


Figure 3.64: PMSM current response to an uncompensated IGBT S_{ap} short fault when the current is in Sec1 (see Figure 3.27) (Experimental result)

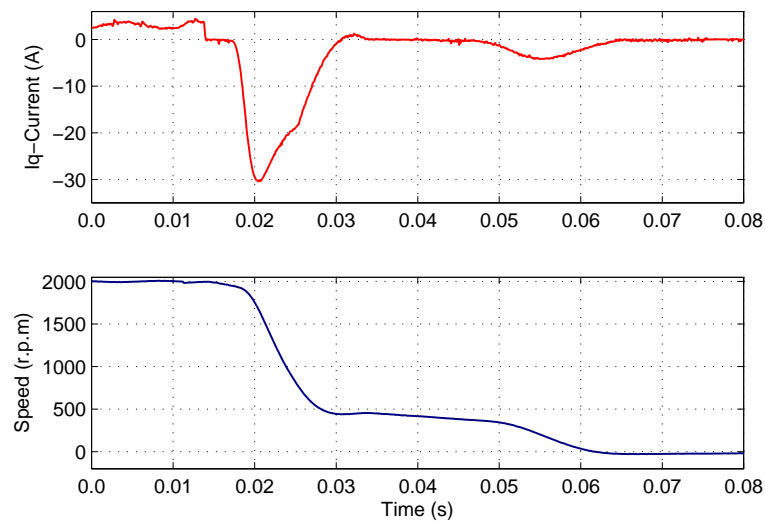


Figure 3.65: PMSM q-axis current and speed response to an uncompensated IGBT S_{ap} short fault when the current is in Sec1 (see Figure 3.27) (Experimental result)

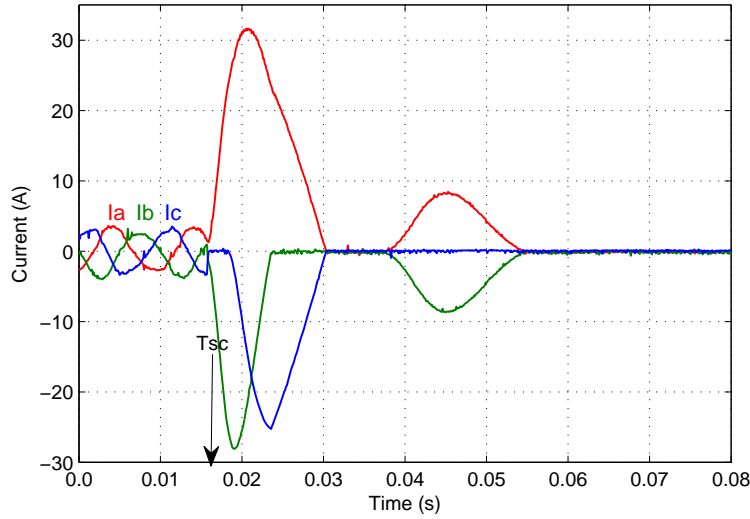


Figure 3.66: PMSM current response to an uncompensated IGBT S_{ap} short fault when the current is in Sec3 (see Figure 3.27) (Experimental result)

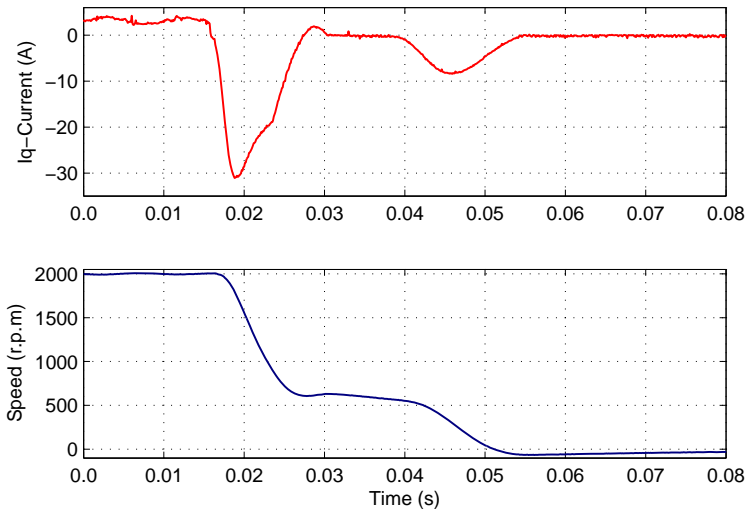


Figure 3.67: PMSM q-axis current and speed response to an uncompensated IGBT S_{ap} short fault when the current is in Sec3 (see Figure 3.27) (Experimental result)

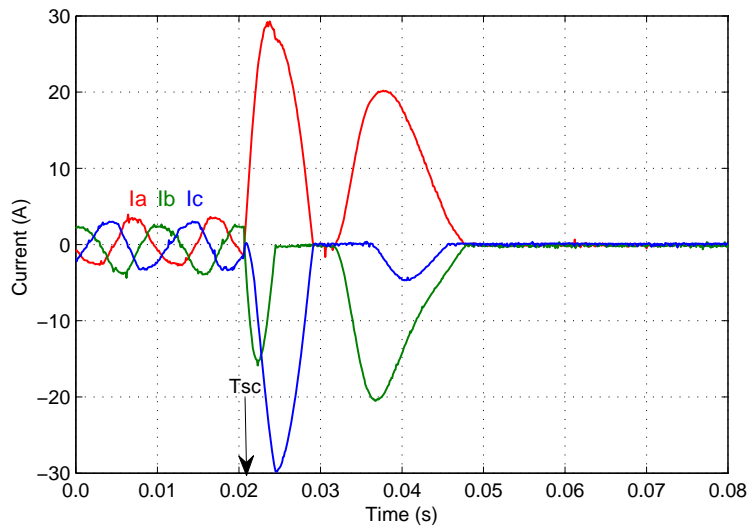


Figure 3.68: PMSM current response to an uncompensated IGBT S_{ap} short fault when the current is having a negative values and negative slope (Experimental result)

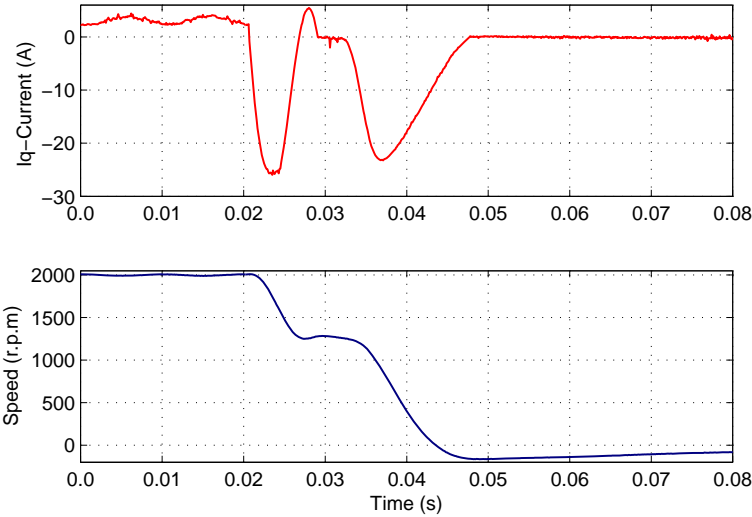


Figure 3.69: PMSM q-axis current and speed response to an uncompensated IGBT S_{ap} short fault when the current is having a negative values and negative slope (Experimental result)

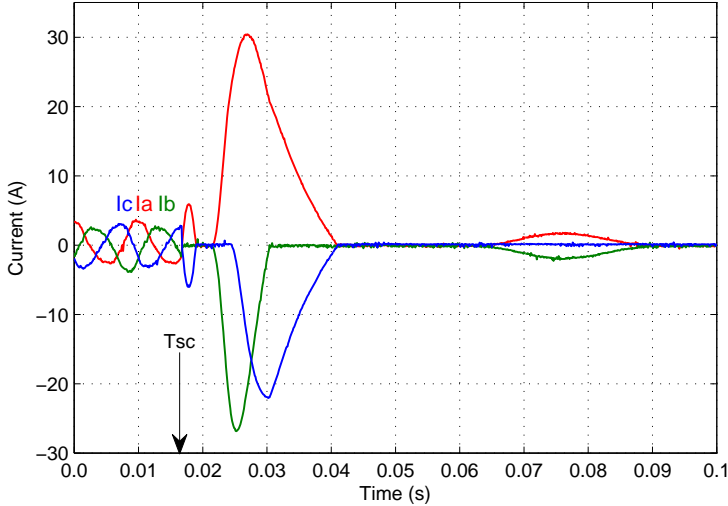


Figure 3.70: PMSM current response to an uncompensated IGBT S_{ap} short fault when the current is having a negative values and positive slope (Experimental result)

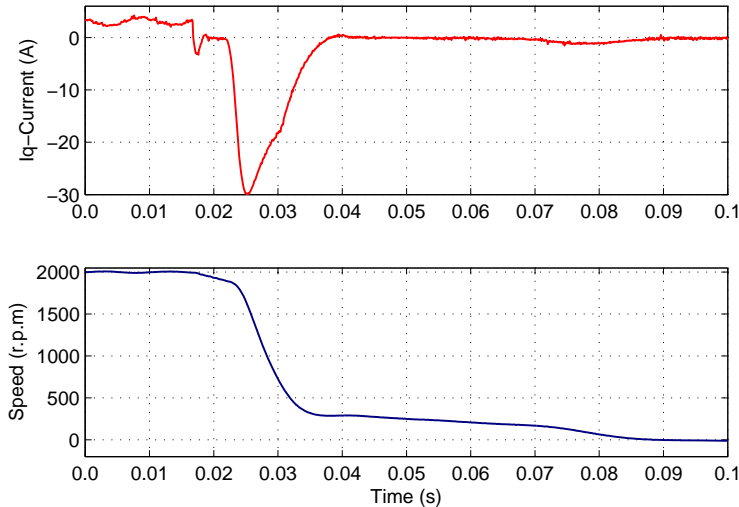


Figure 3.71: PMSM q-axis current and speed response to an uncompensated IGBT S_{ap} short fault when the current is having a negative values and positive slope (Experimental result)

3.6.3.2 Compensated IGBT short circuit fault

As soon as the short circuit is detected in one of the IGBTs, hardware protection disables the gate signals to all IGBTs and to all isolating thyristors. The fault is further reported to the controller. The controller monitors the phase currents of the machine and as soon as all the currents become zero it provides further a delay of around $500\mu\text{s}$ to make sure that the fault leg isolating thyristor is turned OFF and can withstand forward voltage. In order to turn OFF the thyristor, the load current must be reduced below its holding current for sufficient time to allow all the mobile charge carriers to vacate the junction. After the short circuit current has reached zero, to make sure that isolating thyristors are fully turned OFF and can withstand forward voltage, time delay (around $500\mu\text{s}$) is provided before the new leg is inserted and reset command is issued to hardware protection. After this, the new leg is inserted and gate signals of the faulted leg are transferred to the new leg. Figure 3.72 to Figure 3.81 show the machine response to compensated short circuit fault. Short circuit faults are created at the same instances as in the uncompensated cases, in order to show that the thyristors can successfully isolate the faulted leg. From all the responses below it is clear that fault compensation is fast and there is negligible disturbance in the machine response.

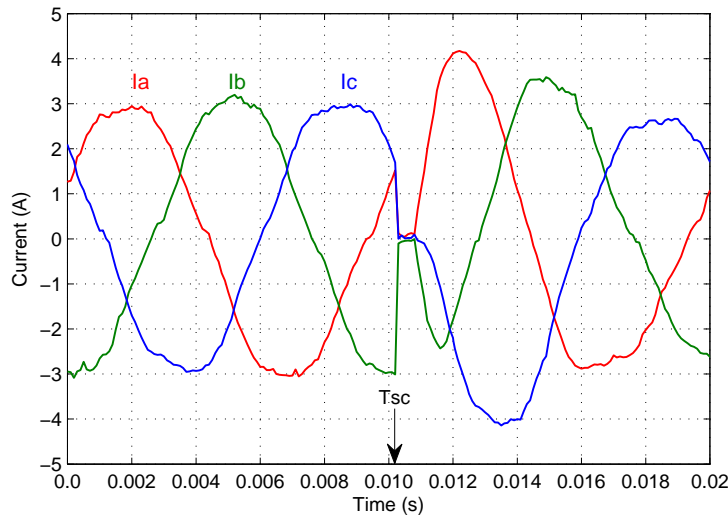


Figure 3.72: PMSM current response to a compensated IGBT S_{ap} short fault when the current is in Sec1 (Experimental result)

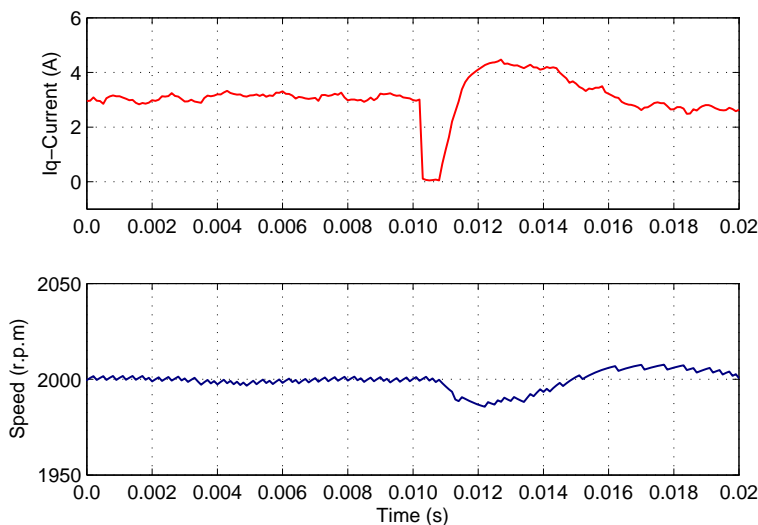


Figure 3.73: PMSM q-axis current and speed response to a compensated IGBT S_{ap} short fault when the current is in Sec1 (Experimental result)

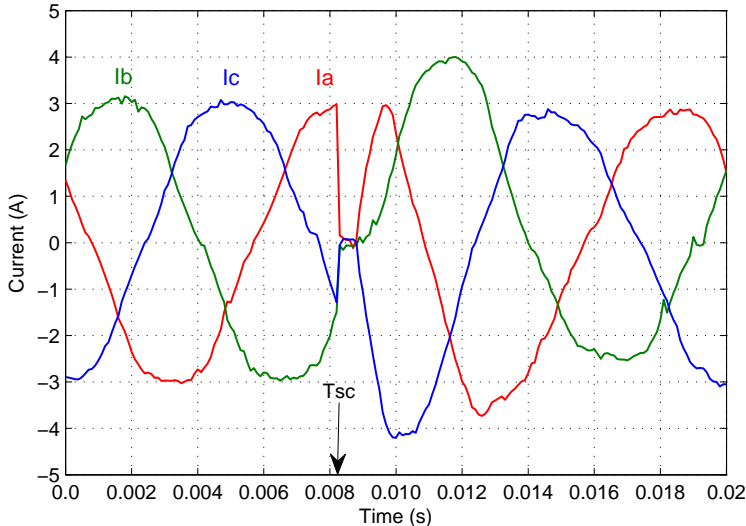


Figure 3.74: PMSM current response to a compensated IGBT S_{ap} short fault when the current is in Sec2 (Experimental result)

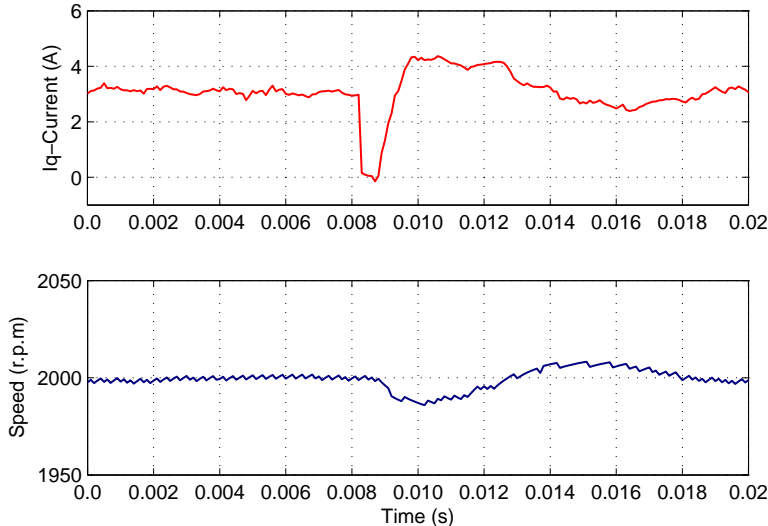


Figure 3.75: PMSM q-axis current and speed response to a compensated IGBT S_{ap} short fault when the current is in Sec2 (Experimental result)

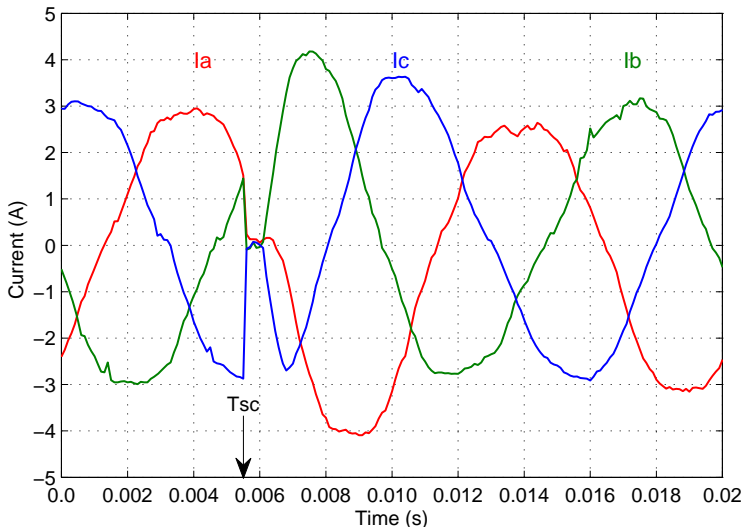


Figure 3.76: PMSM current response to a compensated IGBT S_{ap} short fault when the current is in Sec3 (Experimental result)

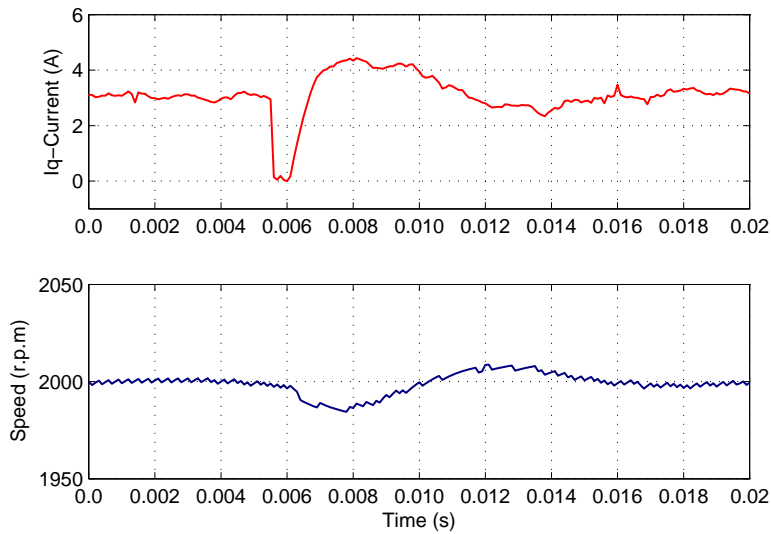


Figure 3.77: PMSM q-axis current and speed response to a compensated IGBT S_{ap} short fault when the current is in Sec3 (Experimental result)

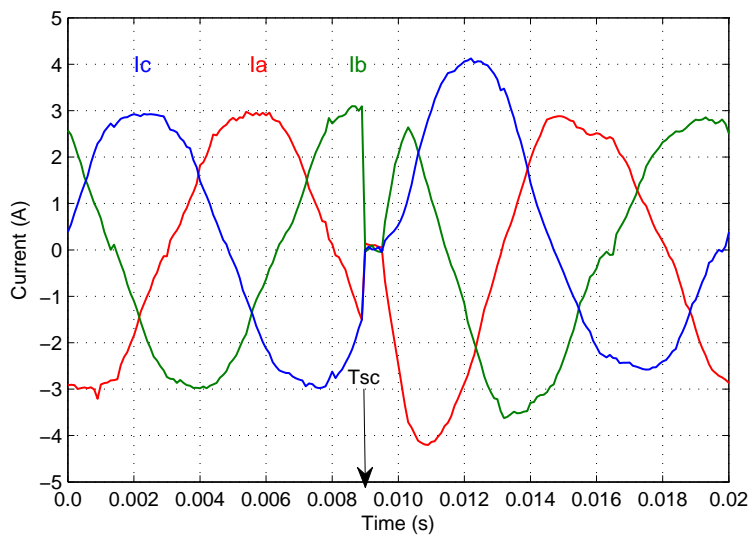


Figure 3.78: PMSM current response to a compensated IGBT S_{ap} short fault when the current is having a negative values and negative slope (Experimental result)

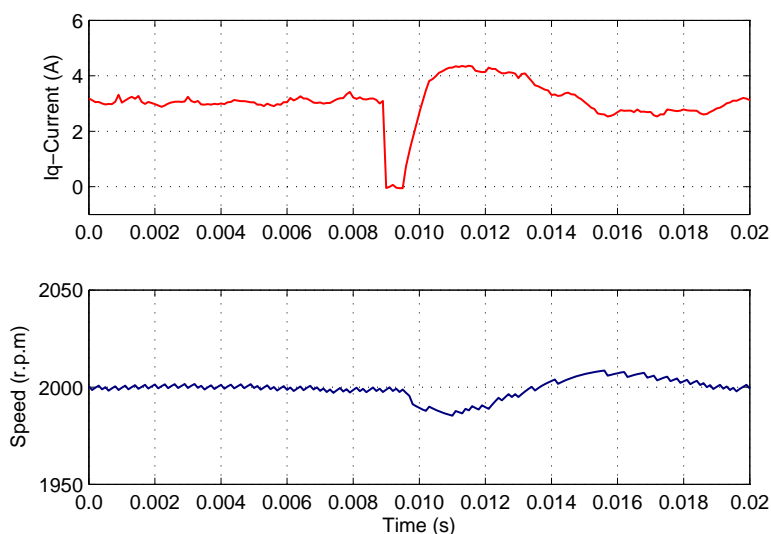


Figure 3.79: PMSM q-axis current and speed response to a compensated IGBT S_{ap} short fault when the current is having a negative values and negative slope (Experimental result)

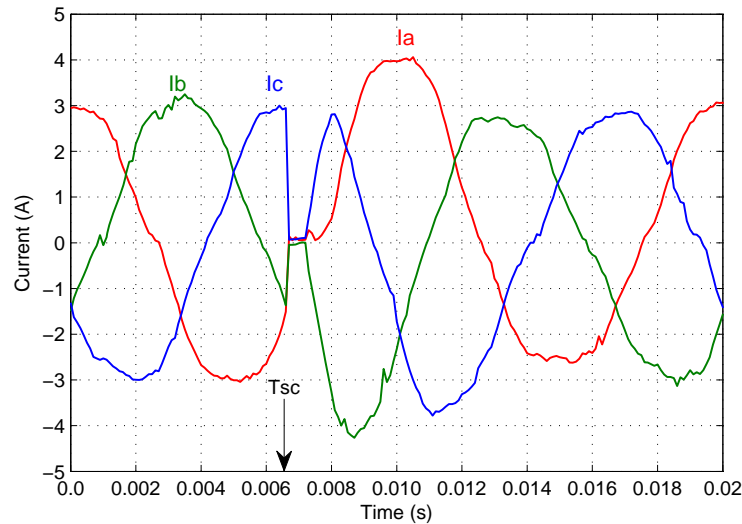


Figure 3.80: PMSM current response to a compensated IGBT S_{ap} short fault when the current is having a negative values and positive slope (Experimental result)

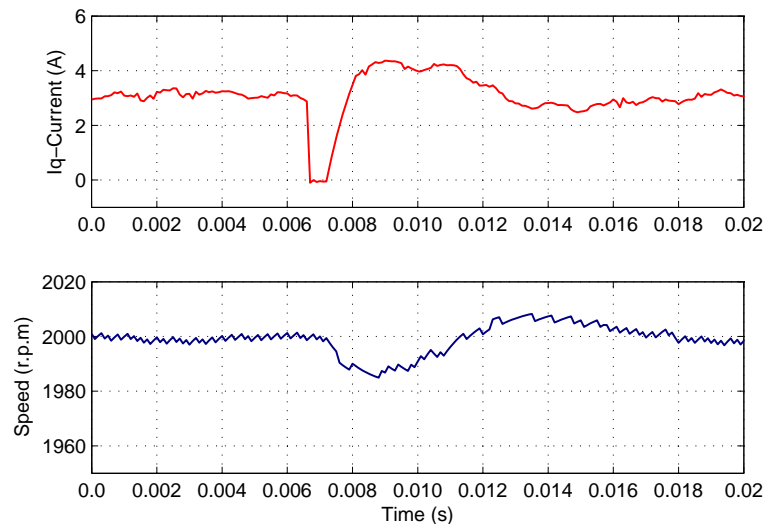


Figure 3.81: PMSM q-axis current and speed response to a compensated IGBT S_{ap} short fault when the current is having a negative values and positive slope (Experimental result)

3.7 Conclusions

In this chapter, modifications to the existing inverter topologies is proposed, which will improve the availability of a PMSM drive. Solutions to the IGBT short and open circuit faults are presented. As a first step, different topologies available in the literature, their advantages and disadvantages are discussed. By making the necessary modifications to the existing topologies, a new topology is proposed such that it will compensate both IGBT short and open circuit faults, delivering the rated post-fault output without significant disturbance to the drive operation. An extra redundant leg used along with the standard three legs of the three-phase two-level inverter and back-to-back connected thyristors are used to isolate the faulted leg and insert the redundant leg. A detailed analysis is done, which shows that thyristors can successfully isolate the faulted leg in case of the IGBT short circuit fault. Simulations and experimental results are presented for different fault cases. The results show that, proposed inverter can compensate and work for both IGBT short and open circuit faults without any significant disturbance to the drive operation.

4 Feedback Sensors with Increased Availability

4.1 Introduction

For an efficient and high dynamic control of a PMSM, feedback information from the machine such as position and current is necessary. From the information of feedback sensors, closed loop control such as FOC can be implemented. FOC of the PMSM provides high dynamic torque control. For proper operation of closed loop control of a PMSM, proper operation of the feedback system is necessary. However, sensors in the drive are not fault free, but they are subjected to faults such as noise, offset in gain, power supply failure or cable disconnection or failure of ICs inside the sensors. Any fault in the feedback system sends incorrect signals to the controller which leads to the degradation of the drive performance or a complete shutdown of the drive [BEN97].

A position encoder or position sensor is an electro-mechanical device which converts the position information of the machine rotor in to an analog or digital code. The output of the position encoder provides the information about the position of rotor which is further processed into information such as speed. The position encoder is mounted on the shaft of the machine and the position information of rotor is send to the controller through analog or digital signals. Different fault modes in a position sensor are cable and supply disconnections, missing pulses due to dirt in the encoder disc, or no pulses received due to a blocked photo receiver [THY99]. A disconnected cable or power supply failure to the encoder leads to interrupted position information of machine to the controller. The open loop effect of missing pulses due to dirt in the encoder disc is a lower estimated speed. The closed loop effect greatly depends on the employed control scheme. In order to make the drive tolerant to position sensor faults, first it is important to detect the fault in the position sensor. Several model based fault detection schemes are proposed in [FRA91], [PAT95] and [ISE06], wherein the model of the load is used to indicate the occurrence of the fault. The authors of [SCH06] proposed the idea of detecting position sensor faults by comparing the output of the position sensor with the estimation of a sensorless algorithm as shown in Figure 4.1.

Hall-effect current sensors are used for an accurate measurement of current with high bandwidth and to provide galvanic isolation to the current measurement. The information from the current measurement is used to implement closed control algorithms such as FOC or DTC of the electric drives. Any fault in the current measurement leads to failure in the closed loop control and subsequent drive shutdown. So, it is important to detect the current sensor faults and take corresponding remedial actions. Some of the current sensor fault detection and isolation (FDI) techniques are presented in literature. In [ABD10] estimators, in [GAL10] a signal-based approach and in [ROT09a], [EDW06], [ROT09b] observers are presented for current sensor fault tolerance. These methods are developed based concept that only two phases of the machine currents are measured and third phase current is computed from the information of the measured two phases, which is possible for a three phase machine with isolated neutral. Machine currents are estimated using different observers, estimators and models and they are compared with the measured currents in order to detect the faults in the current sensors. If a fault is detected in any current sensor, then the current measurement is replaced by the current estimation. A shortcoming of these methods is

model-based methods and estimators are sensitive to parameter variations and/or uncertainties, while signal-based methods present a lack of performance with a closed-loop controller.

The minor faults such as gain drift and non-zero offset would result in torque pulsations synchronized with the inverter output frequency [MEI10]. The faults including the offset and gain drift can be easily detected when the machine is not running [YU05]. Authors of [BAH09] used a simple method based on using three current sensors and detecting the sudden failure in the current sensor when the machine is running. This simple method is used in this work which is effective in detecting any sudden current sensors outages. Here this simple method is implemented with some assumptions and a sophisticated method which detects the current sensor fault in all the cases is left for the future task.

4.2 Position sensorless control of PMSM to increase the drive availability

There are several possibilities to detect encoder faults. Some are based on an abrupt change in the measured speed, which would physically not be possible. Such a step change can be caused by encoder internal problems (e.g. loss of light in optical encoder) or by interrupting the sensor's cable. Here we use a back-EMF based sensorless position estimation method to detect the failure of the position sensor. The estimated position or speed is constantly compared with the one measured using the encoder. Any deviation in the difference between the estimated and measured position (or) speed, beyond a specified tolerance, is considered as failure in the position encoder, under the condition that there is no failure in the current measurement. In order to estimate the position of the PMSM, a disturbance observer is used. The disturbance observed is based on the electrical model of the machine and it estimates the back-EMF.

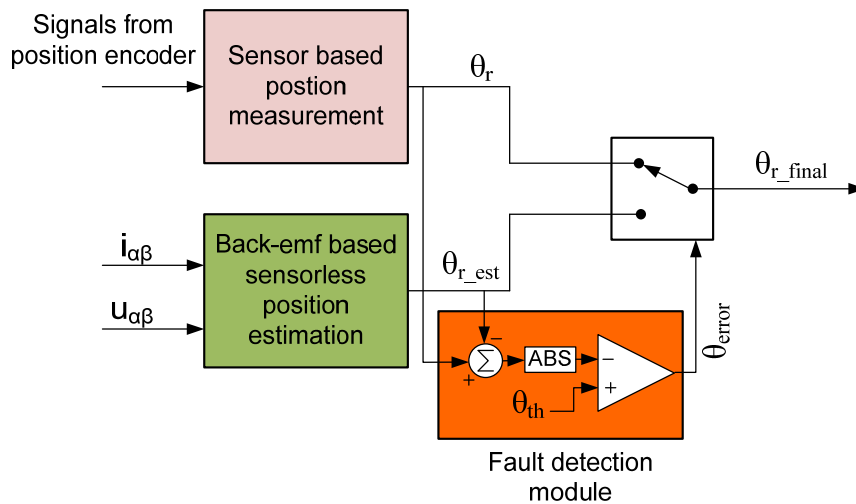


Figure 4.1: Position sensor fault detection

The voltage equation of the PMSM in stationary reference frame can be written as,

$$\begin{bmatrix} u_\alpha \\ u_\beta \end{bmatrix} = R \cdot \begin{bmatrix} i_\alpha \\ i_\beta \end{bmatrix} + \frac{d}{dt} \begin{bmatrix} \psi_{L,\alpha} \\ \psi_{L,\beta} \end{bmatrix} + \begin{bmatrix} e_\alpha \\ e_\beta \end{bmatrix} \quad (4.1)$$

Where u_α , u_β , i_α , i_β , $\psi_{L,\alpha}$, $\psi_{L,\beta}$ are the components of the stator voltage, current and current dependent flux linkage vectors, respectively. R is the phase resistance of the stator windings. e_α , and e_β are the EMF components which can be defined as $-K_E \cdot \omega_e \cdot \sin\theta_e$ and $K_E \cdot \omega_e \cdot \cos\theta_e$. Where, K_E is the EMF constant, ω_e is electrical angular speed of the rotor and θ_e rotor position in electrical angles.

The equation (4.1) has a term of the EMF $e_{\alpha,\beta}$, which is regarded as a kind of disturbance voltage, and the voltage $e_{\alpha,\beta}$ is estimated using the disturbance observer. Usually, the voltages $e_{\alpha,\beta}$ varies sinusoidally, but in order to develop a disturbance observer it is assumed that $\frac{de}{dt} = 0$. The estimation error caused by this assumption is very small which can be neglected [TOM98]. As an error function of the observer, the difference between the measured and estimated currents is used. Based on the above assumptions, the equations of the disturbance observer can be written as [TOM98, LEI07] and [MIH10],

$$\frac{d\hat{\psi}_{L,\alpha}}{dt} = u_{\alpha}^* - R \cdot i_{\alpha} - \hat{e}_{\alpha} + G_{\psi} \cdot i_{\alpha} - \frac{1}{L} \cdot G_{\psi} \cdot \hat{\psi}_{L,\alpha} \quad (4.2)$$

$$\frac{d\hat{\psi}_{L,\beta}}{dt} = u_{\beta}^* - R \cdot i_{\beta} - \hat{e}_{\beta} + G_{\psi} \cdot i_{\beta} - \frac{1}{L} \cdot G_{\psi} \cdot \hat{\psi}_{L,\beta} \quad (4.3)$$

$$\frac{d\hat{e}_{\alpha}}{dt} = G_e \cdot i_{\alpha} - \frac{1}{L} \cdot G_e \cdot \hat{\psi}_{L,\alpha} \quad (4.4)$$

$$\frac{d\hat{e}_{\beta}}{dt} = G_e \cdot i_{\beta} - \frac{1}{L} \cdot G_e \cdot \hat{\psi}_{L,\beta} \quad (4.5)$$

$\hat{\psi}_{L,\alpha}$, $\hat{\psi}_{L,\beta}$, \hat{e}_{α} , and \hat{e}_{β} denote the estimated components of the current dependent flux and of the EMF vectors, respectively. Because the measured values of the machine's phase voltages are not available, their reference values, u_{α}^* and u_{β}^* , will be used instead. L is the phase inductance of the stator windings, G_{ψ} and G_e are the gains of the EMF observer. A detailed explanation about choosing the gains including the stability analysis is explained in [TOM98], [LEI07]. By solving the above equations in the digital controller one can estimate the back-EMF of the PMSM in stationary coordinates. A block diagram representation of the EMF observer is given in Figure 4.2. Using the estimated value of the EMF, the position can be estimated as follow,

$$\hat{\theta}_e = \tan^{-1} \left(\frac{\hat{e}_{\alpha}}{\hat{e}_{\beta}} \right) \quad (4.6)$$

If no position control is implemented then the $\cos(\hat{\theta}_e)$, $\sin(\hat{\theta}_e)$ can be directly computed from the back-EMF vectors as follow,

$$\sin(\hat{\theta}_e) = \left(\frac{\hat{e}_{\alpha}}{|\hat{e}|} \right) \text{ and } \cos(\hat{\theta}_e) = \left(\frac{\hat{e}_{\beta}}{|\hat{e}|} \right) \quad (4.7)$$

Once the information from the back-EMF vectors is available, the speed of the PMSM can be estimated by using different methods: either by using the magnitude of the EMF vector [KIM96], or by differentiating and filtering the estimated position, or by using a speed observer [TOM98], [LEI07].

By using the magnitude of the EMF vector, the speed can be computed as below:

$$\hat{\omega}_m = \frac{|\hat{e}|}{K_E} = \frac{\sqrt{\hat{e}_{\alpha}^2 + \hat{e}_{\beta}^2}}{K_E} \quad (4.8)$$

This way of speed calculation is sensitive to K_E which is not precisely known. By using only the above equation, it is difficult to determine the direction of machine. In order to determine the

direction of machine rotation, a q-axis component of back-EMF can be computed and from the sign of the q-axis components of the back-EMF, the direction of rotation of the machine can be determined.

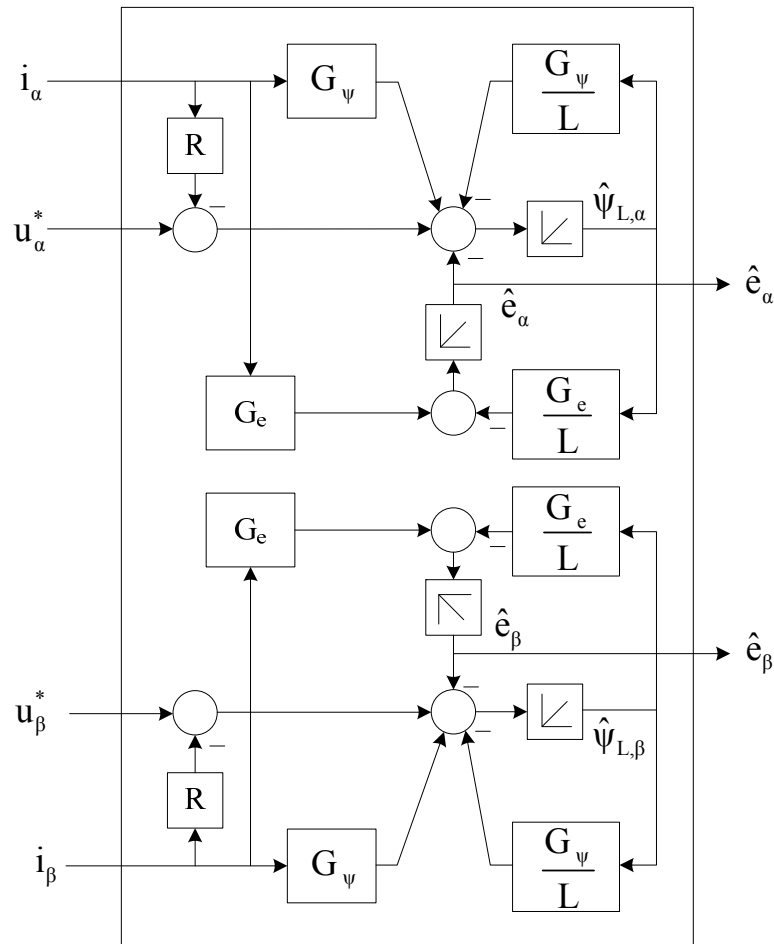


Figure 4.2: Block diagram of an EMF-observer

By differentiating the estimated electrical rotor position $\hat{\theta}_e$ one can also obtain the electrical speed of the rotor. However, differentiation will amplify the noise in the position measurement. In order to remove the noise of the PWM inverter in the estimated speed, a low-pass filter should be used. This approach is used in this work for estimating the speed from the estimated position.

The limitation of EMF based sensorless method is that fault detection is not effective at very low or zero speed operation. If the application demands very low or zero speed operation, then different method of position estimation should be considered such as carrier signal injection, or if suitable, rotor saliency based method, which also works at low speeds. Instead of using sensorless control in the post fault operation, using a redundant position sensor is also possible.

In the case of low speed operation including the starting, where the back-EMF is too small to give the accurate rotor position, high-frequency injection methods in [LEI08], [LEI11], [OGA98] can be used. Although the low-speed sensorless control has been an active research area and can be incorporated into the fault-tolerance scheme presented in this chapter, the main goal of this investigation is focused on the proof of feasibility and practicality of the fault-tolerance scheme. Therefore, the performance when continuously operating at low rotor speeds is not a focus of this investigation.

4.3 Experimental results – tolerance to position sensor fault

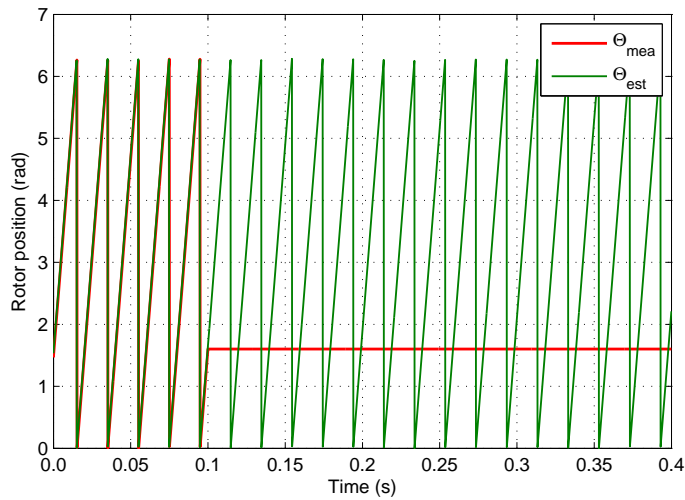


Figure 4.3: Measured and estimated rotor position

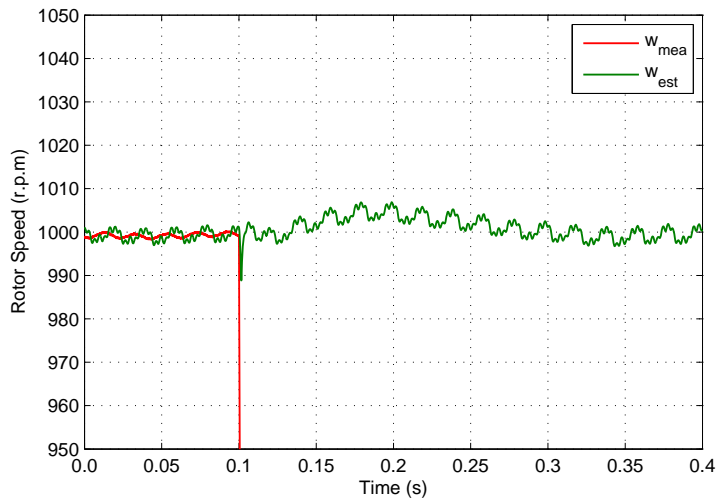


Figure 4.4: Measured and estimated rotor speed

Figure 4.3 and Figure 4.4 show the machine response before and after the position sensor fault. In Figure 4.3, the rotor position waveform with green colour is the estimated one and the one with the red colour is measured position. Similarly, Figure 4.4 presents the estimated and measured speed. Until time 0.1s the machine was running with the measured position and speed. At the time 0.1s, position sensor fault is occurred and after that machine continues to run with estimated position and speed, without any disturbance in machine operation. From Figure 4.3 it is evident that as soon as there is a fault on the position sensor, the position counter in the DSP stops counting and the position information remains at previous value. As the information from the position counter is used further to calculate the speed, the measured speed falls rapidly although it is not from the actual machine. A slight disturbance can be observed during the transition between sensorless and sensor based control. The magnitude of the disturbance depends on the error between the estimated and measured position and the threshold θ_{th} of the fault detection circuit (see Figure 4.1). Though it is compensated continuously, there exists some error between estimated position and measure position. If this error value is high, then θ_{th} should be set to high, this makes delay in the fault detection, causing the disturbance in the transition between sensorless control and sensor based control.

4.4 Current sensors with increased availability

For the Field Oriented Control (FOC) of the PMSM with three-phase windings and isolated neutral, it is enough to have current measurement from any of the two phases. In order to provide the fault tolerance to current measurement, third current sensor is used measuring the third phase current. When three-phase currents are measured, there are different ways in which the $\alpha\beta$ -components of the currents can be computed [BAH09].

Let us say i_a , i_b and i_c are the three-phase currents of the machine, then the different ways in which $\alpha\beta$ -components of the currents can be computed as below,

$$i_{\alpha 1} = i_a \text{ or } i_{\alpha 2} = -(i_b + i_c) \quad (4.9)$$

$$i_{\beta 1} = \frac{1}{\sqrt{3}}(i_b - i_c) \text{ or } i_{\beta 2} = \frac{1}{\sqrt{3}}(i_a + 2 \cdot i_b) \text{ or } i_{\beta 3} = -\frac{1}{\sqrt{3}}(i_a + 2 \cdot i_c) \quad (4.10)$$

When all the current sensors are in healthy state, $i_{\alpha 1}$ and $i_{\alpha 2}$ are equal and similarly, $i_{\beta 1}$, $i_{\beta 2}$ and $i_{\beta 3}$.

From the equation (4.9) and (4.10), it is possible to define different combinations of $\alpha\beta$ -components as given below,

$$C_a = i_{\alpha 2}^2 + i_{\beta 1}^2 \quad (4.11)$$

$$C_b = i_{\alpha 1}^2 + i_{\beta 3}^2 \quad (4.12)$$

$$C_c = i_{\alpha 1}^2 + i_{\beta 2}^2 \quad (4.13)$$

In normal operating condition, the result of the three combinations is equal and at steady state the result of the three combinations is equal to their reference values,

$$C_{ref} = i_{\alpha,ref}^2 + i_{\beta,ref}^2 \quad (4.14)$$

For a three-phase PMSM with isolated neutral and if there would be no offset in the current measurement, the sum of the three currents is zero in healthy case of all the current sensors. This principle is no longer valid when there is a fault in one of the current sensors. By using this principle and constantly comparing the C_{ref} and C_x , ($x = a, b, \text{ or } c$) to an error tolerance value C_{tol} , it is possible to find the fault in a current sensor as shown in Figure 4.5 below and Table 4.1.

If there is a fault in one of the current sensors, then the sum of the three-phase currents is not zero. The same condition is tested in Figure 4.5. The absolute value of the sum of the currents, $|i_{err}|$, is compared with a tolerance value, i_{tol} . If at least two consecutive comparisons satisfies the condition $|i_{err}| > i_{tol}$, it is an indication of failure in one of the current sensors. However, from this information, it is not possible to say which current sensor is having the fault. In order to identify the faulty current sensor, criteria defined in equation (4.11)-(4.14) are used. Criteria C_a is defined such that it will not use the information from the current sensor of phase 'a'. Similarly, C_b and C_c are defined such that they will not use the information from current sensors of phase 'b' and phase 'c' respectively. So, for example, if there is a fault in the current sensor of phase 'a', then criteria C_a is equal to its reference value C_{ref} (because it does not use information from the current sensor of phase 'a'), but C_b and C_c are not equal to reference values C_{ref} (because they use information from the current sensor of phase 'a'). So the deviation between C_{ref} and C_x ($x = a, b, \text{ or } c$) are compared to C_{tol} and if at least two consecutive comparisons are satisfied then F_x (where $x = a, b, \text{ or } c$) is set to 1 as shown in Table 4.1. In case of fault in the current sensor of phase 'a', $F_{fault} = 1$, $F_a = 0$ (because

$C_{err} < C_{tol}$), $F_b = 1$, $F_c = 1$ (because $C_{err} > C_{tol}$). If $I_{fault} = 0$, then the criteria's are not further checked because $C_{err} < C_{tol}$ condition may not be satisfied in case of dynamic operation of the machine. After checking all the fault cases, automatic controller reconfiguration can be easily implemented by using the information from Table 4.1 and equations (4.15)-(4.16). For example, if there is a fault in the current sensor of phase 'a', then K_a is set to one, K_b , K_c and K_x are set to zero in equations (4.15) and (4.16). In this way, i_α and i_β are computed using $i_{\alpha 2}$ and $i_{\beta 1}$, which does not use the information from the current sensor of phase 'a'.

In order to implement the automatic controller reconfiguration in case fault in any current sensor, the following equations are implemented along with information from the Table 4.1.

$$i_\alpha = K_a \cdot i_{\alpha 2} + K_b \cdot i_{\alpha 1} + K_c \cdot i_{\alpha 1} + K_x \cdot i_{\alpha 1} \tag{4.15}$$

$$i_\beta = K_a \cdot i_{\beta 1} + K_b \cdot i_{\beta 3} + K_c \cdot i_{\beta 2} + K_x \cdot i_{\beta 2} \tag{4.16}$$

The limitation of above method is if the current sensor is under fault before the machine is started, then it is difficult to detect the fault in the current sensor. It assumed that during the fault detection there is no earth fault in the machine. If one of the motor's phases were shorted to ground, the sum of the phase currents would no longer equal zero, which fails the concept of fault detection. A fault in the current sensor and reference change to the machine currents at the same time is not considered here.

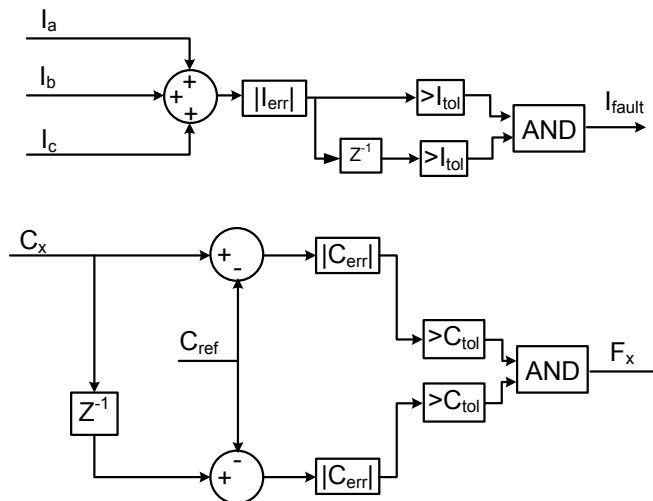


Figure 4.5: block diagram for current sensor fault detection

Table 4.1: Current sensor fault detection

Fault in sensor	I_{fault}	F_a	F_b	F_c	K_a	K_b	K_c	K_x
a	1	0	1	1	1	0	0	0
b	1	1	0	1	0	1	0	0
c	1	1	1	0	0	0	1	0
No fault	0	0/1	0/1	0/1	0	0	0	1

4.5 Experimental results - current sensor with increased availability

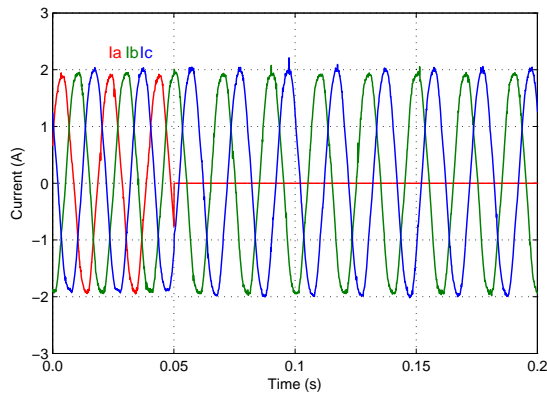


Figure 4.6: Three phase stator currents with current sensor fault (output of the current sensors)

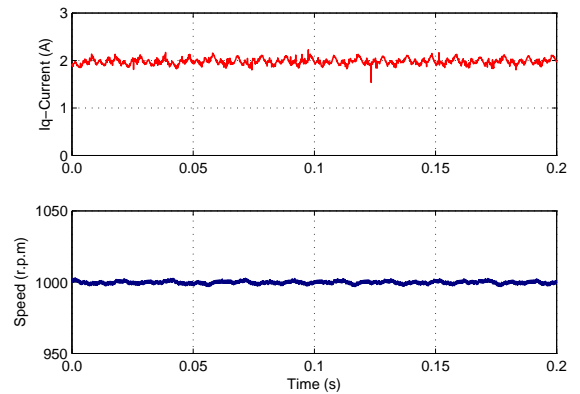


Figure 4.7: q-axis current and rotor speed

Figure 4.6 and Figure 4.7 shows the PMSM response to a fault in the current sensor of phase 'a'. Until time 0.05s the machine is controlled with current sensors of phase 'a' and phase 'b' with phase 'c' as a redundant sensor. At time 0.05s current sensor of phase 'a' is having a fault and then fault detection and compensation algorithm are used to eliminate the faulty sensor (phase 'a') and insert the redundant sensor (phase 'c'). After time 0.05s machine continues to run with current sensors of phase 'b' and phase 'c', without any interference to machine operation.

4.6 Conclusions

A single fault tolerant solution to the position encoder and current sensors are discussed in this chapter. A back-EMF based position sensorless control algorithm is implemented to estimate the rotor position of the PMSM drive. The difference between the measured and estimated position are compared to some tolerance value. If the difference exceeds the allowed tolerance value, it is an indication of failure in the position measurement, with the condition that there is not fault in the current measurement. In this case, the controller ignores the measured position and the machine continues to run with the estimated position.

In order to provide fault tolerance current measurement, a redundant current sensor is used along with necessary two current sensors. Fault detection algorithms are implemented using the information from the three-phase currents measured. If there is a fault in one of the current sensors, then rest of the two current sensors are used further for the machine control.

5 PMSM Drive with Improved Availability of Controller, Converter and Feedback System

5.1 Introduction

Initially, solutions to improve the availability of individual drive components are developed. Chapter 2 presents the solution to increase the availability of the digital controller. Digital controller availability is improved by using TMR based redundancy and safe majority voter concepts. Chapter 3 presents the solution to increase the availability of a 2-level voltage source power converter. A redundant leg is used along with existing three legs, which is used to replace the faulted leg in case of a fault in any of the existing legs. Back-to-back connected thyristors are used to isolate the faulted leg and insert the redundant leg. Chapter 4 presents the solutions to improve the availability of the feedback system. A position sensorless control algorithm is used in case of failure in the position encoder and a redundant current sensor is used in case of failure in the active current sensors. In this chapter, a combined system is presented, which can tolerate a single arbitrary fault in the digital controller, power converter and feedback system. An experimental setup of the combined system is developed providing suitable experimental results.

5.2 System description of PMSM drive with increased availability

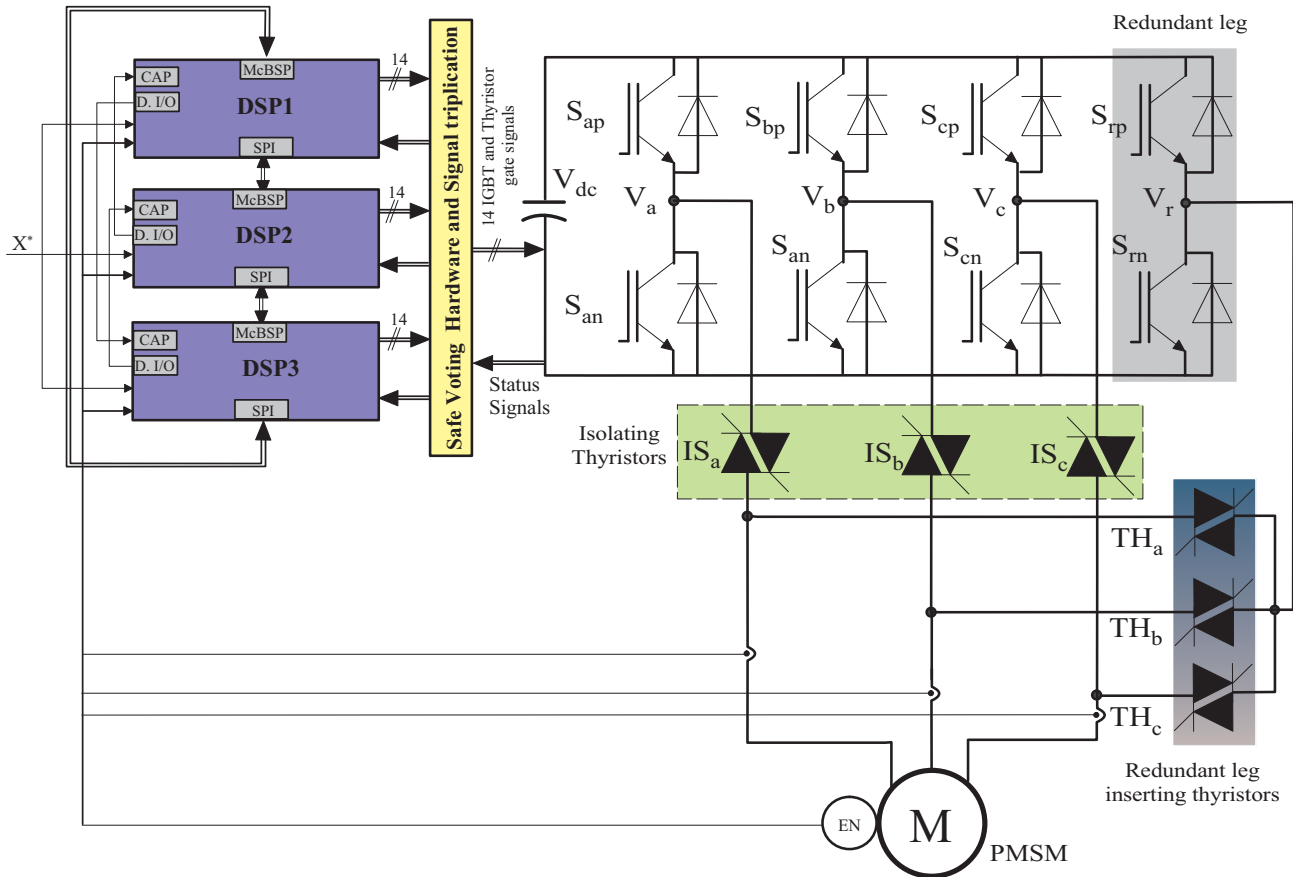


Figure 5.1: PMSM drive with improved availability

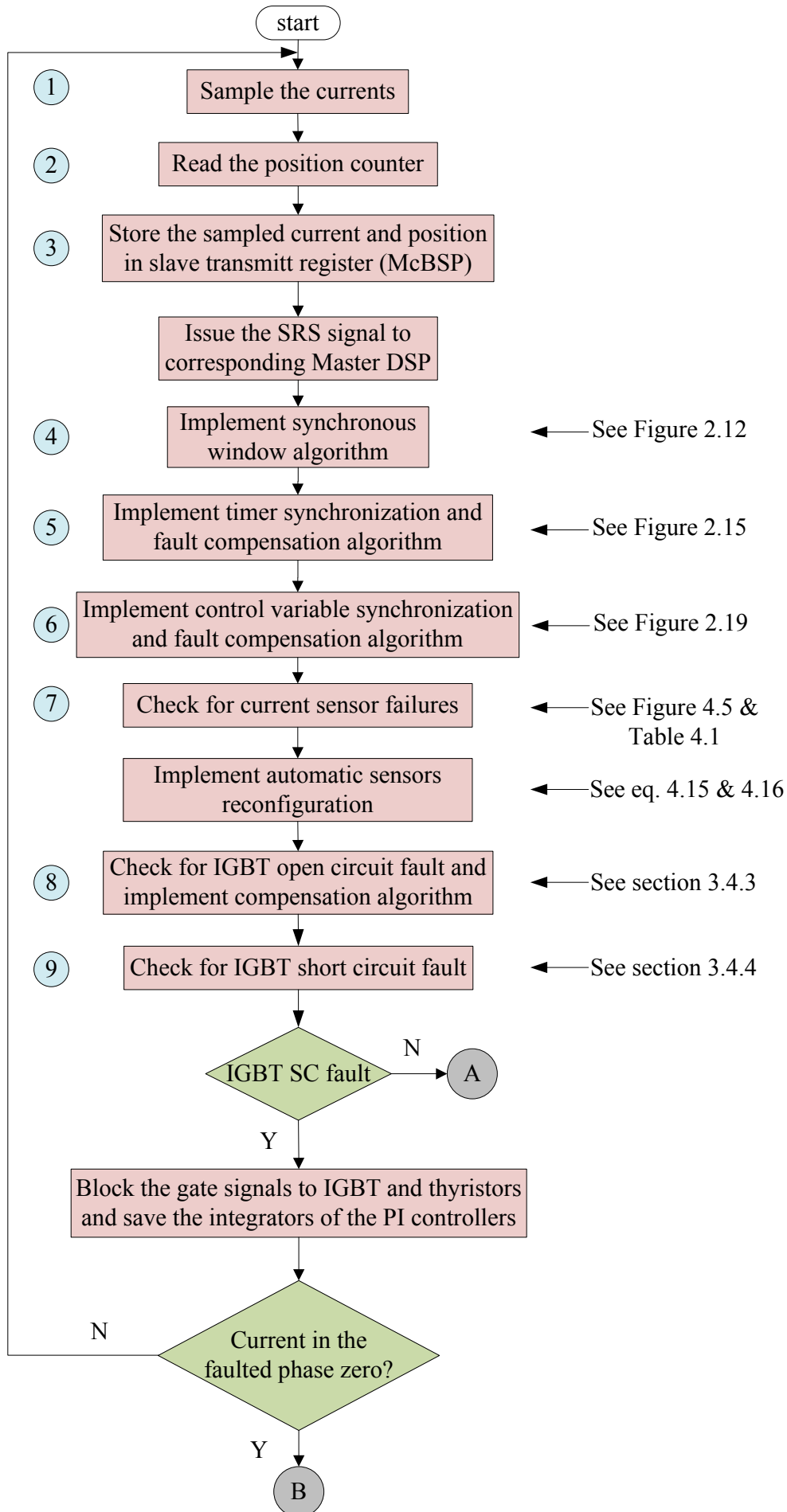
Figure 5.1 shows the schematic diagram of a PMSM drive system with improved availability, which can tolerate a single arbitrary fault in digital controller, power converter and feedback system. The digital controller with increased availability, as elaborated in section 2.3, is implemented based on the concepts of TMR. A transistor based safe voting hardware is built for the

IGBT and thyristor gate signals. A high speed full-duplex SPI based serial communication is implemented between all the DSPs in order to synchronize them in time and also in control variables. The necessary synchronization, fault detection and fault compensation algorithms are explained in section 2.3.1 and section 2.3.2. The VSI with increased availability, as elaborated in section 3.4, is implemented based on the concept that an extra redundant leg is used, which replaces the faulted leg in case of IGBT open or short circuit fault. Back-to-back connected thyristors are used to isolate the faulted leg and to insert the redundant leg. An extensive simulation and experimental results are provided for both IGBT open circuit fault and short circuit fault in the section 3.5 and section 3.6. The position sensor fault detection, as elaborated in section 4.2, is implemented by comparing the result of estimated position with the measured one. In case of fault in the position sensor, the measured position is replaced by estimated position. The availability of current measurement, as elaborated in section 4.4, is increased based on the concept that a redundant current sensor is used along with the necessary two current sensors. The fault detection and automatic controller reconfiguration in case of failure in the current sensors are explained in the section 4.4.

5.3 Control algorithm of the PMSM drive with increased availability

Figure 5.2 shows the complete control algorithm of a PMSM drive with increased availability. The control cycle repeats every 100 μ s. This is a generalized algorithm and valid for any DSP. Different steps of the control algorithm are explained below.

- 1) As a first step, as soon as the control cycle begins, the output values of the current sensors are sampled in a sequential mode. Sampled currents are the outputs of analog to digital converters. They are converted to actual current values using suitable conversion value (depends on gain of the current sensor and amplifier) and corrections for the offsets are made.
- 2) In the next step, the position counter information is read from the position encoder. The position encoder connected to the machine has 5000 counts per revolution. As there are two 90° phase shifted rectangular pulse signals are available from the encoder and the DSP counts both falling and rising edge of each signal, so the total count is 20000 counts per revolution. From this information, actual position of the rotor is calculated by using suitable conversion factor.
- 3) Sampled currents and the position information is stored in the slave transmit register (McBSP) and then a slave ready signal is issued to its corresponding master.
- 4) Immediately next starts the synchronous window loop as explained in Figure 2.12. In the synchronous window loop, DSP waits for SRS signal from its corresponding master and checks if the communication between all the DSPs is in time or not.
- 5) If the communication between all the DSPs is successfully finished within the synchronous window time, the timer synchronization algorithm explained in Figure 2.14 is implemented. If the communication between any of the two DSPs is not in time, then the corresponding fault compensation algorithms are executed as shown in Figure 2.15.
- 6) As a next step, 5% tolerance band check of the exchanged control variables is checked. In healthy case of all the DSPs and if all the variables are within the 5% tolerance band to each other, then the median values of the exchanged variables is selected. In case of fault in any



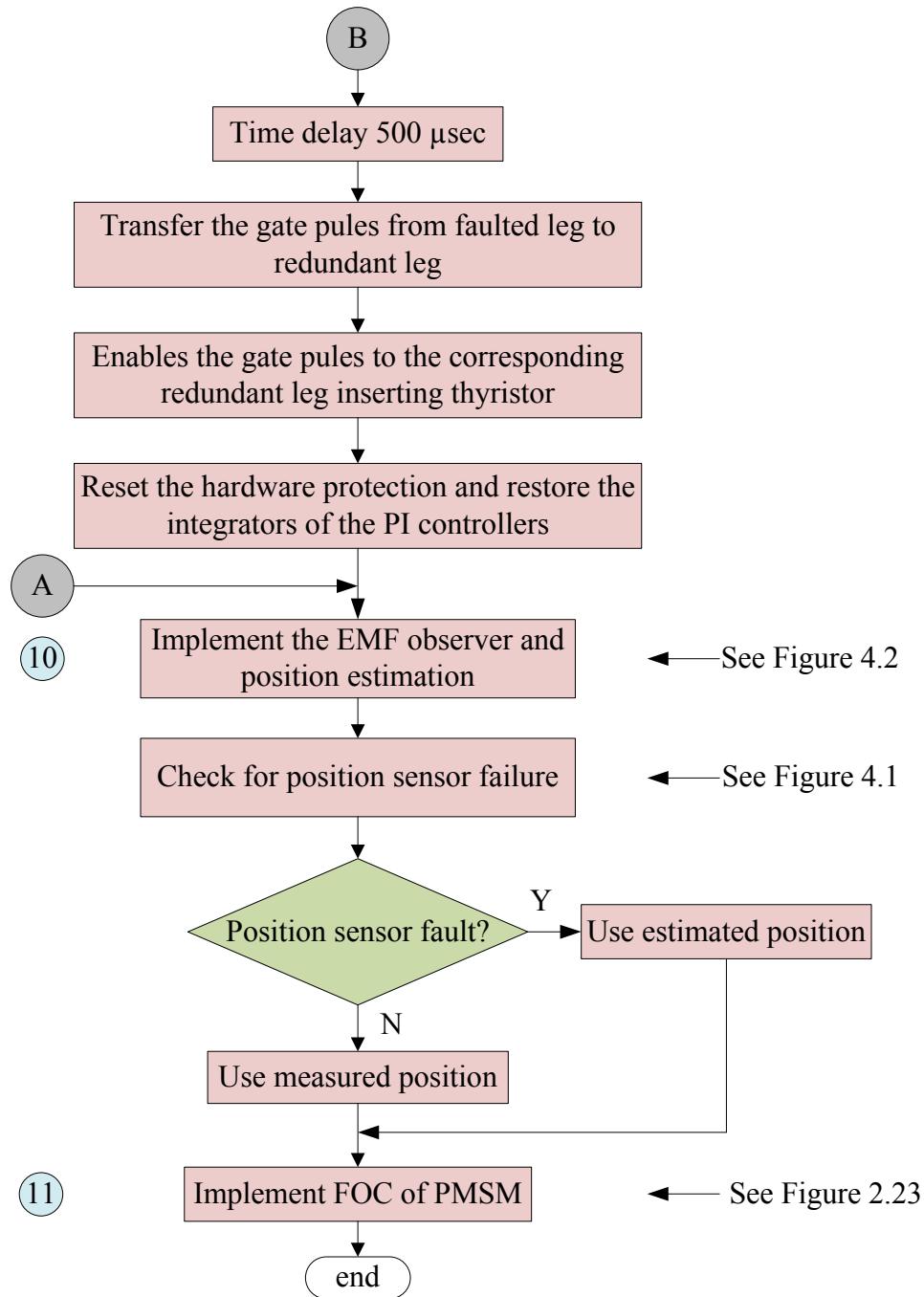


Figure 5.2: Control algorithm of fault tolerant PMSM drive

of the DSP then the corresponding fault compensation algorithms are implemented as shown in Figure 2.19. In chapter 2.3, as only digital controller with increased availability is implemented, only two current values (i_a , i_b) and position value (θ_e) are synchronized. When a complete system is implemented, three phase current values (i_a , i_b and i_c) and position value (θ_e) are synchronized.

- 7) Once the digital controller fault tolerance is finished, current sensors fault tolerance is implemented. First, the fault diagnosis algorithm based on the information from Figure 4.5 and Table 4.1 is implemented. Then, automatic controller reconfiguration in case of currents sensors fault is implemented as per the equations (4.5) and (4.6).

- 8) After the current sensors fault tolerance, fault detection and compensation of IGBT open circuit fault is implemented as explained in section 3.4.3.
- 9) Then, fault status of IGBT short circuit fault is checked. If no fault is reported from the hardware protection, then the control is automatically transferred to step 10). If any fault is reported by the hardware protection, then corresponding compensation algorithms are implemented as explained in section 3.4.4.
- 10) After the inverter fault tolerance, position sensor fault tolerance is implemented. First, position is estimated using a back-EMF based observer as shown in Figure 4.2. In order to detect any failures in the position sensor, the estimated position is constantly compared with the measured position as shown in Figure 4.1. If a fault is detected in the position sensor, the estimated position is used for the further control. If no fault is detected then the measured position is used for further control.
- 11) Once the position information is available, a standard FOC of the PMSM is implemented as shown in Figure 2.23.

5.4 Experimental results

Field Oriented Control (FOC) of Permanent Magnet Synchronous Motor (PMSM) is implemented in order to validate the proposed PMSM drive with improved availability. A laboratory prototype has been built for testing the availability improvement solutions developed. The PMSM is coupled with another PMSM, which is used as a load machine. A three phase variable resistance is connected at the output terminals of the load machine which provides the required load torque. Figure 5.3 shows the experimental setup with three DSP boards, voter board (includes gate drivers and signal triplication) and 3-phase 2-level voltage source inverter with redundant leg. PMSM parameters are presented in Table 3.2.

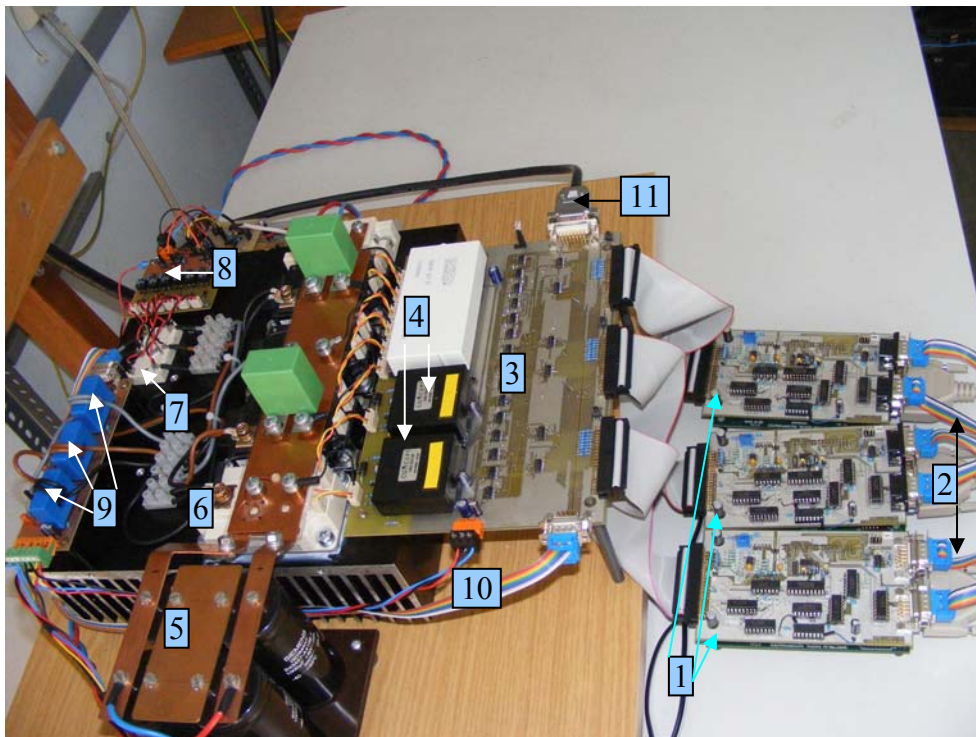


Figure 5.3: Laboratory prototype of PMSM drive components with improved availability

Different components of the PMSM drive with improved availability as listed in Figure 5.3 are,

- 1) Digital controllers (DSP TMS320F2812 and corresponding interfacing boards)
- 2) Serial communication channels between the digital controllers
- 3) Transistor voters
- 4) IGBT gate drivers
- 5) DC link
- 6) IGBT modules
- 7) Thyristor module
- 8) Thyristor gate drive
- 9) Hall effect current sensors
- 10) Current feedback from current sensors
- 11) Position feedback from position encoder

Figure 5.4 to Figure 5.7 show the different responses of the PMSM for different faults. All the faults are inserted one by one. First DSP3 is turned OFF and then the Inverter IGBT short circuit fault is inserted (IGBT S_{ap} short fault at $t = 0.12s$) and then current sensor fault (current sensor of phase 'a', at $t = 0.2s$), finally position sensor fault is inserted (at $t = 0.4s$). With DSP3 under fault system continue to work with DSP1 and DSP2. With one of the IGBT short circuited (upper IGBT of phase leg 'a'), first short circuited phase leg is isolated and redundant leg is inserted and machine continues to run as in pre-fault case. In case of one of the current sensor fault (phase 'a'), remaining two current sensors are used and finally in case of the position sensor fault, machine is running with sensorless control. So after all the faults are compensated, machine is running with two controllers (DSP1 and DSP2), with redundant phase leg for phase 'a', current sensors of phase 'b' and phase 'c' and the position sensors less control. It is evident from the results that system can tolerate arbitrary fault in controllers, inverter, current sensors and position encoder (DC-Link fault is not considered).

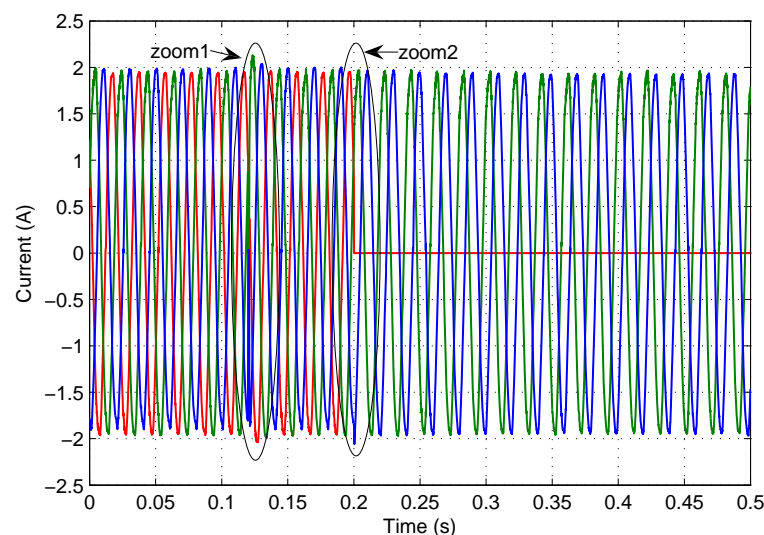


Figure 5.4: Three phase current of the machine (current sensors output) with IGBT short circuit fault inserted at $t = 0.12s$ when the phase 'a' current is at 1.0A with negative slope, current sensor fault inserted on phase 'a' at $t = 0.2s$ and position sensor fault at $t = 0.4s$.

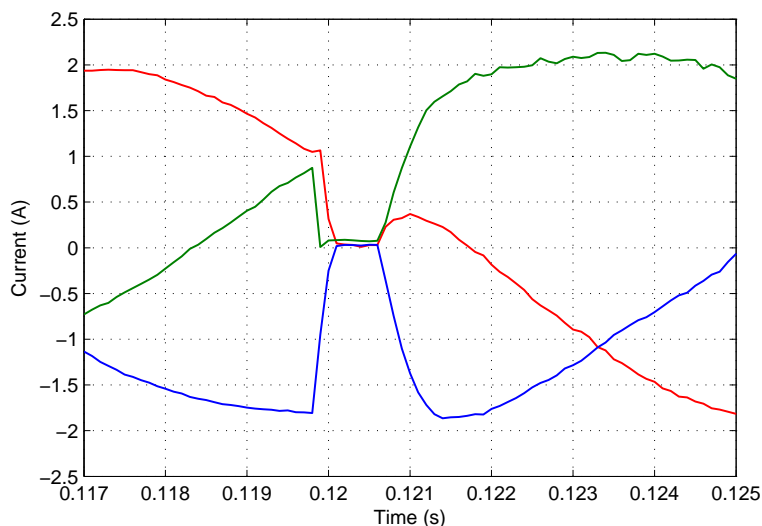


Figure 5.5: Zoom1 of Figure 5.4

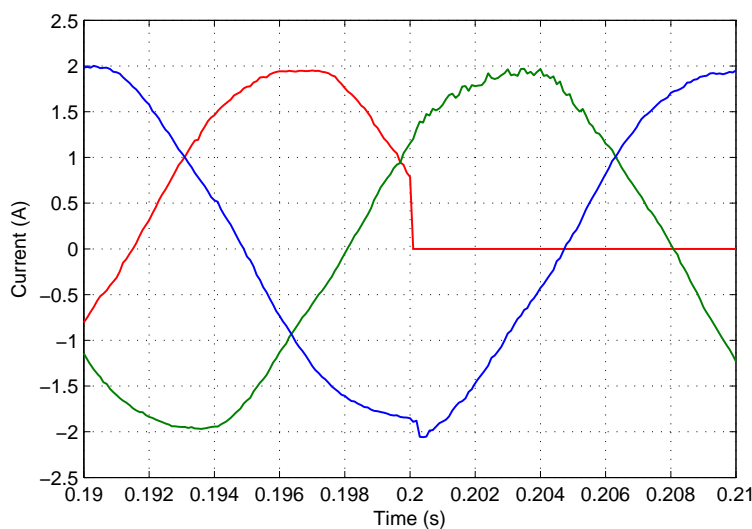


Figure 5.6: Zoom2 of Figure 5.4

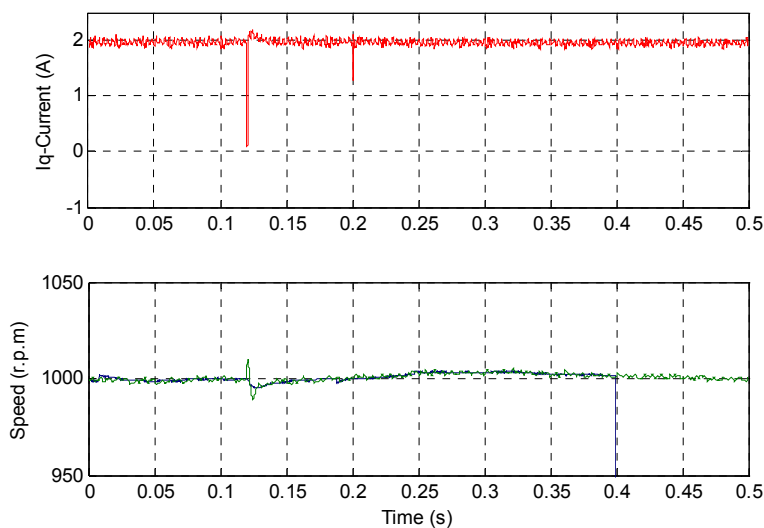


Figure 5.7: Q-axis current, measured speed and estimated speed of the machine for IGBT short circuit fault at $t = 1.2s$, current sensor fault inserted on phase 'a' at $t = 0.2s$ and position sensor fault at $t = 0.4s$ (blue is the measured speed and green is the estimated one)

6 Conclusions and Future Scope

6.1 General conclusions

Fault-tolerant or highly available motor drive systems are more important in the areas such as interlinked production process, medical applications, product sensitive industrial application, transportation and aerospace, military applications, nuclear power plants, *etc.* Fault-tolerant solutions to these applications are very important because the breakdown of a drive may result in tremendous loss of property or human life. Therefore, the motor drives used in such safety critical or product sensitive application should be highly available and they should continue to work, at least with acceptable drive performance, in case of fault in any component of the drive.

In this work, in order to improve the availability of the PMSM synchronous machine drive, solutions to the two-level voltage source inverter, digital controller and feedback system are developed. Availability improvement solutions to each of the aforementioned components are developed individually and tested for their fault-tolerance capabilities experimentally. Finally, a combined system is developed which can sustain faults in the voltage source inverter, digital controller and feedback system. The whole system is developed based on the concept that it will tolerate single arbitrary faults in any of the components aforementioned.

A comprehensive study of the selected redundant digital controllers is done. MTTF calculations of different on-line repairable and non-repairable redundant controller are done. As, a fault-tolerant digital controller should be available 24h at each day, from the results of MTTF calculations it is concluded that a repairable TMR system is the best topology to be selected for fault-tolerant applications. Even, a repairable dual modular redundant topology with perfect fault detection has the MTTF of about half of the repairable TMR system. Moreover, in duplex systems, the probability of detecting all arbitrary errors immediately by the “Error detection” is far below 100%. Developing error detection circuits and algorithms close to 100% error detection makes the system more complex and less reliable. Moreover, in some cases, fault detection methods takes considerable time detecting and localizing the faulted controller. This time delay contradicts the definition of fault tolerance. Whereas in case of TMR systems, they work based on the principle of fault masking. So a bump less output of the controller can be achieved even in case of failure in one of the controllers. So, TMR based controller is selected to increase the availability of the system. The TMR based digital controller with increased availability is developed using three digital signal processors (DSP). In order to synchronize the three DSPs, a high speed full duplex serial communication is developed between all the DSPs. The PWM outputs of all the DSPs are voted-out using a single fault-tolerant transistor based majority voter. The majority voter is developed such that even a short circuit or open circuit failure in one of the transistors will not affect the voter operation. The system was developed for single arbitrary fault and is tested for different faults like a failure in communication between any two processors, a failure in voting logic and a complete failure of any one DSP. The system is able to tolerate all the fault cases and the performance is as normal as when there is no fault. The validity of the above fault-tolerant digital controller was tested using a Field Oriented Control (FOC) of a Permanent Magnet Synchronous Motor (PMSM).

As a next step, solution to improve the availability of power converter is proposed, which can compensate both short circuit and open circuit faults in the switching devices. First, a

comprehensive study of the existing topologies is done and their advantages and disadvantages are discussed. In order to overcome the limitations in the existing topologies, a new topology is proposed, which is simple in construction, modular and easy to control. A standard two-level inverter consists of three legs. In this case of the inverter with increased availability, a redundant leg is added, which replaces the faulted leg. Faulted leg isolation and redundant leg insertion is done by using independent back-to-back connected thyristors. A special control strategy is used to bring the current in the faulted leg to zero and isolate the faulted leg. A theoretical analysis is provided in order to show that thyristors can successfully isolate the faulted leg in case of the IGBT short circuit fault. Extensive simulations are done in MATLAB/Simulink in order to validate the proposed converter with increased availability. An experimental setup is built and experimental results show that thyristors can successfully isolate the faulted leg in all the fault cases. From the results it is clear that compensation strategy is fast enough such that there is negligible disturbance to the drive operation. The post fault performance of the machine is same as the pre-fault and the post fault control algorithm is same as the pre-fault. The achieved results show that this inverter can fit in much safety critical and industrial applications where availability of the drive is of prime importance.

After the VSI fault tolerance, solutions to improve the availability of the feedback system are developed. In case of any failure in the position sensors, first it is important to detect the fault. A position sensorless control is implemented based on a back-EMF observer. The estimated position and the measured position are constantly compared to detect any failures in the position sensor. If any fault is detected in the position sensor, then the control is transferred to position sensorless control. Limitation of such a system is its poor performance at low speeds. For the field oriented control of PMSM drive with isolated neutral, it is enough to have current information from any two phases. In order to improve the availability of current measurement, a redundant current sensor is used, which is measuring the third phase current. The information from the three current sensors is used in order to eliminate the faulty current sensor and the information from the remaining two current sensors is used for further control. A FOC of the PMSM is implemented in order to validate the proposed solutions to improve the availability of feedback system.

Finally, a combined system is developed such that it can tolerate arbitrary faults in the power converter, digital controller and feedback system. Though the system is developed for a single arbitrary fault, by the concept of redundancy, it can tolerate a simultaneous fault on the power converter, digital controller and feedback system. In case of the fault in any of the digital controllers, then the system continues to work with the two remaining controllers after fault compensation, and in case of any fault in the IGBT of the inverter, then that particular leg is isolated, and redundant leg is inserted and the system continues to run as in pre-fault case. If a fault occurs in the position sensor, then after fault compensation, machine continues to work with position sensorless control algorithm. Then, if there is a fault in the current sensor, after isolating the faulted current sensor, machine continues to work with the remaining two current sensors. So finally, the machine can run with position sensorless control algorithm with two current sensors, two digital controllers and two-level converter with redundant leg being used in place of faulted leg. Simultaneous two faults in the same component of the drive are not accepted. Final experimental shows that drive can successfully tolerant arbitrary faults in the VSI, digital controller and feedback

system. From the final results, it can be concluded that such system can be easily adapted to safety critical and product sensitive applications.

6.2 Future scope of the work

Machine faults are not addressed in this work. Different machine faults that can affect the drive operation are, machine inter turn short circuit fault, phase open circuit fault, phase-to-phase short circuit fault, phase to ground short circuit fault, bearing faults, *etc.* Faults on the DC link, diode bridge rectifier, and low voltage power supplies are not addressed in this work. When necessary, fault-tolerant solutions to these components are also an interesting future scope of work. A complete modular fault tolerant system including fault detection and fault tolerant solutions to all the necessary components make system more available.

In case of the proposed inverter with increased availability, a power module with integrated isolating thyristors and redundant leg is developed by [KRI10]. Using such modules in the further product development makes the system more compact and economical. No special IGBT open circuit fault detection method was developed in this work. Selecting an appropriate method and implementing it makes the fault-tolerant inverter a complete system.

In case of position encoder fault detection, sensor less control was implemented based on back-EMF observers. As mentioned before, back-EMF observers have poor performance at low speeds. So selecting and implementing a suitable method which also works at the low speed or zero speed is an interesting area for future implementation.

In case of the current sensor fault detection, the implemented method successfully detects the fault when the machine is running and the fault occurred at the current sensor. If the machine is at the standstill and there is already a fault on the current sensors, then such a method does not perform well enough to detect and isolate the faulted current sensor. If application demands fault detection prior to machine start, then it is necessary to develop a suitable fault detection and isolation strategy.

All the solutions developed in this work to improve the availability of drive components are tested on the PMSM machine. Applying these solutions to a different type of machine and adopting the control laws accordingly is an interesting future area of research.

Bibliography

- [ABD10] Abdellatif M., Pietrzak-David M, and Slama-Belkhodja I., “DFIM vector control sensitivity with current sensor faults,” *COMPEL, The International Journal for Computation and Mathematics in Electrical and Electronic Engineering*, vol. 29, no. 1, pp. 139-156, 2010
- [BAH09] Bahri I., Slama-Belkhodja I., and Monmasson E., “FPGA-based real-time simulation of fault tolerant current controllers for power electronics,” *IEEE International Symposium on Industrial Electronics, ISIE 2009*, pp. 378–383, 2009
- [BEN97] Bennett S. M., and Patton R. J., “Rapid prototyping of a sensor fault tolerant traction control system,” *IEEE Colloquium on Power Electronics*, pp. 2/1-2/6, Apr. 1997
- [BEN04] Bennett J. W., Jack A. G., Mecrow B. C., and Atkinson D. J., “Fault-tolerant control architecture for an electrical actuator,” *35th Annual IEEE Power Electronics Specialists Conference*, Vol.6, pp. 4371-4377, June 2004
- [BHA98] Bhalla A., Shekhawat S., Gladish J., Yedinak J., and Dolny G., “IGBT behavior during desat detection and short circuit fault protection,” in *Proc. Int. Symp. Power Semiconductor Devices ICs (ISPSD)*, pp. 245–248, June 1998
- [BIA96] Bianchi N., Bolognani S, and Zigliotto M., “Analysis of PM synchronous motor drive failures during flux-weakening operation,” in *Conf. Rec. IEEE Power Electronics Specialists Conf.*, vol. 2, pp.1542–1548, June 1996
- [BIN09] Bin Lu, Sharma S. K., “A literature review of IGBT fault diagnostic and protection methods for power inverters,” *IEEE Transactions on Industry Applications*, vol.45, no.5, pp.1770-1777, Sept.-Oct. 2009
- [BOL00] Bolognani S., Zordan M., and Zigliotto M., “Experimental fault-tolerant control of a PMSM drive,” *IEEE Transaction on Industrial Electronics*, vol. 47, pp. 1134–1141, Oct. 2000
- [COR01] Corrêa M. B. deR., Jacobina C. B., da Silva E. R. C., and Lima A. M. N., “An induction motor drive system with improved fault tolerance,” *IEEE Transaction on Industrial Applications*, vol.37, pp. 873–879, May/June 2001
- [DUB07] Dubrova E., “Fault tolerant design: An introduction,” *Kluwer Academic Publishers*, London, 2007
- [EDW06] Edwardsa C., Pin Tan C., “Sensor fault tolerant control using sliding mode observers,” *Elsevier, Control Engineering Practice*, pp.897–908, 2006
- [EMB] <http://www.embedded.com.au/pages/TMR.html>
- [ERT02] Ertugrul N., Soong W., Dostal G., and Saxon D., “Fault tolerant motor drive system with redundancy for critical applications,” in *Conf. Rec. IEEE Power Electronics Specialists Conf.*, vol.3, pp.1457–1462, June 2002
- [FUC03] Fuchs F. W., “Some diagnosis methods for voltage source inverters in variable speed drives with induction machines-a survey,” in *Conf. Rec. Industrial Electronics Society, IECON '03*, vol.2, pp.1378–1385, Nov. 2003

- [FU93] Fu J. R., and Lipo T. A., "A strategy to isolate the switching device fault of a current regulated motor drive," in *Conf. Rec. IEEE IAS Annual Meeting*, vol.2, pp. 1015–1020, Oct. 1993
- [FRA91] Frank P., "Enhancement of robustness in observer based fault detection," *SAFEPROCESS 91*, vol. 1, pp. 275-287
- [GAL10] Gálvez-Carrillo M., and Kinnaert M., "Sensor fault detection and isolation in three phase systems using a signal based approach", *IET Control Theory & Application*, Vol.4, No.9, pp. 1838-1848, Sept. 2010
- [ISE06] Isermann R., "Fault-Diagnosis systems—An introduction from fault detection to fault tolerance," *Springer-Verlag Berlin Heidelberg* 2006, ISBN-10 3-540-24112-4
- [JUN09] Jung Shin-Myung, Park Jin-Sik, Kim Hyoung-Suk, Kim Hag-Wone, and Youn Myung-Joong; "Simple switch open fault detection method of voltage source inverter", *Energy Conversion Congress and Exposition (ECCE)*, pp. 3175–3181, Sept. 2009
- [KAS94] Kastha D., and Bose B. K., "Investigation of fault modes of voltage fed inverter system for induction motor drive," *IEEE Transaction on Industry Applications*, Vol. 30, pp. 1028-1038, July/Aug. 1994
- [KIM96] Kim J.-S., and Sul S.-K., "New approach for the low-speed operation of PMSM drives without rotational position sensors," *IEEE Transaction on Power Electronics*, vol. 11, no. 3, pp. 512-519, May 1996
- [KIR05] Kirmann H., "Fault Tolerant Computing in Industrial Automation," *Tutorial 2005*, ABB research centre, Baden, Switzerland.
- [KOR99] Korzine K. A., Sudhoff S. D., and Whitcomb C. A., "Performance characteristics of a cascaded two-level converter," *IEEE Transaction on Energy Conversion*, vol. 14, no. 3, pp. 433-439, 1999.
- [KRA99] Krautstrunk A., and Mutschler P., "Remedial Strategy for a Permanent Magnet synchronous Motor Drive," in *Conf. Rec. EPE*, 1999. (Proceedings in CD)
- [KRI10] Kriegel K., Melkonyan A., Galek M., Rackles J., "Power module with solid state circuit breakers for fault-tolerant applications," *6th International Conference on Integrated Power Electronics Systems (CIPS)*, March 2010 (Proceedings in CD)
- [LEI07] Leidhold R., and Mutschler P., "Speed sensorless control of a long-stator linear synchronous motor arranged in multiple segments," *IEEE Transaction on Industrial Electronics*, vol. 54, no. 6, pp. 3246-3254, Dec. 2007
- [LEI08] Leidhold R., Mutschler P., "Injection of a carrier with higher than the PWM frequency for sensorless position detection in PM synchronous motors," *13th Power Electronics and Motion Control Conference (EPE-PEMC 2008)*, pp.1353-1358, Sept. 2008
- [LEI11] Leidhold R., "Position Sensorless Control of PM Synchronous Motors based on Zero-Sequence Carrier Injection," *IEEE Transactions on Industrial Electronics*, (IEEE Early Access).
- [LIU93] Liu T. H., Fu J. R., and Lipo T. A., "A strategy for improving reliability of field-oriented controlled induction motor drives," *IEEE Transaction on Industry Applications*, vol.29, pp. 910–918, Sept./Oct. 1993

- [MEI10] Meinguet F., and Gyselinck J., "Sensor and open-phase fault detection and isolation for three-phase AC drives", *Proc. of the Power Electronics, Machines and Drives conference (PEMD)*, April 2010
- [MIH10] Mihalachi M. A., "Position acquisition and control for linear direct drives with passive vehicles," *PhD dissertation, Institute für Stromrichtertechnik und Antriebsregelung, TU Darmstadt*, 2010
- [MUN00] Munk-Nielsen S., Tutelea L.N., and Jaeger U., "Simulation with ideal switch models combined with measured loss data provides a good estimate of power loss," *IEEE Industry Applications Conference*, vol. 5, pp. 2915-2922, 2000
- [NAI10] Naidu M., Gopalakrishnan S., and Nehl T. W., "Fault-Tolerant Permanent Magnet Motor Drive Topologies for Automotive X-By-Wire Systems," *IEEE Trans. Ind. Applications*, vol. 46, pp. 841-848, 2010
- [OGA98] Ogasawara, S., Akagi, H., "Implementation and position control performance of a position-sensorless IPM motor drive system based on magnetic saliency," *IEEE Transactions on Industry Applications*, vol.34, no.4, pp.806-812, Jul/Aug 1998
- [PAT95] Patton R. J., "Robustness in model-based fault diagnosis: the 1995 situation," *Proceeding on IFAC workshop, On-line fault detection and supervision in the chemical process industries*, Newcastle, U.K., pp. 55-77, June 1995
- [PEU98] Peugeot R., Courtine S., and Rognon J.-P., "Fault detection and isolation on a PWM inverter by knowledge-based model," *IEEE Transaction on Industry Application*, vol. 34, pp. 1318–1326, Nov. /Dec. 1998
- [POL96] Poledna S., "Fault-tolerant real-time systems: The problem of replica determinism," *Kluwer Academic Publishers*, London, 1996.
- [QIN97] Qin D., Lua X., and Lipo T. A., "Reluctance motor control for fault-tolerant capability," in *Conf. Rec. IEEE Int. Electronic Machines and Drives Conf. (IEMDC)*, pp. WA1-1.1–WA1-1.6, 1997
- [RIB01a] Ribero R. L. A., Jacobina C. B., Lima A. M. N., and da Silva E. R. C., "A strategy for improving reliability of motor drive systems using a four-leg three-phase converter," in *Conf. Rec. IEEE APEC'01*, vol. 1, pp.385–391, 2001
- [RIB01b] Ribero R. L. A., Jacobina C. B., da Silva E. R. C., and Lima A. M. N., "A fault tolerant induction motor drive system by using a compensation strategy on the PWM-VSI topology," in *Conf. Rec. IEEE Power Electronics Spec. Conf.*, vol. 2, pp. 1191–1196, June 2001
- [RIB03] Ribeiro R. L. de A., Jacobina C. B., da Silva E. R. C., and Lima A. M. N., "Fault detection of open-switch damage in voltage-fed PWM motor drive systems," *IEEE Trans. Power Electron.*, vol. 18, pp. 587–593, Mar. 2003
- [RIC07] Richardeau F., Mavier J., Piquet H., Gateau G., "Fault-tolerant inverter for on-board aircraft EHA," in *Conf. Rec. EPE 2007 (Proceedings in CD)*
- [ROT09a] Rothenhagen K., and Fuchs F.W., "Doubly fed induction generator model-based sensor fault detection and control loop reconfiguration," *IEEE Transaction on Industrial Electronics*, vol. 56, pp. 4229-4238, Oct. 2009

- [ROT09b] Rothenhagen K., Fuchs F. W., “Current sensor fault detection, isolation, and reconfiguration for doubly fed induction generator,” *IEEE Transaction on Industrial Electronics*, vol. 56, no.10, pp. 4239-4245, Oct. 2009
- [SCH03] Schwab H., Klönne A., Reck S., and Ramesohl I., “Reliability evaluation of a permanent magnet synchronous motor drive for an automotive application,” in *Conf. Rec. EPE 2003* (Proceedings in CD)
- [SCH06] Schulz, S. E., *et.al.* “Position sensor fault tolerant control for automotive propulsion system,” *U.S. Patent number: US7002318B1*, Feb. 2006.
- [SPR61] SPRU061: TMS320x281x DSP Multi channel Buffered Serial Port (McBSP) Reference Guide.
- [STE93] Stemmler H., and Guggenbach P., “Configurations of high-power voltage source inverter drives,” in *5th European Conference on Power Electronics and Applications (EPE)*, vol. 5, pp. 7-14, Sept. 1993
- [TOM98] Tomita M., Senjyu T., Doki S., and Okuma S., “New sensorless control for brushless DC motors using disturbance observers and adaptive velocity estimations,” *IEEE Transaction on Industrial Electronics*, vol. 45, no. 2, pp. 274-282, Apr. 1998
- [THO95] Thorsen O. V., and Dalva M., “A survey of the reliability with an analysis of faults on the variable frequency drives in industry,” in *Conf. Rec. 6th European Power Electronics and Applications Conference*, Sevilla, Spain, pp. 1033–1038, Sept. 1995
- [THY99] Thybo C., “Fault-tolerant control of inverter fed induction motor drives,” *Ph.D. dissertation, Dept. Control Eng., Aalborg Univ., Grasten, Denmark*, 1999, ISBN 87-90664-07-8
- [UTE00] UTE, RDF 2000: *Reliability data Handbook*, July 2000
- [VAN84] Van Der Broeck H. W., and Van Wyk J. D., “A comparative investigation of a three-phase induction machine drive with a component minimized voltage-fed inverter under different control options,” *IEEE Trans. Industrial Applications*, vol. 20, pp. 309–320, Mar./Apr. 1984
- [WEL01] Welchko B. A., and Lipo T. A., “A novel variable-frequency three-phase induction motor drive system using only three controlled switches,” *IEEE Transaction on Industrial Applications*, vol. 37, pp. 1739–1745, Nov./Dec. 2001
- [WEL04] Welchko B. A., Lipo T. A., Jahns T. M., Schulz S. E., “Fault tolerant three-phase AC motor drive topologies: a comparison of features, cost, and limitations,” *IEEE Transaction on Power Electronics*, Volume 19, Issue 4, pp.1108–1116, July 2004
- [WEN82] Wensley J. H., “Fault tolerant techniques for power plant computers,” *IEEE Transactions on Power Apparatus and Systems*, Volume PAS-101, Issue 1, PP. 100-106, Jan. 1982
- [WIKI1] <http://de.wikipedia.org/wiki/Hochverfügbarkeit>
- [YU05] Yu-seok Jeong, Seung-Ki Sul, Schulz, S. E., Patel, N. R., “Fault detection and fault-tolerant control of interior permanent-magnet motor drive system for electric vehicle,” *IEEE Transactions on Industry Applications*, vol. 41, no.1, pp. 46-51, Jan.-Feb. 2005

Author publications:

- [ERR11a] Errabelli R. R., and Mutschler P., "Fault tolerant voltage source inverter for permanent magnet drives," *IEEE Transaction on Power Electronics*, 2011 (IEEE Early Access)
- [ERR11b] Errabelli R. R., and Mutschler P., "A fault tolerant control and power electronic for a permanent magnet synchronous motor drive," in *14th European Conference on Power Electronics and Applications*, EPE 2011, Birmingham, Aug/Sept 2011 (Proceeding in CD)
- [ERR11c] Errabelli R. R., Leidhold R., and Mutschler P., "Fault tolerant digital controller and feedback system for PMSM drives," *PCIM 2011*, Nürnberg, May 2011 (Proceedings in CD)
- [ERR09] Errabelli R. R., and Mutschler P., "A Fault tolerant digital controller for power electronic applications," in *13th European Conference on Power Electronics and Applications*, EPE 2009, Barcelona, Sept. 2009 (Proceeding in CD)

Supervising the „Studienarbeit“:

- [DRA10] Dragan P., "Erkennung von Unterbruch- Fehlern für IGBT's und Dioden in Umrichter gespeisten Antrieben," *Studienarbeit, Institute für Stromrichtertechnik und Antriebsregelung*, TU Darmstadt, 2010

Appendix A

A1. Datasheet for IGBT module SK30GB123

SK30GB123



SEMIPOT[®] 2

IGBT Module

SK30GB123
SK30GAL123
SK30GAR123

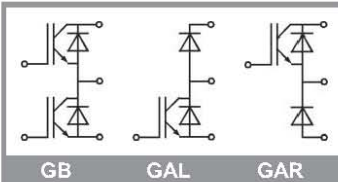
Preliminary Data

Features

- Compact design
- One screw mounting
- Heat transfer and isolation through direct copper bonded aluminium oxide ceramic (DCB)
- N-channel homogeneous silicon structure (NPT-Non punch-through IGBT)
- High short circuit capability
- Low tail current with low temperature dependence

Typical Applications*

- Switching (not for linear use)
- Inverter
- Switched mode power supplies
- UPS



Absolute Maximum Ratings		$T_s = 25\text{ °C}$, unless otherwise specified		
Symbol	Conditions	Values	Units	
IGBT				
V_{CES}	$T_j = 25\text{ °C}$	1200	V	
I_C	$T_j = 125\text{ °C}$	$T_s = 25\text{ °C}$	33	A
		$T_s = 80\text{ °C}$	22	A
I_{CRM}	$I_{CRM} = 2 \times I_{Cnom}$	50	A	
V_{GES}		± 20	V	
t_{psc}	$V_{CC} = 600\text{ V}; V_{GE} \leq 20\text{ V}; T_j = 125\text{ °C}$ $V_{CES} < 1200\text{ V}$	10	μs	
Inverse Diode				
I_F	$T_j = 150\text{ °C}$	$T_s = 25\text{ °C}$	37	A
		$T_s = 80\text{ °C}$	25	A
I_{FRM}	$I_{FRM} = 2 \times I_{Fnom}$		A	
I_{FSM}	$t_p = 10\text{ ms}; \text{half sine wave } T_j = 150\text{ °C}$	350	A	
Module				
$I_{t(RMS)}$			A	
T_{vj}		-40 ... +150	$^{\circ}\text{C}$	
T_{stg}		-40 ... +125	$^{\circ}\text{C}$	
V_{isol}	AC, 1 min.	2500	V	

Characteristics		$T_s = 25\text{ °C}$, unless otherwise specified				
Symbol	Conditions	min.	typ.	max.	Units	
IGBT						
$V_{GE(th)}$	$V_{GE} = V_{CE}, I_C = 1\text{ mA}$	4,5	5,5	6,5	V	
I_{CES}	$V_{GE} = 0\text{ V}, V_{CE} = V_{CES}$	$T_j = 25\text{ °C}$		0,15	mA	
		$T_j = 125\text{ °C}$			mA	
I_{GES}	$V_{CE} = 0\text{ V}, V_{GE} = 30\text{ V}$	$T_j = 25\text{ °C}$		120	nA	
		$T_j = 125\text{ °C}$			nA	
V_{CE0}		$T_j = 25\text{ °C}$		1,2	V	
		$T_j = 125\text{ °C}$		1,2	V	
r_{CE}	$V_{GE} = 15\text{ V}$	$T_j = 25\text{ °C}$		52	$\text{m}\Omega$	
		$T_j = 125\text{ °C}$		76	$\text{m}\Omega$	
$V_{CE(sat)}$	$I_{Cnom} = 25\text{ A}, V_{GE} = 15\text{ V}$	$T_j = 25\text{ °C}_{chiplav.}$	2	2,5	3	V
		$T_j = 125\text{ °C}_{chiplav.}$		3,1	3,7	V
C_{res}			1,65		nF	
C_{oes}	$V_{CE} = 25, V_{GE} = 0\text{ V}$		0,25		nF	
C_{res}			0,11		nF	
$t_{d(on)}$	$R_{Gon} = 25\ \Omega$	$V_{CC} = 600\text{ V}$ $I_C = 25\text{ A}$		40	ns	
t_r				45	ns	
E_{on}			3,5		mJ	
$t_{d(off)}$	$R_{Goff} = 25\ \Omega$	$T_j = 125\text{ °C}$ $V_{GE} = \pm 15\text{ V}$		300	ns	
t_f				45	ns	
E_{off}			2,6		mJ	
$R_{th(j-s)}$	per IGBT			1	K/W	

SK30GB123



SEMITOP® 2

IGBT Module

SK30GB123

SK30GAL123

SK30GAR123

Preliminary Data

Features

- Compact design
- One screw mounting
- Heat transfer and isolation through direct copper bonded aluminium oxide ceramic (DCB)
- N-channel homogeneous silicon structure (NPT-Non punch-through IGBT)
- High short circuit capability
- Low tail current with low temperature dependence

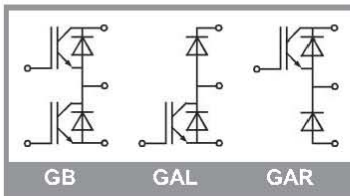
Typical Applications*

- Switching (not for linear use)
- Inverter
- Switched mode power supplies
- UPS

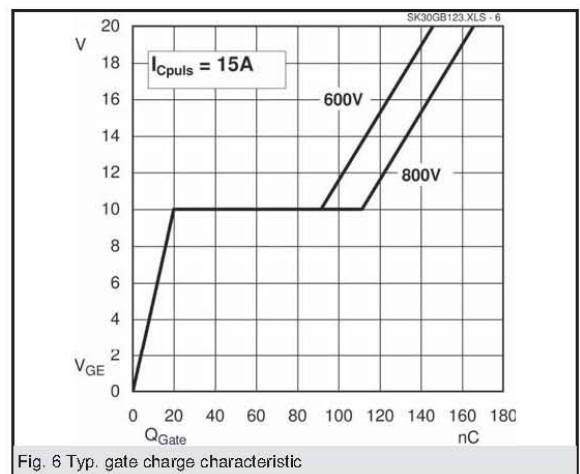
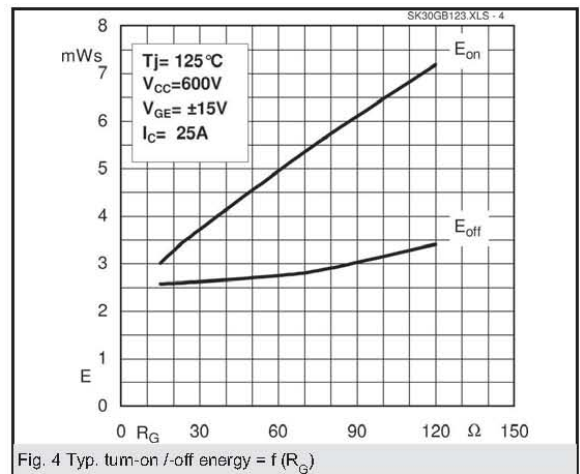
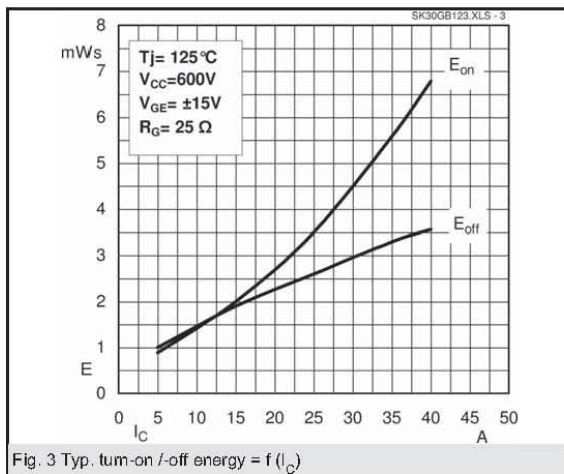
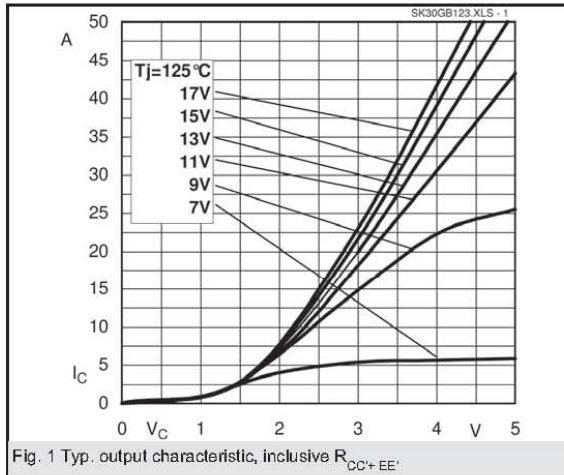
Characteristics					
Symbol	Conditions	min.	typ.	max.	Units
Inverse Diode					
$V_F = V_{EC}$	$I_{Fnom} = 25 \text{ A}; V_{GE} = 0 \text{ V}$				
			2	2,5	V
			1,8	2,3	V
V_{F0}			1	1,2	V
r_F			32	44	mΩ
I_{RRM}	$I_F = 22 \text{ A}$		25		A
Q_{rr}	$di/dt = -500 \text{ A/}\mu\text{s}$		4,5		μC
E_{rr}	$V_{CC} = 600\text{V}$		1		mJ
$R_{th(j-s)D}$	per diode			1,2	K/W
M_s	to heat sink M1			2	Nm
w			19		g

This is an electrostatic discharge sensitive device (ESDS), international standard IEC 60747-1, Chapter IX.

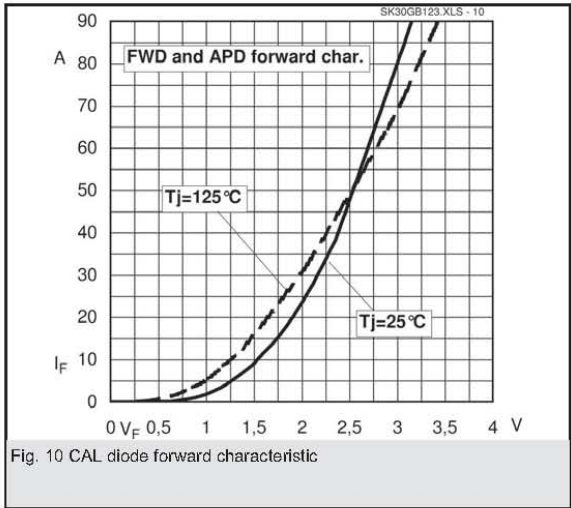
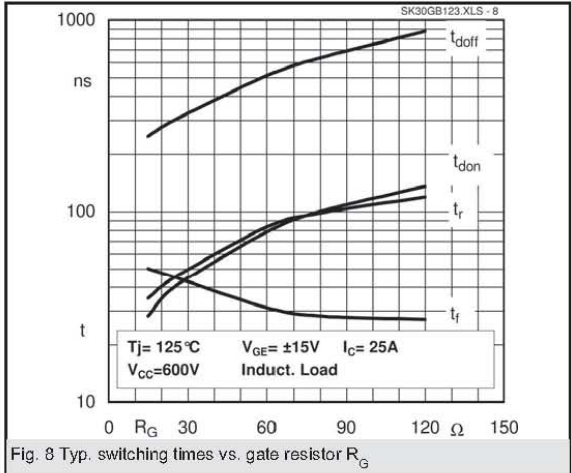
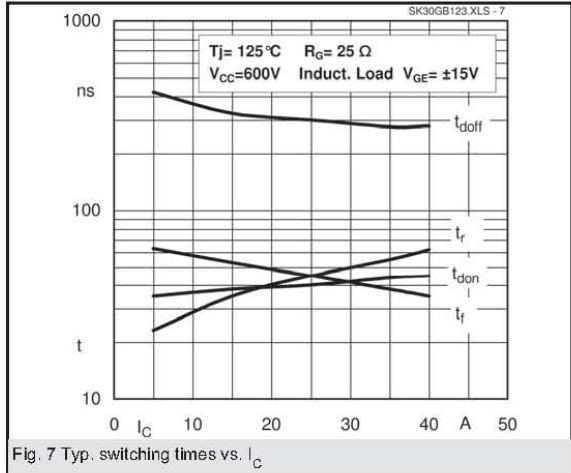
* The specifications of our components may not be considered as an assurance of component characteristics. Components have to be tested for the respective application. Adjustments may be necessary. The use of SEMIKRON products in life support appliances and systems is subject to prior specification and written approval by SEMIKRON. We therefore strongly recommend prior consultation of our personal.



SK30GB123

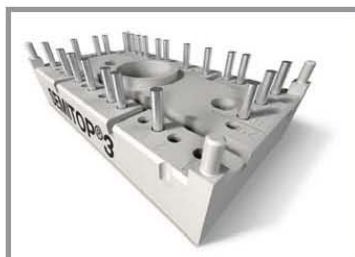


SK30GB123



A2. Datasheet for thyristor module SK25UT

SK 25 UT



SEMISTOP® 3

Antiparallel Thyristor Module

SK 25 UT

Preliminary Data

Features

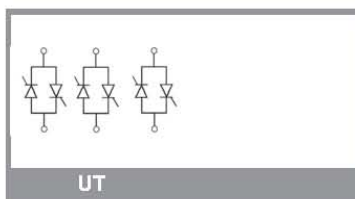
- Compact Design
- One screw mounting
- Heat transfer and isolation through direct copper bonded aluminium oxide ceramic (DBC)
- Glass passivated thyristor chips
- Up to 1600V reverse voltage
- UL recognized, file no. E 63 532

Typical Applications*

- Soft starters
- Light control (studios, theaters...)
- Temperature control

V_{RSM} V	V_{RRM} , V_{DRM} V	$I_{RMS} = 29$ A (full conduction) ($T_s = 85^\circ\text{C}$)
900	800	SK 25 UT 08
1300	1200	SK 25 UT 12
1700	1600	SK 25 UT 16

Symbol	Conditions	Values	Units
I_{RMS}	W1C ; sin. 180° ; $T_s = 100^\circ\text{C}$	20	A
	W1C ; sin. 180° ; $T_s = 85^\circ\text{C}$	29	A
I_{TSM}	$T_{vj} = 25^\circ\text{C}$; 10 ms	320	A
	$T_{vj} = 125^\circ\text{C}$; 10 ms	280	A
\hat{i}_t	$T_{vj} = 25^\circ\text{C}$; 8,3...10 ms	510	A ² s
	$T_{vj} = 125^\circ\text{C}$; 8,3...10 ms	390	A ² s
V_T	$T_{vj} = 25^\circ\text{C}$; $I_T = 75$ A	max. 2,45	V
$V_{T(TO)}$	$T_{vj} = 125^\circ\text{C}$	max. 1,1	V
r_T	$T_{vj} = 125^\circ\text{C}$	max. 20	m Ω
I_{DD} , I_{RD}	$T_{vj} = 125^\circ\text{C}$; $V_{RD} = V_{RRM}$	max. 8	mA
t_{gd}	$T_{vj} = 25^\circ\text{C}$; $I_G = 1$ A ; $dI_G/dt = 1$ A/ μ s	1	μ s
t_{gr}	$V_D = 0,67 \cdot V_{DRM}$	1	μ s
$(dv/dt)_{cr}$	$T_{vj} = 125^\circ\text{C}$	1000	V/ μ s
	$T_{vj} = 125^\circ\text{C}$; $f = 50...60$ Hz	50	A/ μ s
t_q	$T_{vj} = 125^\circ\text{C}$; typ.	80	μ s
I_H	$T_{vj} = 25^\circ\text{C}$; typ. / max.	80 / 150	mA
I_L	$T_{vj} = 25^\circ\text{C}$; $R_G = 33 \Omega$; typ. / max.	150 / 300	mA
V_{GT}	$T_{vj} = 25^\circ\text{C}$; d.c.	min. 2	V
I_{GT}	$T_{vj} = 25^\circ\text{C}$; d.c.	min. 100	mA
V_{GD}	$T_{vj} = 125^\circ\text{C}$; d.c.	max. 0,25	V
I_{GD}	$T_{vj} = 125^\circ\text{C}$; d.c.	max. 3	mA
$R_{th(j-s)}$	cont. per thyristor	1,7	K/W
	sin 180° per thyristor	1,78	K/W
$R_{th(j-s)}$	cont. per W1C	0,85	K/W
	sin 180° per W1C	0,89	K/W
T_{vj}		-40 ... +125	$^\circ\text{C}$
T_{stg}		-40 ... +125	$^\circ\text{C}$
T_{solder}	terminals, 10s	260	$^\circ\text{C}$
V_{sol}	a. c. 50 Hz ; r.m.s. ; 1 s / 1 min.	3000 / 2500	V~
M_s	Mounting torque to heatsink	2,5	Nm
M_t			Nm
a			m/s ²
m		30	g
Case	SEMISTOP® 3	T 13	



1

12-05-2008 DIL

© by SEMIKRON

SK 25 UT

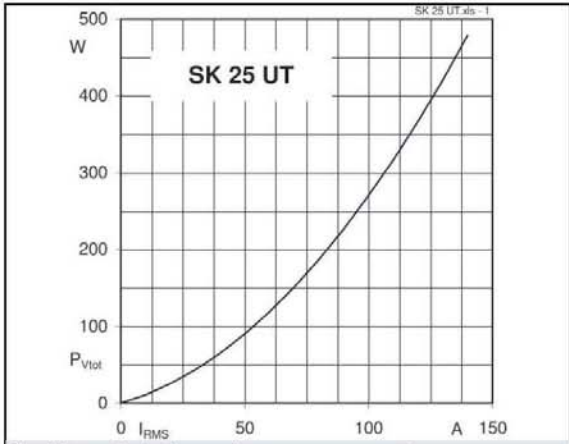


Fig. 1 Power dissipation per phase vs. r.m.s. current

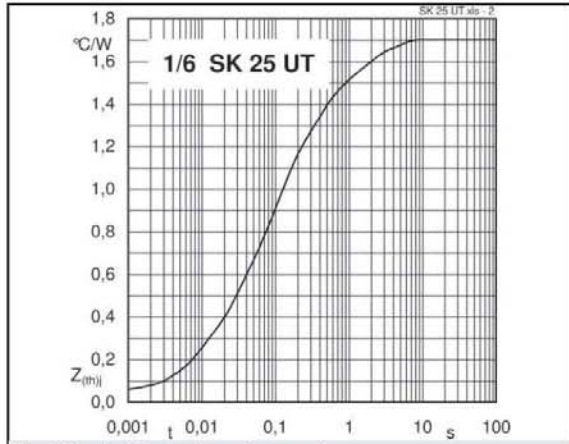


Fig. 2 Transient thermal impedance vs. time

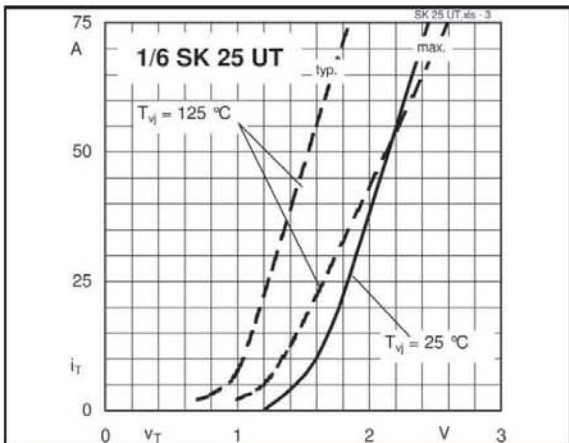


Fig. 3 On-state characteristics

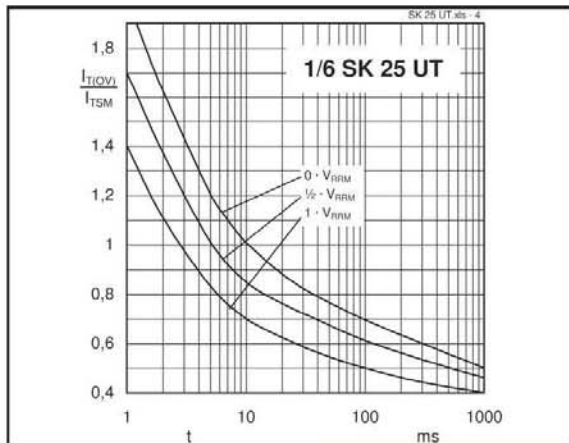


Fig. 4 Surge overload current vs. time

Academic Profile

Rammohan Rao Errabelli,

Born in Warangal, India, on August 08th, 1979.

Since 2007	Working as an assistant at the Department of Power Electronics and Control of Drives, Technische Universität Darmstadt, Germany
2005 - 2006	Project Associate in Power electronics group at Indian Institute of Science (IISc), Bangalore, India
2003 - 2005	Master of Technology in the area of Power and control in Electrical engineering at Indian Institute of Technology Kanpur (IITK), Kanpur, India
1998 - 2002	Bachelor of Technology in Electrical and electronics engineering at Jawaharlal Nehru Technological University, Ananthapur, India

