REPUBLIC OF TURKEY
YILDIZ TECHNICAL UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

MISSION CRITICAL SAFE AND RELIABLE CONTROLLER DESIGN WITH CONSIDERATION HUMAN AND OCCUPATIONAL SAFETY AND HEALTH

ERSİN HASAN DOĞRUGÜVEN

PH.D. THESIS
DEPARTMENT OF CONTROL AND AUTOMATION ENGINEERING
PROGRAM OF CONTROL AND AUTOMATION ENGINEERING

ADVISER
ASSIST. PROF. DR. İLKER ÜSTOĞLU

İSTANBUL, 2018

REPUBLIC OF TURKEY

YILDIZ TECHNICAL UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

MISSION CRITICAL SAFE AND RELIABLE CONTROLLER DESIGN WITH CONSIDERATION HUMAN AND OCCUPATIONAL SAFETY AND HEALTH

A thesis submitted by Ersin Hasan DOĞRUGÜVEN in partial fulfillment of the requirements for the degree of **DOCTOR OF PHILOSOPHY** is approved by the committee on 14.12.2018 in Department of Control And Automation Engineering, Control And Automation Engineering Program.

Thesis Adviser

Assist. Prof. Dr. İlker ÜSTOĞLU

Yıldız Technical University

Approved By the Examining Committee

Assist. Prof. Dr. İlker ÜSTOĞLU

Yıldız Technical University _____

Assoc. Prof. Dr. Akın DELİBAŞI

Yıldız Technical University _____

Prof. Dr. Tankut ACARMAN

Galatasaray University _____

Assist. Prof. Dr. Sıddık Murat YEŞİLOĞLU

İstanbul Technical University _____

Assist. Prof. Dr. Yavuz EREN

Yıldız Technical University _____

ACKNOWLEDGEMENTS

I would like to express my deep appreciation and thanks to my advisor Assist. Prof. Dr. İlker ÜSTOĞLU for his guidance and comments during my PhD study, to Assoc. Prof. Dr. Akın DELİBAŞI and to Prof. Dr. Tankut ACARMAN for their valuable comments during thesis progress meetings; Assist. Prof. Dr. Sıddık Murat YEŞİLOĞLU for accepting to be in the examining committee and explaining me long years ago the program very detailed I have graduated from, Assist. Prof. Dr. Yavuz EREN for accepting to be in the examining committee and for his comments during graduation examination.

Many thanks to my company ASELSAN INC. for supporting me joining to the international conferences to present my studies.

Special thanks to my family for supporting me during my education life and for expressing the importance of science and education during my childhood.

I present this thesis and the Dr. title to my mother.

December, 2018

Ersin Hasan DOĞRUGÜVEN

TABLE OF CONTENTS

Page

LIST OF SYMBOLS

μ	Repair rate
μ_{FSR}	Rate for repair from FS to OK OK state (i.e. to go and change the system with the new ones, can be assumed as 1/MTTR)
μ_{OFS}	Rate for online diagnostic and bringing the system to fail safe state
μ_{PR}	Rate for proof test and repair
C_1	Die complexity failure rate
C_2	Package Failure Rate
f_M	Frequency of wrong (corrupted) messages
f_W	Maximum frequency of messages for one receiver
k_1	Factor for hardware faults including safety margin
k_2	Factor which describes the percentage of hardware faults that result in undetected disabling of transmission decoding
m	Safety factor included within k_1.
n	Number of consecutive corrupted messages until the safe fallback state is entered
p_{US}	Probability of undetected failure due to the performance of the safety code
p_{UT}	Probability of undetected failure due to the performance of the safety code
R_H	Target hazardous failure rate of the complete transmission system
R_{H1}	Hazardous failure rate of hardware faults without transmission code checker
R_{H2}	Hazardous failure rate of EMI
R_{H3}	Hazardous failure rate of transmission code checker
R_{HW}	Hardware failure rate of the non-trusted transmission system
ß	The fraction of undetected failures that have a common cause
$ß_d$	Of those failures that are detected by the diagnostic tests, the fraction that have a common cause
T	Time span, if more than a defined number of corrupted messages were received within this time, the safe fall back state will be entered
T_1	Proof test interval (year)
z	CC factor for SU failures
z_D	CC factor for SD failures
λ	Total failure rate (per hour) of a channel in a subsystem
λ_1	Control Unit 1 Failure
λ_{1D}	Control Unit 1 Dangerous Failure (Independent + CC)
λ_{1DD}	Control Unit 1 Dangerous Detected Failure
λ_{1DU}	Control Unit 1 Dangerous Undetected Failure
λ_{1ID}	Control Unit 1 Independent Dangerous Failure
λ_{1IDD}	Control Unit 1 Independent Dangerous Detected Failure
λ_{1IDU}	Control Unit 1 Independent Dangerous Undetected Failure

λ_{1IS} Control Unit 1 Independent Safe Failure
λ_{1ISD} Control Unit 1 Independent Safe Detected Failure
λ_{1ISU} Control Unit 1 Independent Safe Undetected Failure
λ_{b} Base failure rate
λ_{CD} CCF Dangerous Detected Failure
λ_{CDD} CCF Dangerous Detected Failure
λ_{CDU} CCF Dangerous Undetected Failure
λ_{CS} CCF Safe Failure
λ_{CSD} CCF Safe Detected Failure
λ_{CSU} CCF Safe Undetected Failure
λ_{d} Dangerous failure rate (per hour)
λ_{dd} Detected dangerous failure rate (per hour)
λ_{du} Undetected dangerous failure rate (per hour)
λ_{IA} Initial assessment of the failure rate based on component failure rate estimates
λ_{p} Part failure rate
λ_{s} Safe failure rate (per hour)
λ_{sd} Detected safe failure rate (per hour)
π_{D} Design process multiplier
π_{E} Environmental factor
π_{G} Reliability growth factor
π_{I} Induced process multiplier
π_{IM} Infant mortality factor
π_{L} Learning Factor
π_{M} Environmental factor
π_{M} Manufacturing process multiplier
π_{N} No-defect process multiplier
π_{P} Parts process multiplier
π_{Q} Quality Factor
π_{S} System management process multiplier
π_{SW} Software failure rate prediction
π_{W} Wearout process multiplier

LIST OF ABBREVIATIONS

ASSR	Assessor
ATP	Automatic Train Protection
AsBo	Assessment Body
BIU	Break Interface Unit
BFR	Binomial Failure Rate
BTM	Balise Transmission Module
CC	Common Cause
CCF	Common Cause Fault
CCS	Control Command and Signalling
CENELEC	European Committee for Electrotechnical Standardization
COTS	Commercial of the Shelf
CPU	Central Processing Unit
CSM	Common Safety Method
CSM-RA	Common Safety Methods – Risk Assessment
CU	Control Unit
DC	Diagnostic Coverage (expressed as a fraction in the equations and as a percentage elsewhere)
DC	Duty Cycle (should be evaluated in context to distinguish from Diagnostic Coverage)
DD	Dangerous Detected
DD	Dangerous Detected
DeBo	Designated Body
DI	Designer
DMI	Driver Machine Interface
DoC	Declaration of Conformity
DU	Dangerous Undetected
EC	European Commission
EN	European Norm
ERA	European Railway Agency
EU	European Union
EVC	European Vital Computer
FFFIS	Form Fit and Functional Interface Specification
FIS	Functional Interface Specification
FMECA	Failure Modes, Effects and Criticality Analysis
FS	Full Supervision
FTA	Fault Tree Analysis

GASC	Generic Application Safety Case
GSM-R	Global System for Mobile communication – Railways
HMI	Human Machine Interface
HR	Highly Recommended
HW	Hardware
IS	Isolation
IM	Input Module
ISA	Independent safety assessor
IXL	Interlocking
JRU	Juridical Recording Unit
KMC	Key Management Centre
LEU	Lineside Electronic Unit
LRBG	Last Relevant Balise Group
LS	Limited Supervision
LTM	Loop Transmission Module
M	Mandatory
MA	Movement Authority
MRSP	Most Restrictive Speed Profile
MRT	Mean repair time (hour)
MTTR	Mean time to restoration (hour)
N/A	Not Applicable
NL	Non-Leading
NNR	Notified National Technical Rules
NoBo	Notified Body
NP	No Power
NR	Not Recommended
NSA	National Safety Authority
NNTR	Notified National Technical Rules
OBU	On Board Unit
OM	Output Module
OS	On Sight
PDS	(Norwegian abbreviation for) Reliability of safety instrumented systems
PFH	Preliminary Hazard Analysis
PHA	Average frequency of a dangerous failure
PM	Project Manager
PS	Passive Shunting
PT	Post Trip
PYP	Project Management Plan
RIAC	Reliability Information Analysis Center
QAP	Quality Assurance Plan / Project Quality Plan
QLM	Quality Lifecycle Management
R	Recommended
RAMS	Reliability, Availability, Maintainability and Safety
RBC	Radio Block Centre
REV	Reviewer
RIU	Radio Infill Unit
RV	Reversing mode
SB	Stand By
SCC	Safety Critical Computer
SD	Safe Detected

SGÖ	System Requirements Specification
SH	Shunting
SIF	Safety Implemented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SİTEP	System Operational Test Plan (Sistem İşletme Test Planı)
SL	Sleeping
SMR	Safety Management Report
SR	Safety Responsible
SR	Staff Responsible
SRAC	Safety Related Application Conditions
SRS	System Requirements Specification
STM	Specific Transmission Module
STT	System Design Specification (Sistem Tasarım Tanımı)
SU	Safe Undetected
SW	Software
THR	Tolerable Hazard Rate
TIU	Train Interface Unit
TIU	Train Interface Unit
TR	Trip
TSI	Technical Specification for Interoperability
TSR	Technical Safety Report
UIC	International Union of Railways
UN	Unfitted mode
UNIFE	European Rail Industry Association
UNISIG	UNIFE ETCS Working group
VAL	Validator
VER	Verifier

LIST OF FIGURES

Page

LIST OF TABLES

Page

ABSTRACT

MISSION CRITICAL SAFE AND RELIABLE CONTROLLER DESIGN WITH CONSIDERATION HUMAN AND OCCUPATIONAL SAFETY AND HEALTH

Ersin Hasan DOĞRUGÜVEN

Department Of Control And Automation Engineering

Ph.D. Thesis

Adviser: Assist. Prof. Dr. İlker ÜSTOĞLU

The interest in safety critical systems in various industries such as process, nuclear power and transportation increases continuously with the development of societies due to technological enhancements and increased attachment of importance to the human life, property and environment. Especially, the requests for faster and more comfortable transportation systems and the developments in accordance with these requests can be observed concretely. Airline and Railway transport are the safest among all transport modes according to the report of European Commission [1]. Still, safer and more reliable systems can be developed to decrease the risk of accidents and resulted fatalities and injuries.

Data interchange between CPUs, synchronization, computation speed and diagnostic measures are exhaustively evaluated for designing safety critical computing units. These functional and performance criteria are considered together with the safety and availability concerns ex tunc as any change in the design requires re-performing the whole development processes. Therefore, firstly the system under control is to be analyzed correctly, the requirements shall be set consistently and completely as Einstein's approach, which underlines using fifty-five minutes thinking about the problem and five minutes thinking about the solutions for a given time of one hour to solve the problem. While being applicable to all safety areas as the main safety standard [2] is followed along the entire work, the domain selected in this study is railway, and in this context, the requirements for the unmanned CBTC metro systems and ERTMS ETCS used especially at the high-speed railway lines and across the borders are researched deeply. For this

purpose, international and European norms as well as domain specific standards are studied.

Since the main interest of this study is vital computing system with low PFH_G, dual, triple or more redundant architectures are from the main concerns. Safety, availability, reliability as well as dependant failure models in the literature are investigated for the redundant systems. It is found that reliability calculations are also dependent on several parameters such as reference handbook and data usage method (field, datasheet, library, direct calculation, adjustment factor etc.). Consequently, for the same unit results might differ from each other. After exhaustive analyses, it is shown that at the level of five times better results can be yielded for each computing unit when several items are taken into account during the reliability predictions.

Similar to reliability prediction, safety analysis requires much attention due to incorporation of several parameters. Hence, safety parameters are simulated for various architectures to select correct architecture with minimum design effort and costs, which is also a topic of optimization. It is illustrated that some parameters are dependent upon each other although they seem being independent in the formulas. Besides, some parameters affect the outcomes for some architectures unexpectedly such as the influence of the parameter DC for the architecture 1oo2D. Furthermore, a novel definition of a dual redundant system is formed owing to the ambiguous definition in the safety standard for the architectures 1oo2 and 1oo2D and owing to not covering the relevant designs, hence resulting in wrong formulas. As per the simulation results, a design route map is created newly in this study which is to be utilized when designing mission critical vital safe controller.

The international standard for safety critical electronic systems provides formulas for some architectures. Yet, it does not give a clue or reference how these formulas are derived, whether there is some confidence level and if this is the case, what is this value. In the literature and in the industry, it has been met that, reliability block diagrams, fault tree analyses and Markov models are mainly used for the safety calculations. In this study, a new PFH calculation model is proposed for the safety calculations. It is shown that it can conduct more accurate results in comparison to the previous works in the literature and current safety standard. It is also applicable to diverse redundancy differently from the formulas in the standard and literature, which is crucial forasmuch as diversity plays a major role to decrease the rate of dependant failures.

Next, a safety critical computer design for a real application in the aforementioned domain and application areas is proposed. The reliability predictions for several cases are realized in a detailed way and compared with each other. Then, the safety calculations based on the formulas in the safety standard and in the literature with conventional models are conducted. Finally, the proposed model is applied to the application design and the results are compared. The outcomes for the computing platform developed to be used on-board and wayside applications for unmanned CBTC metro system and ERTMS ETCS high speed train lines show that the proposed model conducts 3.44 times lower hazard rates than the IEC 61508 [2] standard and 16.86 times lower than the conventional Markov model in the literature.

Not only the technical safety, but also safety management is considered in this study, since a broad understanding of the safety management is compulsory for the independent safety assessment and finally SIL 4 certification of the vital product. Consequently, safety management in the international safety standards and in the industry is examined.

In addition, despite the fact that current norms are very detailed and strict as they are related to complex safety critical electronic systems, several ambiguities and misinformation are revealed in these standards by providing use cases, and proposals are given for both qualitative and quantitative parts to overcome these problems which is seen an important contribution of this study to the aforementioned norms. These are in the scope of redefinition of V&V, innovative safety organization responding current safety management requirements, corrections to the failure and hazard analysis methods, discussing the subjective approach for techniques / measures, different perspectives for safety critical tool usage and CCF scoring table, drawbacks of statement SIL 0 SW, comparison of different requirements for single faults, unexpected DC effect on PFH for the architecture 1oo2D, the lack of explicit placement of the planning phase for the development process, the ambiguity of the required THR, the relation between RAM and Safety.

Key words: Technical safety, reliability, mission critical safe computer, Markov analysis, communication based train control system

ÖZET

GÖREV KRİTİK EMNİYETLİ VE GÜVENİLİR KONTROLÖR TASARIMI VE İŞ SAĞLIĞI VE GÜVENLİĞİNİN DE GÖZ ÖNÜNDE BULUNDURULMASI

Ersin Hasan DOĞRUGÜVEN

Kontrol ve Otomasyon Anabilim Dalı

Doktora Tezi

Tez Danışmanı: Dr. Öğr. Üyesi İlker ÜSTOĞLU

Toplumların teknolojik ilerlemeleri ve insan hayati, mülkiyet ile çevreye verilen önemin her geçen gün artması nedeniyle, süreç, nükleer enerji, ulaşım gibi çeşitli endüstrilerde emniyet kritik sistemlere olan ilgi artmaktadır. Özellikle daha hızlı ve konforlu ulaşım sistemleri için oluşan talepler ve bu talepler neticesinde gelişmeler somut olarak gözlemlenmektedir. Havayolları ve demiryolları Avrupa Komisyonu raporuna [1] göre diğer ulaşım modları arasında en güvenli olanlarıdır. Ancak kaza risklerinin ve bunun sonucu oluşacak yaralanmaları ve ölümlerin, daha da güvenli ve güvenilir sistemler geliştirilerek azaltılması mümkündür.

Merkezi işlemci birimleri, senkronizasyon, işlem hızı ve teşhis önlemleri emniyet kritik hesaplama üniteleri tasarımı için etraflıca değerlendirilir. Bu fonksiyonel ve performans kriterleri güvenlik ve elde edilebilirlik kavramlarıyla en başta düşünülmelidir, çünkü tasarımdaki herhangi bir değişiklik tüm geliştirme sürecinin tekrarlanmasına neden olacaktır. Bunun için, öncelikle kontrol edilmek istenen sistem doğru bir şekilde analiz edilmeli, gereksinimler tutarlı ve tam bir şekilde belirlenmelidir. Bu yaklaşım, Einstein'ın bir soru çözümü için verilen bir saatlik sürenin 55 dakikasını soruyu anlamaya, kalan beş dakikasını ise soruyu çözmeye ayırması yaklaşımına benzerdir. Çalışma, genel emniyet standardını [2] baz aldığından dolayı tüm emniyet alanlarında uygulanabilir olmakla birlikte, seçilen çalışma alanı temel olarak demiryollarıdır, bu bağlamda insansız CBTC metro sistemleri ve özellikle yüksek hızlı demiryollarında kullanılan ERTMS ETCS sistemleri etraflıca araştırılmıştır. Bu amaç için, uluslararası ve Avrupa normları ile alana özel standartlar incelenmiştir.

Bu çalışmanın temel amacı düşük PFH_G'ya sahip hayati bilgisayar olması sebebiyle, çift, üç ya da daha fazla yedekli mimariler temel ilgi alanıdır. Yedekli mimariye sahip sistemler için güvenlik, elde edilebilirlik, güvenilirlik aynı zamanda literatürdeki bağımlı hata modelleri araştırılmıştır. Yapılan çalışmalar göstermiştir ki güvenilirlik hesapları, referans el kitabına ve veri kullanım yöntemine (saha, veri sayfası, kütüphane, direk hesaplama, ayarlama faktörü vb.) bağlıdır. Netice itibariyle, aynı birim için sonuçlar birbirinden farklılık gösterebilmektedir. Yoğun analizler neticesinde gösterilmiştir ki güvenilirlik tahmini analizinde farklı konular dikkatlice incelendiğinde her hesaplama birimi için beş kat mertebesinde daha iyi sonuçlar elde edilebilmektedir.

Güvenilirlik tahminine benzer şekide, emniyer analizi de bir çok parametre içermesi nedeniyle çok dikkat gerektirmektedir. Bu nedenle, optimizasyonun bir konusu olan en düşük efor ve maliyet ile doğru mimariyi seçebilmek adına, güvenlik parametrelerinin etkisi ile ilgili farklı mimariler için ayrıntılı benzetim çalışmaları yapılmıştır. Bu çalışmalar göstermiştir ki formüllerde bağımsız olarak gözüken bazı parametreler aslında birbirine bağımlıdır. Bunun yanında, 1oo2D mimarisinde DC parametresinin etkisinde olduğu gibi bazı parametreler sonuçları beklenmedik şekilde etkilemektedir. Ayrıca, güvenlik standardında 1oo2 ve 1oo2D mimarilerinin tanımları iki anlamlılığa yol açmaktadır, bazı tasarımları karşılamamaktadır ve bu nedenle doğru olmayan formüllerin kullanılmasına neden olmaktadır. Bu çalışmada, yedekli yapı için bu ihtiyaçları karşılayan yeni bir tanım oluşturulmuştur. Bahsedilen simülasyon sonuçlarına göre, hayati bilgisayar tasarımda faydalanılabilecek, daha önceki çalışmalarda bulunmayan bir tasarım yol haritası oluşturulmuştur.

Güvenlik kritik elektronik sistemler için uluslararası emniyet standardı, çeşitli mimariler için formüller sunmaktadır. Ancak, bu formüllerin nereden ve nasıl elde edildiği hakkında referans ya da bilgi vermemektedir. Bu formüllerin doğruluk anlamında hangi güvenilirlik seviyesinde olduğu bilgisi de yer almamaktadır. Güvenilirlik blok diyagramları, hata ağacı analizleri ve Markov modellerinin literatürde ve endüstride güvenlik hesapları için kullanıldığı tespit edilmiştir. Bu çalışmada, güvenlik hesaplamaları için yeni bir PFH hesaplama modeli önerilmiştir. Bu hesaplama modelinin güncel güvenlik standardına göre gerçeğe daha yakın sonuçlar ürettiği gösterilmiştir. Bu model aynı zamanda standarttan farklı olarak yedeklilikte çeşitlilik içeren sistemlere uygulabilmektedir, bu etken de oldukça ehemmiyetlidir, nitekim yedeklilikte çeşitlilik bağımlı hataların oranını düşürmek için çok büyük önem taşımaktadır.

Daha sonra, belirtilen alanda gerçek bir uygulamada kullanılmak üzere bir güvenlik kritik bilgisayar tasarımı önerilmiştir. Birçok farklı durum için güvenilirlik tahminleri detaylı olarak gerçekleştirilmiştir ve birbirleri ile karşılaştırılmıştır. Akabinde, konvansiyonel modelle güvenlik standartlarında yer alan formülleri temel alan güvenlik hesapları yapılmıştır. Bunun sonucunda, önerilen model tasarıma uygulanmış ve hesaplamalar karşılaştırılmıştır. CBTC ve ERTMS-ETCS araç-üstü ve hat-boyu uygulamalarda da kullanılması için geliştirilen bilgisayar için elde edilen sonuçlar göstermektedir ki önerilen model IEC 61508 [2] standardına göre 3.44 kat, konvansiyonel Markov modele göre 16.86 kat daha iyi sonuçlar vermiştir.

Sadece teknik güvenlik değil aynı zamanda güvenlik yönetimi de bu çalışmada ele alınmıştır, lakin bağımsız emniyet değerlendirmesi ve hayati ürünün SIL 4 sertifikasyonu için güvenlik yönetiminin derinlemesine kavranması gerekmektedir. Uluslararası standartlarda yer alan ve endüstride uygulanan güvenlik yönetimi incelenmiş ve aşağıda bahsedildiği üzere standartlardaki çeşitli konular hakkında yeni önerilerde bulunulmuştur.

Güncel normlar, karmaşık emniyet kritik elektronik sistemler ile ilgili çok detaylı ve sıkı olmasına rağmen, bu standartlarda birçok iki anlamlılık ve tam doğru olmayan bilgiler ortaya çıkarılmış, bunların giderilmesi amacıyla hem niteliksel hem de niceliksel kısımlar hakkında öneriler sağlanmıştır. Tez, bu yönüyle de, yukarıda ifade edilen temel standartlara önemli katkı sağlayacaktır. Bu çalışmalar, V&V'nin yeniden tanımlanması, günümüz güvenlik yönetimi ihtiyaçlarına cevap verebilen yeni bir güvenlik organizasyonu yapısı, hata ve tehlike metotlarına düzeltmeler, teknik ve önlemlerde yer alan öznel yaklaşımlar, emniyet kritik araç kullanımı ile ilgili farklı bakış açıları, ortak nedenli hata değerlendirme tablosu, SIL 0 SW, tek hatalar için olan gereksinim, DC'nin 1oo2D mimarisine beklenmedik etkisi, planlama fazının geliştirme sürecinde eksik olması, RAM ve emniyet arasındaki ilişki, THR değerindeki iki anlamlılık konularında yapılmıştır.

Anahtar Kelimeler: Teknik güvenlik, güvenilirlik, görev kritik güvenli bilgisayar, Markov analizi, haberleşme tabanlı tren kontrol sistemi.

CHAPTER 1

INTRODUCTION

With the recent advances in the technology, humankind is able to build complex systems that can perform more and more features while at the same time the hazards due to these developments are increased. Talking about the accidents, one can simply recall the sinking of the Titanic in 1912, Chernobyl in 1986, Space Shuttle Colombia Explosion in 2003, and Queen of the Sea Train crash in Sri Lana in 2004 where 1700 people died. Leveson [3] summarizes the significant changes of today's systems resulting the causes of hazards as fast pace of technological change, reduced ability to learn from experience, changing nature of accidents, new types of hazards, increasing complexity and coupling, more complex relationships between humans and automation, changing regulatory and public views on safety etc.

Every activity of mankind includes some amount of risk which results in risks for any equipment. From the opposite perspective, there is no activity that can guarentee to eliminate the risk for an operation. Thereof, the science RAMS deals with the optimization of the operation quality and the costs to be paid for this quality, i.e. RAMS interest in balancing and optimising the risk in systems, subsystems, equipment or in any process. For achieving high RAMS performance, a systematic development process shall be followed. An illustrative example for a development life cycle integrated with RAMS is given in [4].

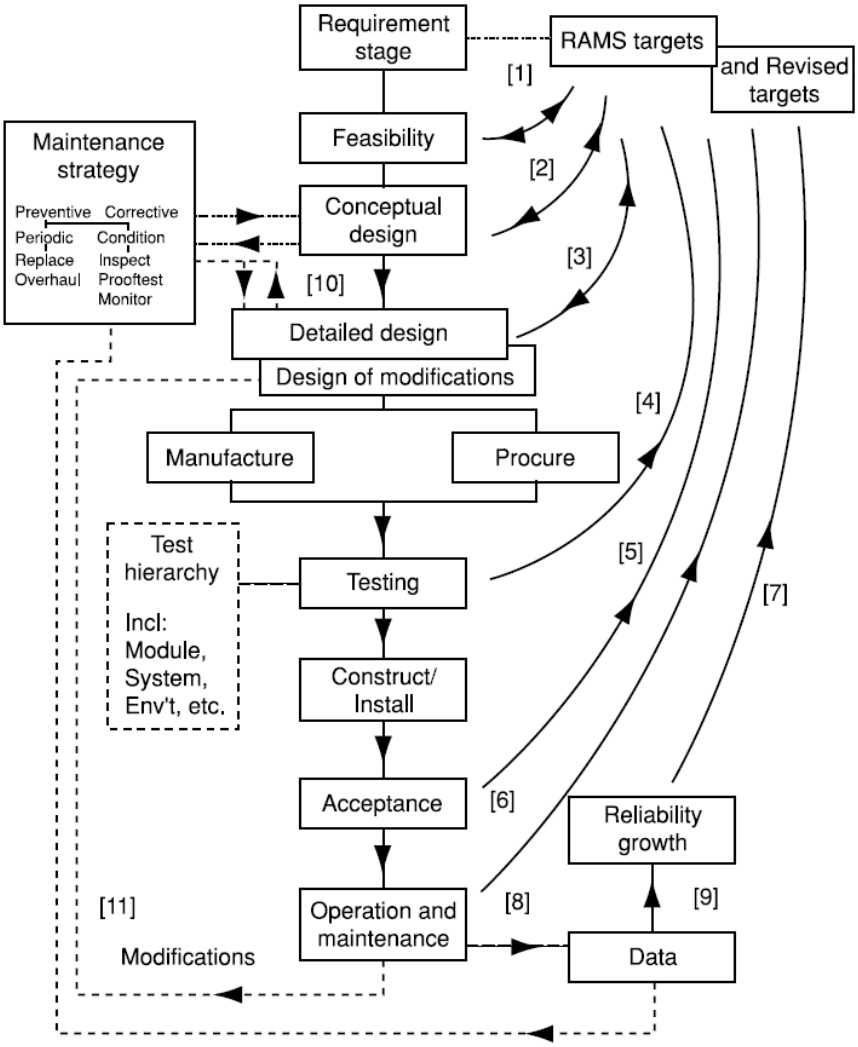


Figure 1.1 RAMS-Cycle model [4]

Unlike many people would think at first glance that safety is freedom from any accident, safety is defined as freedom from unacceptable. As Murthy et al. [5] explain regulatory requirements, customer requirements, and technical requirements shall be fulfilled when producing a safety-instrumented system.

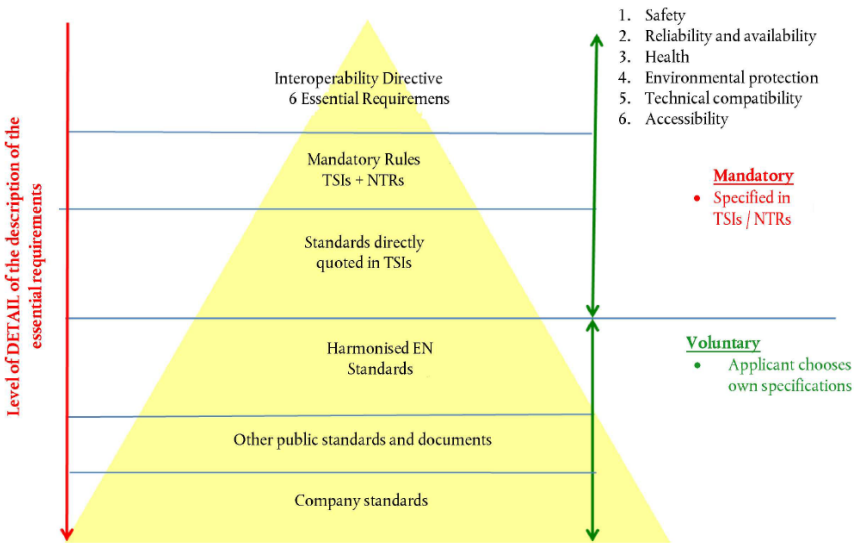


Figure 1.2 Level of detail of the specifications [6]

Regarding the rules to be applied to increase the safety of the systems, various authorities come together to create standards. The main international safety standard is IEC 61508[2] outlining key requirements to all phases of the safety life cycle. Domain specific standards such as IEC 62061 [7] for machinery systems, ISO 26262 [8] for the automobile industry, IEC 61511 [9] for the process industry, IEC 62425 [10] for the railway industry, IEC 61513 [11] for the nuclear power industry, IEC 60601 [12] for medical devices are derived from the aforementioned norm. Certifications, which are required to put the system into operation are realized according to the relevant standards. Both the development processes, i.e. system, hardware and software and the products are the topics of the certification.

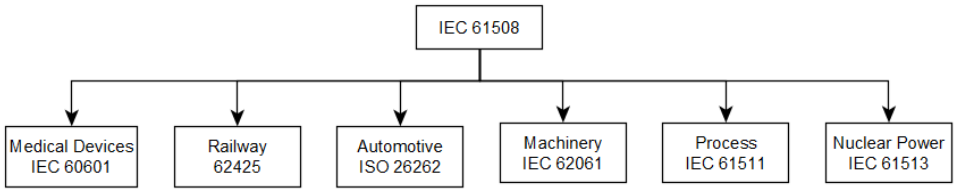


Figure 1.3 International Safety Standards

If the system performance such as speed of transportation vehicle increases, then we can often not decrease the effect of the consequences. Yet, we can endeavor to reduce the frequency resulting in the decrease of the risk posed. Sklet [13] categorizes the safety barriers into active and passive classes. If not possible to place all the barriers, as much as shall be accommodated in a safety critical application. In this thesis, active barriers are

dealt with from both quantitative and qualitative perspectives in consideration of international and European standards.

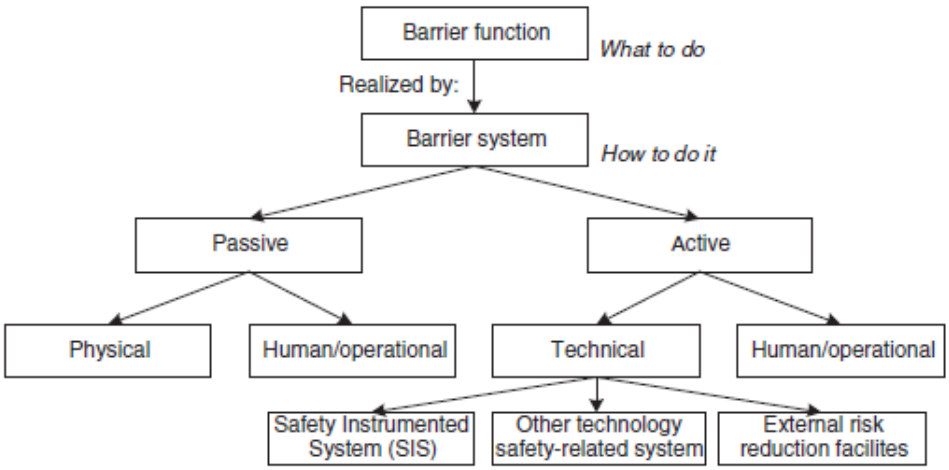


Figure 1.4 Classification of safety barriers [13]

Safety of electronic system is relevant with the Occupational health and safety (OH&S). It is defined in [14] as conditions and factors that affect, or could affect, the health and safety of employees or other workers (including temporary workers and contractor personnel), visitors, or any other person in the workplace. The employer should perform risk assessment and has the responsibility of taking all necessary measures to ensure occupational safety and health [15]. Safety of the electronic system development is related with the OH&S for not only the hazard and risk analyses for the requirements and design from the consideration of OH&S, but also with the entire development cycle and with the results of the final system. The people exposed to the risk can be the users of the system and the maintenance people above all.

1.1 Literature Review

We live in an era in which the intelligence of modern systems evolves fastest by far in the entire history. One of the main reason for this is the development in the microelectronics. In parallel to the development of the technology, the importance of the safety increases as the systems developed have been getting more miscellaneous and complicated while at the same time humans have been attaching more value on their life, property and environment.

From concept until decommissioning, safety standards shall be adhered to avoid and control of systematic faults as well as control the random faults. The safety standards

possess detailed complex information and evolving continuously. A deep understanding of these standards is required to apply the requirements given in these standards, for that both theoretical and practical knowledge is compulsory.

International & national standards, regulations, and directives are to be followed for the safety acceptance. In today's technical safety-critical systems, independent safety assessment against the international standards shall be realized for the acceptance and approval of the system. The main international norm for the electronic systems is IEC 61508 [2], a very detailed standard consisting of 628 pages except the reference standards given in this norm itself to be used while applying this standard. Then, domain specific norms are derived from it. For the railway electronic systems, which is the selected domain in this study, the European Norms EN 50126 [16], EN 50129 [17], EN 50128 [18], and EN 50159 [19], dealing with RAMS, electronic system, SW, and transmission, respectively, are referenced in European countries and in several other countries outside Europa.

For the quantitative part of the safety, despite EN 50129 [17] defines some basic formulation concerning safety calculations regarding railway domain, IEC 61508 [2] provides formulas for quantitative analyses with respect to several architectures, however there is neither information nor reference about how these formulas are derived. Moreover, the formulas are only relevant for the homogenous configurations, i.e. in case the design utilizes diversity, the formulas are not applicable. Fuqua [20] explains Markov model from the reliability perspective, however no common cause faults (CCFs) are considered in this study. Kim et al. [21] analyses triple modular and dual system with Markov model where all the modules are same and no CCF is considered. Chen et al [22] gives Markov state transition for homogenous redundant system without CCF. Zhang et al [23] apply Markov model to IEC 61508 [2] to analyze availability of systems with self-diagnostic components, but no diverse design is dealt with neither CCF is involved as stated in the paper. Börcsök [24] gives the same formulas in the safety standard and places a Markov model creating state transition matrix without taking account the diversity, safe common cause failures or detected failures in dangerous undetected state. Börcsök and Schaefer [25] claim that the failure probability of a 1oo2 system can be determined with the fault tree, however as stated in Practitioner's Guide [26], when independence between component failures and/or repairs should not be assumed, stochastic processes should be used. Therefore, combinatorial models like FTA and RBD cannot be utilized for complex

safety systems with dependant failures. Ugljesa and Börcsök [27] evaluate sophisticated hardwares and develop PFD_{avg} for 2oo4 architecture, which does not scrutinize the effect of detected common cause failures. In the European Project STSARCES [28] , a Markov model is presented but it is mentioned that because of the total different structure of the two channels no common cause failures are presumed. The failure rate and unavailability equations are evaluated in [29] for parallel subsystems for revealed failures having a mean downtime of MDT, but underline that these are for identical subsystems.

Therefore, in this study, an innovative model for safety calculations is developed. Firstly, it places diverse design, which results in more states, but gives results that are more correct. It takes into account all plausible transitions and states including safe failures and safe common cause failures, both detected and undetected. In addition, new states such as “OK-SD”, “OK-DU&DD”, “OK-DU&SD” are defined. Moreover, special attention is paid to the detected faults, which is one of the main contribution of this study. In case there is a DD transition while the unit is at DU state, the unit shall transit to DU&DD state. Similar is also valid for SD transition at DU state where the unit will transit to DU&SD state. In the current studies, these conditions are overlooked, however they are crucial since when these conditions are occurred, then the system will not go a failure state in case of the second unit fails undetected or a CCF happens, but the system will go to FS state as the fault is detected. By this way, a better safety performance is reached. On the other hand, if there exists a SU failure while the unit is at DU state, this will not change the safety performance since the failure is not detected and no counter-measure can be applied for safety. Moreover, indicating SU faults in different states are important for reliability and availability analyses, since in case of their occurrence, the system cannot perform its intended function, but this state does not cause a dangerous result. Thereof, to avoid state explosion, SU faults are shown in FS state. In case, there exist SU fault, the system moves to FS state, however, in any other case such as while the system is at OK-DU state, if SU occurs, the system cannot transform to FS since there is DU fault. CCF for safe failures are also required, because in previous studies the safe failures are simply added, however it is not correct since after adding failure rates, the CCF shall be subtracted, i.e. $A \cup B = A + B - (A \cap B)$, otherwise it would be considered two times in a wrong way. As in the dangerous failures, two different CCF are defined for the safe failures, namely safe detected and safe undetected. The proposed model is developed for generic product and applied to the safety critical kernel computer to be used in an

unmanned CBTC metro systems and ERTMS ETCS for the specific application. The results are compared with the conventional methods. It is shown that results that are more accurate can be reached and the PFH calculation can be improved.

Besides, allocation of quantitative hazard rates is discussed in this work by revealing that there are different approaches for SIL attachments in the literature and industry. Beugin [30] complains about diverse interpretations and applications that exist for SIL definition in IEC 61508 [2] and unclearness to understand the SIL concept. Misumi and Sato [31] underline the essence of allocation of SILs to safety-related systems such that appropriate algorithms are to estimate average hazardous-event frequencies that can be obtained for arbitrary conditions of demands. Tang [32] in cooperation with Norwegian National Rail Administration concludes that the system complies with the SIL 4 random failure integrity. ETCS_OB01 is defined in SUBSET 091 [33] as the hazard rate for the ETCS on-board system, less those parts forming part of the transmission paths, shall be shown not to exceed a THR of 0.67x1E-09 dangerous failures/hour. Proposals are provided to overcome these ambiguities between system and functional approach of SIL allocation that cause different system safety performances for the same safety requirement needed. Besides, tool usage regarding IEC 61508 [2] and EN 50128 [18] and HMI related functions in SUBSET 091 and in the industry are indicated as disputable and new approaches are suggested.

In addition, while working on the study, the deficiency of detailed safety simulations is recognised. Chen et al. [22] simulated RAMS of triple-modular-redundant system and a dual-modular-duplex-redundant system and compared using the estimates of actual hardware failure rates. King [34] analyzed Hazardous Event Frequency per year with respect to demand rate. Nevertheless, neither effect of each parameter nor the crucial dependent failures were discussed in these studies. Smith and Gruhn [35] showed dependency of the safety system on some parameters at some level, however this study is not very detailed, the results were shown in bar charts with only two values such as low or high. Moreover, the architectures 1oo2D and 1oo3 were not covered and high demand/ continuous mode was not evaluated, but the behavior of parameters in high demand mode are very different as the algebraic equations differ essentially from each other in low and high demand mode for the same architecture. There are some studies like the one from Liu and Rausand [36] about proof testing effect or the one from Ilavsky et al. [37] about ß factor effect, but the work is limited to some parameters and some architectures.

Hokstad [38] interested only in how the DC is influenced when comparison of channels is applied as part of the diagnostic testing for multiple channel systems and suggests an alternative to define two betas, i.e. β for DU failures, and β_D for DD failures. With this dissertation, the gap of a detailed safety simulation is filled. Special attention is paid for the architecture 1oo2D regarding its model and normative definition. It is shown that some parameters affect unexpectedly the outcomes for some architectures such as the influence of the parameter DC for the architecture 1oo2D. It has also been uncovered that there are correlations between some parameters that seem independent. An advising route map is created newly to distill what kind of methods can be applied to decrease the hazard rates.

Furthermore, an evaluation of the aforementioned international safety standards, the CBTC standard IEEE Std. 1474.1 [39] and ERTMS ETCS Subset 091 [33] are realized about consistency of the information provided in these standards and their applicability. Open discussion and proposals for essential moot questions utilizing experiences gained in various safety-critical projects are provided. Moreover, the safety management plays a major role to keep critical development process under control by avoiding systematic faults. V&V concepts and organizational independence are handled in the study because they are neither clearly comprehensible in the safety standards nor discussed in the previous works. As Lundteigen et al. [40] states, verification and validation are important activities in all phases of the project development process, whilst the validation is illustrated as to be performed only at the end against system requirements in the standards. A new illustrative lifecycle for demonstrating verification and validation activities correctly is created. A new role as safety responsible is defined in the organizational diagram as this role fulfills the activities with special qualification and essential independency. An appropriate relation between verification, validation, quality and safety management is constructed in a consecutive way as proposed in this study such that the safety management report is produced step by step resulting in a ready safety management report at the end of the project that could be simply integrated into the safety case to be assessed by the independent assessor.

1.2 Objective of the Thesis

The objectives of this thesis are to perform researches on the quantitative and qualitative methods to design mission critical safe and reliable controller with very low average

frequency of a dangerous failure, to propose new qualitative and quantitative approaches including safety calculation modelling in the light of the performed researches and to compare the proposed approaches with the state of the art. The studies are listed below:

- Identifying the characteristics of selected application domain, namely unmanned CBTC metro systems and ERTMS ETCS; and allocating the THR to the safety critical controller constituent.
- Examining the correctness, completeness and consistency of the safety requirements, safety management and V&V concepts in the international safety standards and in the industry; and contributing to the enhancement of these standards by proposing new approaches to fil gaps,
- Investigating reliability, safety, maintainability and availability calculation methodologies including modelling of dependant failure which has the vital importance for the redundant systems,
- Simulating PFH of various architectures with respect to safety parameters to analyze their influences on the safety performance, to develop a design route map to decrease the hazard rates, creating a new definition for a safety architecture which is neither in the class of 1oo2 nor 1oo2D.
- Developing a new model for safety calculations,
- Performing reliability, availability and safety calculations of the safety critical kernel computer to be used in unmanned CBTC metro systems and ERTMS ETCS in accordance to different reliability handbooks, IEC 61508 [2] safety standard and proposed model and comparing the results.

1.3 Hypothesis

Developing safety critical systems require long years of planned investments, broad theoretical knowledge and domain experience as the resulted system will have impacts on human life, property and environment. Besides, any change in the design requires re-performing of exhaustive verification, validation and assessment from the planning phase to the commissioning phase regarding all system, HW and SW development life cycles. Therefore, the current state of art is oriented to Generic Application or Product (GAP) designs rather than specific developments. On the other hand, development of GAP increases the complexity since the designed system shall be able to work at several applications with different configurations.

Safety requirements aim avoidance and control of systematic faults as well as control of random faults. For demonstrating that random faults are kept under the tolerable rates, quantitative hazard analyses are performed. Paramount importance shall be attached to the definition of THR since the definition of what the hazard rate is allocated to influences the expected outcomes and the correct operation of the safety-critical system. In the domain of this study, the quantitative requirements allocated to functions of critical constituents are obtained much lower than the highest SIL defined in the safety standard. To reach these very low PFH, methods are researched. Besides, in this dissertation, a new calculation model is proposed which is more accurate than the formulas provided in the main functional safety standard of electrical/ electronic/ programmable electronic safety-related systems IEC 61508 [2]. In addition, the aforementioned standard only provides formulas for homogenous redundancy. However, to decrease dependent failures, diverse design is crucial. The model given in this study places diverse design, which results in more states, but enables results that are more correct, since otherwise formulas for homogenous redundancy were used. The proposed model is developed for generic product and applied to the safety critical kernel computer to be used in unmanned CBTC metro systems and ERTMS ETCS for the specific application. The results are compared with the conventional methods. It is shown that results that are more accurate can be reached and the PFH calculation can be improved.

CHAPTER 2

ERTMS ETCS AND CBTC DESCRIPTION AND THEIR QUANTITATIVE SAFETY REQUIREMENTS

In this section, the European Railway Traffic Management System (ERTMS) / European Train Control System (ETCS) and Communication Based Train Control (CBTC), which is the selected domain in this thesis and thereof the most possible application areas, but not limited to, of the mission critical computer is explained with the intent of establishing background knowledge about the domain.

2.1 ERTMS ETCS

The ERTMS has been being developed by five European Rail Industry Association (UNIFE) members - Alstom Transport, Ansaldo STS, Bombardier Transportation, Siemens Mobility and Thales – to which new members AZD Praha, CAF, Mermec are added recently, in cooperation with the European Union (EU), railway stakeholders and the GSM-R industry. It is the new concept of train control and signalling that consist of automatic train protection (ATP), named as European Train Control System (ETCS), and radio system, Global System for Mobile Communication – Railway (GSM-R), with the purpose of providing voice and data communication between the track and the train, that uses specific frequencies reserved for rail application with certain specific and advanced functions.

Currently there are more than 20 train control systems across the EU. Besides varying in safety levels required by different operators, these are stand-alone and non-interoperable, and hence require extensive integration, engineering effort, raising total delivery costs for cross-border traffic. For instance, Thalys train sets running between Paris-Brussels-Cologne and Amsterdam have to be equipped with 7 different types of train control systems, which brings considerable costs [41]. With the ERTMS concept, the aim is to

develop one harmonised system, such that it replaces the domestic train control and command systems stepwise.

ERTMS has been deployed not only in Europa, but also outside of Euro zone. Below, the actual status of the contracted lines and vehicles equipped with ERTMS are given.

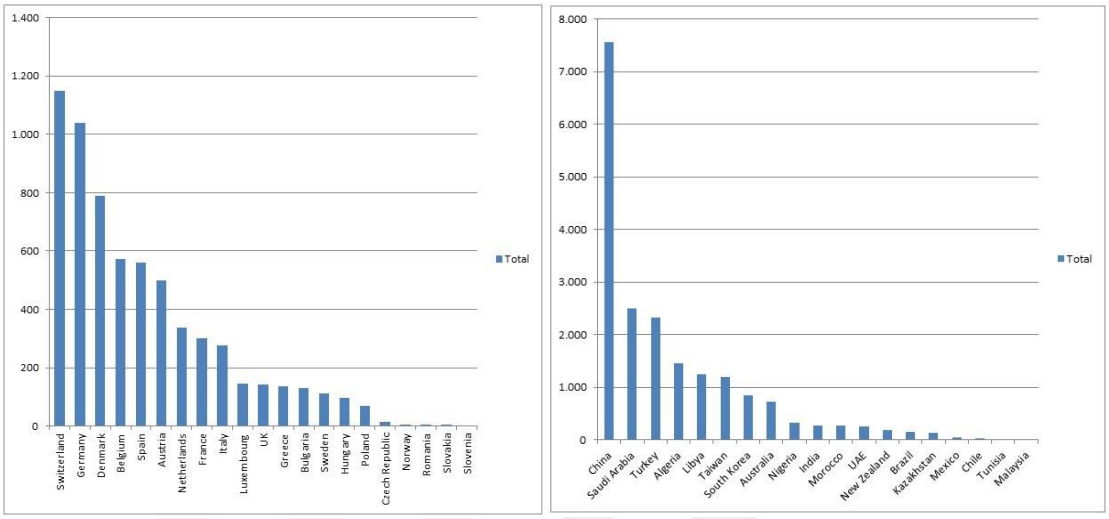


Figure 2.1 Global ERTMS contracted tracks (km) and vehicles in Europe [41]

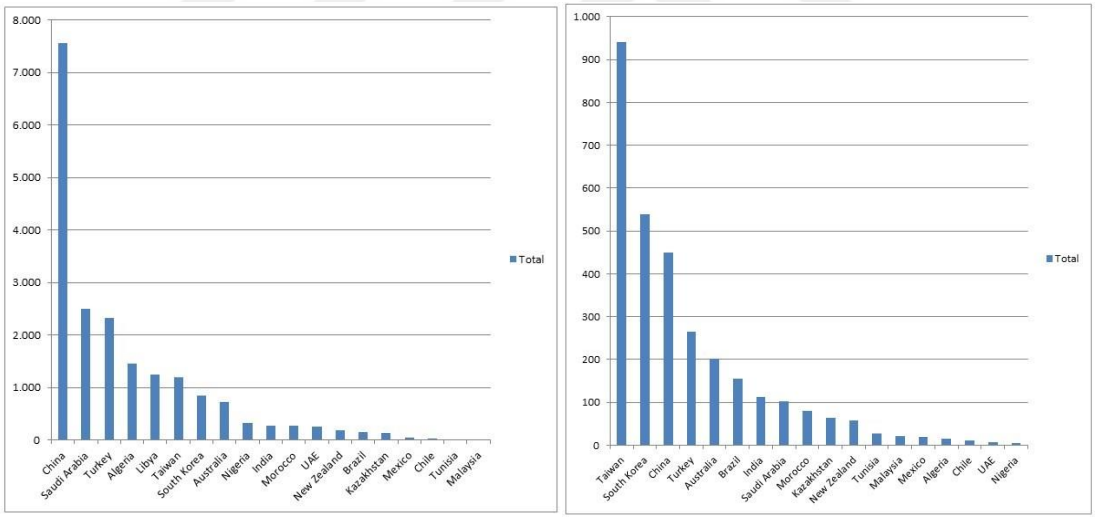


Figure 2.2 Global ERTMS contracted tracks (km) and vehicles in non-European countries [41]

2.1.1 ERTMS History

In 1989 the EC launched a study on the issue of using various different systems. With the aim of creating an initial version of functional specifications, the ERTMS User Group (EUG EEIG) consisted of infrastructure administrators was created in 1990 and later on suppliers were added. In 1998, UNISIG was created by the main European signalling companies, with the aim of helping to finally develop the system specifications. The first

version of the System Requirement Specifications (SRS), was delivered April 1999. With the final signature by the European Commission on ERTMS specifications (Class 1 version 2.0.0) in April 2000, the interoperability of railway control, command and signalling started working towards removing borders. As well as the development of the technical ERTMS specifications, in 1993 the EU council issued the Interoperability Directive and a decision was taken to create a structure to define the Technical Interoperability Specifications. The EU Council Directives 96/48/EC and 1001/16/EC were developed for the interoperability of the trans-European high speed and the conventional rail system. Subsequent decisions have created a greater commitment to ERTMS by Member States. In 2004, the European Railway Agency (ERA) was created and designated as the ERTMS system authority, and thus is in charge of managing system specifications [42].

2.1.2 ERTMS/ETCS Context

As described in SUBSET 091 [33], the operational environment requires that the on-board part of the ERTMS/ETCS Reference Architecture must interface with defined entities throughout Europe in order to achieve technical and operational interoperability. These are denoted by the items within the Harmonised Domain. The ERTMS/ETCS Reference Architecture and the harmonised items are required to work in conjunction with national signalling systems. These items are shown within the National Signalling Domain. The scope of the UNISIG work is the analysis of the ERTMS/ETCS Reference Architecture.

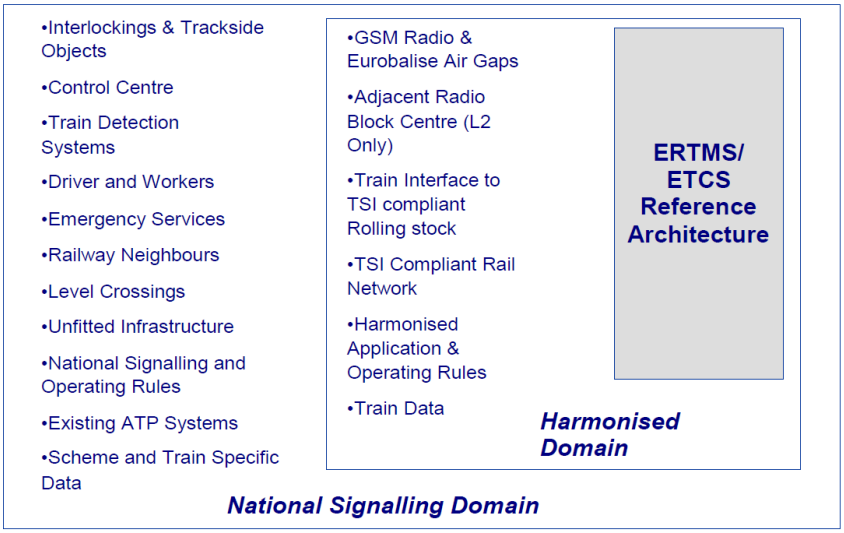


Figure 2.3 Signalling domains [43]

2.1.3 ETCS System Architecture

ETCS system is comprised by the on-board and trackside subsystems.

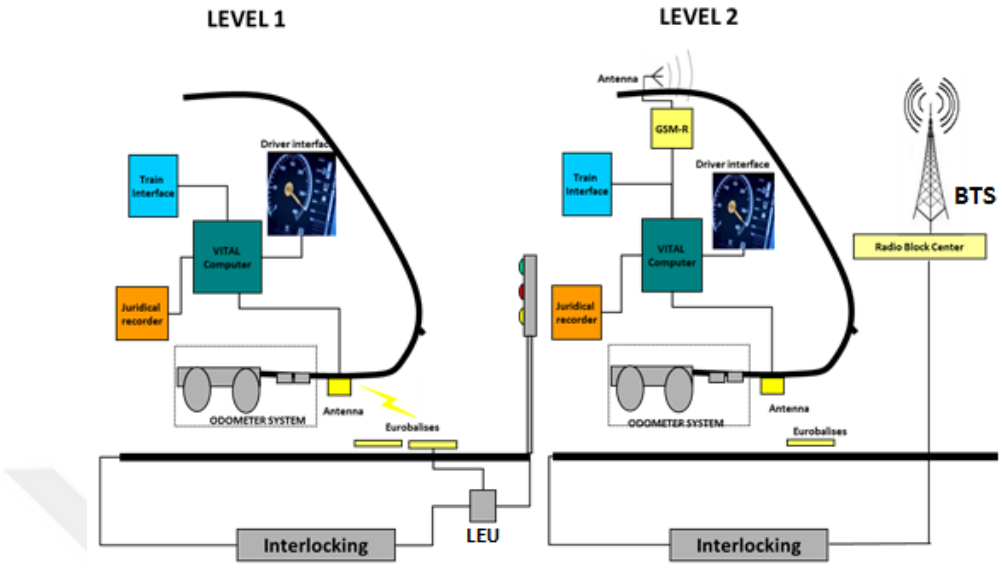


Figure 2.4 ETCS constituents [42]

Constituents composing both subsystems with their functions are described below.

ETCS trackside constituents

- Eurobalise is spot transmission equipment sending fixed or variable information to the onboard and is energized by an electromagnetic field.
- Lineside Electronic Unit (LEU) connects Eurobalises and Euroloops to the signaling system.
- The radio communication network (GSM-R) is the radio network distributed along the railway providing bi-directional exchange of data between the onboard and RBC. Voice communication is realized over GSM-R, too.
- The Radio Block Centre (RBC) receives information from interlocking and sends MAs to train as messages.
- Euroloop transmits signaling information activated by a magnetic field to the train semi-continuously.
- Radio Infill unit (RIU) transfers the signaling information to the train with regard to the main signal via the GSM-R radio channel.
- Key Management Centre (KMC) manages the configuration and the deployment of the cryptographic keys as transmission links implemented over open GSM-R is vulnerable to attacks.

ETCS on board constituents

The ERTMS/ETCS On-Board equipment and the On-Board part of the GSM-R radio system constitute the On-Board subsystem. The On-Board equipment supervises the train movement on basis of information exchanged with the trackside sub-system. The GSM-R On-Board radio system is used for the bi-directional exchange of messages between On-Board sub-system and RBC.

- European Vital Computer (EVC) provides the supervision of the train movements against all the inputs received from the trackside equipment, onboard odometry, the driver and other stored information. The EVC provides outputs to the driver through the DMI, to other train systems and functions through the TIU and transmits information back to the RBC if provided.
- GSM-R Mobile Unit is used for the bidirectional exchange of messages between onboard subsystem and RBC.
- Juridical Recorder Unit (JRU) provides an interface for the provision of juridical data, which can be used to support investigation of incidents and routine system monitoring.
- Train Interface Unit (TIU) provides the necessary interfaces for the control of other train's onboard functions below:
    - Train braking system control: Service and emergency brake control,
    - Train control: Change of traction, raising / lowering of an overhead pantograph and activation/deactivation of air tightness,
    - Engine control: Traction power cut-off,
    - Cab status information: Determination of the position of the direction controller and open/closed cab desk,
    - Cold Movement Detector: Detection and recording of vehicle movements while the ATP equipment is in no power mode,
    - Isolation Switch: Physically isolation of the On-Board system from the traction unit’s braking system and other onboard systems.
- Odometry consists of different type of sensors for informing about both speed and distance travelled with high integrity and accuracy.
- Driver Machine Interface (DMI) realizes the following functions:
    - Providing the means for the driver to enter data into the ATP system,
    - Displaying actual train speed,

- Displaying supervised speed and changes ordered by the ERTMS trackside equipment,
- Displaying information about the route ahead,
- Alerting the driver to changes in supervision, errors and other warnings (visually and audibly), including text messages.

- Balise Reader Subsystem energizes the balise, enabling the balise to transmit messages to the train and then receives the message and passes it on to the EVC via a Balise Transmission Module (BTM).

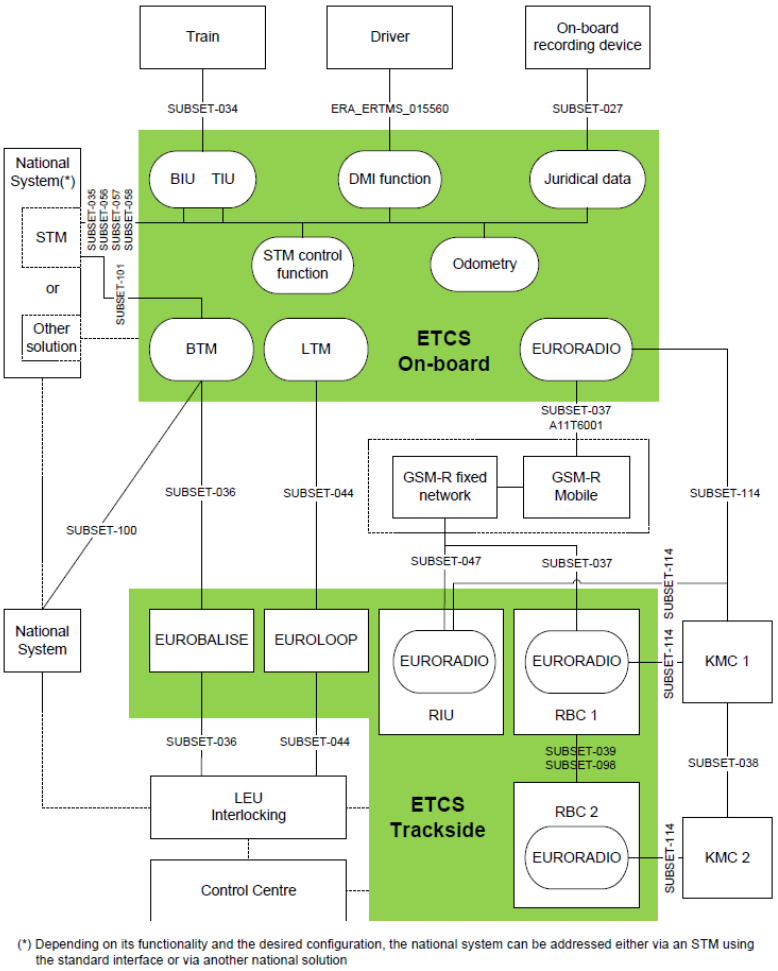


Figure 2.5 ETCS Architecture [43]

The internal and external interfaces for on-board system are classified as below:

On-board Internal Interfaces

- EVC – Odometer Subsystem Interface
- EVC – Balise Reader Subsystem Interface
- EVC – GSM-R Subsystem Interface

- EVC – DMI Interface
- EVC – JRU Interface
- EVC – TIU Interface

On-board External Interfaces

- Train – Odometer Interface
- Balise – Balise Reader Subsystem Interface
- Driver – Cab Radio Interface*
- RBC – On-Board GSM-R Subsystem
- DMI – Driver Interface
- Maintainer - JRU Interface
- Driver – TIU Interface
- EVC2(TIU of EVC2) – TIU Interface
- ATS-TIU Interface**
- Pantograph – TIU Interface
- Master Controller – TIU Interface
- Braking Subsystem – TIU Interface
- Traction – TIU Interface
- Ventilation – TIU Interface
- Doors – TIU Interface
- TCMS – TIU Interface

*Cab Radio is not mandatory for the ERTMS ETCS architecture. It a stand-alone constituent and it has no interface to EVC.

**ATP will activate or deactivate the ATS using a vital output according to the type of wayside area the train is running on. This control is fail-safe such that not energized output activates ATS while energized output deactivates ATS. Applying emergency brake will not be affected by the status of ATS.

2.1.4 ERTMS/ETCS Application Levels

Track and train co-operations differ due to various operating needs and goals. Therefore, different levels are categorized in accordance with to the data medium to on-board system, trackside equipment and also functions processed in SUBSET 026 [43].

Application Level 0

ERTMS Level 0 covers operation of ERTMS equipped trains on lines not equipped with ERTMS or national systems or on lines where trackside ERTMS infrastructure and/or national systems may exist but operation under their supervision is currently not possible. The movement authority is provided by the lineside optical signals, train borne equipment only supervises the train with regard to the maximum speed and no supervisory information is displayed on the DMI except the train speed. The onboard equipment reads the Eurobalises to ensure that level transition can take place and to supervise temporary speed restrictions.

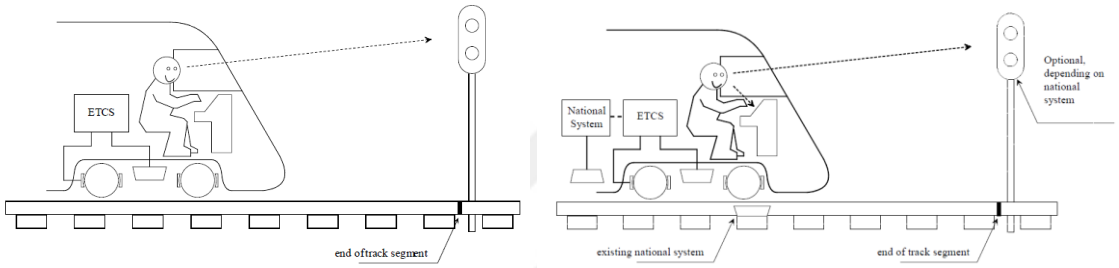


Figure 2.6 ERTMS/ETCS Level 0 and NTC [33]

Application Level NTC

The train is equipped with ERTMS/ETCS operating on a line equipped with a national system. Train control information generated trackside by the national train control system is transmitted to the train via the communication channels of the underlying national system. Level NTC uses no ERTMS/ETCS track-train information except to announce/command level transitions and specific commands related to balise transmission. Eurobalises therefore still have to be read.

Application Level 1

ERTMS Level 1 is a spot transmission based train control system to be used as an overlay on an underlying signaling system.

In Level 1, Eurobalises, which are installed on the track, receive signaling data from the existing lineside signals via signal adapter and telegram encoder (LEU) together with the route data to the train. The ATP uses this data to calculate the maximum speed and the braking curve. Since Eurobalises are installed near the main signal and spot transmission used, the train has to travel over the Eurobalises in order to get a new movement authority.

In Level 1, Euroloop or RIU can be used to send in advanced semi-continuous signaling information to the train regarding the next main signal in the train running direction. In the case of RIU the signaling information is sent via the GSM-R network, therefore GSM-R coverage is required even though this is not mandatory for Level 1.

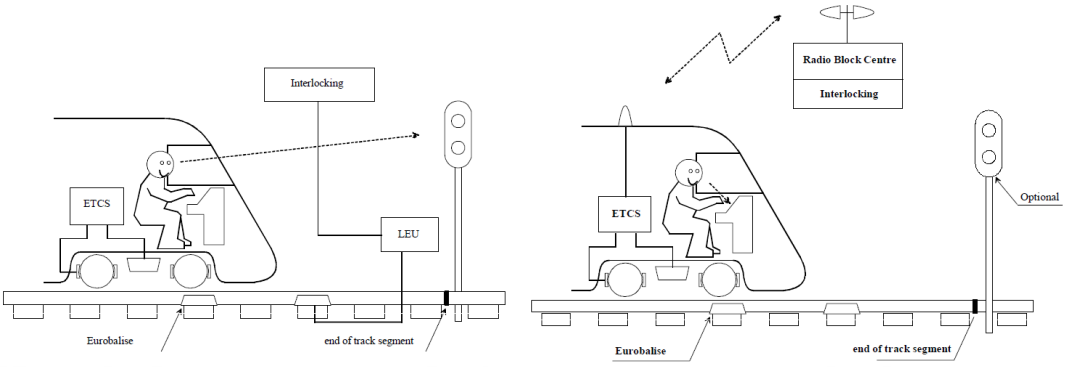


Figure 2.7 ERTMS/ETCS Level 1 and 2 [43]

Application Level 2

ERTMS Level 2 is a radio based train control system, which is used as an overlay on an underlying signaling system.

Level 2 does not require lineside signals. Information about the status of the track occupancy is sent by the interlocking to the RBC. Based on this information and the train position information sent regularly by onboard ERTMS/ETCS, the RBC generates the correct movement authorities for the different trains in the section. In Level 2, the Eurobalises are used to transmit fixed data such as train location, gradient, speed limit etc.

Application Level 3

It is a radio based train control system where movement authorities are generated trackside and are transmitted to the train via Euroradio. ERTMS/ETCS Level 3 provides a continuous speed supervision system, which also protects against overrun of the authority. Train position and train integrity supervision are performed by the trackside radio block center in co-operation with the train (which sends position reports and train integrity information). Level 3 is based on Euroradio for track to train communication and on Eurobalises as spot transmission devices mainly for location referencing. The trackside RBC, which provides the information to the trains, knows each train individually by the ERTMS/ETCS identity of its leading ERTMS/ETCS onboard equipment. In this level, there is no track occupancy detection system like track circuit or

axle counter as the traffic is not based on fixed blocks, but moving blocks. In fixed block systems, a predefined static track sections is allocated for a train movement whereas in the moving block, the block lengths are dynamically allocated to movements which decreases headways, hence allowing more trains on the track without comprising safety.

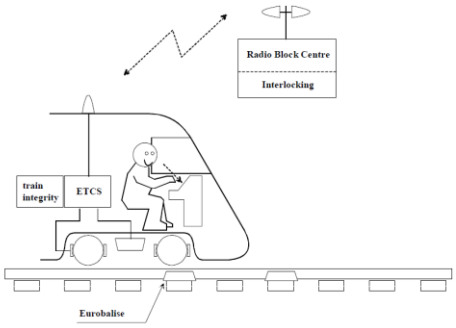


Figure 2.8 ERTMS/ETCS Level 3 [43]

2.1.5 Modes, Transitions and Procedures

There are sixteen operation modes defined in SUBSET 026 [43]. Although a grouping is not provided in the SUBSET, these can be grouped as following taking into account their functionality, to make them more comprehensible.

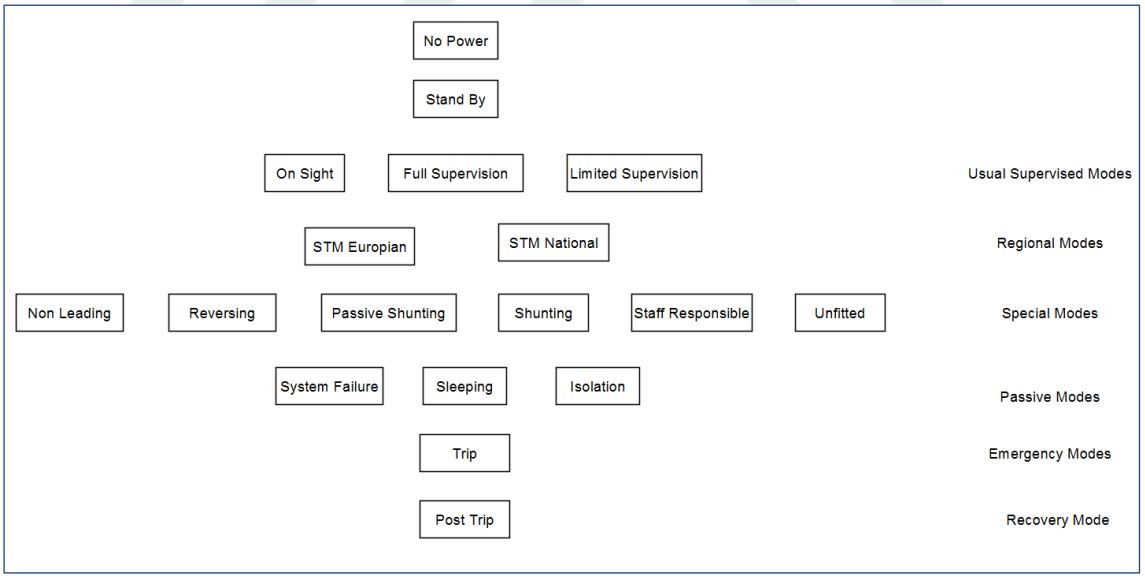


Figure 2.9 ERTMS modes in groups

These modes are elaborated as follows.

- NO POWER (NP): A transition to NP will be initiated automatically when the normal power supply to the ERTMS onboard equipment is interrupted.

- FULL SUPERVISION (FS): The full protection and highest level of supervision. All non-permissive moves should be implemented in FS. System design must maximize FS use.
- ON SIGHT (OS): OS enables the train to enter into a track section that could be occupied by another train or obstacle.
- LIMITED SUPERVISION (LS): Transitory step where the underlying signalling system is not life expired and full ERTMS infrastructure fitment is not cost effective, but there is an operational benefit in providing some supervision and protections.
- STAFF RESPONSIBLE (SR): Staff Responsible mode (SR) is offered to the driver when the ETCS onboard equipment does not have all the data necessary to enter FS or OS mode.
- SHUNTING (SH): The driver can select Shunting (SH) mode and is responsible for the movement of the train.
- UNFITTED (UN): In Application Level 0 (area of track not fitted with ETCS equipment), the ETCS onboard equipment operates in Unfitted (UN) mode.
- NON-LEADING (NL): NL is designed to facilitate tandem working and can be used for banking movements (where two or more ERTMS fitted traction units form part of the same train formation but are not electrically connected and require a driver on each traction unit) and is the ERTMS operating mode used by other than the leading traction unit.
- ISOLATION (IS): Onboard equipment physically isolated from the brakes and other equipments/systems depending on isolation switch.
- TRIP (TR): If the ETCS onboard equipment determines that the train has exceeded its permitted MA, it applies the emergency brakes and enters Trip (TR) mode.
- POST-TRIP (PT): A transition to PT will be initiated automatically by the ERTMS onboard equipment when the train is at a stand and the driver has acknowledged the transition to TR.
- SLEEPING (SL): A train, or locomotive, may have more than one set of ETCS onboard equipment. When one set is active, all other sets are in Sleeping (SL) mode.

- STAND-BY (SL): SB is the default operating mode for the ERTMS onboard equipment and is the initial mode used at the start of mission process.
- SYSTEM FAILURE (SF): The ERTMS/ETCS on-board equipment shall switch to the System Failure mode in case of a fault, which affects safety.
- REVERSING (RV): The Reversing mode allows the driver to change the direction of movement of the train and drive from the same cab, i.e. the train orientation remains unchanged. This shall be possible only in areas so marked by trackside.
- NATIONAL SYSTEM (SN): In SN mode, according to the specific on-board implementation, the National System may access the DMI, Juridical Recording interface, odometer, train interface and brakes via the ERTMS/ETCS on-board equipment.

To switch between the modes, seventy-four conditions are defined in SUBSET 026 [43]. For instance, to switch from NP to SH, the conditions are 5, 6, and 50 which are given below in the same order:

(train is at standstill) AND (ERTMS/ETCS level is 0 or NTC or 1) AND (driver selects Shunting mode)

OR

(train is at standstill) AND (ERTMS/ETCS level is 2 or 3) AND (reception of the information “Shunting granted by RBC”, due to a Shunting request from the driver)

OR

(An ackn. request for Shunting is displayed to the driver) AND (the driver acknowledges)

There is also prioritization for the conditions to avoid any race between the modes i.e. discrete states.

Table 2.1 Transition table [43]

NP	<29 -p2-	<29 -p2-	<29 -p2-	<29 -p2-	<29 -p2-	<29 -p2-	<29 -p2-	<29 -p2-	<29 -p2-	<29 -p2-	<29 -p2-	<29 -p2-	<29 -p2-		<29 -p2-	<29 -p2-
4> -p2-	SB	<22 -p4-	<19, 27, 30 -p5-	<28 -p5-	<28 -p5-	<28, -p5-	<28, -p5-	<2, 3 -p3-	<28, 47 -p3-	<28, -p6-		<28, -p4			<28 -p6-	<28 -p4-
		PS	<26 -p5-													
	5, 6, 50> -p7-	23> -p4	SH	<5,6, 50,51 -p6-	<5,6, 50,51 -p6-	<5,6, 51 -p6-	<5,6 50,51 -p6-			<5,61 -p7-	<68 -p4	<5,6, 50 -p5-			<5,61 -p7	
	10> -p7-			FS	<31,32 -p6-	<31,32 -p6-	<31,32 -p6-			<25 -p7-		<31 -p5-			<25 -p7-	
	70> -p7-			70,72> -p6-	LS	<72 -p6-	<70,74 -p6-			<71 -p7-		<70 -p5-			<71 -p7-	
	8,37> -p7-			37> -p6-	37> -p6-	SR	<37 -p6-			<44,45 -p4-		<8,37 -p5-			<44,45 -p4-	
	15> -p7-			15,40> -p6-	15,73> -p6-	40> -p6-	OS			<34 -p7-		<15 -p5-			<34 -p7-	
	14> -p5-	14> -p4						SL								
	46> -p6-		46> -p5-	46> -p6-	46> -p6-	46> -p6-	46> -p6-		NL							
	60> -p7-			21> -p6-	21> -p6-	21> -p6-	21> -p6-			UN	<62 -p4-				<21 -p7-	
	20> -p4-		49,52, 65> -p4-	12,16, 17,18, 20,41, 65,66, 69> -p4-	12,16, 17,18, 20,41, 65,66, 69> -p4-	18,20, 42, 43, 36, 54,65> -p4-	12,16, 17,18, 20,41, 65,66, 69> -p4-			67,39, 20> -p5-	TR				<67, 39,38, 35,20 -p5-	
											7> -p4-	PT				
	13> -p3-	13> -p3-	13> -p3-	13> -p3-	13> -p3-	13> -p3-	13> -p3-			13> -p3-	13> -p3-	13> -p3-	SF		<13 -p3-	<13 -p3-
1> -p1-	1> -p1-	1> -p1-	1> -p1-	1> -p1-	1> -p1-	1> -p1-	1> -p1-	1> -p1-	1> -p1-	1> -p1-	1> -p1-	1> -p1-	1> -p1-	IS	<1 -p1-	<1 -p1-
	58> -p7-			56> -p6-	56> -p6-	56> -p6-	56> -p6-			56> -p7-	63> -p4-				SN	
				59> -p6-	59> -p6-		59> -p6-									RV

Beside mode and transitions, procedures are required to operate ERTMS ETCS system. SUBSET 026-5 details the procedures in about 90 pages. They define the necessary reaction of the ERTMS/ETCS entities (subsystems and components like on-board equipment, RBC, balise or the driver) to either information exchanged between ERTMS/ETCS entities or events (triggered by external entities or internal events). The procedures are given below:

- Procedure Start of mission
- Procedure End of Mission
- Shunting Initiated by Driver

- Entry in Shunting with Order from Trackside
- Procedure Override
- Procedure On-Sight
- Level Transitions
- Procedure Train Trip
- Change of Train Orientation
- Train Reversing
- Joining / Splitting
- RBC/RBC Handover
- Procedure passing a non-protected Level Crossing
- Changing Train Data from sources different from the driver
- Indication of Track Conditions
- Procedure Limited Supervision

Flowcharts visualize procedure flows in a more comprehensive way as provided below for the start of mission procedure.

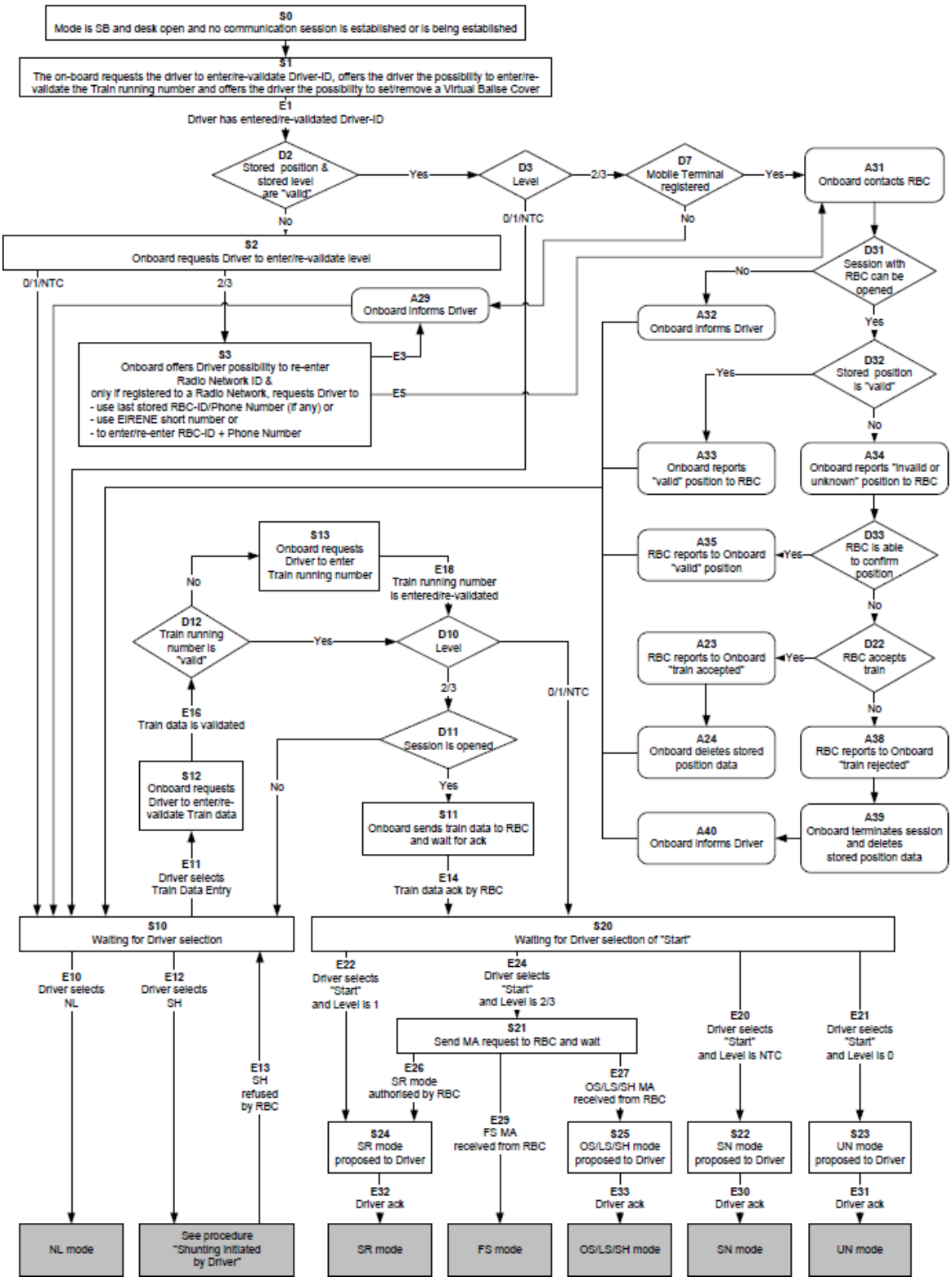


Figure 2.10 Flowchart for “Start of Mission” [43]

2.1.6 ERTMS Documentation Structure

In this part, first ERTMS interoperability documents are presented to give an idea about the project extent and complexity. Afterwards, the main documents to be considered in the thesis are mentioned.

A. Interoperability Documentation

For the project ERTMS, there have been created several documents that can be categorized as set of specifications - binding, supporting informative specifications - used to derive the specifications, and supporting documents - giving further explanations about some specific items. These can be obtained free of charge from the ERA webpages [44], [45] and [46], respectively. The number (#) symbol for set of specification means that # 1 relates with the ETCS baseline 2 and GSM-R baseline 1 whereas # 2 stands for ETCS baseline 3 and GSM-R baseline 1.

Table 2.2 Set of specifications # 2 (ETCS baseline 3 and GSM-R baseline 1)

Index	Reference	Title
3	SUBSET-023	Glossary of Terms and Abbreviations
4	SUBSET-026	System Requirements Specification
5	SUBSET-027	FIS Juridical Recording
6	ERA ERTMS 015560	ETCS Driver Machine Interface
7	SUBSET-034	Train Interface FIS
8	SUBSET-035	Specific Transmission Module FFFIS
9	SUBSET-036	FFFIS for Eurobalise
10	SUBSET-037	EuroRadio FIS
11	SUBSET-038	Offline key management FIS
12	SUBSET-039	FIS for the RBC/RBC handover
13	SUBSET-040	Dimensioning and Engineering rules
14	SUBSET-041	Performance Requirements for Interoperability
16	SUBSET-044	FFFIS for Euroloop
19	SUBSET-047	Trackside-Trainborne FIS for Radio infill
20	SUBSET-048	Trainborne FFFIS for Radio infill
23	SUBSET-054	Responsibilities and rules for the assignment of values to ETCS variables
25	SUBSET-056	STM FFFIS Safe time layer
26	SUBSET-057	STM FFFIS Safe link Layer
27	SUBSET-091	Safety Requirements for the Technical Interoperability of ETCS in Levels 1 and 2
29	SUBSET-102	Test specification for interface "K"
31	SUBSET-094	Functional requirements for an on-board reference test facility
32	EIRENE FRS	GSM-R Functional Requirements Specification

Table 2.2 Set of specifications # 2 (ETCS baseline 3 and GSM-R baseline 1) (cont'd)

33	EIRENE SRS	GSM-R System Requirements Specification
34	A11T6001	(MORANE) Radio Transmission FFFIS for EuroRadio
36c	SUBSET-074-2	FFFIS STM Test cases document
37b	SUBSET-076-5-2	Test cases related to features
37c	SUBSET-076-6-3	Test Sequences
38	6,00E+68	ETCS marker-board definition
39	SUBSET-092-1	ERTMS EuroRadio Conformance Requirements
40	SUBSET-092-2	ERTMS Euroradio Test cases Safety Layer
43	SUBSET-085	Test specification for Eurobalise FFFIS
44	Intentionally deleted	Odometry FIS
45	SUBSET-101	Interface "K" Specification
46	SUBSET-100	Interface "G" Specification
48	Reserved	Test specification for mobile equipment GSM-R
49	SUBSET-059	Performance requirements for STM
50	SUBSET-103	Test specification for Euroloop
52	SUBSET-058	FFFIS STM Application layer
60	SUBSET-104	ETCS System Version Management
63	SUBSET-098	RBC-RBC Safe Communication Interface
64	EN 301 515	Global System for Mobile Communication; Requirements for GSM operation on railways
65	TS 102 281	Detailed requirements for GSM operation on railways
66	TS 103 169	ASCI Options for Interoperability
67	(MORANE) P 38 T 9001	FFFIS for GSM-R SIM Cards
68	ETSI TS 102 610	Railway Telecommunication; GSM; Usage of the UUIE for GSM operation on railways
69	(MORANE) F 10 T 6002	FFFS for Confirmation of High Priority Calls
70	(MORANE) F 12 T 6002	FIS for Confirmation of High Priority Calls
71	(MORANE) E 10 T 6001	FFFS for Functional Addressing
72	(MORANE) E 12 T 6001	FIS for Functional Addressing
73	(MORANE) F 10 T 6001	FFFS for Location Dependent Addressing
74	(MORANE) F 12 T 6001	FIS for Location Dependent Addressing
75	(MORANE) F 10 T 6003	FFFS for Presentation of Functional Numbers to Called and Calling Parties
76	(MORANE) F 12 T 6003	FIS for Presentation of Functional Numbers to Called and Calling Parties
77	ERA/ERTMS/033281	Interfaces between CCS track-side and other subsystems
78	Intentionally deleted	Safety requirements for ETCS DMI functions
79	SUBSET-114	KMC-ETCS Entity Off-line KM FIS
80	Intentionally deleted	GSM-R Driver Machine Interface
81	SUBSET-119	Train Interface FFFIS
82	SUBSET-120	FFFIS TI - Safety Analysis

Table 2.3 List of supporting informative specifications - Set of specifications # 3

Index	Reference	Title
1	02S126	RAM requirements (chapter 2 only)
2	97S066	Environmental Conditions
3	SUBSET-074-1	Methodology for testing FFFIS STM
4	9,70E+268	Odometer FFFIS
5	O_2475	ERTMS GSM-R QoS Test Specification
7	SUBSET-074-3	FFFIS STM Test Specification traceability of test cases with Specific Transmission Module FFFIS
8	SUBSET-074-4	FFFIS STM test specification traceability of testing the packets specified in the FFFIS STM Application Layer
9	SUBSET-076-0	ERTMS/ETCS Class 1, test plan
16	SUBSET-076-6-1	Test database
19	SUBSET-077	UNISIG Casual Analysis Process
20	SUBSET-078	Failure Modes and Effects Analysis for the Interface to/from an Adjacent RBC - in Application Level 2
21	SUBSET-079	MMI: failure modes and effects analysis
22	SUBSET-080	TIU: failure modes and effects analysis
23	SUBSET-081	Transmission system: failure modes and effects analysis
24	SUBSET-088	ETCS Application levels 1 and 2 - safety analysis
25	TS50459-1	Railway applications - Communication, signalling and processing systems - European Rail Traffic Management System - driver machine interface
27	TS50459-3	Railway applications - Communication, signalling and processing systems - ERTMS - driver machine interface Part 3 - Ergonomic arrangements of ERTMS/GSM-R information
28	TS50459-4	Railway applications - Communication, signalling and processing systems - ERTMS - driver machine interface Part 4 - Data entry for the ERTMS/ETCS/GSM-R systems
29	TS50459-5	Railway applications - Communication, signalling and processing systems - ERTMS - driver machine interface Part 5 - Symbols
30	TS50459-6	Railway applications - Communication, signalling and processing systems - European Rail Traffic Management System - driver machine interface Part 6 - Audible information
37	SUBSET-093	GSM-R Interfaces - Class 1 requirements
40	ERA/ERTMS/040063	Test sequences evaluation and validation
43	4,00E+83	Safety Requirements and Requirements to Safety Analysis for Interoperability for the Control-Command and Signalling Sub-System
44	4,00E+84	Justification Report for the Safety Requirements and Requirements to Safety Analysis for Interoperability for the Control-Command and Signalling Sub-System
47	SUBSET-113	Report from UNISIG Hazard Log
48	TS50328-2	Railway applications - Compatibility between rolling stock and train detection systems - Part 2: Compatibility with track circuits

Table 2.3 List of supporting informative specifications - Set of specifications # 3 (cont'd)

49	TS50238-3	Railway applications - Compatibility between rolling stock and train detection systems - Part 3: Compatibility with axle counters
53	SUBSET-118	Functional Safety Analysis of ETCS DMI
54	SUBSET-119	Train Interface FFFIS
55	SUBSET-120	FFFIS Train Interface -" Safety analysis
56	SUBSET-129	FIS for the RBC/RBC Handover involving a Baseline 2 RBC
57	SUBSET-116	Eurobalise On-board equipment susceptibility test specification
58	O-2875	ERTMS/GSM-R Quality of Service test specification for EIRENE QoS requirements Voice and non-ETCS data

And the supporting documents are grouped as below.

Supporting documents concerning the braking aspects:

- Introduction to ETCS braking curves
- Braking curves simulation tool

Supporting documents concerning certification:

- Report on ERTMS equipment certification

Supporting documents concerning studies contracted by ERTMS unit:

- Survey of Safety approvals for the first ERTMS implementations
- Feasibility study for the formal specifications of ETCS functions
- Final report of the study on DMI safety
- Study for the evolution of the railways communications system
- Study for the evolution of GSM-R
- Study on migration of railway radio communication
- Study on co-existence of GSM-R and other radio technologies

Supporting documents concerning GSM-R test cases:

- Test Plans
- Test Reports
- Test Specification
- Network assessment (draft)

- Cab radio (draft)

B. Reference ERTMS Documentation for this Study

The relevant subsets of this study are SUBSET 026 System Requirements Specification [43], SUBSET 091 Safety Requirements for the Technical [33] and SUBSET 088 ERTMS ETCS Safety Analysis [47]. SUBSET 026 and 088 are comprised of various parts expressed below.

a. System Requirements Specification SUBSET 026

- Introduction
- Basic System Description
- Principles
- Modes and Transitions
- Procedures
- Management of older System Versions
- ERTMS_ETCS Language
- Messages

b. ERTMS ETCS Safety Analysis SUBSET 088

- ETCS Application Levels 1 & 2 - Safety Analysis - Part 0 Document Overview
- ETCS Application Level 1 - Part 1 Safety Analysis Functional Fault Tree
- ETCS Application Level 2 - Part 1 Safety Analysis Functional Fault Tree
- ETCS Application Level 1 - Part 2 - Functional Analysis Safety Analysis
- ETCS Application Level 2 - Part 2 - Functional Analysis Safety Analysis
- ETCS Application Levels 1 & 2 - Safety Analysis - Part 3 - THR Apportionment

c. Reference SUBSETs to SUBSET 088:

- SUBSET-078 v.3.3.3 Failure Modes and Effects Analysis for the Interface to/from an Adjacent RBC - in Application Level 2
- SUBSET-079-1 v.3.13.0 Failure Modes and Effects Analysis for DMI-Subsystem in Application Level 1
- SUBSET-079-2 v.3.13.0 Failure Modes and Effects Analysis for DMI-Subsystem in Application Level 2
- SUBSET-080 v.3.0.12 Failure Modes and Effects Analysis for TIU in Application Level 1 and Level 2
- SUBSET-081-1 v.3.4.3 Failure Modes and Effects Analysis for Transmission System in Application Level 1

- SUBSET-081-2 v.3.4.3 Failure Modes and Effects Analysis for Transmission System in Application Level 2
- SUBSET-118 v.1.3.0 Functional Safety Analysis of ETCS DMI for ETCS Auxiliary Hazard

2.1.7 ERTMS ETCS Certification Procedure

The certification is inevitable issue to bring products into the market. The certification procedures for ERTMS ETCS projects are quite complicated. Even in the ERTMS formal report [48], this situation is uttered and complained. As the certification is directly connected for safety, it is researched in this thesis to clarify.

A. The Actors

The following actors are given in the aforementioned document as being involved in the certification and placing in service processes: Ministry (MS), National Safety Authority (NSA), Notified Body (NoBo), Designated Body (DeBo), Railway Undertaking (RU), Infrastructure Manager (IM), Vehicle Keeper (VK), Assessor of the common safety methods (AsBo), Independent Expert (IE), Competent Person (CP), Manufacturer, Contracting Entity (CE), Specific Technical Committee, Registering Entity (RE), Temporary Technical Committee or Technical Supervision Board, Competent Authority (CA). Below the main tasks of main actors are explained.

i. Ministry

The Ministry of Transports is often the state authority for railways. In some countries, the Ministry is also acting as NSA (e.g. EL, CH). It designates the bodies (DeBo) responsible for the verification of conformity with Notified National Technical Rules (NNRs).

ii. NSA

In most, but not all, countries, the NSA is separate but under supervision of its relevant Ministry. The ministry itself can also be the NSA. NSA defines the Notified National Technical Rules (NNTR) and assigns the NoBo and DeBo. In addition, NSA fulfills the homologation with respect to Report for Conformity to National Rules given by DeBo, Safety Assessment Report given by AsBo and other relevant test reports. Note that in case no TSI is required, such a homologation report is not required, either.

iii. ERA

ERA is the European Railway Agency and assigns the AsBo who is responsible for Common Safety Modes (CSM).

i. NoBo

The NoBo checks the conformity with European Technical Specification Interoperability. The TSI cover safety and technical aspects.

ii. DeBo

The DeBo checks the conformity with notified national regulation, where safety and technical aspects are included.

iii. AsBo

The AsBo assesses the application of risk management activities following the CSM-RA process. The assessor of the common safety methods may or may not be a notified body himself and the same notified body may perform conformity verification with respect to safety as well as to the other essential requirements.

2.1.8 The Certification Process

There are seven subsystems, which can be thought of as subsystems of the total Railway Systems. Four of these are of a structural nature and three of an operational nature [49].

Structural areas:

- Infrastructure,
- Energy,
- Control-command and signaling
- Rolling stock;

Functional areas:

- Traffic operation and management,
- Maintenance,
- Telematics applications for passenger and freight services.

Control-Command and Signaling is the ERTMS scope for TSI. A subsystem may not be taken into service or operation before the conformity of the subsystem with the essential requirements is demonstrated. The essential requirements are:

- Reliability and availability
- Health

- Environmental protection
- Safety
- Technical compatibility

A constituent having an EC declaration of conformity can be incorporated into a subsystem without further verification of its conformity. Its suitability for use (in the context of the actual subsystem) must however be assessed by the notified body of the subsystem.

Here, the term constituent and subsystems should be clarified. Subsystems are assemblies of constituents that are an elementary component or group of components to be incorporated in a subsystem. They are generic parts to be used within subsystems. For instance, odometer, GSM-R, recording unit and mission critical computer can be argued as being in the class of constituent.

The purpose of the conformity assessment of a CCS constituent is to verify:

- that all mandatory functions applicable to the interoperability of the constituent have been implemented,
- which optional functions applicable to the interoperability of the constituent have been implemented, and whether these are in line with the requirements,
- that any additional functions implemented are not in conflict with either the mandatory or optional functions applicable to the interoperability of the constituent,
- that any part of the constituent covered by the National Rules (e.g. national functions in STMs) have been assessed and approved by the Member State.

The purpose of the subsystem EC verification is to verify:

- that all mandatory functions applicable to the assembly (on board or trackside) have been implemented (chapter 6.2 of the conventional rail CCS TSI),
- that all optional functions required by the assembly's (on board or trackside) specific implementation have been implemented (chapter 6.2 of the conventional rail CCS TSI),
- that any additional functions implemented in the assembly are not in conflict with the mandatory/optional functions applicable to the interoperability of the constituent (chapter 6.2 of the conventional rail CCS TSI),

- that the interoperability constituents of the subsystem are provided with the EC Declaration of conformity in accordance with Article 13 of the 2001 / 16 directive,
- that the subsystem complies with any other applicable regulations, i.e. that the subsystem has whatever EC declarations are required by any applicable Directives.

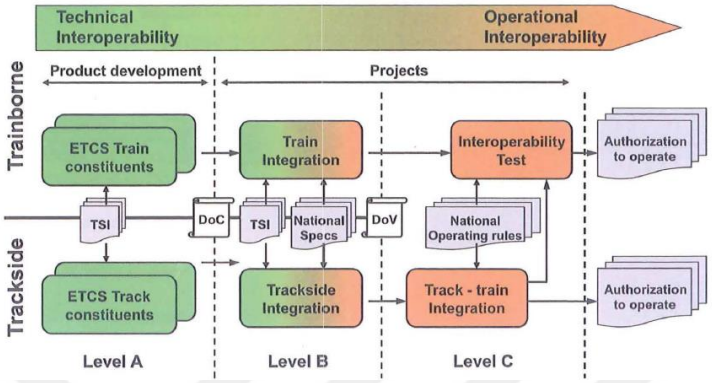


Figure 2.11 The normative basis and results for certification [49]

From this figure, it can be deduced that the mission critical computer needs Level A certification, further described as follows:

- Certification base: TSI/CENELEC
- Test Responsibility: ETCS Supplier
- Assessment: NoBo (endorsing ISA)
- Certification: Declaration of Conformity (DoC)
- Test environment: Supplier or independent laboratory with generic track layout, generic train and operating principles

Three documents are the resulted output document, the ISA certificate - for safety, the NoBo certificate - for conformity with TSI, the Declaration of Conformity - on basis of the Interoperability certificate for its constituent, the supplier issues a Declaration of Conformity.

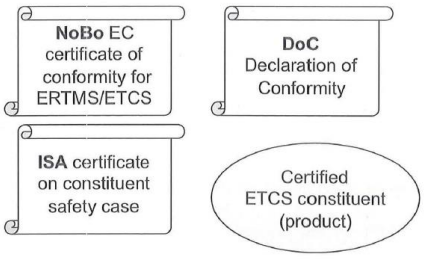


Figure 2.12 Level A outputs [49]

2.1.9 The Reference Norms

There are several standards used in the industries having different application conditions and purposes.

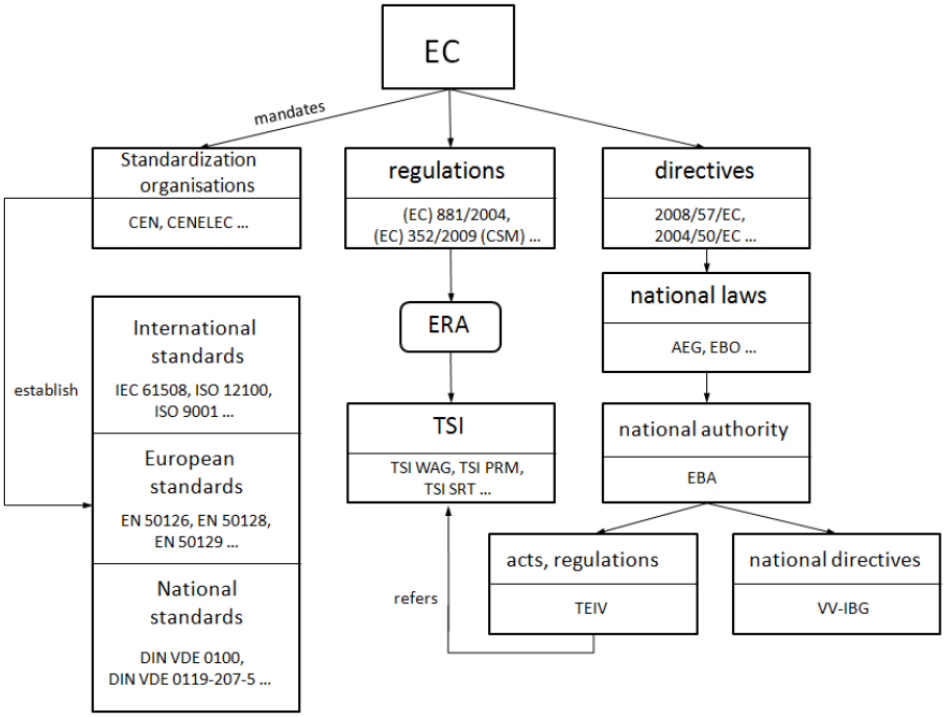


Figure 2.13 The hierarchy of laws [50]

As the domain is railway, the main norms to be utilized in this study are CENELEC EN 50126 - "Railway applications, The specification and demonstration of Reliability, Availability, Maintainability and Safety"[16], EN 50128 - "Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems" [18], EN 50129 - Railway applications - Communications, signalling and processing systems - Safety related electronic systems for signalling" [17], and EN 50159 – "Railway applications - Communications, signalling and processing systems - Safety-related communication in transmission systems [19] which are derived from IEC 61508 [2]- Functional safety of electrical/electronic/programmable electronic safety-related systems" [2] comprised of seven parts with more than six hundreds of pages. For sure, all these norms refer further norms, hence it does not mean that the norms used in this thesis are limited to above norms, but further norms are used, too and these are referred when used. Furthermore, Regulations like EU Regulation (No 402/2013) "Common safety method for risk evaluation and assessment" [51] are also referenced.

2.2 CBTC System

In the ERTMS ETCS part above, very detailed information is provided for various subjects such as certification procedure and processes, modes levels etc. Though several differences mentioned below, the main idea is similar for the CBTC, hence, not every detail is provided in this part at system level for CBTC.

CBTC is a continuous Automatic Train Control (ATC) system utilizing high-resolution train location determination, independent of track circuits; continuous, high capacity, bidirectional train-to wayside data communications; and train-borne and wayside processors capable of implementing vital functions [39].

Different from the ERMS ETCS, CBTC is not an interoperable system and there are not very detailed subsets as in ERTMS as Farooq and Soler [52] complains that IEEE CBTC standard is frequently overlooked because its scope is limited. Another difference is that CBTC is an entire closed loop system such that it includes central traffic control, wayside equipment and on-board subsystems as one system.

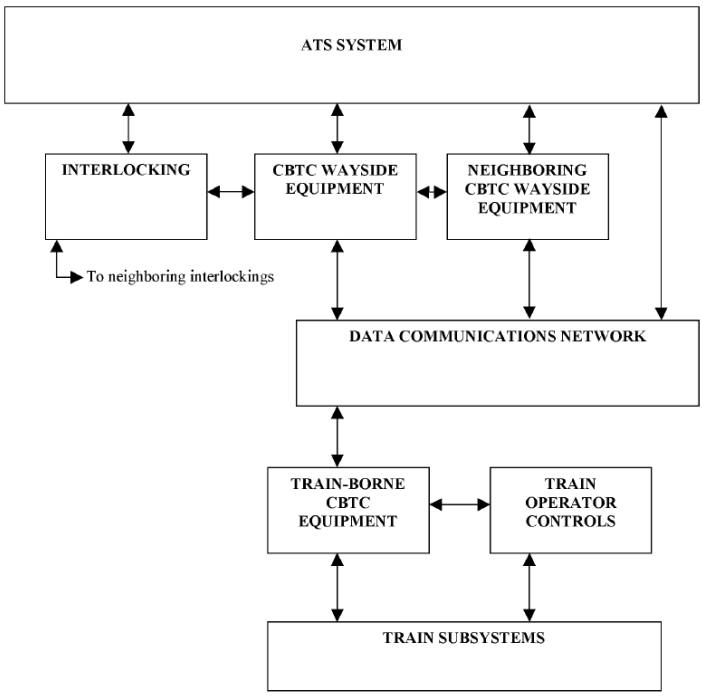


Figure 2.14 CBTC block diagram [39]

ATC is the system for automatically controlling train movement, enforcing train safety, and directing train operations. ATC must include Automatic Train Protection (ATP) and may include Automatic train operation (ATO) and/or Automatic Train Supervision (ATS). ATO is the subsystem within the ATC system that performs any or all of the

functions of speed regulation, programmed stopping, door control, performance level regulation, or other functions otherwise assigned to the train operator. ATP is the subsystem within the ATC system that maintains fail-safe protection against collisions, excessive speed, and other hazardous conditions through a combination of train detection, train separation, and interlocking. ATS is the subsystem within the ATC system that monitors trains, adjusts the performance of individual trains to maintain schedules, and provides data to adjust service to minimize inconveniences otherwise caused by irregularities.

The primary characteristics of a CBTC system include the following:

a) High-resolution train location determination, independent of track circuits

b) Continuous, high capacity, bidirectional train-to-wayside data communications

c) Train-borne and wayside processors performing vital functions [39]

A CBTC system may

a) Provide ATP functions only, with no ATO or ATS functions.

b) Provide ATP functions, as well as certain ATO and/or ATS functions, as required to satisfy the operational needs of the specific application.

c) Be the only train control system in a given application or may be used in conjunction with other auxiliary wayside systems [39].

The CBTC system is intended to be applicable to the full range of transit applications, including light rail, heavy rail, and commuter rail transit systems, and shall be applicable to other transit applications, such as automated people movers (APMs) if CBTC is used for ATC.

Main functions of the CBTC system are:

Main ATP Functions:

1. Train location/train speed determination
2. Safe train separation
3. Overspeed protection and brake assurance
4. Rollback protection
5. End-of-track protection
6. Parted consist protection and coupling and uncoupling of trains

7. Zero speed detection
8. Door opening control protection interlocks
9. Departure interlocks
10. Emergency braking
11. Route interlocking
12. Traffic direction reversal interlocks
13. Work zone protection
14. Broken rail detection
15. Highway grade-crossing warning
16. Restricted route protections

Main ATO Functions:

1. Automatic speed regulation
2. Platform berthing control
3. Door control

Main ATS Functions:

1. ATS user interface
2. CBTC train identification and train tracking
3. Train routing
4. Automatic train regulation
5. Station stop functions
6. Restricting train operations
7. Passenger information system interfaces
8. Fault reporting

The system architecture for the CBTC system is provided below in .

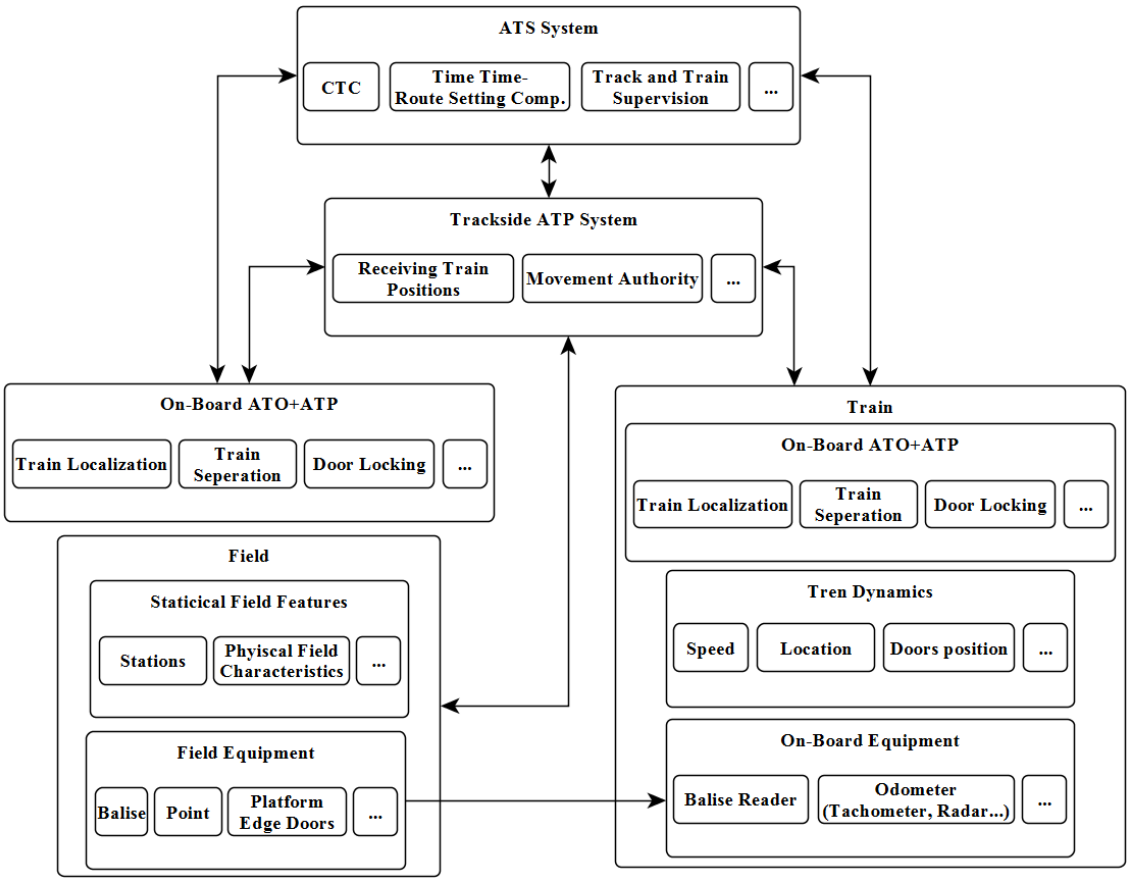


Figure 2.15 ATS, ATP and ATO system architecture

2.3 Quantitative Safety Requirements and SIL Usage

Safety requirements aim avoidance and control of systematic faults as well as control of random faults. For demonstrating that random faults are kept under the tolerable rates, quantitative hazard analyses are performed. Paramount importance shall be attached to the definition of tolerable hazard rates (THR) since the definition of what the hazard rate is allocated to influences the expected outcomes and the correct operation of the safety-critical system. In this section, approaches used in railway industry are discussed by mentioning technical specifications and referencing railway standards. It is found that there are misinterpretations for the quantitative hazard rates and use cases are provided to show the results of different approaches. Moreover, safety integrity level (SIL) of the human-machine interface (HMI) related functions for on-board and trackside applications are investigated, and their drawbacks are explained for the mission-critical systems. Next, some findings of tool usage for fulfilling SIL requirements are detailed.

The norm IEC 61508 [2] defines SIL per average frequency of a dangerous failure of the safety function. A safety function is defined in IEC 61508-4 [2] as a function to be

implemented by an E/E/PE safety-related system or other risk reduction measures that are intended to achieve or maintain a safe state for the equipment under control (EUC), in respect of a particular hazardous event. In contrast, the allocation of SIL is widely misinterpreted by the industry despite its significance for the system design and final attainment of system safety. AIChE [53] classifies safety functions into the following groups: (a) safety systems that automatically respond to the initiating event (e.g., automatic shutdown systems), (b) alarms that alert the operator(s) when the initiating event occurs (e.g., fire alarm systems), (c) operator procedures following an alarm, and (d) barriers or containment methods that are intended to limit the effects of the initiating event. In this study, the group (a), namely SIS will be scrutinized in this work.

2.3.1 Quantitative ERTMS ETCS Safety Requirements

ERTMS ETCS defines safety requirements in Subset–091 [33] after performing the analyses in Subset–088 (in five parts) and Subset–118 [54] (for Driver Machine Interface, DMI). As provided in EN 50129 [17], Table E.6 – Failure and hazard analysis methods, a defined set of analyses shall be realized for the complete and correct derivation of safety requirements. In Subset–088, there are very exhaustive fault tree analyses (FTA) and functional analyses in the form of failure modes, effects and criticality analysis (FMECA) for both Level–1 and Level–2 about several different modes such as full supervision or shunting. On the other hand, not every method such as Hazard and Operability [55] that shall be used for SIL 4 are selected. For FTA, the concept is provided in the figure below. For details about FTA the standard in [56] can be appealed.

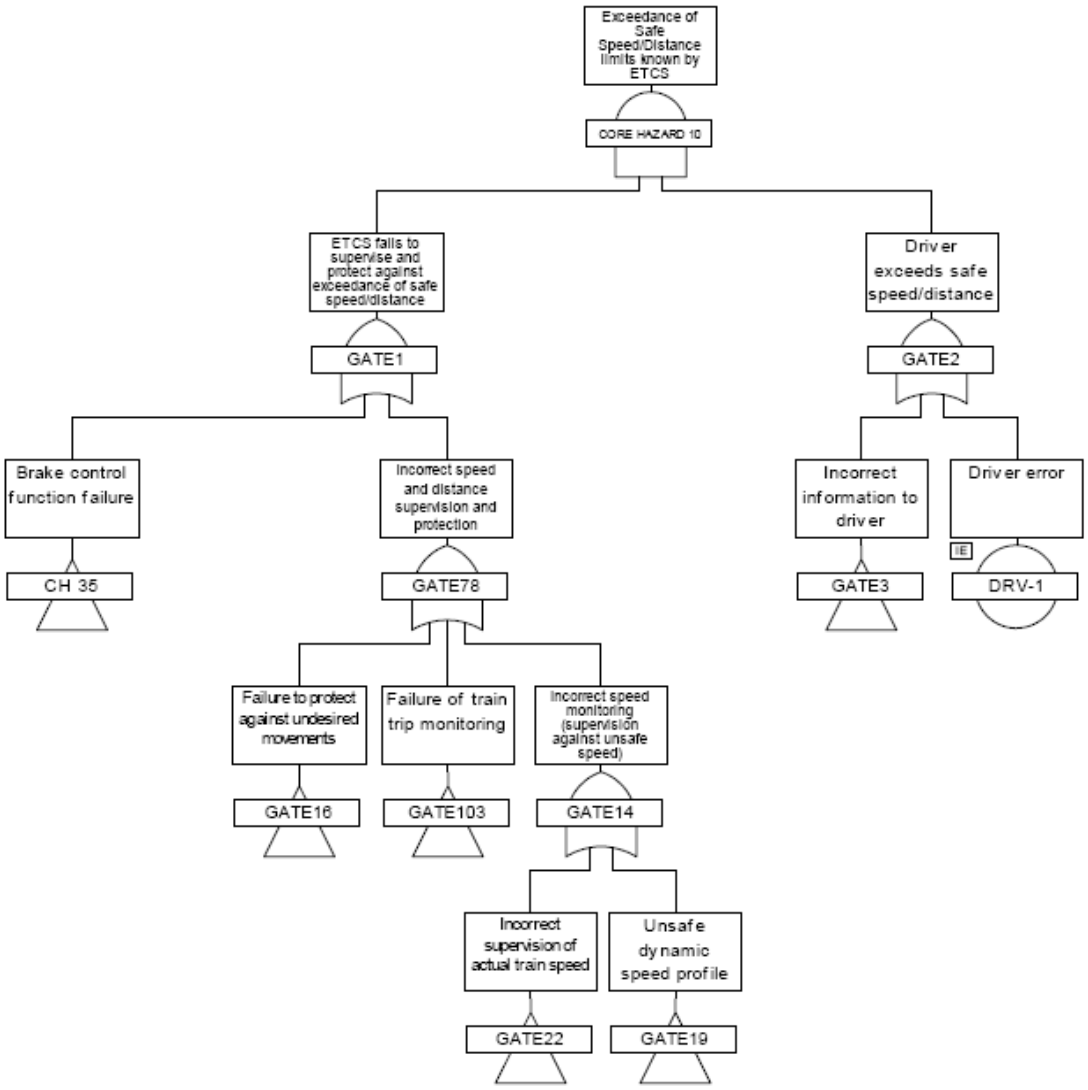


Figure 2.16 Conceptual Fault Tree in Subset–088 [33]

The core hazard for ETCS on-board is defined in Subset–091 in clause 4.2.1.8 as "Exceedance of the safe speed or distance as advised to ETCS". This core hazard is resulted by several child hazards provided in comprehensive FTAs. Following this, in clause 6.1.1.3, the quantitative value of the tolerable hazard rate (THR) is apportioned to on-board, transmission and finally to trackside, as 0,67x1E-09 [1/h], by mentioning functions. The below figure introduces the terms THR on-board and THR trackside denoting the numerical safety requirement for the purely on-board and trackside functions.

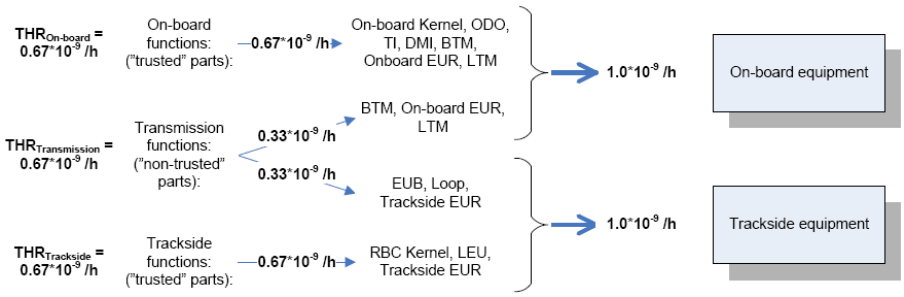


Figure 2.17 Apportionment of THRs to ETCS in Subset 091 [43]

In clause 7.2 in Subset 091, the requirement is set as on-board system shall not exceed THR of the apportioned value which is 0,67xE-09 [1/h]. Accordingly, the failure frequency for the entire ETCS on-board is 15 times lower than the SIL 4 limit.

7.2 ETCS on-board equipment except transmission system

ETCS_OB01	ETCS Core Hazard THR The hazard rate for the ETCS on-board system, less those parts forming part of the transmission paths, shall be shown not to exceed a THR of $0.67*10^{-9}$ dangerous failures/hour (background information is provided by Subset-088 Part 3, paragraph 12.3.1.1)

Figure 2.18 ETCS Core Hazard THR in Subset 091

It defines ETCS_OB01 as the hazard rate for the ETCS on-board system, less those parts forming part of the transmission paths, shall be shown not to exceed a THR of 0.67x1E-09 dangerous failures/hour. It further explains that each supplier shall prove the attainment of the THR on-board is taking into account at least the following events: KERNEL–1 - KERNEL–34, ODO–1 - ODO–4, TI–1 - TI–11, MMI–1 - MMI–6, BTM–H4, OB–EUR–H4, and LTM–H4. These functions are defined in the following part of the subset as mentioned earlier. For instance, KERNEL–9 is defined as speed calculation underestimates train speed and TI–1 as service brake/emergency brake not commanded when required.

According to the data provided above, the central question arises about the scope of the THR such that:

a) Is this THR apportioned to each function named in the Subset–091? This issue would yield for example in following quantitative requirements and results:

i. The Hazard Rate (HR) of Kernel–9 (Speed calculation underestimates train speed) shall be less than 0,67xE-09 [1/h]. That results in for instance that, if HR of Kernel–9 is calculated to be equal to 1xE-010 [1/h], then the requirement is fulfilled.

ii. The HR of TI–1 (Emergency brake not commanded when required) shall be less than 0,67xE-09 [1/h]. That results in for instance that, if HR of TI–1 is calculated as 6xE-010 [1/h], then the requirement is fulfilled.

b) Is this THR for the sum of all the functions of the on-board equipment? Alternatively, in other words, is the THR allocated to the entire on-board system? If the answer is yes, then this would yield for example in following quantitative requirement and result:

i. The SUM of the HRs of all the on-board functions which means [(HR of Kernel-1-Kernel-1-34) + (HR of ODO-1- ODO-3) + (HR of TI-1- TI-11) + (HR of MMI-1-MMI-6) + (HR of BTM-H4)], considering minimum cut sets, shall be less than 0,67xE-09 [1/h]. If for instance, the HR of Kernel-9 is calculated as to be 1xE-010 [1/h], and HR of TI-1 is equal to 6xE-010 [1/h] as given above, then the requirement is not fulfilled.

Considering the explanations above, we believe that there are essential uncertainties about the attachment of the THR. These uncertainties explained above has have been discussed with several independent safety assessors (ISAs) around the Europa, and it has been observed that the approaches of the ISAs are different, as well. On the other hand, this a clear understanding of this issue is very crucial to design the safe computer and other constituents like DMIs, odometers or Balise Transmission Modules (BTMs). Since, for instance, in the first scenario, a Kernel with an HR of 1E-010 [1/h] would satisfy the quantitative requirement, a Kernel with an HR less than 1E-12 [1/h] is required for the second case. Besides, this ambiguity would bring different system safety performances of the ERTMS ETCS on-board systems.

As a result, for this study, the requirement for the ERTMS ETCS is assumed as the second scenario which is the more conservative and on which more ISAs are agreed. So, for the ERTMS ETCS, the overall safety requirement for on-board computer PFH_{EOBC} is found as 1E-12 [1/h] where EOBC denotes ERTMS ETCS On-Board Computer (same as EVC-Euro Vital Computer such that both can be used for ERTMS ETCS On-board Computer in this study).

2.3.2 Quantitative CBTC Safety Requirements

Quantitative CBTC safety performance requirements are provided in section 5.3.4 of the CBTC standard IEE1474.1 as below:

For any CBTC system application, the CBTC wayside and train-borne equipment located within any contiguous portion of a one-way route that can be traversed by a train traveling at the specified maximum authorized speed for one hour or less shall have a total calculated aggregate MTBHE (total of all critical and catastrophic hazards) of at least 10^9 operating hours. This includes the maximum number of other trains that can be located in this contiguous portion of a one-way route under the specified peak operating headway.

Further, following note is presented.

NOTE—If the end-to-end trip time for a given route is greater than 1 h, the MTBHE requirement for that route would be adjusted proportionately. As an illustrative example, if the specified end-to-end trip time (per 5.2 -of the standard-) for a given one-way route is 2 h, and if the route includes 4 sets of wayside CBTC equipment, and if a maximum of 10 trains can be operating on the route at a given time (when operating at the specified peak headway, per 5.1), then the MTBHE of the combined 4 sets of wayside CBTC equipment and 10 sets of train-borne CBTC equipment on that route would be at least 0,5E-9 [1/h] operating hours.

According to the information above, if a similar method is applied as in ERTMS subset such that the HR is allocated to wayside and onboard as equal, then for the case below, a safety requirement can be deduced for the on-board computer as following:

- Journey: 2h
- Wayside CBTC: 4 sets
- Train number: 10

a) HR for 4 Wayside CBTC for 2h journey (incl. trackside-onboard transmission part) is (0,5E -9 [1/h])/(2) or 2,5E-10 [1/h]. HR for 1 Wayside CBTC for 2h journey (incl. trackside-onboard transmission part) is (2, 5E-10 [1/h])/4 or 6,25E-11 [1/h]. Hence, HR for 1 Wayside CBTC for 1h journey (incl. trackside-onboard transmission part) is then (6,25E-11 [1/h])/2 which results in 3,125E-11 [1/h].
b) HR for 10 sets of train-borne CBTC equipment for 2h journey (incl. trackside-onboard transmission part) is (0.5E -9 [1/h])/(2) or 2,5E-10 [1/h]. HR for 1 set of

train-borne CBTC equipment for 2h journey (incl. trackside-onboard transmission part) = (2,5E-10 [1/h])/10 or 2,5E-11 [1/h]. Hence HR for 1 set of train-borne CBTC equipment for 1h journey (incl. trackside-onboard transmission part) is (2,5E -11 [1/h])/2 or 1,25 E-11 [1/h].

If considered that the safety functions are performed not only by On-board Computer but also including Odometer, BTM, TIU, Interface elements like vital relays etc., then a 1/10 allocation seems plausible. In this case; the safety requirement for the CBTC On-board Computer is PFH_{COBC}= (1,25E-11)/10 or PFH_{COBC}=1,125E-12 [1/h] where the subscript COBC denotes CBTS On-Board Computer.

2.3.3 Quantitative Safety Requirements for Trackside

In Figure 2.19 a track system is illustrated. The control centre sends requests for setting routes and for changing positions of trackside elements like points or level crossing barriers. The IXL receives the aforementioned requests from control centre and decides in a safe manner to accept or rejects them. In case of acceptance, it commands field elements over I/O modules and interfaces for the correct states such as moving points to the required positions for the route, closing the level crossing, changing the color of the signal to proceed aspect, sending movement authority telegrams to balises. The position and health statuses of the field elements are evaluated and sent back to control center over IXL.

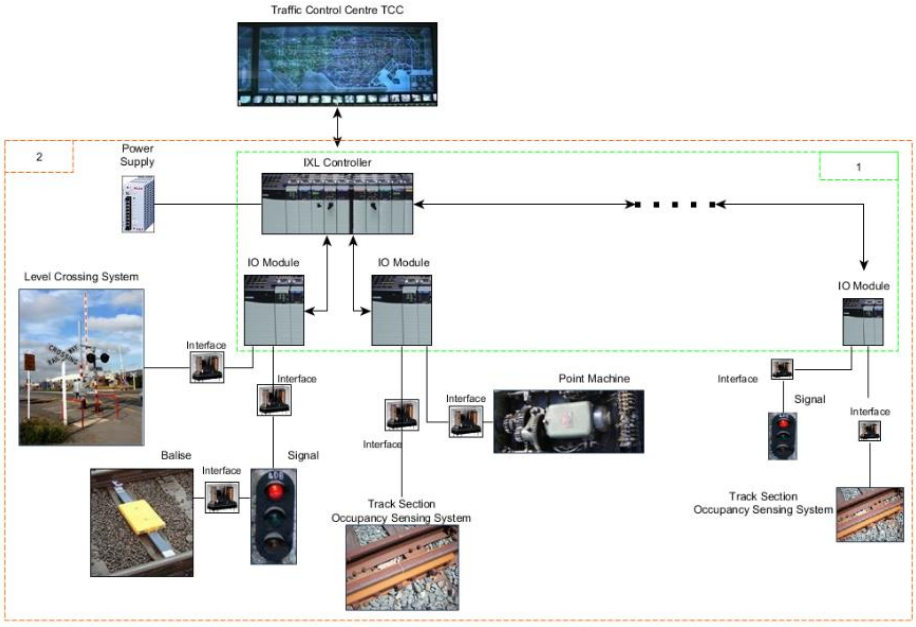


Figure 2.19 Signaling system with possible different IXL limits.

For the trackside part, it has been observed in various projects that misinterpretations for the SIL are widely made by both the public enterprises and the private sector. For instance, the primary safety requirement set for the IXL system of the Konya-Karaman high-speed line-signaling project [57] is that the IXL system shall be SIL 4. Similarly, Blaauboer [58] explains the details about an SIL 4 IXL designed for the station Santpoort Noord including six points, ten signals, one level crossing (LC) and some track circuits (TC). For the Ankara Metro project, the technical specification [59] underlines that the system shall be fail-safe and all vital equipment shall be redundant and SIL 4. Moreover, different companies share that their electronic IXL systems meet SIL 4. Another study by Tang [32] in comparison with Norwegian National Rail Administration concludes that the system complies with the SIL 4 random failure integrity. The attachment of SIL both to a system and to a piece of equipment is a misuse and brings many problems with itself. The first question to be answered is; what is an IXL system and where are its boundaries? For instance, is it the scope within the frame-1 or frame-2 in Figure 2.19? Several further permutations are evidently possible for the system definitions mentioned in the previous paragraph.

Integrated European Signaling System (INESS) is a European project on which International Union of Railways (UIC) and Association of Europe's Rail Supply Companies (UNIFE) have agreed for an ERTMS compliant IXL development. [60] defines the interlocking in INESS documentation as a system that, under the commands from a signaler or signaling control system, manages trackside equipment and the safe movement of rail traffic. According to this definition, frame-1 including IXL controller and input/output (I/O) modules (object controller) is the scope of the IXL. Moreover, not only IXL but also the field elements signals, point machines, level crossing controllers, and track circuits, as well as all interfaces, shall be vital for such a mission-critical system. Therefore, the safety requirements mentioned at the beginning of the section skip the quantitative safety valuation of field elements and interfaces. The IEEE 1474.1 CBTC standard [39] defines in 3.1.20 the IXL as an arrangement of a switch, lock, and signal devices that are located where rail tracks cross, join, separate, and so on. The devices are interconnected in such a way that their movements must succeed each other in a predefined order, thereby preventing opposing or conflicting train movements. This definition differs from the previous definitions in such a way that it involves the field elements as given in frame-2 in Figure 2.19.

Taking into account maximum I/O numbers for an electronic IXL (for both Computer-based IXL, and Programmable Logic Controller-based IXL), an IXL system usually controls approximately five mid-size stations, and one typical station is illustrated in Figure 2.20.

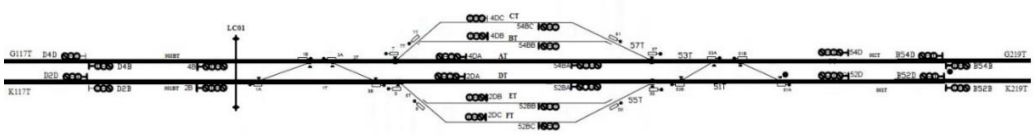


Figure 2.20 Typical signaling station

The number of safety-relevant input and output channels, as well as module numbers for this example are listed in Table 2.4. The module number evaluation is based on 32 channels per output module (OM) and 64 channels per input module (IM).

Table 2.4 Number of I/O signals, channels, and modules

Number	Field Elements									
	Track Ciruit	Simple Point	S Point	3 Aspect Short Signal	3 Aspect High Signal	4 Aspect High Signal	Level Crossing	Extra input (CRC)	PS Control / Station	Day/Night Voltage
Input Number per Element	2	2	4	4	3	5	3	11	1	0
Output Number per Element	0	2	4	4	3	5	1	0	0	1
Element Number	22	8	4	8	12	4	1	1	1	1
Subtotal Input Number	44	16	16	32	36	20	3	11	1	0
Subtotal Output Number	0	16	16	32	36	20	1	0	0	1
Total Input Number	179									
Total Output Number	122									
Input Number per Input Module	64									
Input Number per Output Module	32									
Input Module Number (ceiled up)	3									
Output Module Number (ceiled up)	4									
Total Station	5									
Total Input Module for all Stations	15									
Total Output Module for all Stations	20									

From Table 2.4, it can be deduced that 179 input, 122 output channels corresponding to 3 IMs each with 64 channels and 4 OMs each with 32 channels are required only for the electronic control system for this station. Considering, for example, five stations, the number of required IMs and OMs are 15 and 20, respectively. With challenging hazard rates of modules given Table 2, the result for electronic control part only is 5.70E-08 [1/h] that is less than SIL 4 lower limit. To sum up, even if the hazard rates of the interface elements and field elements are excluded, Table 2 shows precisely how difficult it is to achieve an SIL 4 IXL system.

Table 2.5 Hazard rates of the module and system

DI 64 Channel	4.00E-10
DO 32 Channel	6.00E-10
Bus Module	4.00E-10
CPU	2.00E-10
Input Module Number x Hazard DI	5.00E-08
Output Module Number x Hazard DO	6.00E-09
Bus Module x 1	6.00E-10
CPU x 1	4.00E-10
SUM	5.70E-08

A further derivation of the system approach is that the entire field equipment could be integrated to the calculation of the system HR following the definition of IXL in CBTC standard. In this case, it is evident that the HR of the total system would be much less than SIL 4 value where the HRs of field elements should be incorporated. SIL is defined in IEC 61508–1 [2] neither for systems nor subsystems, but for safety functions. Therefore, attaching SIL to an IXL system or equipment is misleading and technically wrong. Hence, above all, safe states and safety functions should be defined, and all calculations have to be performed for these functions. Recall that, the question to be answered at this point is the definition and boundary of these functions. During the design phase, a safety function can be portioned into sub-functions and elements such as the processing unit or actuator parts. Later, the apportionment of quantitative hazard rate can be realized for these sub-functions. However, a global safety function in a SIS starts from the sensing element and ends at the actuator, i.e., the whole chain shall be taken into account. It consists of sensors on the field, the interface from sensors to IM, IM itself, the interface between IM and control unit (CU), CU, the interface between OM and CU, OM itself, the interface between OM and actuator and finally actuator. Accordingly, there exists a significant difference between system and function approaches as well as for the definition of limits of the safety function. For instance, it is possible to describe two safety functions with similar meaning. The first one is switching the signal aspect to stop, and the second one is switching the signal aspect to stop when a possibly dangerous situation occurs. For the first function, the physical parts implementing the safety function are one output channel with CPU and bus module. For this scenario, the PFH of the safety function has been calculated as 1.2E-08 [1/h] with the HRs of the modules given in Table 2.5. For the second scenario; the calculation shall consider more items; the requirement is described as follows, where SGSA stands for signal stop aspect: SET SGSA = (point trailed fault) OR (point end position fault) OR (point not at the correct position) OR (point not locked) OR (TS unexpected occupancy fault) OR ((the first TS occupied) AND (waiting time for the driver elapsed)) OR (TS blocked) OR (start signal fault at the start signal) OR (end signal fault) OR (signal fault at a signal that gives movement authorization to the rail vehicles onto the track sections of the route) OR (start signal closed) OR (start signal blocked) OR (the level crossing open)

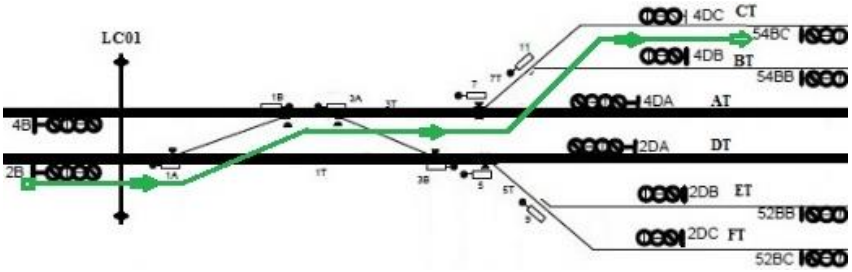


Figure 2.21 The route from 2B to CT.

This function addresses some field elements of the station given in Figure 2.21 for the signal 2B of the route 2B–CT (station entrance route from West, signal 2B into the station, onto track CT). Here, these field elements are track circuits (1T, 3T, CT), point machines (1A, 1B, 3A, 7, 11), signals (2B, 4B, 2DC, 2DB, 2DA, 4DA, 4DB, 4DC, 54BC) and a level crossing (01). The field indications shall be considered for each type of element as given in Table 2.6.

Table 2.6 Indications used by safety function

	Input				
	1	2	3	4	5
TC	Occupied	Vacant			
Simple Point	Normal	Reverse			
S Point	Normal	Reverse	Normal	Reverse	
3 Short SG	Red	Yellow	Green	Flash	
3 High SG	Red	Yellow	Green		
4 High SG	Red	Yellow	Green	Yellow	Flash
LC	Closed	Broken			

Considering this information, the number of IM and OM is one for each, and the quantitative value for this particular safety function is calculated in Table 5 regarding the hazard rates provided in Table 2.6, the data in Table 2.7 and Table 2.8 for excluding and including field elements as 1.60E-09 [1/h], 1.01E-08 [1/h], respectively.

Table 2.7 Number of I/O signals, channels, and modules for the safety function

Number	**Field Elements**									
	Track Ciruit	**Simple Point**	**S Point**	**3 Aspect Short Signal**	**3 Aspect High Signal**	**4 Aspect High Signal**	**Level Crossing**	**Extra input (CRC)**	**PS Control / Station**	**Day/ Night Voltage**
Input Number per Element	2	2	4	4	3	5	3	11	1	0
Output Number per	0	2	4	4	3	5	1	0	0	1
Element Number	3	2	2	5	0	4	1	1	1	1

As a result, it can be concluded that the attainment of the required quantitative hazard rate hinges on the definitions. To overcome misinterpretations and miscalculations and to harmonize systems by different manufacturers, the author proposes that (1) the customer

should be pro-actively integrated into the risk analysis process, (2) the attachment of SIL and quantitative hazard rates should be realized for safety functions, (3) the safety functions should be defined in the technical tender specifications within the responsibility of the customer, and (4) the safety functions should include the physical elements constituting it in a way without leaving a further comment to the contractor or sub-contractor.

Table 2.8 Hazard rates ex-/including field equipment

	HR	**Number**
DI 64 Channel	4,00E-10	1
DO 32 Channel	6,00E-10	1
Bus Module	4,00E-10	1
CPU	2,00E-10	1
SG	2,00E-10	40
TC	1,00E-11	6
PM	4,00E-11	12
Total HR excl. Field El.	1,60E-09	
Total HR incl. Field El.	1,01E-08	

2.3.4 SIL of HMI Related Functions

As the safety standards, the interoperability requirements are evolving continuously. Baseline–2 of ERTMS/ETCS mentions the core hazard, which is exceedance of the safe speed/distance as advised to ETCS while baseline–3 adds up an auxiliary hazard to the core hazard that is the failure to interact correctly with the driver regarding information not supervised by ETCS. Recall that, thirty-one hazardous events are associated with this auxiliary hazard. DMI–04j is the hazard with the lowest THR in Subset–091 [33] and is defined as false isolation command with a THR of 2.0x1E-07 [1/h]. This value corresponds to SIL 2 DMI functions, i.e., while in baseline–2, a DMI performing SIL 0 functions was satisfying, DMI in on-board systems compatible with baseline–3 shall be able to realize at least SIL 2 safety functions. However, the author claims according to the analysis below that even being capable of performing SIL 2 functions is not enough for ETCS on-board systems for the attainment of the safety requirements.

In 7.2.1.4 of Subset–091 [33], it is provided that the overall safety performance of ETCS be critically dependent on the train data that is entered in the ETCS on-board equipment. Therefore, there is a requirement ETCS_OB02 that is formulated as the ETCS on-board data entry process must be of a quality level that is appropriate to the required safety level.

For instance, train weight is a train data, and the driver enters it at the beginning of the day.

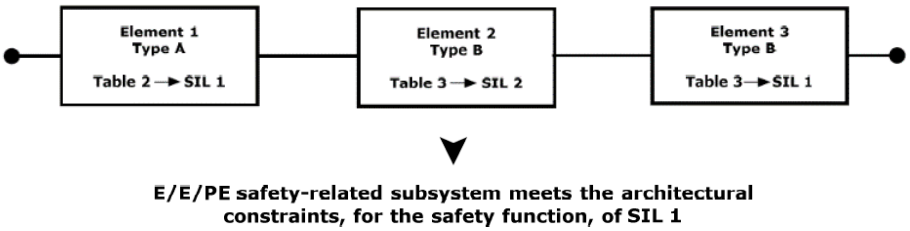


Figure 2.22 Determination of the maximum SIL for specified architecture [2]

The calculation of the braking curve, i.e., braking distance/maximum speed is an SIL 4 function of which one input comes from DMI as data entry. Hence, DMI is a ring in the safety function chain and therefore, the data entry shall be a vital process. IEC 61508–2 [2] illustrates maximum achievable SIL for a series of elements as given in Figure 2.22. It is evident that the lowest SIL of the chain determines the maximum achievable SIL. If DMI can perform SIL 0 or SIL 2 functions, then it is not faithful to claim that braking curve can be calculated below the hazard rate required for SIL 4. Consequently, the braking is not an SIL 4 function of which malfunction would result in the core hazard and catastrophic accidents. One claim about the correct data input is that the driver validates the data after entering. However, it does not cover the case whether the data is corrupted when the telegram is calculated or during its transmission as an SIL 2 hardware cannot create SIL 4 telegram or transmission. To make it clearer, following scenario is created:

1. The driver enters train data, e.g., train weight as 500 tons.

2. DMI receives the data as to be 500 tons.

3. This data is miscoded into the DMI – Euro Vital Computer (EVC) telegram as 250 tons since the telegram is miscalculated (i.e., not SIL 4 because DMI HW is not SIL 4, so the telegram cannot be claimed to be SIL 4).

4. The data train weight 250 tons is received by EVC.

5. The data train weight 250 tons is sent back from EVC to DMI for driver's validation.

6. The data train weight 250 tons is decoded wrongly as 500 tons by DMI.

7. The DMI displays the data train weight as 500 tons to the driver.

8. Driver validates the train data.

9. The Movement Authority is received over GSM–R, e.g., 5 km until the signal at the station.

10. The train calculates the braking curve, taking into account that the train weight is 250 tons.

11. The train cannot stop at the station and intrudes into the route of another train, and the trains collide catastrophically.

Several similar scenarios such as displaying the train speed when the ETCS mode is staff responsible can be created which results in catastrophic accidents. Consequently, the author proposes that the THR requirement for such HMI functions shall be lower than SIL 4 which is neither the case in today's projects and nor stated in the interoperability requirements subset.

Consequently, the above scenarios describe the importance of designing safety-critical systems and safety-critical functions. Notably, in case that there are equipment or non-vital sub-systems in a system, it should be taken into account how to apportion the safety sub-functions to the pertinent parts.

2.3.5 SIL Appropriateness of Tools

Tool usage is inevitable and used at most stages of the V-model from system requirements to validation, for HW and/or SW development. There are restrictions when using them in a safety-critical project. Both IEC 61508 (Part 4) [2] and CENELEC EN 50128 [18] group these tools in three categories. The tool class T1, the so-called requirement or configuration control tool, generates no outputs which can directly or indirectly contribute to the executable code (including data) of the SW. T2 supports the test or verification of the design or executable code, where errors in the tool can fail to reveal defects but cannot directly create errors in the executable SW. Test harness generators or test coverage measurement tools can be considered as T2 tools. T3 generates outputs which can directly or indirectly contribute to the executable code (including data) of the safety-related system, e.g., compiler. However, according to the definitions, a tool classified as T1 might also obviously be in the class of T3. Since, if requirement tool is faulty, or if it has a bug and removes a requirement or changes the position of the point and thus the decimal number, then the design and implementations are erroneous. As a consequence, it generates outputs that contribute to the executable code. Alternatively, assume that a

configuration tool replaces a version of a configuration item with an old and wrong configuration item that has not passed the tests, then the system is constituted of mishap configuration items that would result in catastrophic accidents. Moreover, if a test tool were wrong, then it would affect the executable code and data indirectly since otherwise the bugs in the executable code/data would be revealed and so they would be replaced with the corrected versions. Consequently, the author proposes tool classification should be classified according to the SIL of the function where it will be used, i.e., if a tool is used for SIL 4 application, then all the tools should be of the same quality since all of them affect the ultimate safety function, code, and system. A second issue with the tool qualification is toolchains for VHDL (Very High Speed Integrated Circuit Hardware Description Language) synthesis and simulation. Similar approaches are valid again for this in IEC and CENELEC norms. There is still a widely disputed question about FPGAs (Field Programmable Gate Array) whether they are pure HW or shall be treated as incorporating SW. In the latter case, tools for SW are engaged in the certification process. FPGA is handled in part two of IEC 61508 [2] where Table F.2 describes the techniques and measures to avoid introducing faults during ASIC design and development: ICs (User programmable Integrated Circuits such as FPGA/PLD/CPLD where PLD stands for Programmable Logic Design and C in CPLD stands for Complex). On the other hand, FPGAs are programmed before the step place and routing. Thus, the measures in the table as mentioned earlier per se does not suffice, but besides, the tools for synthesis shall be qualified according to items referred to in IEC 61508-3 [2] / EN 50128 [18] for the tool class 3, too.

CHAPTER 3

RAMS BACKGROUND

In this section, RAMS relevant concepts are dealt and relation of reliability, availability, maintainability with safety is scrutinized which affect the design of the safety critical control system. By doing this, International and European and international norms will be utilized. If there is a discrepancy between these norms for these definitions, these will be discussed in this section, too. Moreover, quantitative analyses methods are described which will be the base for the calculations in this thesis.

3.1 Definitions of Concepts

The concepts can differ in different standards, thereof to avoid any ambiguity the concepts that are used in this thesis are explained below utilizing the standards IEC 61508 [2], EN 50126 [16], EN 50129 [17], CLC/TR 50126-2 [61], ISO8402 [62], MIL-STD CN2 [63].

Reliability

The probability that an item can perform a required function under given conditions for a given time interval (t1, t2), see EN 50126 [16].

Quality

The totality of features and characteristics of a product or service that bear on its ability to satisfy stated or implied needs, see ISO8402 [62].

Maintainability

The probability that a given active maintenance action, for an item under given conditions of use can be carried out within a stated time interval when the maintenance is performed under stated conditions and using stated procedures and resources, see EN 50126 [16].

Availability

The ability of a product to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval assuming that the required external resources are provided, see EN 50126 [16].

Dependability

A measure of the degree to which an item is operable and capable of performing its required function at any (random) time during a specified mission profile, given item availability at the start of the mission. (Item state during a mission includes the combined effects of the mission-related system R& M parameters but excludes non-mission time), see MIL-STD CN2 [63].

To understand the meaning of safety, terms will be given consecutively.

Safety

Freedom from unacceptable risk, see IEC 61508 [2].

Risk

Combination of the probability of occurrence of harm and the severity of that harm, see IEC 61508 [2].

Harm

Physical injury or damage to the health of people or damage to property or the environment, see IEC 61508 [2].

Environment

All relevant parameters that can affect the achievement of functional safety in the specific application under consideration and in any safety lifecycle phase, see IEC 61508 [2].

NOTE: This would include, for example, physical environment, operating environment, legal environment and maintenance environment.

Functional Safety

Part of the overall safety relating to the EUC and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures, see IEC 61508 [2].

Technical Safety

That part of safety that is dependent on the technical characteristics of a product derived from the system requirements and/or from the system design, see CLC/TR 50126-2 [61].

Technical requirements may address e.g. presence of sharp edges, presence of electric voltage, presence of combustible material, etc.).

Systematic Faults

Failure, related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors, see IEC 61508 [2].

Random Faults

Failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware, see IEC 61508 [2].

System failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted.

Safety Integrity

Probability of an E/E/PE safety-related system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time, see IEC 61508 [2].

Safety Integrity Level (SIL)

Discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest, see IEC 61508 [2].

The SIL is defined in EN 50129 [17] as fallowing:

A number which indicates the required degree of confidence that a system will meet its specified safety functions with respect to systematic failures, see EN 50129 [17].

However, this definition is disputable, because SIL is not only a measure for systematic failures but also random failures.

Software safety integrity

Part of the safety integrity of a safety-related system relating to systematic failures in a dangerous mode of failure that are attributable to software, see IEC 61508 [2].

Systematic Safety Integrity

Part of the safety integrity of a safety-related system relating to systematic failures in a dangerous mode of failure, see IEC 61508 [2].

Hardware Safety Integrity

Part of the safety integrity of a safety-related system relating to random hardware failures in a dangerous mode of failure, see IEC 61508 [2].

Safe Failure Fraction (SFF)

Property of a safety related element that is defined by the ratio of the average failure rates of safe plus dangerous detected failures and safe plus dangerous failures, see IEC 61508 [2].

Probability of Dangerous Failure on Demand (PFD)

Safety unavailability of an E/E/PE safety-related system to perform the specified safety function when a demand occurs from the EUC or EUC control system, see IEC 61508 [2].

Average Frequency of a Dangerous Failure per Hour (PFH)

Average frequency of a dangerous failure of an E/E/PE safety related system to perform the specified safety function over a given period of time, see IEC 61508 [2].

3.2 Organizational Structure and Verification & Validation Concepts for Safety Critical Developments

Development of a Generic Application or Product (GAP) is always challenging, because it should be designed as much as generic and simply configurable for the final specific applications. If such a development is also safety critical, then the complexity increases dramatically as the resulted system will have impacts on human life, property and environment. The safety management plays a major role to keep this tough development process under control by avoiding systematic faults. Setting up correct organizational structure as well as applying Verification & Validation (V&V) concepts, which are two fundamental elements of safety management, in an accurate way are therefore crucial. This part discusses railway safety management in terms of organizational structure and

V&V with regards to the current normative status with its drawbacks. Proposals are provided for an updated organization and more harmonized V&V concepts including relations with safety management and quality assurance by sharing practical experiences.

The organizational independence for SIL 4 is illustrated in EN 50129 [17], see Figure 3.1 referred to the System and HW development. In the illustration, same person and same organization arrangements are depicted as solid and dashed lines, respectively. In the figure, PM stands for Project Manager, DI for Designer/Implementer, VER for Verifier, VAL for Validator. Having provided the illustration and mentioned the independence of roles in Table E.3 in this standard, there are no more additional explanations about the independence of roles.

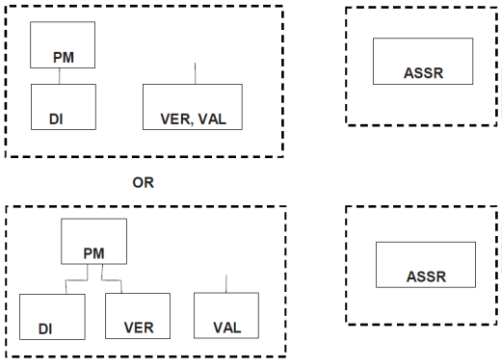


Figure 3.1 Organizational independence [17]

When the SW norm EN 50128 [18] is examined, it gives much more detail about the organizational independence as in Figure 3.2:

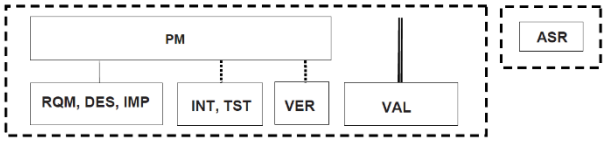


Figure 3.2 Preferred organizational structure [18]

It defines not only new roles such as Requirements Manager (REQ), Implementer (IMP), Integrator (INT) and Tester (TST), but also new type of vertical lines for the responsibility dependency such that RQM, DES (Designer), IMP shall report to the PM; INT, TST and VER can report to the PM whereas VAL shall not report to PM. Differently from the norm for electronic systems, this norm elaborates the roles by thirteen clauses. In addition, it offers two options for the roles validator and verifier. It allows that the VAL and the VER can be same person guarantying independence from the PM where in this case there

shall be a further person who reviews the documents of VER and who does not report to PM. A similar approach is brought to the role of VER in the way that VER and INT/TST can be the same person provided VAL performs verification tasks, too, such that there are double checks.

If considered, the similar tasks are also realized in system and HW development phases. For instance, there will also be HW tests, and a test report and a further verification report, however though the integrity level is the same, the organizational independencies differ from each other which means that the VER can perform test activities and write both test and verification report. The author therefore proposes at this step that the organizational structures in these norms shall be harmonized and the one stated in EN 50128 [18] can be used for this harmonization purpose, as it declares more roles and therefore more checks, which are inevitable in a safety critical system. Another problem for the independency requirements arises from the need of several verifiers in a project, as the verification activities do require specialization in the technique. In this case, a lead verifier can be assigned to the interface and will be responsible for fulfilling all the verification activities. In case there are a limited number of available specialized personnel, this time there arise personnel availability problems. To overcome this issue, it can be proposed that VER of a work-package can be allocated as DI of another work-package.

Table 3.1 Failure and hazard analysis [17]

Techniques/Measures	**SIL 4**
Preliminary hazard analysis	HR
Fault tree analysis	HR
Markov diagrams	HR
FMECA	HR
HAZOP	HR
Cause-consequence diagrams	HR
Event tree	R
Reliability block diagram	R
Zonal analysis	R
Interface hazard analysis	HR
Common cause failure analysis	HR
Historical event analysis	R

Besides, intensive safety analyses (see Table 3.1) shall be performed in safety critical systems to derive safety requirements, both at system and subsystem level. These analyses require broad technical knowledge and long term of experiences, in short special qualification. Therefore, it is far more above than the specialization of a designer. Additionally, as Oedewald and Gotcheva [64] take attention, many safety activities are carried out by subcontractor networks which means that the subcontractors and their deliverables shall be checked for correctness, completeness and consistency by an expert of the main system owner. Hence, the author proposes a new role, namely the "safety responsible (SR)" to be added to this structure with the tasks provided below:

- Developing the safety plan,
- Performing safety analyses,
- Creating and maintaining the hazard log,
- Ensuring that the entries in the hazard log are successfully closed or further allocated in an appropriate manner,
- Being responsible for ensuring that safety requirements are met successfully,
- Deciding whether a deviation or change is safety relevant or not and ensuring that it is successfully closed,
- Obtaining safety evidence of the third party items including their Safety Related Application Conditions,
- Deriving the Safety Related Application Conditions for the developed item(s) in the project
- Composing the safety case

The addition of the new role "SR" arises from another necessity, as well that in terms of the independence and appropriateness of the tasks of VAL, a considerable number of tasks are usually fulfilled by the VAL, which does not coincide with the primary validation tasks. For instance, there is no statement in the norms about the responsible person for the safety plan. It has been observed in the industry that the safety plan is usually written by the VAL. However, the safety plan itself needs both verification and validation. The same is also valid for the safety analyses as well as hazard log and safety case. To make this point clearer, the author analyzes the V&V concept in the further in the next part.

Beside the safety responsible as acting person for safety technical pertinent issues, another work package in a safety critical project is the safety management activities such as planning and coordination of the V&V activities, the internal and external audits and assessments, reviews, management of subcontractors concerning RAMS activities. Both the SR and VAL can perform safety management activities as these activities do not contradict with the validation activities. Below, the proposed organizational structures for all three-development processes, system, HW, SW, are depicted. The SR is preferable independent from the PM considering his/her activities explained above such as deciding for the safety relevance of a change request to avoid any stress factor that can be caused by the PM due to time and/or costs pressure. Another issue is that EN 50128 [18] does not allow REQ, DES or IMP to be INT, however, considering the role of INT in the norm, this is not contrary to the independency, and thus it can be proposed to update the organization as Figure 3.3.

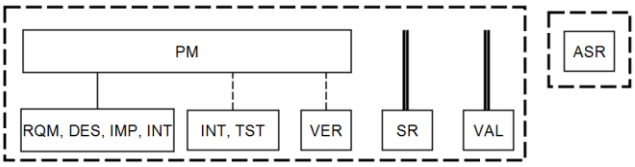


Figure 3.3 Proposed Organizational Structure

Furthermore, an important role during safety critical system development is allocated to the customer/operator. However, in GAPs, there is neither customer nor operator, at least during the design phase, which increases the difficulty as the customer has in fact significant tasks in safety relevant projects as explained in

Table 3.2. The customer and operator are incorporated once during the specific application projects on the field. Especially when identifying hazards and assessing risks, the customer is needed, as the standard IEC 61882 [55] clarifies that both the contractor and the client should constitute the HAZOP team. To meet these needs, a person inside the company having experience in the domain and technical knowledge about the specifications can be assigned as a customer to the project. However, it should be noted that, the customer and the PM have very different responsibilities which shall be performed in an independent manner and it should not be confused that customer and PM can be the same person as there is no limitation in the organizational structure given in the aforementioned norms

Table 3.2 Responsibilities within the RAMS Process [16], x full, (x) partial responsibility

	Customer/ Operator	Approval Authority	(Main) Contractor	Sub-Contractor	Suppliers
Concept Phase	X				
System Definition & Application Conditions	X				
Risk Analysis	X		X		
System Requirements	X	(X)			
Apportionment of System Requirements	(X)		X		
Design and Implementation			X	(X)	
Manufacture			X	X	X
Installation			X	(X)	
System Validation	X	X	X	(X)	
System acceptance	X	X			
Operation and Maintenance	X		(X)	(X)	
Performance Monitoring	X		(X)	(X)	
Modification and Retrofit	X		X	X	
De-commissioning and Disposal	X		(X)		

Although verification and validation definitions should be consistent in the CENELEC Norms, these are defined somehow differently in these norms which causes ambiguity when creating plans and performing activities.

- Verification in EN 50126 [16]: confirmation by examination and provision of objective evidence that the specified requirements have been fulfilled.
- Verification in EN 50129 [17]: the activity of determination, by analysis and test, at each phase of the life-cycle, that the requirements of the phase under consideration meet the output of the previous phase and that the output of the phase under consideration fulfils its requirements.
- Verification in EN 50128 [18]: the process of examination followed by a judgment based on evidence that output items (process, documentation, software or application) of a specific development phase fulfil the requirements of that phase with respect to completeness, correctness and consistency.

TST is not defined in EN 50129 [17], the verification activity here involves test whereas in EN 50128 [18], the verification is based on the review. EN 50129 [17] comments verification as a process, rather than a product. For each phase in EN 50126 [16], there are verification steps of the phase considering the requirements of the phase. EN 50128 [18] makes these more comprehensible and inclusionary, therefore for avoiding misapplication during the project and the harmonization of the verification definition, it is proposed to use the definition in EN 50128 [18] in the whole project.

Coming to the validation, the situation requires the same level of attention. According to the definitions given below, again here, the test is underlined in EN 50129 [17] while EN 50128 [18] uses tests for checking the results.

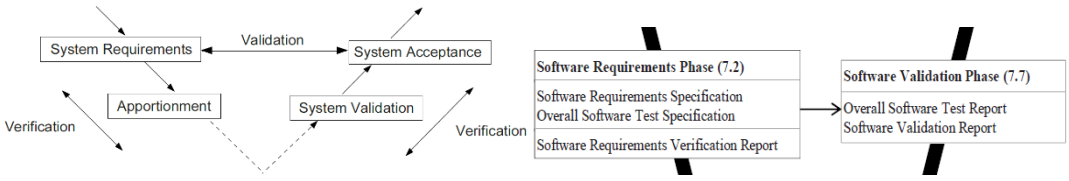


Figure 3.4 V&V EN 50126 [16] (left), SW Validation against SW Requirements EN 50128 [18] (right).

- Validation in EN 50126 [16]: Confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use have been fulfilled.
- Validation in EN 50129 [17]: The activity applied in order to demonstrate, by test and analysis, that the product meets in all respects its specified requirements.
- Validation in EN 50128 [18]: Process of analysis followed by a judgment based on evidence to deter-mine whether an item (e.g. process, documentation, software or application) fits the user needs, in particular with respect to safety and quality and with emphasis on the suitability of its operation in accordance with its purpose in its intended environment.

For the harmonization, the author of this thesis proposes that the definition in EN 50128 [18] should be used. Moreover, validation is depicted (see Figure 3.4) in all the CENELEC norms in a way that it is realized against system requirements. However, the validation is to be performed not only at the end against system requirements, but as Lundteigen et al. [40], verification and validation are important activities in all phases of the project development process. For instance, at the planning phase, the tools shall be validated or if they are already pre-validated, this should be checked against the intended use or the risk analyses are to be validated. Another task can be witnessing the independence during the design and test. Thereof, the author proposes Figure 3.5 to represent the V&V activities.

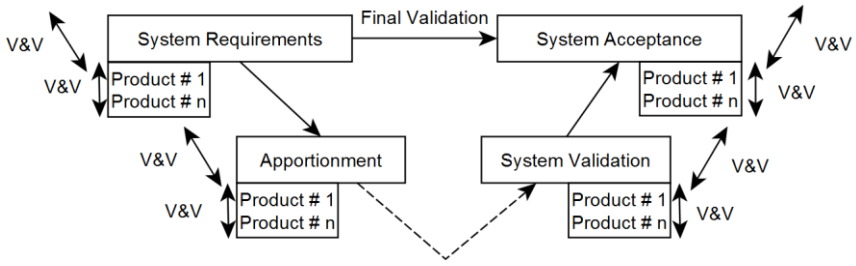


Figure 3.5 Proposed V&V representation

Several management reports are to be created in a safety critical system. The main reports included in the safety case are verification, validation, safety management, quality assurance and assessment reports. An important issue to be tackled is the creation order of these reports, since there must be relations between them. For the order, the following procedure, also approved by an independent assessor, can be applied. After the deliverables are produced, the products of the phase and the process itself shall be verified against EN 50126 [16]. Then, the validator can create his/her report considering the deliverables and verification report. Sometimes, the validator can prefer to compile some phases as shown in Figure 3.6. Following this, the safety management report can be developed using checklist so that every item is closed, or if necessary, transferred to the next phase in an appropriate manner. After this, quality assurance team can verify phase related quality requirements recording the results in their reports. Having applied the illustrated order in Figure 3.6. during the project, the safety management report to be incorporated in the safety case can only refer to the individual phase relevant safety management reports by summarizing their results.

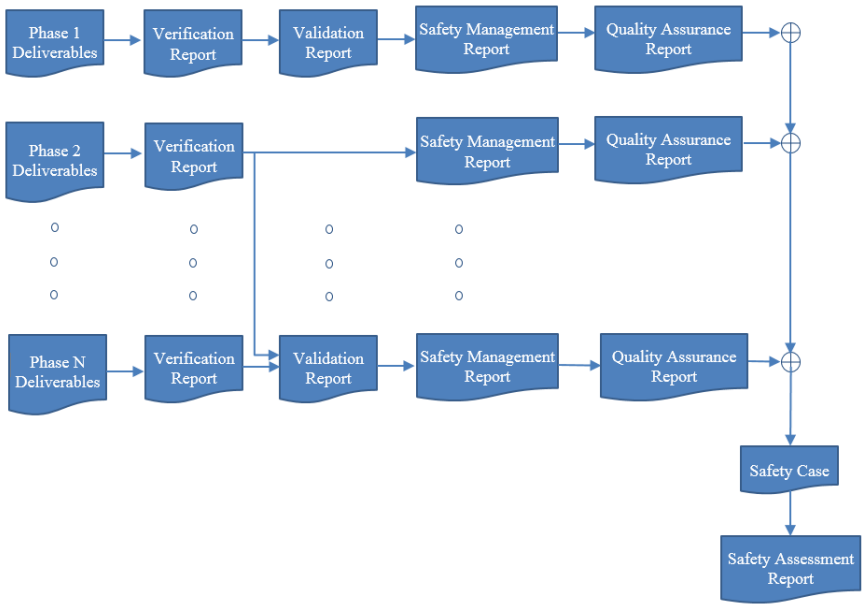


Figure 3.6 Relations between Verification, Validation, Safety Management, Quality Assurance and Assessment Reports

3.3 Further Arguments about the Safety Norms

Although being developed for tens of years, when used these norms, it has been revealed that there are still several inconsistencies. The existence of these inconsistencies is possible, since there are too much data and too many requirements. Within this study,

these are mentioned and detailed when the relevant topic is related with the item in the standards. In addition, this section explains further points that are to be cleared in the safety standards.

3.3.1 Failure and Hazard Analysis Methods

In EN 50129 [17], Table E.6 is "Failure and hazard analysis methods". In this table, the Preliminary Hazard Analysis (PHA), the Interface Hazard Analyses (IHA) and the Common cause failure analysis are not the "analysis methods", but the "tasks" to be performed. These studies can be undertaken by using the "analysis methods" such as FMEA, FMECA, and FTA. To make a better understanding, these items could be removed from this table and they can be added as "tasks" under the section "Phase Related Safety Tasks" to the "Figure 9: Project Phase Related Tasks" in EN 50126 [16]. And they can further be referenced in the relevant sections in this norm in the same way as other tasks are referenced.

3.3.2 Subjective approach instead of objective for Techniques / Measures

There are techniques and measures defined in the standards to be used during the development both system, HW, and SW. The "HR" is defined in the standards IEC 61508 [2], EN 5012-8/-9 [17], [18] as "This symbol means that the measure or technique is Highly Recommended for this safety integrity level. If this technique or measure is not used the rationale behind not using it shall be detailed." However, this brings an unequal competition in the market considering that applying a method such as FTA analyses takes effort of months. In this case, an assessor can approve a method (maybe changeable from one country to another country) while another does not, also a subjective approach instead of objective, but the goal of a standard is actually to "standardize". So a company may need to do all the "HR" items while another can only realize one and just give rational, which is accepted by the assessor. It is proposed that these methods should more be specialized or removed such that only "M" (Mandatory) and "R" (Recommended) -used for optional requirements- are provided. For instance, while developing an HW, the standard may put FTA and Common cause failure analysis as mandatory and leave other ones as "R" in such a way that it does not leave so much flexibility, which would result in an unfair competition between the companies in the market, especially for the newcomers to the sector.

In addition, how depth the methods will be applied are not provided in the standards, either. For instance, the SW part of the standard IEC 61508-3 [2] Table A.4 and EN 50128 [18] Table A.3 sets “Defensive programming” for SIL 3 and 4 “HR”. But the question arises is that whether the entire SIL 3/4 part of the SW shall consider “Defensive programming” or not. One could choose this method and apply at some parts and can claim that this method is applied. When asked this question to a reputable ISA (Independent Safety Assessor) company in Europa, the answer was surprising that we should not use the method in every relevant section. Similar is also valid for “Limited size and complexity of Functions, Subroutines, and Methods”, “Limited number of subroutine parameters” or “Limited use of Global Variables”. What is “Limited” according to the standard, e.g. a limited number for a company can be five while it can be hundred for another company. How can the ISA judge such a statement? These kind of “open-ended” points bring also ambiguities so we propose to take out such “open-ended” items from the standards or update them with objective perspectives.

3.3.3 Common Cause Failure (CCF) Scoring Table

Table D.1 in IEC 61508-6 [2] is scoring table to calculate the common cause factors. In this table, there are points for systematic failures, and this contributes to the quantitative failures for instance, in maintenance section there is the question: “Is all maintenance of printed-circuit boards, etc. carried out off-site at a qualified repair center and have all the repaired items gone through a full pre-installation testing? However, for 1oo1 and 2oo2 architectures, systematic HW failures are not considered although some items as in the given example are independent of the architecture. This seems not to be consistent, and a proposal is to add a parameter for systematic HW faults in all architectures or to remove all questions that are also relevant with non-redundant architectures such as 2oo2.

A further issue with the table is that the table has two columns, namely “Logic subsystem” and “Sensors/final elements”. However, in the questionnaire inputs and outputs are given in the logic subsystem. For instance, there is the question “Is the system simple, for example, no more than 10 inputs or outputs per channel?” Nevertheless, “Logic subsystem” and “Input/Output module” should be handled differently. Since the section “D.3 Points taken into account in the methodology” of the same part of the standard explains the methodology for quantifying the effect of hardware-related common cause failures in E/E/PE systems where it is mentioned that because sensors, logic subsystem,

and final elements are subject to, for example, different environmental conditions and diagnostic tests with varying levels of capability, the methodology should be applied to each of these subsystems separately. And as shown in Figure 3.7 below (Figure B.2 of the same standard), the inputs modules are taken into account as outside the logic voting component.

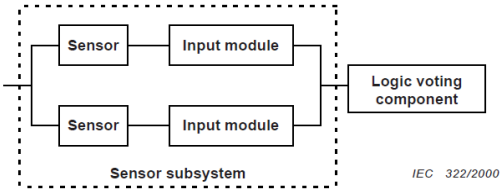


Figure 3.7 The Relationship Example configuration for two sensor channels [2]

3.3.4 SIL 0 SW

The standard IEC 61508 [2] does not mention about SIL 0, and EN 50129 [17] does not define this SIL while only mentioning “no specific requirements” in section A.5.1. EN 50128 [18] gives more details and requirements for this SIL. This issue results in the inconsistencies both in theoretical and practical manner. Firstly, the SIL is to be attached to a safety function. A safety function is defined in IEC 61508-4 [2] as a function to be implemented by an E/E/PE safety-related system or other risk reduction measures that are intended to achieve or maintain a safe state for the equipment under control (EUC), in respect of a particular hazardous event. And the safety function is defined for the SIF (Safety implemented function) at system level, which is then apportioned to the subsystems and then the SW and HW parts of these subsystems/components. And as there is no quantitative SIL 0 defined in these aforementioned norms, from this normative point of view, the integrity level “0” is not applicable.

EN 50128 [18] states in 4.4 that “At least the SIL 0 requirements of this European Standard shall be fulfilled for the software part of functions that have a safety impact below SIL 1. This is because uncertainty is present in the evaluation of the risk, and even in the identification of hazards. In the face of uncertainty, it is prudent to aim for a low level of safety integrity, represented by SIL 0, rather than none.”. In contrast, the goal of developing a safety critical system according to these though norms and performing the intensive hazard analyses as mentioned before are to extinguish any uncertainties that could cause a hazard with an unacceptable risk level. In case there is uncertainty, then this uncertainty shall be revealed in a safety critical system with appropriate methods.

Otherwise the uncertainty may have been required a SIL 4 development process but could be overlooked with such an approach and it is not claimable that the system is safe, i.e. safety is defined as “freedom from unacceptable risk” in IEC 61508-4 [2]. If the risk is unknown, how can it be argued that it is acceptable? And these unclear statements are very open to being commented subjectively, which is not the aim of any kind of standard including very significant safety standards. As a result, we propose to remove the “SIL 0” statement from EN 50128 [18] to be compliant with “safety” philosophy and avoid any misuses.

3.3.5 Single Faults

In EN 50129 [17], section B.3 Effects of Single Faults, it is mentioned that “It is necessary that SIL 3 and SIL 4 systems remain safe in the event of any kind of single random hardware fault, which is recognized as possible”. Then three methods are defined to achieve safety in the event of a single fault. These are composite fail-safety, reactive fail-safety, and inherent fail-safety. On the other hand, a common cause failure (CCF) in redundant systems like 1oo2, 1oo2D or 2oo3 architectures are random hardware faults, they are also recognized as possible and the SIL 3 or SIL 4 systems do not remain safe in the event of CCF. Moreover, this CCF parameter (ß factor) is also considered in the PFD/PFH calculations as CCF results in system dangerous failure. Therefore, there is a contradiction in the definition of single faults. Proposal to eliminate this contradiction can be to mention that common cause failure are to be considered not in this class or there can be added a probability for the “impossibility” mentioned at the beginning sentence of B.3.

3.3.6 The Planning phase of the Development

Although the planning phase is one of the most important phases of a safety-relevant project, neither in IEC 61508 [2] nor in EN 50126[16], this phase is defined explicitly. In IEC 61508-1 [2], an overall planning step is shown after step 5, Overall safety requirements allocation, however, this step is for maintenance, validation and installation planning. There is no step where development plan or safety plan is referenced. Moreover, EN 51029 [17] is also confusing at some places for planning. For instance, establishing the RAM Program is given as a task in phase four – System requirements, however performing RAM analyses is a task in phase two – System definition and application

conditions. Nevertheless, without planning the analysis how can the RAM analyses be performed, i.e. which tools will be used, by whom and when it will be done etc. Therefore, the RAM program should be established at the first phase or second before RAM analyses as it is the case for the safety plan. Hence, it is proposed to set a clear planning phase at the beginning of the development for every task to be performed during the project.

3.3.7 The Relation between RAM and Safety

As a holistic approach to RAMS requirements is lacking in 61508 [2], provides a model for a holistic approach. A related discussion in the safety industry is how the relationship between the RAM and safety is to be set up. While some argue that RAM is not in the scope of safety, the others claim the opposite. It has been observed in different projects that safety assessors have also distinct approaches such that while some set RAM tasks in their assessment plans and perform RAM assessments, other do not attach importance to RAM, so they do not undertake any RAM assessments. Having investigated the standards, RAM is included in EN 50129 [17] in the "Safety Case". The "Safety Case" consists of 6 parts and the part 4 is the "Technical Safety Report". This report has again 6 sections and section 2 is the "Assurance of correct functional operation". This part includes 6 sections and section 5 of it is "Assurance of correct hardware functionality". The content of this part is given as a description of the system/sub-system/equipment hardware architecture, and explain how the design achieves the required integrity, as laid down by the requirements specification and any relevant standards, in respect of - reliability,- availability, - maintainability, - safety. Accordingly, RAM activities are to be undertaken correctly for the proper safety demonstration and safety assurance according to the current state of EN 50129 [17]. On the other hand, no tasks or activities regarding RAM are given in the main safety standard, the IEC 61508 [2], which provides tables in section A.2 of the first part for the documentation in the life cycles where no RAM document is mentioned. Although RAM should be placed in the Safety Case according to this safety standard, we believe that RAM and Safety are to be considered independently from each other. For instance, an airplane that is unavailable to fly is actually safe. Therefore, the author proposes to remove RAM from the Safety Case detailed in EN 50129 [17].

3.4 Mathematical Descriptions

For the mathematical descriptions, mainly the reference [65] and [66] utilized.

- **Reliability**

$$R(t) = P(T > t) \tag{3.1}$$

Reliability equals the probability that T, failure time, is greater than t, operating time interval. R(t) is a cumulative distribution function. It begins at a probability of one and decreases to a probability of zero. Reliability is a function of failure probability and operating time interval. Reliability is a measure that is usually applied to situations such as aircraft flights and space missions where no repair is possible. In these circumstances, a system must operate continuously without any failure to achieve mission success.

- **Unreliability**

In terms of the random variable T,

$$F(t) = P(T \leq t) \tag{3.2}$$

Unreliability equals the probability that failure time will be less than or equal to the operating time interval. Since any device must be either successful or failed, F(t) is the one's complement of R(t).

$$F(t) = 1 - R(t) \tag{3.3}$$

F(t) is also a cumulative distribution function. It begins with a probability of zero and increases to a probability of one.

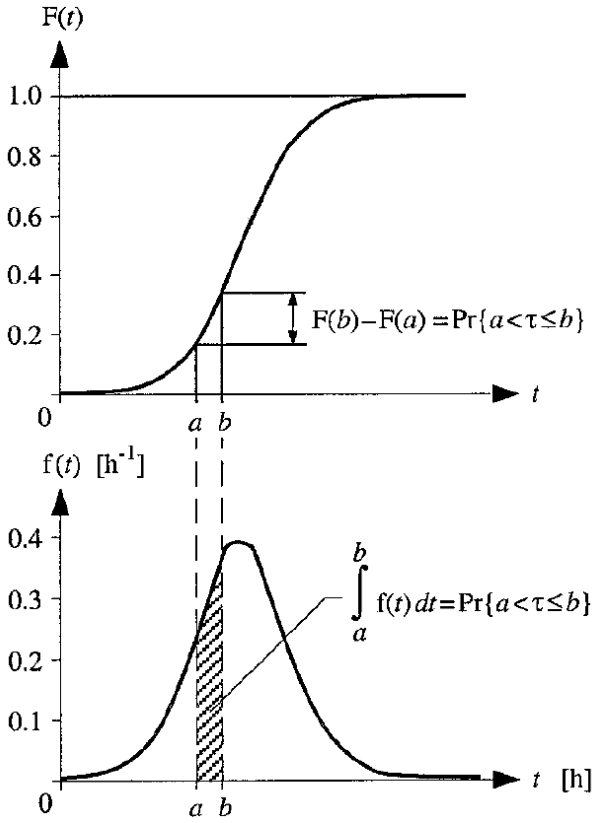


Figure 3.8 The Relationship between the distribution function F(t) and the density f(t) for a continuous random variable to > 0 [65]

- **Availability**

Reliability is a measure that requires success (that is, successful operation) for an entire time interval. No failures (and subsequent repairs) are allowed. This measurement was not enough for engineers who needed to know the chance of success when repairs may be made. Another measure of success was required for repairable devices. Availability is a function of failure probabilities and repair probabilities whereas reliability is a function of failure probabilities and operating time interval.

- **Unavailability**

$$U(t) = 1 - A(t) \tag{3.4}$$

- **Probability of Failure**

The probability of failure during any interval of operating time is given by a probability density function (See Chapter 2). Probability density functions for failure probability are defined as

$$f(t) = dF(t)/dt \tag{3.5}$$

The probability of failure function can be mathematically described in terms of the random variable T:

$$\lim_{\Delta t \to 0} P(t < T \leq t + \Delta t) \tag{3.6}$$

This can be interpreted as the probability that the failure time, T, will occur between a point in time t and the next interval of operation, t + t, and is called the "probability of failure function.

The probability of failure function can provide failure probabilities for any time interval. The probability of failure between the operating hours of 2000 and 2200, for example, is:

$$P(2000,2200) = \int_{2000}^{2200} f(t)dt \tag{3.7}$$

- **Mean Time to Failure (MTTF)**

It is defined from the statistical definition of expected or "mean" value. The mean represents the "center of mass" of a distribution. Mean is defined for continuous random variables as:

$$E(t) = \int_{-\infty}^{+\infty} xf(x)dx \tag{3.8}$$

The mean represents the "center of mass" of a distribution and it should not be confused with median that is a measure of center. The median value is defined as the data sample where there are an equal number of samples of greater value and lesser value. It is the "middle" value in an ordered set. If there are two middle values, it is the value halfway between those two values.

Using the random variable operating time interval, t, and recognizing that there is no negative time we can update the mean value equation and substitute the probability density function f(t):

$$E(t) = \int_{-\infty}^{+\infty} xf(x)dx \tag{3.9}$$

$$f(t) = -\frac{dR(t)}{dt} \tag{3.10}$$

$$E(t) = \int_{0}^{+\infty} tdR(t) \tag{3.11}$$

$$E(T) = -[t(R(t)]_0^{\infty} - [-\int_{0}^{+\infty} tdR(t)] \tag{3.12}$$

The first term equals zero at both limits. This leaves the second term, which equals MTTF:

$$MTTF = E(T) = \int_{0}^{+\infty} R(t)dt \tag{3.13}$$

MTTF is the definite integral evaluation of the reliability function. Note that the definition of MTTF is NOT related to the inverse of (failure rate), that is only a special case derived for a constant failure rate for single components or series of components, all with constant failure rates.

$$MTTF \neq \frac{1}{\lambda} \tag{3.14}$$

- **Mean Time to Restore (MTTR)**

The term MTTR applies only to repairable devices. MTTF represents the average time required to move from successful operation to unsuccessful operation. MTTR is the average time required to move from unsuccessful operation to successful operation. The term Mean Dead Time (MDT) is an older term which means the same as MTTR.

- **Mean Time Between Failures (MTBF)**

MTBF is a term that applies only to repairable systems. Like MTTF and MTTR, it is an average value, but it is the time between failures. This implies that a device has failed and then has been repaired. For a repairable device,

MTBF = MTTF + MTTR (3.15)

- **Failure Rate**

Reliability parameter (λ(t)) of an entity (single components or systems) such that λ(t).dt is the probability of failure of this entity within [t, t+dt] provided that it has not failed during [0, t].

In [65], failure rate is provided as the number of failures per unit time from a quantity of components exposed to failure.

$$\lambda(t) = \frac{Failures\ per\ Unit\ Time}{Quantity\ Exposed} \tag{3.16}$$

However, it should be "the number of failures per unit time from a quantity of working components exposed to failure".

$$\lambda(t) = \frac{Failures\ per\ Unit\ Time}{Quantity\ of\ Working\ Componens\ Exposed} \tag{3.17}$$

Failure rate is also equal to the ratio of failure probability density function to reliability.

$$\lambda(t) = \frac{f(t)}{R(t)} \tag{3.18}$$

For instance, if 300 resistors have been operating in a plant for seven years and if five failures have occurred, then the failure rate is 5/(295x7x8760) FIT where FIT represents one billion.

A useful probability density function in the field of reliability engineering is the exponential. For this distribution:

$$f(t) = \lambda e^{-\lambda t} \tag{3.19}$$

$$F(t) = 1 - e^{-\lambda t} \tag{3.20}$$

$$R(t) = e^{-\lambda t} \tag{3.21}$$

$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{\lambda e^{-\lambda t}}{e^{-\lambda t}} = \lambda \tag{3.22}$$

This means that a collection of components that have an exponentially decreasing probability of failure will have a constant failure rate. If components exhibit a decreasing failure rate, the constant failure rate can still be used as it represents a worst-case assumption.

The MTTF of a device with an exponential probability density function (PDF):

$$MTTF = \int_0^{+\infty} R(t)dt = \int_0^{+\infty} e^{-\lambda t}dt = -\frac{1}{\lambda}[e^{-\lambda t}]_0^{\infty} = 1/\lambda \tag{3.23}$$

This is valid for single components with an exponential PDF or a series system (a system where all components are required for successful operation) composed of components, all of which have an exponential PDF.

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \cdots \tag{3.24}$$

if x is sufficient small, then

$$e^x \approx 1 + x \tag{3.25}$$

Hence, when λt is sufficiently small, then

$$F(t) = 1 - e^{-\lambda t} = 1 - (1 + \lambda t) = \lambda t \tag{3.26}$$

The approximation gives pessimistic result, therefore it is on the conservative side, i.e. safer side.

- **Steady-State Availability**

For long-term conditions it is assumed that the "restore rate" (1/MTTR) is constant.

$$\mu = \frac{1}{MTTR} \tag{3.27}$$

For single components with a constant failure rate and a constant restore rate, steady-state availability can be calculated:

$$A = \frac{\mu}{\mu + \lambda} = \frac{MTTF}{MTTF + MTTR} \tag{3.28}$$

This is a common formula for steady-state availability for a single component with a constant failure rate and a constant restore rate and applies to series systems.

- **Diagnostic Coverage (DC)**

Fraction of dangerous failures detected by automatic on-line diagnostic tests. The fraction of dangerous failures is computed by using the dangerous failure rates associated with the detected dangerous failures divided by the total rate of dangerous failures.

$$\mathrm{DC} = \frac{\lambda \mathrm{dd}}{\lambda \mathrm{d}} \tag{3.29}$$

- **Safe Failure Fraction (SFF)**

Property of a safety related element that is defined by the ratio of the average failure rates of safe plus dangerous detected failures and safe plus dangerous failures.

$$\mathrm{SFF} = \frac{\lambda \mathrm{s} + \lambda \mathrm{dd}}{\lambda} \tag{3.30}$$

3.5 Analysis Techniques for Safety

Several techniques can be usable for the quantitative analyses for different purposes. They can be divided both as static or dynamic such as Boolean and states/transitions, respectively and analytical or simulation (Monte Carlo). While there are the static logical links between the elementary failures and the whole system failure in Boolean models like RBD and FTA, system behaviors (jumps from states to states) according to arising events (failures, repairs, tests, etc.) are handled in states/transitions models like Markovian and Petri nets.

- **Reliability Block Diagram (RBD)**

The target of the analysis is represented as a success path consisting of blocks, lines and logical junctions. A success path starts from one side of the diagram and continues via the blocks and junctions to the other side of the diagram. A block represents a condition or an event, and the path can pass it if the condition is true or the event has taken place. If the path comes to a junction, it continues if the logic of the junction is fulfilled. If it reaches a vertex, it may continue along all outgoing lines. If there exists at least one success path through the diagram, the target of the analysis is operating correctly.

An importing issue is that when calculating, the subsystems shall be classified correctly. For example, in the figure below a sensor subsystem is composed parallel connection of series sensor and input module.

For parallel connection of components, a CCF is to be inserted.

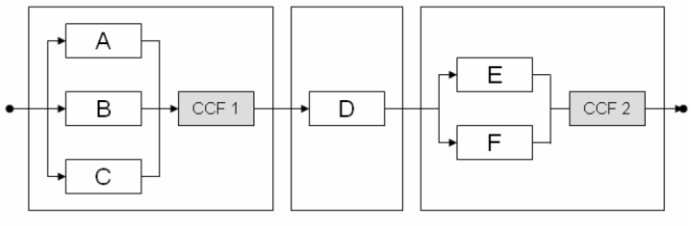


Figure 3.9 RBD of a whole safety loop [2]

- **Fault Tree Analysis (FTA)**

Fault trees have exactly the same properties as RBD but in addition they constitute an effective deductive (top-down) method of analysis to develop models step by step from the top event (unwanted or undesirable event) to the individual components failures. The minimal cut sets should be considered when calculating. While RBD is based on the system working, FTA considers system failures.

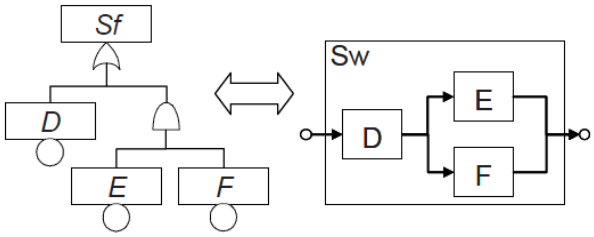


Figure 3.10 FTA and RBD presentation [2]

Applying basic probabilistic mathematics on logical functions lead straightforwardly to the probability of failure P_{Sf} of the system:

$$P_{Sf} = P(D) + P(E \cap F) - P(D \cap E \cap F) \tag{3.31}$$

If the components are independent, and Pi is the probability that component i is failed, then:

$$P_{Sf} = P_D + P_E P_F - P_D P_E P_F \tag{3.32}$$

Although this is valid for time independent models, if the probability of failure of each individual component at time t is independent of what happens on the other component over [0, t] the above formula remains valid at any time

The instantaneous unavailability U_{Sf} is:

$$U_{Sf}(t) = U_D(t) + U_E U_F(t) - P_D(t)P_E(t)P_F(t) \tag{3.33}$$

The conclusion is that fault trees or reliability block diagrams allow calculating directly the instantaneous unavailability $U_{Sf}(t)$ of E/E/PE safety-related systems and additional calculations are needed. From the unavailability case,

$$PFD_{avg}(T) = \frac{1}{T} MDT(T) = \frac{1}{T}\int_0^T U_{sf}(t)dt \tag{3.34}$$

single failure (D):

$$PFD(\tau) = \frac{1}{\tau}\int_0^\tau \lambda_D t dt = \frac{\lambda_D \tau}{2} \tag{3.35}$$

double failure (E, F):

$$PFD(\tau) = \frac{1}{\tau}\int_0^\tau \lambda_E \lambda_F t^2 dt = \frac{\lambda_E \lambda_F \tau^2}{3} \tag{3.36}$$

- **Markov Diagrams**

In systems with shared load, the component failure increases the load on other components, hence the failure rate of the entire system while at the same time the CCF arises. RBD and FTA can be sometimes not sufficient to model the system behavior. Consider a system with standby mode where the failure of the standby component will be important when it is operated. Therefore the rate of failure is a function of the time and not constant. The failure time of the first operating component affects the operation time of the standby component resulting in the failure rate of the system. This shows that components might not be evaluated independently for some cases. Moreover, the order of the component faults is to be taken into account. When the assumption for the independence between component failures and/or repairs is not possible, combinatorial

models such as RBD or FTA cannot answer to the requirements and stochastic processes must be used [26]. Moreover, combinatorial models are not sufficient to evaluate reliability of a parallel system with repairable components as the history of component failure and repair events are parameters in the function beside the interested time. system depends not only on the set of component states at a specified time but also on. Furthermore, availability calculation of single components is not feasible because possible sequences of failures and the repairs are needed.

Stochastic process is collection of random variables by time. Stochastic processes can handle complex and sequence-dependent situations and dynamic system behaviors such as repairs, shocks, common cause and dependent failures, sequence/state-dependent failure rates, complex error handling and recovery mechanisms, phased mission requirements [26]. As stated in [67], the Markov technique that is in the class of stochastic processes make use of a state transition diagram to represent and calculate the reliability, availability, maintainability, and safety behaviours of a system.

Table 3.3 Markov Solution Techniques and Applicability [65]

Markov model characteristics	Continuous time dependent solution via differential equations	Steady State Availability solution via algebraic equations	MTTF (State) solution via matrix inversion	Discrete time probability solution via matrix multiplication	MTTF (State) solution via matrix multiplication
Model represents a fu11y reparable system (regular Markov model) with constant failure and repair probabilities	Yes	Yes	Yes	Yes	Yes
Model represents a non-repairable system (absorbing states) with constant failure and repair probabilities	No	No	Yes	Yes	Yes

Table 3.3 Markov Solution Techniques and Applicability [65] (cont'd)

Model represents a fully repairable system with non-constant failure or non-constant repair probabilities	No	No	No	Yes	Yes
Model represents a non-repairable system (model has absorbing states) with non-constant failure and repair probabilities like a Safety Instrumented System (SIS) in low demand mode	No	No	No	Yes	Yes

Transitions for maintenance can be evaluated from repair times for maintenance procedures or from the norm MIL-HDBK-472 Procedures 2, 5A and 5B [68].

- **Mathematics of Markov Analysis**

In this thesis, the Markovian approach is used and in this section, a simplified Markovian model is provided for the background information about Markov analysis. In the real world, the equations are surely much more complex, but the basis does not change, hence it is valuable to give a brief math explanation at this step.

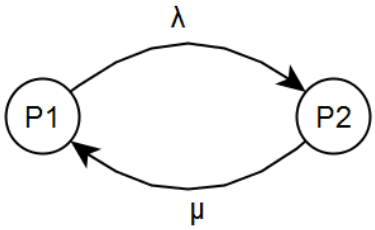


Figure 3.11 Two states Markov diagram

$$T = \begin{bmatrix} 0 & \lambda \\ \mu & 0 \end{bmatrix} \tag{3.37}$$

The matrix T is called a state transition rate matrix. The elements tij (row i and column j) represent the transition rate from state i to state j. T is a square (n x n) matrix of which diagonal elements are zero.

P(0) is the initial state and a row vector.

$$P(0) = [P_1(o), P_2(o)] \tag{3.38}$$

$P(t + \Delta t)$: The probability of state i at time t+Δt.

$P(t + \Delta t)$: The sum of the following two mutually exclusive events.

E_1: The system is in state 1 at time t and continues to remain in state 1 throughout the interval Δt.

E2: The system is in state 2 at time t and it transits to state 1 during the interval Δt.

$$P_1(t + \Delta t) = \Pr\{E_1\} + \Pr\{E_2\} \tag{3.39}$$

$$\Pr\{E_1\} = P_1(t).[1 - \lambda\Delta t] \tag{3.40}$$

$$\Pr\{E_2\} = P_2(t).\mu\Delta t \tag{3.41}$$

$$P_1(t + \Delta t) = P_1(t).[1 - \lambda\Delta t] + P_2(t).\mu\Delta t \tag{3.42}$$

$$P_2(t + \Delta t) = P_1(t).\lambda\Delta t + P_2(t).[1 - \mu\Delta t] \tag{3.43}$$

If the equations are rearranged and if Δt → 0, then

$$P_1'(t) = -\lambda.P_1(t) + \mu P_2(t) \tag{3.44}$$

$$P_2'(t) = \lambda.P_1(t) - \mu P_2(t) \tag{3.45}$$

$$\begin{bmatrix} P_1'(t) \\ P_2'(t) \end{bmatrix} = \begin{bmatrix} -\lambda & \mu \\ \lambda & -\mu \end{bmatrix} \begin{bmatrix} P_1(t) \\ P_2(t) \end{bmatrix} \tag{3.46}$$

This is in the form of:

$$Ax=B \text{ or } A.P(t)=B \tag{3.47}$$

Then the equations can be solved by utilizing linear algebra rules like Cramer's rule, or taking inverse. Laplace transform can also be utilized for a faster solution.

Availability Calculation

Because the system is operational only in state 1, the availability of the system is given below where the repair rate μ is considered in the Markov:

$A(t) = P_1(t)$.

Reliability Calculation

For reliability, the system shall be always at good state. Once the system reaches a failed state, it cannot be repaired. Considering state 2 is the failed state, repairs should not be considered in this state.

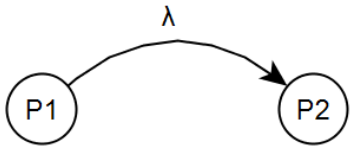


Figure 3.12 Reliability Model for two states Markov diagram

Accordingly, the set of equation is:

$$\begin{bmatrix} P_1'(t) \\ P_2'(t) \end{bmatrix} = \begin{bmatrix} -\lambda & 0 \\ \lambda & 0 \end{bmatrix} \begin{bmatrix} P_1(t) \\ P_2(t) \end{bmatrix} \quad (3.48)$$

The reliability of the system is given below where the repair rate μ is eliminated from the Markov diagram.

$$R(t) = P_1(t) \quad (3.49)$$

MTTF

$$MTTF = \int_0^{+\infty} R(t)dt \quad (3.50)$$

Frequency of Transition

Frequency of transition is the expected number of occurrences of a particular transition per unit time (at a specified time or at a steady state). This may be useful to know the total number of occurrences of an event (transition) within a specified time. Frequency of a transition from state to state can be found by multiplying $P_i(t)$ and t_{ij} (transition rate).

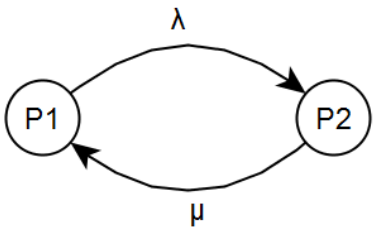


Figure 3.13 Two states Markov diagram for Showing Transition Frequency

The frequency of transition from state 2 to state 1 illustrated at the above figure is $P_2(t)\mu$. The expected number transitions can be found by integrating the frequency of transition over a specified interval.

Frequency of Visits to a State

The number of outward transitions in a state is the sum of the frequencies of all transitions that can occur in that state.

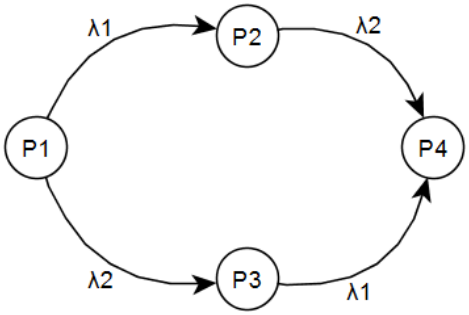


Figure 3.14 Four states Markov diagram for Showing State Frequency

The frequency of outward transition in state 1 is:

$$P_1(t)(\lambda_1 + \lambda_2) \tag{3.51}$$

The frequency of inward transition in state 4 is:

$$P_2(t)\lambda_2 + P_3(t)\lambda_1 \tag{3.52}$$

Under steady-state conditions, the frequency of inward transitions is equivalent to the frequency of outward transitions. This information can be used to find steady-state probabilities like Availability, Reliability and MTBF.

Failure and Recovery Frequencies

Failure frequency is the summation of frequencies of all transitions from good states to failed states. For the above drawing, it is:

$$P_2(t)\lambda_2 + P_3(t)\lambda_1 \tag{3.53}$$

Total number of failures within an interval can be found by integrating the failure frequency over that interval.

Similarly, for the recovery (repair) frequency, the transitions from failed states to good states should be considered. Under steady-state conditions, system failure frequency is equivalent to system recovery (success) frequency.

Steady-State State Probabilities

The steady-state probabilities can be found by substituting infinity for the time t. Steady-state probabilities can be utilized for Availability, Reliability, MTTF, MTBF calculations.

$$A(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu}\exp(-(\lambda+\mu)t) \tag{3.54}$$

By substituting t→ ∞

$$A(t=\infty) = \frac{\mu}{\lambda+\mu} \tag{3.55}$$

Another method is considering that at steady state condition, there is no change in the states. So, if the equation is in the form below,

$$\begin{bmatrix} P_1'(t) \\ P_2'(t) \end{bmatrix} = \begin{bmatrix} -\lambda & \mu \\ \lambda & -\mu \end{bmatrix} \begin{bmatrix} P_1(t) \\ P_2(t) \end{bmatrix} \tag{3.56}$$

then

$$Ax=B \text{ or } A.P(t)=B \tag{3.57}$$

where B=0 for the steady state.

$$\begin{bmatrix} 0 \\ 0 \end{bmatrix} = \begin{bmatrix} -\lambda & \mu \\ \lambda & -\mu \end{bmatrix} \begin{bmatrix} P_1(t) \\ P_2(t) \end{bmatrix} \tag{3.58}$$

In fact, if there are n states in the system, n-1 independent equations can be found. But, at any time, the sum of the probabilities of all states is equivalent to 1. This information can be used to make the number of unknowns and equations the same.

$$\sum_{1}^{n} P_i = 1 \tag{3.59}$$

Hence considering the steady state and the sum of the probabilities as equivalent to 1, the equation becomes:

$$\begin{bmatrix} -\lambda & \mu \\ 1 & 1 \end{bmatrix} \begin{bmatrix} P_1(t) \\ P_2(t) \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{3.60}$$

MTBF

MTBF (Mean Time Between Failure) of a system is the time between two successive failures of the system. It is the sum of the MDT (Mean Down Time) and MTTF (Mean Time to Failure). There exists a reciprocal relationship between MTBF and failure frequency. Therefore, if v is the steady-state failure frequency of the system, then

$$MTBF = \frac{1}{v} \tag{3.61}$$

$$v = P_1(t)\lambda \tag{3.62}$$

$$\begin{bmatrix} -\lambda & \mu \\ 1 & 1 \end{bmatrix} \begin{bmatrix} P_1(t) \\ P_2(t) \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{3.63}$$

$$P_1(t) = \frac{\mu}{\lambda + \mu} \tag{3.64}$$

$$v = \frac{\mu}{\lambda + \mu}\lambda \tag{3.65}$$

Markov Chain Simplification Rules

Parallel Transitions:

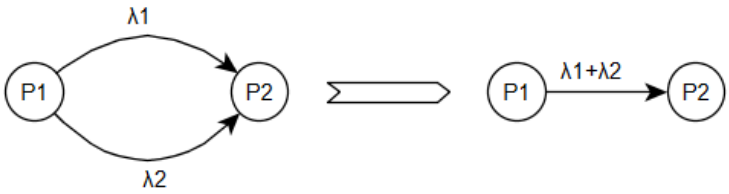


Figure 3.15 Four states Markov diagram for Showing State Frequency

Intermediate States:

If the states have the same outgoing events leading to the same state(s) and there is no other incoming/outgoing exist.

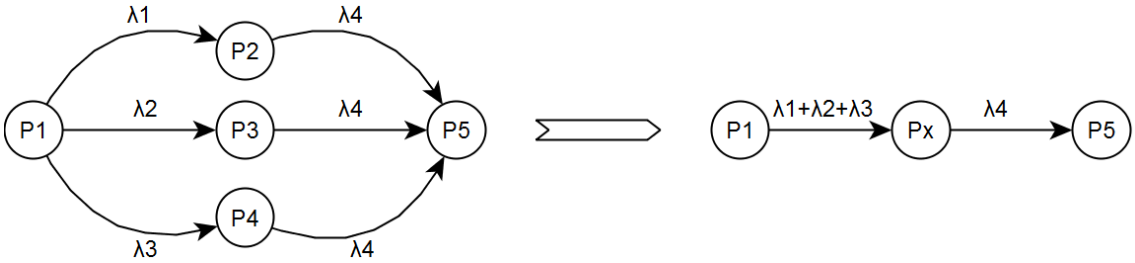


Figure 3.16 Four states Markov diagram for Showing State Frequency

CHAPTER 4

DEPENDENT FAILURES

This section summarizes different dependent failure models in the literature. There are two reasons to give place this section in the thesis. The first one is to build up a strong basis which is required for the calculations, thereof comparing and choosing the correct dependant failure model. The second reason is that during the research, it has been revealed that there are several mistakes including misspelling of parameters, which cause wrong result or absence in the reference studies. For instance, in [28], λ is used instead of δ in the Model Multiple Greek Letters on page 10/52, or in [26], for the same model, ρ1 is written equal to zero instead of one on page 5-28 or the expression Q_3 on page 5-29 in [26] is misspelled as

$$Q_3 = \frac{\beta\gamma}{3}(1-\gamma)\mathrm{Q_t} \tag{4.1}$$

instead of the equation below.

$$Q_3 = \frac{\beta\gamma}{3}(1-\delta)Q_t \tag{4.2}$$

Further in [69], only three methods are mentioned or the standard IEC 61508-6 [2], namely the models Beta Factor and Binomial Failure Rate. This section is compiled by utilizing the references [2], [6], [28], [69], [70], [71], [72], [73], [74], [75], [76], [77], [78], [79], [80].

4.1 Overview to Dependent Failures

Independent random HW errors can occur in all channels of a multichannel system in a way that all channels were in a faulty state at the same time. The probability of such failures concurrently affecting parallel channels is low in comparison to the probability

of a single channel failing since random HW failures are assumed to occur randomly as a function of time.

In the literature, Dependent Failures are splitted in three categories, namely Common Cause Failure, Common Mode Failures, and Cascade Failures. Common Cause Failure causes multiple failures from a single shared cause. The multiple failures may occur simultaneous or over a period. Common Mode Failures are a special case of CCF in which items of multiple equipment fail in the same mode. Cascade failures are the failures that propagate. Note that the term CCF is used to cover all kind of dependant failures in the main safety standard [2].

CCF Definitions in Different Domains

CCF is defined with slight different meanings in various domains. Below, these are summarized.

- Nuclear industry [77]: The event either contains multiple failures that qualify as-a CCF or the event is one of a set of events that are part of a CCF event.
- Space industry [81]: The failure (or unavailable state) of more than one component due to a shared cause during the system mission
- Process industry [9]: Failure, which is the result of one or more events, causing failures of two or more separate channels in a multiple channel system, leading to system failure.
- Electrical/electronic/programmable electronic safety related systems [2]: Failure that is the result of one or more events, causing concurrent failures of two or more separate channels in a multiple channel system, leading to system failure.

Another significant point that dependant failures can be resulted due to clear deterministic causes that should be analysed, modelled and quantified in a conventional way and residual potential multiple failure events not explicitly considered in the analysis because of not enough accuracy, no clear deterministic causes or impossibility to gather reliability data. The later class should be evaluated as shown in the informative Annex D of IEC 61508-6 [2].

4.2 Modelling Approach for Dependent Failures

There are different models to evaluate common cause failure (CCF) quantitatively. CCF can be modelled in two main ways: the explicit model and the implicit model.

i. **Explicit Modelling**: The cause is identified as a separate event in the model such as power failure or lightning. An illustrative example is shown below for the explicit modelling.

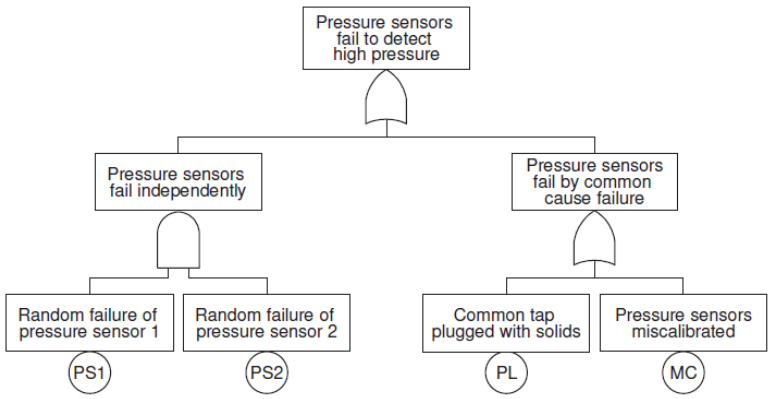


Figure 4.1 Four states Markov diagram for Showing State Frequency [69]

ii. **Implicit (Parametric) Modelling**: In case there are a number of root causes shared and coupling factors between items present, then implicit modelling is used as modelling explicitly could be very complex and some causes can be uncovered, the (residual) shared causes are modelled as a "combined" basic event/element. Implicit modeling implies using a CCF modeling approach. The term parametric modelling is used instead of implicit modelling, as well.

The basis standard IEC 61508-6 [2] proposes two methods for the implicit modeling, the β-factor and the binomial failure rate while mentioning that alternative methodologies may be preferred in some cases, for example, where a more accurate β -factor can be proven as a result of the availability of data on common cause failures or when the number of impacted elements is higher than four.

In the following, first mathematical background is provided. Then, different models are explained and compared with each other.

4.3 Implicit Models

Implicit models are used to model CCFs. The categories for the number of parameters required for modeling common cause events are:

- Single Parameter Models
- Multiple Parameter Models

With respect to how multiple failures occur, there are two categories:

- Shock Models
- Nonshock Models

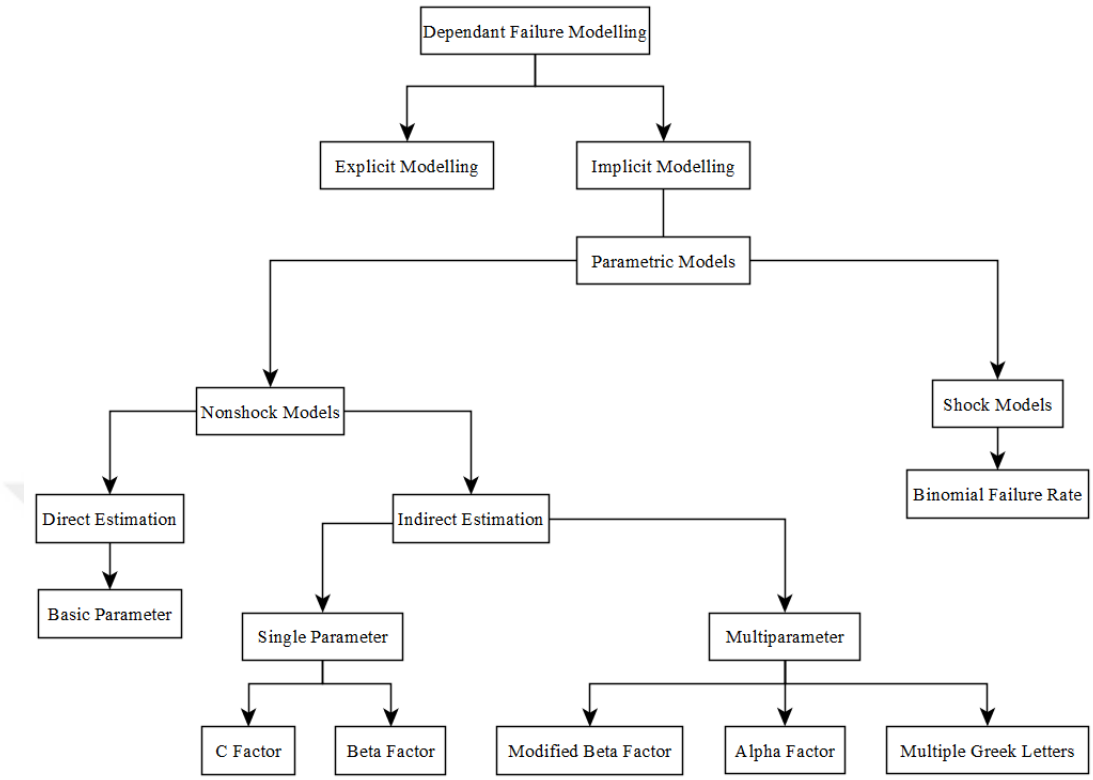


Figure 4.2 Dependent Failure Modelling

The specific models will be detailed in the subsequent sections.

4.3.1 Probabilistic Background and CCF Attributes

In this part, a mathematical background is provided for explaining mathematical calculations for implicit modelling.

Conditional probability is defined as below for the probability that A happens in case B happens.

$$P(A\backslash B\ ) = \frac{P(A \cap B)}{P(B)} \tag{4.3}$$

Bayesian Theory is defined as below:

$$P(A\backslash B)=P(B\backslash A)P(A)/P(B) \tag{4.4}$$

The probability that both items are in a failed state is

$$Pr(E_1 \cap E_2) = Pr(E_1 \setminus E_2) \,.\, Pr(E_2) = Pr(E_2 \setminus E_1) \,.\, Pr(E_1) \quad (4.5)$$

where Ei represents failed state of component i.

The two events, E1 and E2 are said to be statistically independent if

$$Pr(E_1 \setminus E_2) = Pr(E_1) \text{ and } Pr(E_2 \setminus E_1) = Pr(E_2) \quad (4.6)$$

such that

$$Pr(E_1 \cap E_2) = Pr(E_1) \,.\, Pr(E_2) \quad (4.7)$$

Two items, 1 and 2, are dependent when

$$Pr(E_1 \setminus E_2) \neq Pr(E_1) \text{ and } Pr(E_2 \setminus E_1) \neq Pr(E_2) \quad (4.8)$$

For reliability and safety analyses, positive dependency is related and it is defined as below.

$$Pr(E_1 \setminus E_2) > Pr(E_1) \text{ and } Pr(E_2 \setminus E_1) > Pr(E_2) \quad (4.9)$$

such that

$$Pr(E_1 \cap E_2) > Pr(E_1) \,.\, Pr(E_2) \quad (4.10)$$

On the other hand, for some cases one should also think negative dependency such that if the faults influence other components positively, for instance in case the components dissipate heat and by this way make an effect on the other component, then the fault of one component affects the other component positively.

Negative dependence between components is defined as following.

$$Pr(E_1 \setminus E_2) < Pr(E_1) \text{ and } Pr(E_2 \setminus E_1) < Pr(E_2) \quad (4.11)$$

such that

$$Pr(E_1 \setminus E_2) < Pr(E_1) \,.\, Pr(E_2) \quad (4.12)$$

- **Intrinsic or Extrinsic Dependency**

The dependency is also categorized as being intrinsic or extrinsic [77].

i. **Intrinsic dependency:** A situation where the functional status of a component is affected by the functional status of other components.

Sub-classes:

- Functional requirement dependency
- Functional input dependency
- Cascading failure

ii. **Extrinsic dependency:** A situation where the dependency or coupling is not inherent or intended in the functional characteristics of the system.

- Physical or environment stresses.
- Human intervention

- **Multiplicity of Failures**

Multiplicity: The number of items in a group that actually fails in the CCF event. For instance, a system of three components 1, 2, and 3, and let E_i be the event that item i is in a failed state and E_i^* that it is not

A failure event can have 3 different multiplicities:

A single failure:

$$P(SF) = (E_1 \cap E_2^* \cap E_3^*), (E_1^* \cap E_2 \cap E_3^*), (E_1^* \cap E_2^* \cap E_3) \quad (4.13)$$

A double failure:

$$P(DF) = (E_1 \cap E_2 \cap E_3^*), (E_1 \cap E_2^* \cap E_3), (E_1^* \cap E_2 \cap E_3) \quad (4.14)$$

A triple failure:

$$P(TF) = (E_1 \cap E_2 \cap E_3) \quad (4.15)$$

Let $g_{k,m}$ denote the probability of a specific combination of functioning and failed items such that exactly k items are in failed state and (m - k) items are functioning.

$$g_{1,3} = Pr(E_1 \cap E_2^* \cap E_3^*) = Pr(E_1^* \cap E_2 \cap E_3^*) = Pr(E_1^* \cap E_2^* \cap E_3) \quad (4.16)$$

$$g_{2,3} = Pr(E_1 \cap E_2 \cap E_3^*) = Pr(E_1 \cap E_2^* \cap E_3) = Pr(E_1^* \cap E_2 \cap E_3) \quad (4.17)$$

$$g_{3,3} = Pr(E_1 \cap E_2 \cap E_3) \quad (4.18)$$

Let $Q_{k:m}$ denote the probability that a CCF event in a system of m items has multiplicity k, for $1 \leq k \leq m$.

For a system of m = 3:

$$Q_{1:3} = \binom{3}{1} . g_{1,3} = 3. g_{1,3} \quad (4.19)$$

$$Q_{2:3} = \binom{3}{2} . g_{2,3} = 3. g_{2,3} \quad (4.20)$$

$$Q_{3:3} = \binom{3}{3} . g_{3,3} = 1. g_{3,3} \quad (4.21)$$

Recall that combination is defined as below.

$$\text{Combination: } C(n, r) = \binom{n}{r} = \frac{n!}{(n-r)! \, . \, r!} \quad (4.22)$$

The probability of system failure for 2-out-of-3 (2oo3) system functions as long as at least 2 of its 3 items function, and fails when 2 or more items fail is

$$Pr(\text{System failure}) = Q_{2:3} + Q_{3:3} \quad (4.23)$$

$$Pr(\text{System failure}) = 3. g_{2,3} + g_{3,3} \quad (4.24)$$

Let's define $f_{k,m}$ as the conditional probability that a CCF event in a system of m channels has multiplicity k, when we know that a specific channel has failed.

For a 2oo3 system of 3 identical items, if it is observed that item 1 is failed, so the conditional probability that this is a triple failure is:

$$f_{3,3} = Pr(E_1 \cap E_2 \cap E_3 \backslash E_1) = Pr(E_1 \cap E_2 \cap E_3)/Pr(E_1) = g_{3,3}/Pr(E_1) = g_{3,3}/Q \quad (4.25)$$

Q denotes the probability that item 1 fails, i.e., $Pr(E_1)$

The conditional probability that the failure is a double failure is:

$$f_{2,3}=Pr(E_1 \cap E_2 \cap E_3^{*} \backslash E_1)+Pr(E_1 \cap E_2^{*} \cap E_3 \backslash E_1)=g_{2,3}/Q+g_{2,3}/Q=2.g_{2,3}/Q \quad (4.26)$$

The conditional probability that the failure is a single failure is:

$$f_{1,3} = Pr(E_1 \cap E_2^{*} \cap E_3^{*} \backslash E_1) = g_{1,3}/Q \quad (4.27)$$

And important to notice that

$$f_{1,3} + f_{2,3} + f_{3,3} = 1 \quad (4.28)$$

- **Other CCF attributes:**

The shared cause has two elements, a root cause and a coupling factor.

i. **Root cause:** Most basic cause of item failure that, if corrected, would prevent recurrence of this and similar failures. E.g. design, manufacturing, maintenance, environmental stresses.

ii. **Coupling factor:** Property that makes multiple items susceptible to the same root cause. E.g. same design (principles), same HW/SW, same maintenance staff.

iii. **Common-cause component group (CCCG):** A group of (usually similar [in mission, manufacturer, maintenance, environment, etc.]) components that are considered to have a high potential for failure due to the same cause or causes.

4.3.2 Common Cause Basic Events

To facilitate subsequent application of data on historical independent and dependent failure events to the estimation of model parameters, it is convenient to define common cause basic events; that is, basic events that represent failures of specific components in a common cause component group (CCCG). This step is equivalent to a redefinition of the logic model basic events from a component-level basis to a lower level of detail that identifies the particular impacts that common cause events of specified multiplicity may have on the system. Thus, the common cause basic events are written in terms of the particular combination of components affected. The common cause basic events also provide an unambiguous and useful technical vocabulary for discussing each of the parametric models.

The expansion of this component-level Boolean expression down to the common cause impact level can be illustrated by representing each component-level basic event as a subtree.

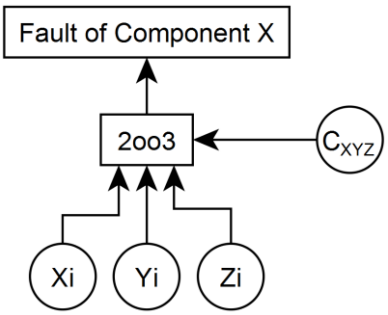


Figure 4.3 2oo3 system fault description

The equivalent Boolean representation of total failure of component X is

$$X_T = X_I + C_{XY} + C_{XZ} + C_{XYZ} \tag{4.29}$$

X_T: total failure of component X.

X_I : failure of component X from independent causes.

C_{XY}: failure of components X and Y (and not component Z) from common causes.

C_{XZ}: failure of components X and Z (and not component Y) from common causes.

C_{XYZ}: failure of components X, Y, and Z from common causes.

When all the components of our two-out-of-three example system are expanded similarly, the minimal cutsets obtained are $\{X_I, Y_I\}$; $\{X_I, Z_I\}$; $\{Y_I, Z_I\}$;$\{C_{XY}\}$; $\{C_{XY}\}$; $\{C_{BZ}\}$; $\{C_{XYZ}\}$.

The reduced Boolean representation of the system failure in terms of these cutsets is:

$$S = X_I.Y_I + X_I.Z_I + Y_I.Z_I + Z_{XY} + C_{XZ} + C_{YZ} + C_{XYZ} \tag{4.30}$$

The algebraic equivalent of Equation is:

$$P(S) = P(X_I).P(Y_I) + P(X_I).P(Z_I) + P(Y_I).P(Z_I) + P(C_{XY}) + P(C_{XZ}) + P(C_{YZ}) + P(C_{XYZ}) \tag{4.31}$$

where P(x) represents probability of the event x.

It is a common practice in risk and reliability analysis to assume that the probabilities of similar events involving similar types of components are the same. This approach takes advantage of the physical symmetries associated with identically redundant components in reducing the number of parameters that need to be quantified.

$$P(X_I) = P(Y_I) = P(Z_I) = Q_1 \quad (4.32)$$

$$P(C_{XY}) = P(C_{XZ}) = P(C_{YZ}) = Q_2 \quad (4.33)$$

$$P(C_{XYZ}) = Q_3 \quad (4.34)$$

Note that the probability of failure of any given basic event within a common cause component group depends only on the number and not on the specific components in that basic event. This is called the symmetry assumption.

Hence, for 2oo3, Qs can be written as follows:

$$Q_S = 3.Q_1^2 + 3.Q_2 + Q_3 \quad (4.35)$$

Q_S denotes Probability of System Failure. Generalization of this concept is straightforward; for the basic events corresponding to a common cause group of m components, the following probabilities can be defined:

Q_k : probability of a basic event involving k specific components; $1 \leq k \leq m$.

The total probability of failure of a specific component can be obtained from the Q_k's.

$$Q_t = Q_1 + 2.Q_2 + Q_3 \quad (4.36)$$

where Q_t is the total failure probability of component i. In general, the total failure probability of a component in a common cause group of m components is

$$Q_t = \sum_{k=1}^{m} \binom{m-1}{k-1} Q_k \quad (4.37)$$

The binomial expression $\binom{m-1}{k-1}$ represents the number of different ways that a specific component can fail with (k-1) other components in a group of m similar components.

4.3.3 Dependant Failure Models From Non-Shock Perspective

Ideally, Q_k's can be calculated from data in which case there is no need for further probabilistic modeling. Unfortunately, the data required to estimate Q_k's directly are not

normally available. Other models have been developed that put less stringent requirements on the data. This, however, is only done at the expense of making additional assumptions that address the incompleteness of the data. The models can be categorized in several different ways, based on the number of parameters, their assumptions regarding the cause, coupling mechanism, and impact of common cause failures. The mathematical models can be illustrated as below:

A. Direct Estimation

- **Basic Parameter Model**

The model that uses Q_k's to calculate system failure probability is called the basic parameter model. Except for the basic parameter model, all common cause models discussed in the report [72] estimate the probability of basic events indirectly; i.e., through the use of other parameters. In general, the types of parameters, estimation method, and data requirements vary from one model to another. However, with the current state of data that involve large uncertainties, the numerical impact of selecting one model over another is not significant, given a consistent treatment of data in all cases.

B. Indirect Estimation

B.1. Single Parameter Models

B.2.1. Beta Factor Model

The single parameter models refer to those parametric models that use one parameter in addition to the total component failure probability to calculate the common cause failure probabilities. The most widely used single parameter model, and the first such model to be applied to common cause events in applied risk and reliability analysis, is known as the beta factor model. According to the beta factor model, a fraction (β) of the component failure rate can be associated with common cause events shared by the other component in that group. According to this model, whenever a common cause event occurs, all components within the common cause component group are assumed to fail. Therefore, based on this model, for a group of m components, all Q_k's defined before are zero except Q_1 and Q_m. The last two quantities are written as

$$Q_k = (1-\beta)\mathrm{Q_t} \qquad for\ k = 1 \tag{4.38}$$

$$Q_k = 0 \qquad for\ m > k > 1 \tag{4.39}$$

$$Q_k = \beta Q_t \qquad for\ k = m \tag{4.40}$$

Described in other way, if a system consists of m identical channels and a channel has failed, then the conditional probability that this is a CCF of multiplicity k is:

$$f_{1,m} = (1- ß) \tag{4.41}$$

$$f_{k,m}= 0 \text{ for } k= 2, 3,..., m-1 \tag{4.42}$$

$$f_{m,m}= ß \tag{4.43}$$

Considering again the expression as in the format of Q_k

$$Q_1 = (1- \beta)\, Q_t \tag{4.44}$$

$$Q_k = 0 \tag{4.45}$$

$$Q_m = ß.Q_t \tag{4.46}$$

if m=2 and system is 1oo2 then,

$$P(A_T) = P(A_I) + P(C_{AB}) \tag{4.47}$$

$$Q_{AT} = Q_1 + Q_2 \tag{4.48}$$

$$Q_{BT} = Q_1 + Q_2 \tag{4.49}$$

$$P(S) = P(A_I)P(B_I) + P(C_{AB}) \tag{4.50}$$

$$Q_S = Q_1^2 + Q_2 \tag{4.51}$$

$$Q_S =(1- \beta)^2\, Q_t^2 + \beta Q_t \tag{4.52}$$

For 2oo3, Q_S was found before, accordingly, using ß factor for CCF results in

$$Q_S = 3(1- \beta)^2\, Q_t^2 + \beta Q_t \tag{4.53}$$

A practical and useful feature of this model is that the estimators of β do not explicitly depend on system or component success data, which are not generally available. This feature, the fact that estimates of the β parameter for widely different types of components vary much less than estimates of Q_k, and the simplicity of the model are the main reasons for wide use of this method in risk and reliability studies. It should be noted, however,

that estimating β factors, just as with any reliability analysis parameter, requires specific assumptions concerning the interpretation of data.

Although historical data collected from the operation of nuclear power plants indicate that common cause events do not always fail all redundant components, experience from using this simple model shows that, in many cases, it gives reasonably accurate (only slightly conservative) results for redundancy levels up to about three or four items. However, beyond such redundancy levels, this model generally yields results that are conservative. When interest centers around specific contributions from third or higher order trains, more general parametric models are recommended.

The limitation of the method is if a system consists of m identical items, then each item failure can have two distinct causes: (i) an independent cause (i.e., a cause that only affects the specific item), and (ii) a shared cause that will affect all the m items – and cause all m to fail at the same time.

This means that the multiplicity of each CCF event must be either 1 or m. It is not possible to have CCF events with intermediate multiplicities.

Another disadvantage of using the ß factor model is that an effort to reduce an item's susceptibility to CCFs will reduce the parameter ß, but will at the same time increase the rate of independent failures as

$$\lambda = \lambda_I + \lambda_C \tag{4.54}$$

$$\lambda_I = (1-ß)\,\lambda \tag{4.55}$$

$$\lambda = (1-ß)\,\lambda + ß\lambda \tag{4.56}$$

$$ß = \lambda_C / \lambda \tag{4.57}$$

When using the beta-factor model, the total failure rate λ is kept constant. It is obviously possible to compensate for this strange behavior, but this is often forgotten in practice.

B.2.1.1. Beta Factor Determination

The beta-factor may be determined by expert judgment, checklists and estimation based on observed data.

i. Expert Judgment:

It provides generic β factors. This means that they are based on the expert belief. Data may be collected through e.g. work shops where experts are gathered to discuss and agree upon representative values. See the OLF 070 guideline [80] or the PDS data handbook [82]. It is easy to apply, however it does not consider plant specific conditions.

ii. Checklist:

- **Humphrey's method**

An approach for determining a plant-specific beta was proposed by Humphreys [71]. Eight factors are important for the value of ß (grouped as design, operation, and environment). Each factor is classified as "a, b, . . . , e" and given scores according to a specific table, where "a" is the best state and "e" is the worst state. The factors are weighted based on expert judgment. The application-specific ß is determined by adding the scores and dividing by 50.000, resulted value is between 0.01% and 30%.

Table 4.1 Determining a plant-specific beta [71]

Factor	Subfactor	Scores				
		a	b	c	d	e
Design	Separation	2 400	580	140	35	8
	Similarity	1 750	425	100	25	6
	Complexity	1 750	425	100	25	6
	Analysis	1 750	425	100	25	6
Operation	Procedures	3 000	720	175	40	10
	Training	1 500	360	90	20	5
Environment	Control	1 750	425	100	25	6
	Tests	1 200	290	70	15	4

In some resources like in [4], this model is named as "Partial Beta Model".

- **IEC 61508** [2]

In this standard, there are 40 questions covering following issues:

1. Degree of physical separation/segregation

2. Diversity/redundancy

3. Complexity/maturity of design/experience

4. Use of assessments/analyses and feedback data

5. Procedures/human interface

6. Competence/training/safety culture

7. Environmental control

8. Environmental testing

For all questions with answer “yes”; the corresponding X values and Y values are summed up. Y is used for the diagnosis evaluation.

A table is used to determine the beta-factor based on the sum of X and Y. The method represents a ß factor between 0.5% and 5% (for logic solvers) and between 1% and 10% for sensors and final elements.

- **IEC 62061**

The safety of machinery standard IEC 62061 includes a similar, but a simplified list in compared to IEC 61508 [2].

1. Separation/segregation

2. Diversity/redundancy

3. Complexity/design/application

4. Assessment/analysis

5. Competence/training

6. Environmental control

- **Unified Partial Method**

The unified partial method (UPM) was proposed by Brand [83]. It is the standard approach in the UK nuclear industry. UPM assumes that the beta-factor is influenced by eight underlying factors (s_1, s_2, …, s_8). Each underlying factor s_i is associated with a weight and a score. A mathematical relationship is established between some underlying factors and the beta-factor.

The eight underlying factors are:

1. Environmental control

2. Environmental tests

3. Analysis

4. Safety culture

5. Separation

6. Redundancy and diversity

7. Understanding

8. Operator interaction

The factors are not independent of each other. A lineal relationship is assumed between the beta-factor and the "status" for each factor:

$$ß \approx \sum_{i=1}^{8} w_i . x_i \quad (4.58)$$

In practice, it is difficult to obtain statistically significant results for the correlation because CCF events are rare and it is not obvious that a linear relationship exists.

There is argue that the UPM model fails to take existing interactions among defences into account.

iii. Analyzing historical events and thereby find a β:

Data sources are to a large extent from the nuclear industry. There are ICDE data base (ICDE = international Common Cause Failure Data Exchange) and SKI data reports (SKI=Statens Karnkraft Inspektion). Altough the oil industry does not collect CCFs, they can collect in the future, due to the recommendations in the new version of ISO 14224 [84].

B.2.1.1. Updating the ß factor

The β may be updated to reflect plant specific conditions. In the operational phase, one may request to update (e.g. to take credit for improvements) the β parameter (for each group of components). Some approaches have been suggested. These can be summarized as the PDS approach, the checklists (that were previously presented) and see if any improvements lead to an improvement in the β, counting events and insert into a β-estimator equation.

a. The PDS Approach

There are also two alternative approaches presented in the PDS method [82], namely simple and extended. The "simple" approach corrects the β by k_β.

$$\beta^* = k_\beta \beta \quad (4.59)$$

And the "extended" method adds another correction factor k_s.

$$\beta^{**} = k_S\, k_\beta\, \beta \tag{4.60}$$

b. Using Checklists

Here refer back to the previous mentioned methods.

c. Counting events and using β-estimator equations

Here, one may choose a "rough" approach or a "comprehensive" approach. The formula for the rough approach is given below.

$$\beta = \frac{The\ number\ of\ CCF\ events\ for\ a\ group\ of\ similiar\ or\ same\ equipment}{All\ (dangerous)\ failures\ recorded\ for\ the\ same\ equipment} \tag{4.61}$$

For example, one CCF is observed in a period of 1 year for (safety critical) level transmitters. In the same period, we observed 5 other dangerous failures. We have all together 20 level transmitters at the installation. Then $\hat{\beta}$ = 1/5 = 20%.

In the rather comprehensive approach,

$$\beta^* = \frac{\sum_{j=2}^{n} jX_{j,n}}{\sum_{j=1}^{n} jX_{j,n}} \tag{4.62}$$

For instance, 5 events involving one channel, 1 event involving two channels, 0 events involving three channels are observed, then

$$\beta^* = \frac{2.1 + 3.0}{1.5 + 2.1 + 3.0} = 28\% \tag{4.63}$$

The even more comprehensive approach uses Bayesian method with prior and posterior distribution such that:

1. We may estimate a $\lambda_{C,init}$ as:

$$\lambda_{C,init} = \beta_{init}\lambda_{BE} \tag{4.64}$$

2. Then we may update the $\hat{\lambda}_{C,init}$which we may refer to as

$$\hat{\lambda}_C = \frac{\alpha + x}{\delta + t} \tag{4.65}$$

3. And then find how much (in%) the $\hat{\lambda}_C$ has increased,
4. And eventually allocate the increase to the β.

For example, if $\lambda_{C,init} = 0.6E-6$ and β_{init} = 0.1. We then get a new $\hat{\beta}$ = 0.017 (or 1.7%) which is quite different from other results.

B.2.1.2. C Factor Model

A variant of ß model is called the C-factor method, employed the same model, but, in order to address the incompleteness of the data sources, used a different method of estimating the parameter.

The C-factor model is mainly the same model as the beta-factor model, but the rate of dependent failures, λ_c is defined as a fraction (C) of the independent failure rate , λ_I instead of as a fraction of the total failure rate (as is done in the beta-factor model), such that

$$\lambda = \lambda_I + C.\ \lambda_I \quad (4.66)$$

This means that an effort to reduce the item's susceptibility to CCFs will reduce the total failure rate λ, and not as in the beta-factor model to increase the independent failure rate.

B.2. Multiparameter Models

B.2.1. The Modified Beta-Factor Model

The dependent and independent parts in beta-Model are modified. New β_k parameters are introduced in addition to the β-factor. For a configuration of three redundant components and omitting the independent failures for this example.

$$\beta_2 = Pr\ (3_{rd}\ \text{component fails} \backslash\ \text{Component 1 and 2 have already failed}) \quad (4.67)$$

$$PFD_{koon} = C_{koon}\ \beta\ PFD \quad (4.68)$$

The β_2 is used to calibrate the correction factor C_{koon}.

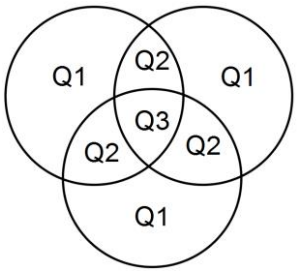


Figure 4.4 Modified Beta-Factor Model

$$Q_1 = 1-[2(1-\beta_2)\ \beta\ Q + \beta_2\ \beta\ Q] = 1-(2-\beta_2)\ \beta\ Q \quad (4.69)$$

$$Q_2 = (1- \beta_2)\, \beta\, Q \quad (4.70)$$

$$Q_3 = \beta_2\, \beta\, Q \quad (4.71)$$

For a 2oo3 system, the SIF fails if two or more component fail (tolerates one component failure).

$$PFD_{2oo3,\ CCF} = f_{2oo3} + f_{3oo3} \quad (4.72)$$

Where

$$f_{2oo3} = 3(1- \beta_2)\, \beta Q \quad (4.73)$$

$$f_{3oo3} = \beta_2 \beta Q \quad (4.74)$$

$$f_{2oo3} + f_{3oo3} = (3-2\beta_2)\, \beta Q \quad (4.75)$$

For a general expression, Q_1 was given in above equation, the Q_k's and Q_m can be written as below.

$$Q_k = (1-ß_2)ßQ \quad (4.76)$$

$$Q_m = ß_2 ß Q_t \quad (4.77)$$

B.2.2. Multiple Greek Letter Model (MGL)

For a more accurate analysis of systems with higher levels of redundancy, models that represent the range of impact levels that common cause events can have are more appropriate. These models involve several parameters with which to quantify the specific contribution of various basic events.

The MGL model is the most general of a number of recent extensions of the beta factor model. The MGL model was the one used most frequently in the International Common Cause Failure Reliability Benchmark Exercise. In this method, other parameters in addition to the β-factor are introduced to distinguish among common cause events affecting different numbers of components in a higher order redundant system.

The MGL parameters consist of the total component failure frequency, which includes the effects of all independent and common cause contributions to that component failure, and a set of failure fractions, which are used to quantify the conditional probabilities of

all the possible ways a common cause failure of a component can be shared with other components in the same group, given component failure has occurred. For a system of m redundant components and for each given failure mode, m different parameters are defined. For example, the first four parameters of the MGL model are:

Q_t : total failure frequency of the component due to all independent and common cause events.

β: conditional probability that the common cause of a component failure will be shared by one or more additional components.

γ: conditional probability that the common cause of a component failure that is shared by one or more components will be shared by two or more components additional to the first.

δ: conditional probability that the common cause of a component failure that is shared by two or more components will be shared by three or more components in addition to the first.

$$Q_k = \frac{1}{\binom{m-1}{k-1}} \prod_{i=1}^{k} p_i \, (1 - p_{k+1}) Q_t \tag{4.78}$$

$$p_1 = 1;\ p_2 = \beta; p_3 = \gamma; p_4 = \delta; \ldots;\ p_{m+1} = 0 \tag{4.79}$$

If m = 4, then

$$Q_1 = (1 - \beta)\mathrm{Q_t} \tag{4.80}$$

$$Q_2 = \frac{\beta}{3}(1 - \gamma)\mathrm{Q_t} \tag{4.81}$$

$$Q_3 = \frac{\beta\gamma}{3}(1 - \delta)\mathrm{Q_t} \tag{4.82}$$

$$Q_4 = \beta\gamma\delta Q_t \tag{4.83}$$

If the maximum number of components that can share a common cause is three (m = 3), then γ is the conditional probability that the common cause of failure of a component will be shared by exactly two additional components, and δ = 0.

If m = 3, then

$$Q_1 = (1-\beta)\mathrm{Q_t} \tag{4.84}$$

$$Q_2 = \frac{1}{2}\beta(1-\gamma)\mathrm{Q_t} \tag{4.85}$$

$$Q_3 = \beta\gamma\mathrm{Q_t} \tag{4.86}$$

For 2oo3, Q_S was found before, accordingly, using ß factor for CCF results in

$$Q_S = 3(1-\beta)^2 Q_t^2 + 3/2\ \beta(1-\gamma)Q_t + 3\beta\gamma Q_t \tag{4.87}$$

Note that the beta factor model is a special case of the MGL model. For this example, the MGL model reduces to the beta factor model if $\gamma = 1$ (and also $\delta=1$, if $m>3$).

B.2.3. Alpha Factor Model

As explained in References [73], [74] and [75], rigorous estimators for the β factor model and its generalization, the MGL model parameters, are fairly difficult to obtain although approximate methods have been developed and used in practice [76]. A rigorous approach to estimating β factors is presented in [74] through introducing an intermediate event-based parameter, which is much easier to estimate from observed data. Reference [79] uses the multiparameter generalization of event-based parameters directly to estimate the common cause basic event probabilities. This multiparameter common cause model is called the α-factor model.

The difference between the α-factor parameters and the MGL parameters is that the former are system-failure based, while the latter are component-failure based. The α-factor parameters are thus more directly related to the observable number of events than are the MGL parameters.

Like the MGL model, the alpha-factor model develops common cause failure frequencies from a set of failure ratios and the total component failure rate. The parameters of the alpha-factor model are defined as

Q_t : total failure frequency of each component due to all independent and common cause events

a_k : fraction of the total frequency of failure events that occur in the system involving the failure of k components due to a common cause

If, for example, for m=3, a_2 = 0:05 (or $a_{2:3}$ = 0:05), this means that 5% of all failure events in a group of 3 items is a CCF with multiplicity equal to 2.

$$\alpha_1 + \alpha_2 + ... + a_m = 1 \tag{4.88}$$

If, for example, for m=3, a_1 = 0:92, a_2 = 0:05, a_3 = 0:03, this means that 92% of all failure events in a group of 3 items is a CCF with multiplicity equal to 1, 5% of all failure events in a group of 3 items is a CCF with multiplicity equal to 2, and 3% of all failure events in a group of 3 items is a CCF with multiplicity equal to 3.

The general equation relating the basic event probabilities, Q_k 's to the α-factor model parameter is given below.

$$Q_k = \frac{\mathrm{k}}{\binom{m-1}{k-1}} \frac{\mathrm{a_k}}{a_t} Q_t, k = 1, \dots, m \tag{4.89}$$

$$a_t = \sum_{k=1}^{m} k\, a_k \tag{4.90}$$

The key difference between α in this model and the parameters of the MGL and β-factor models is that the former is a fraction of the events that occur within a system, whereas the latter are fractions of component failure rates.

The alpha-factor can be calculated as:

$$a_k = \frac{\binom{m}{k} Q_k}{\sum_{j=1}^{m} \binom{m}{j} Q_j} \tag{4.91}$$

where $\binom{m}{k} Q_k$ is the probability of a failure events involving exactly k items, and the denominator is the sum of such probabilities. a_k for m items is therefore the conditional probability of a CCF with multiplicity k, given that a failure event has occurred in a group of m items.

For 2oo3, Q_s was found before, accordingly, the probabilities of the basic events of the three-component system of 2oo3 (m=3) and the system unavailability are:

$$Q_1 = \frac{\alpha_1}{\alpha_t} \mathrm{Q_t} \tag{4.92}$$

$$Q_2 = \frac{\alpha_2}{\alpha_t} \mathrm{Q_t} \tag{4.93}$$

$$Q_3 = 3\frac{\alpha_3}{\alpha_t} \mathrm{Q_t} \tag{4.94}$$

$$a_t = a_1 + 2a_2 + 3a_3 \tag{4.95}$$

Therefore, the system unavailability for 2oo3 example is:

$$Q_s = 3\left(\frac{\alpha_1}{\alpha_t}\right)^2 \mathrm{Q_t^2} + 3\left(\frac{\alpha_2}{\alpha_t}\right) \mathrm{Q_t} + 3\left(\frac{\alpha_3}{\alpha_t}\right) \mathrm{Q_t} \tag{4.96}$$

4.3.4 Dependant Failure Models From Shock Perspective (Binomial Failure Rate Model)

The "shock models" estimate the frequency of multiple component failures by assuming that the system is subject to common cause "shocks" at a certain rate and estimating the conditional probability of failure of components within the system, given the occurrence of shocks. The common cause failure frequency is the product of the shock rate and the conditional probability of failure, given a shock. The binomial failure rate (BFR) model was proposed by Vesely [85] .

The BFR model in [77] considers two types of failures. The first represents independent component failures; the second type is caused by shocks that can result in failure of any number of components in the system. According to this model, there are two types of shocks: lethal and nonlethal. When a nonlethal shock occurs, each component within the common cause component group is assumed to have a constant and independent probability of failure. The name of this model arises from the fact that, for a group of components, the distribution of the number of failed components resulting from each nonlethal shock occurrence follows a binomial distribution. The binomial distribution with parameters n and p is a discrete probability distribution of the number of successes in a sequence of n independent experiments, each asking a yes–no question, and each with its Boolean outcome: a random variable containing single bit of information which can be success, true, one or as opposite to these failure, false, zero. The success probabilities are denoted p and the failure with q such that q is equal to 1 – p.

The BFR model is therefore more restrictive because of these assumptions than all other multiparameter models presented in Table below. When originally presented and applied, the model only included this nonlethal shock. Because of its structure, the model tended to underestimate the probabilities of failure of higher order groups of components in a highly redundant system; therefore, the concept of lethal shock was included. This version of the model is the one recommended. When a lethal shock occurs, all components are assumed to fail with a conditional probability of unity. Application of the BFR model with lethal shocks requires the use of the following set of parameters.

Q_I = independent failure frequency for each component.

μ = frequency of occurrence of nonlethal shocks.

ρ = conditional probability of failure of each component, given a nonlethal shock.

ω = frequency of occurrence of lethal shocks.

The general form of the probability of basic events according to the BFR model is given in below.

$$Q_k = Q_1 + \mu p(1-p)^{m-1} \qquad for\ k = 1 \tag{4.97}$$

$$Q_k = \mu p^k (1-p)^{m-k} \qquad for\ k \geq 2 \tag{4.98}$$

$$Q_k = \mu p^m + w \qquad for\ k = m \tag{4.99}$$

As an example for 2oo3, Q_s was found as before accordingly, the probabilities of the basic events of the three-component system of 2oo3 and the system unavailability are

$$Q_1 = Q_I + \mu p(1-p)^2 \tag{4.100}$$

$$Q_2 = \mu p^2 (1-p) \tag{4.101}$$

$$Q_3 = \mu p^3 + w \tag{4.102}$$

Therefore,

$$Q_w = 3[Q_I + \mu p\ (1-p)^2]^2 + 3\mu p^2\ (1-p) + \ \mu p^3 + w \tag{4.103}$$

It should be noted that the basic formulation of the BFR model was introduced in terms of the rate of occurrence of failures in time, such as failure of components to continue

running while in operation. Here, consistent with the presentation of other models, the BFR parameters are presented in terms of general frequencies that can apply to both failures in time and to failure on demand for standby components.

The model can be written more generally as following:

In the BFR model, each item in the CCCG has total (dependent) failure rate

$$\lambda_c = \lambda^{(i)} + pv \tag{4.104}$$

Let Z denote the number of items, among the n items in the CCCG that fail in a non-lethal shock. The probability distribution of Z is

$$Pr\ (Z = z) = \binom{n}{z} p^z (1-p)^{n-z} \quad \text{for z} = 0, 1, 2, \ldots \text{ n} \tag{4.105}$$

The rate of dependent total failures of the CCCG (i.e., that n-out-of-n items fail) is hence $\lambda^{(i)} + pv$. The rate of dependent failures of the CCCG of multiplicity k is:

$$\lambda_{G,c} = v\ Pr\ (Z = k) = v \binom{n}{z} p^k\ (1-p)^{n-k} \tag{4.106}$$

It is problematic to estimate the rate *v* of non-lethal shocks from observed data. This is because a non-lethal shock may not give any item failures (i.e., Z = 0) and thus may be unnoticed. It may also be assumed that each item may fail due to individual deterioration with rate λ_I such that the total failure rate of an item is $\lambda = \lambda_I + \lambda_c$.

Consider a voted group (CCCG) that is functioning if at least 2 of its four identical items are functioning. Lethal shocks are assumed to occur with $\lambda^{(i)} = 5.10^{-7}$ per hour. Non-lethal shocks are assumed to occur with rate $v = 8.10^{-6}$ per hour. When a non-lethal shock occurs, each item will fail (independently) with probability p = 0,40. The failure rate of each component is then $\lambda_c = \lambda^{(i)} + vp = 3{,}7\ .\ 10^{-6}$ per hour. The rate $\lambda_{G,c}$ of dependent group failures is

$$\lambda_{G,c} = \lambda^{(i)} + v\ Pr\ (Z > 2) = \lambda^{(i)} + v\left[\binom{4}{3} p^3\ (1-p)^{4-3} + p^4\right] = 1{,}93.10^{-6}[\frac{1}{h}] \tag{4.107}$$

4.4 Dependent Failures for Programmable Systems

The architecture of programmable systems allows them to carry out internal diagnostic testing functions during their on-line operation. These can be employed in a number of ways, for example in addition to internal testing, each channel in a PE system can monitor the outputs of other channels in a multi-channel PE. Therefore, if a failure occurs in one

channel, this can be detected and a safe shut-down initiated. This cross- monitoring can be carried out at a high rate, so that, just before a non-simultaneous common cause failure, a cross-monitoring test is likely to detect the failure of the first channel to fail and is able to put the system into a safe state before a second channel is affected.

In the case of the cooling fan example, the rate of temperature rise and the susceptibility of each channel are slightly different, resulting in the second channel failing possibly several tens of minutes after the first. This allows the diagnostic testing to initiate a safe shutdown before the second channel succumbs to the common cause fault. As a result of the above PE-based systems have the potential to incorporate defences against common cause failures and, therefore, be less susceptible to them when compared to other technologies and a different β -factor may be applicable to PE-based systems when compared to other technologies. Therefore, β -factor estimates based on historic data are likely to be invalid.

CHAPTER 5

SAFE AND RELIABLE PLATFORM CONSIDERATIONS

Safety standards, both international and European provides very detailed and complex information for designing safety critical platform. IEC 61508 [2] consists of seven chapters, 648 pages in total. Not only mastering the standard itself suffices for the design, but also the references given to other standards should be covered where necessary. For instance, part two lists sixteen main references such as IEC 61165 - Application of Markov techniques [86], IEC 60300 Dependability management – Part 3-2: Application guide [87]. The European norms EN 50126 [16], EN 50128 [18], EN 50129 [17], EN 50159 [19] and their several annexes and the references given inside them apply for Railway signalling and communication systems derived from IEC 61508 [2]. Yet the mathematical calculations in IEC 61508 [2] per se apply Railway Industry in that vein.

In section 3.5 Analysis Techniques for Safety, it is explained that there are several techniques that can be applied for the quantitative reliability analyses. In IEC 61508 [2], the RBD paradigm is used for deriving equations in accordance with various architectures. Another method accepted and used widely for sophisticated architectures is Markov Diagrams of which superiorities are discussed in the previous section. Applying different paradigms will surely result in different algebraic outcomes.

5.1 HW Architectures and Algebraic Formulations

Karydasa and Brombacherb [88] explain that architectural modeling deals with the development of a detailed block diagram of the programmable electronic system identifying each subsystem and the interconnections related to the safety function under consideration. IEC 61508 [2] defines six architectures providing the formulas depending on the parameters In this section, various HW Architectures are provided along with the

formulations based on the unconditional failure intensity and reliability block diagrams. The formulas use ß –factor approach for modelling CCFs.

5.1.1 The Architecture 1oo1

This architecture consists of a single channel, where any dangerous failure leads to a failure of the safety function when a demand arises.

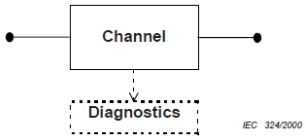


Figure 5.1 1oo1 physical block diagram

$$PFH_G = \lambda_{\mathrm{DU}} \tag{5.1}$$

5.1.2 The Architecture 1oo2

This architecture consists of two channels connected in parallel, such that either channel can process the safety function. It is assumed that any diagnostic testing would only report the faults found and would not change any output states or change the output voting.

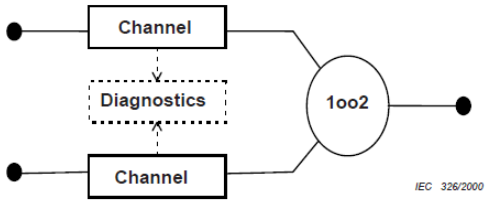


Figure 5.2 1oo2 physical block diagram

$$PFH_G = 2\big((1-\beta_{\mathrm{D}})\big)\lambda_{\mathrm{DD}} + (1-\beta)\lambda_{\mathrm{DU}}(1-\beta)\lambda_{\mathrm{DU}}t_{CE} + \beta\lambda_{\mathrm{DU}} \tag{5.2}$$

$$t_{ce} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR \tag{5.3}$$

5.1.3 The Architecture 2oo2

This architecture consists of two channels connected in parallel so that both channels need to demand the safety function before it can take place. It is assumed that any diagnostic testing would only report the faults found and would not change any output states or change the output voting.

$$PFH_G = 2\lambda_{DU} \quad (5.4)$$

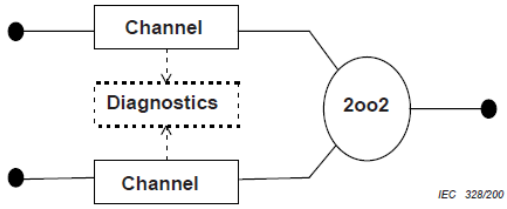


Figure 5.3 2oo2 physical block diagram

5.1.4 The Architecture 1oo2D

Special attention shall be paid for this architecture. This architecture consists of two channels connected in parallel. During normal operation, both channels need to demand the safety function before it can take place. In addition, if the diagnostic tests in either channel detect a fault then the output voting is adapted so that the overall output state then follows that given by the other channel. If the diagnostic tests find faults in both channels or a discrepancy that cannot be allocated to either channel, then the output goes to the safe state. In order to detect a discrepancy between the channels, either channel can determine the state of the other channel via a means independent of the other channel. The channel comparison / switch over mechanism may not be 100 % efficient therefore K represents the efficiency of this inter-channel comparison / switch mechanism, i.e. the output may remain on the 2oo2 voting even with one channel detected as faulty.

The parameter K will need to be determined by an FMEA.

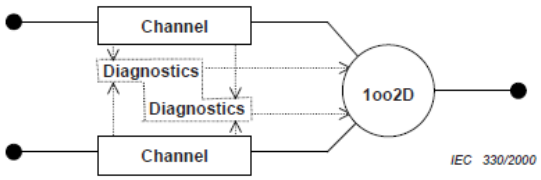


Figure 5.4 1oo2D physical block diagram

It should specially be noted that there is a major difference between 1oo2 and 1oo2D. For the former, diagnostic testing would only report the faults found and would not change any output states or change the output voting while diagnostic testing affect the output for the latter case.

$$PFH_G = 2(1-\beta)\lambda_{\mathrm{DU}}\big((1-\beta)\lambda_{\mathrm{DU}} + (1-\beta_{\mathrm{D}})\lambda_{\mathrm{DD}} + \lambda_{\mathrm{SD}}\big)t'_{CE} + 2(1-K)\lambda_{\mathrm{DD}} + \beta\lambda_{\mathrm{DU}} \quad (5.5)$$

$$t'_{ce} = (\lambda_{DU}\left(\frac{T_1}{2} + MRT\right) + (\lambda_{DD} + \lambda_{SD})MTTR)/\,(\lambda_{DU} + \lambda_{\mathrm{DD}} + \lambda_{\mathrm{SD}}) \quad (5.6)$$

5.1.5 The Architecture 2oo3

This architecture consists of three channels connected in parallel with a majority voting arrangement for the output signals, such that the output state is not changed if only one channel gives a different result, which disagrees with the other two channels. It is assumed that any diagnostic testing would only report the faults found and would not change any output states or change the output voting.

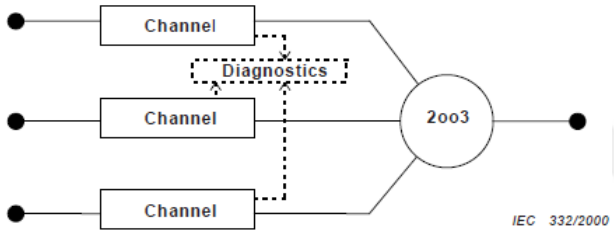


Figure 5.5. 2oo3 physical block diagram

$$PFH_G = 6\big((1-\beta_{\mathrm{D}})\big)\lambda_{\mathrm{DD}} + (1-\beta)\lambda_{\mathrm{DU}})(1-\beta)\lambda_{\mathrm{DU}}t_{ce} + \beta\lambda_{\mathrm{DU}} \quad (5.7)$$

5.1.6 The Architecture 1oo3

This architecture consists of three channels connected in parallel with a voting arrangement for the output signals, such that the output state follows 1oo3 voting. It is assumed that any diagnostic testing would only report the faults found and would not change any output states or change the output voting.

$$PFH_G = 6\big((1-\beta_{\mathrm{D}})\big)\lambda_{\mathrm{DD}} + (1-\beta)\lambda_{\mathrm{DU}})^2\ (1-\beta)\lambda_{\mathrm{DU}}t_{CE}t_{GE} + \beta\lambda_{\mathrm{DU}} \quad (5.8)$$

5.2 Discussion about the Architectures 1oo2 & 1oo2D and Proposing New

Architecture and Its Definition

When evaluating the safety architectures in the industry, it has been observed that there are different interpretations for the architectures. While a company presents its architecture as being 1oo2, the other claims its architecture as being 1oo2D although they have almost the same design principles. This happens because the definitions provided in the norm are not very clear. However, as will be proved in the next section, there can be a massive difference between 1oo2 and 1oo2D. Furthermore, Hokstad [89] searches how the DC is influenced when comparison of channels is applied as part of the diagnostic testing for multiple channel systems and suggests an alternative to define two betas, i.e. β for DU failures, and β_D for DD failures.

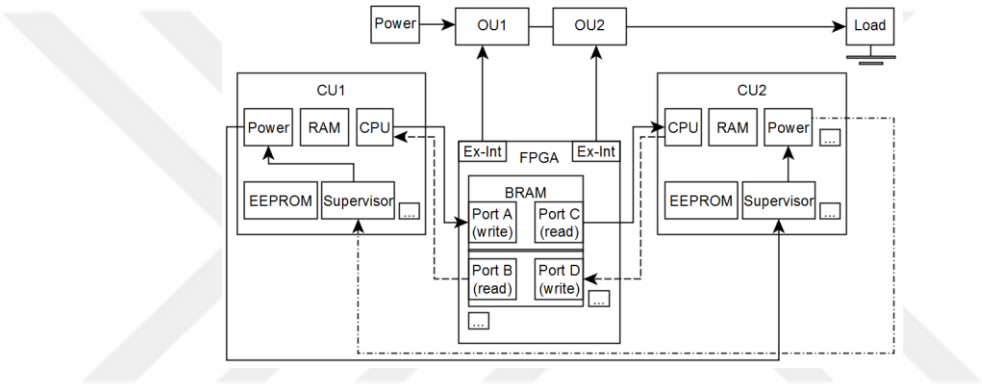


Figure 5.6. Sample safe computer architecture description.

A simplified example architecture is provided in Figure 5.6 where both of the control units (CU) can demand safety function independently over the output units (OU) communicated via FPGA. Moreover, when diagnostic testing (Supervisor) detects a fault, then the output changed to a safe state. Considering these two features, this architecture does fit neither to 1oo2 nor 1oo2D. It cannot be classified as 1oo2, because the diagnostic testing changes the output state when compared the definition of 1oo2 cited from the standard in section two. Furthermore, the diagnostic testing is used not only for reporting purposes as specified in the standard, but also to manipulate the output state, i.e. safety function. On the other hand, it can also not be classified as 1oo2D, since during normal operation, it is adequate that one CU can process the safety function, for instance CU 2 can process safety function by changing the output status of OU2 without requiring diagnostic results by the other channel while CU 1 does not process any safety function. This scenario is possible for many cases, for instance when there exists an undetected fault in channel 1. Moreover, an architecture can be built up with reciprocal diagnostic

testing of each channel, but in case of a discrepancy found, then safety function is not adapted so that the overall output state then follows that given by the other channel (1oo1), but the safety function immediately applied, for instance by shutting down the power. We therefore propose the need to renew the definition of 1oo2D where the safety function can be processed by one channel during normal operation; the output goes safe state and not adapted by the healthy channel if one channel fails. Another option can be to define a “new 1oo2” architecture definition with an adapted algebraic formula.

5.3 Effects of Safety Parameters for Various Architectures

This part focuses on the SIL 4 HW with regards to effects of safety parameters on the candidate architectures. The algebraic safety formulations of Average Frequency of a Dangerous Failure per Hour (PFH) for various architectures are provided in the IEC 61508 [2] without informing how they are derived. In these algebraic formulations, ß-Factor is used for modelling the dependant failures. A table is provided to track the values of variables in the equation. The parameter of interests is shown as "PoI", variating value as "v". Furthermore, special attention is paid for the architectures 1oo2D and 1oo2 and also 2oo3 as they are the most plausible architectures for reaching high PFH values. Besides, considering the simulation results for 1oo2D its normative definition is discussed and a novel definition is proposed to cover contemporary needs.

The units of the variables used in the following are provided as below:

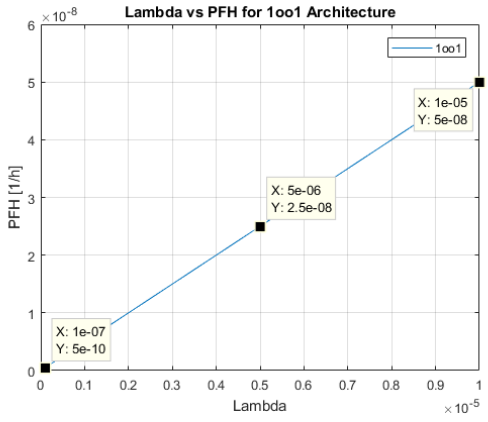
- λ and its derivations used in [1/h],
- MTTR, MRT used in [h],
- T1 (proof Test Interval) used in [y]

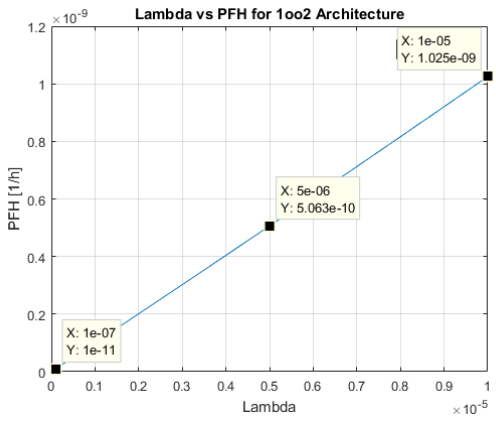
DC, SFF, ß, ßd and K used without any unit.

5.3.1 The Influence of λ

Table 5.1 Parameters used for the analysis of λ effect

λ (PoI)	λ_s	λ_{sd}	λ_d	λ_{dd}	λ_{du}	DC	SFF	ß	$ß_d$	MTTR	MRT	K	T1
1E-07<λ<1E-05	v	v	v	v	v	0.99	0.995	0.02	0.01	8	8	0.98	1





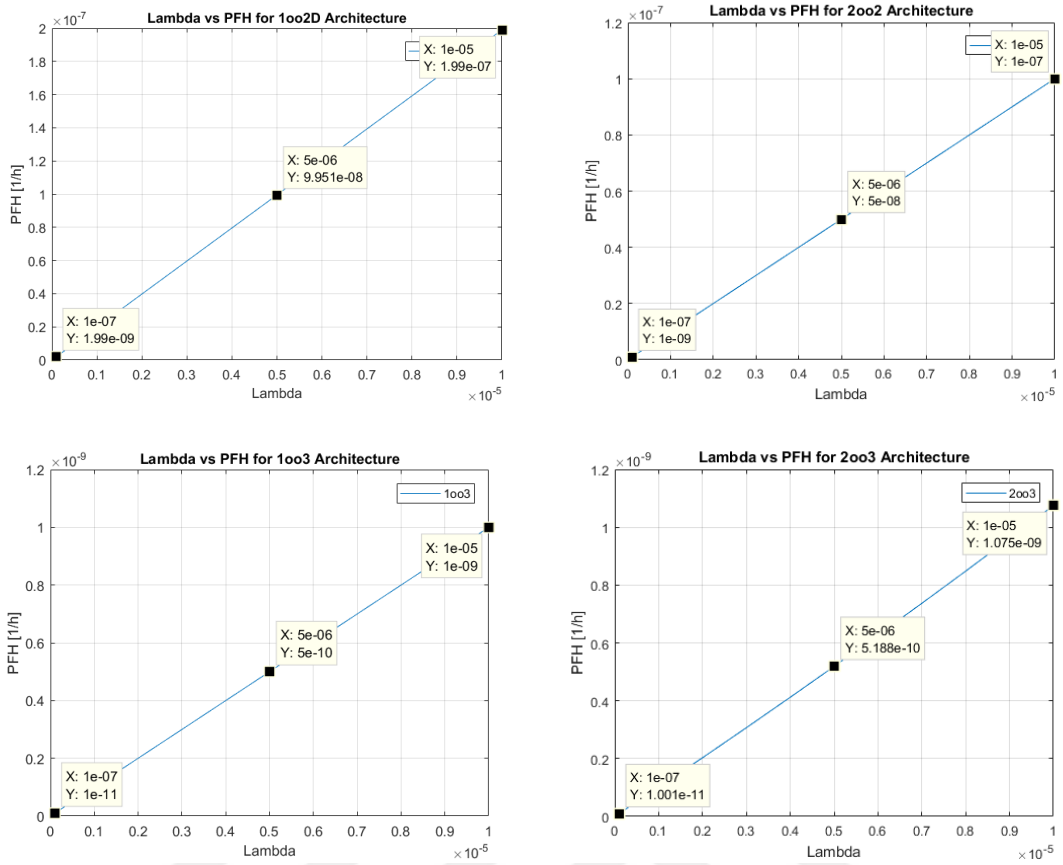


Figure 5.7 The influence of λ for different architectures

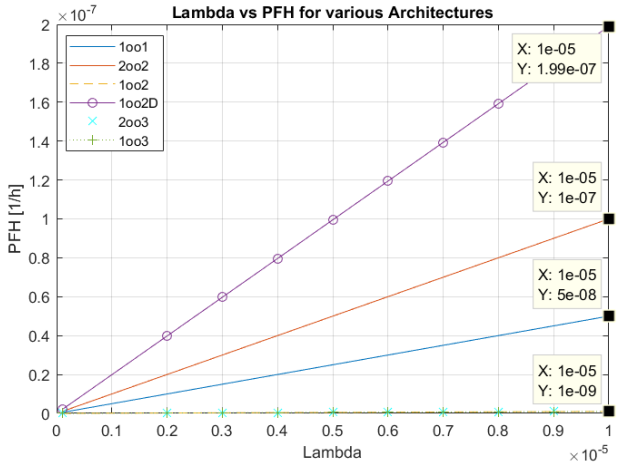


Figure 5.8 Comparison of the influence of λ for different architectures

Deduction:

There is a positive correlation between λ and PFH for all architectures. 1oo2D is the most affected architecture.

5.3.2 The Influence of ß and ßd

A. Influence of ß

ß limitations and calculation tables for logic subsystem are given in the standard as following.

$$S = X + Y \tag{5.9}$$

$$S_D = X(Z + 1) + Y \tag{5.10}$$

Table 5.2 Value of Z – programmable electronics

Diagnostic coverage	Diagnostic test interval		
	Less than 1 min	Between 1 min and 5 min	Greater than 5 min
≥ 99 %	2,0	1,0	0
≥ 90 %	1,5	0,5	0
≥ 60 %	1,0	0	0

Table 5.3 Calculation of $ß_{int}$ and $ß_{Dint}$

Score (S or S_D)	Corresponding value of β_{int} or $\beta_{D\ int}$ for the:	
	Logic subsystem	Sensors or final elements
120 or above	0,5 %	1 %
70 to 120	1 %	2 %
45 to 70	2 %	5 %
Less than 45	5 %	10 %
NOTE 1 The maximum levels of $\beta_{D\ int}$ shown in this table are lower than would normally be used, reflecting the use of the techniques specified elsewhere in this standard for the reduction in the probability of systematic failures as a whole, and of common cause failures as a result of this.		
NOTE 2 Values of $\beta_{D\ int}$ lower than 0,5 % for the logic subsystem and 1 % for the sensors would be difficult to justify.		

In accordance with the tables, Z is between 0 and 2, S is between 45 and 120, $ß_{int}$ and $ß_{Dint}$ are between 0.5% and 5%.

Table 5.4 Calculation of ß for systems with levels of redundancy greater than 1oo2

MooN		N			
		2	3	4	5
M	1	β_{int}	0,5 β_{int}	0,3 β_{int}	0,2 β_{int}
	2	-	1,5 β_{int}	0,6 β_{int}	0,4 β_{int}
	3	-	-	1,75 β_{int}	0,8 β_{int}
	4	-	-	-	2 β_{int}

Using the tables, following max and min values can be obtained as below.

Table 5.5 The max and min ß values for various architectures [%]

MooN		N			
		2	**3**	**4**	**5**
M	**1**	0,50	0,25	0,15	0,10
	2	-	0,75	0,30	0,20
	3	-	-	0,88	0,40
	4	-	-	-	1,00

MooN		N			
		2	**3**	**4**	**5**
M	**1**	5,00	2,50	1,50	1,00
	2	-	7,50	3,00	2,00
	3	-	-	8,75	4,00
	4	-	-	-	10,00

Table 5.6 Parameters used for the analysis of ß effect [%]

λ	λ_s	λ_{sd}	λ_d	λ_{dd}	λ_{du}	DC	SFF	ß (PoI)	$ß_d$	MTTR	MRT	K	T1
1E-07	5E-08	4,95E-08	5E-08	4,95E-08	5E-10	0.99	0.995	0.02<ß<0.2	beta/2	8	8	0.98	1

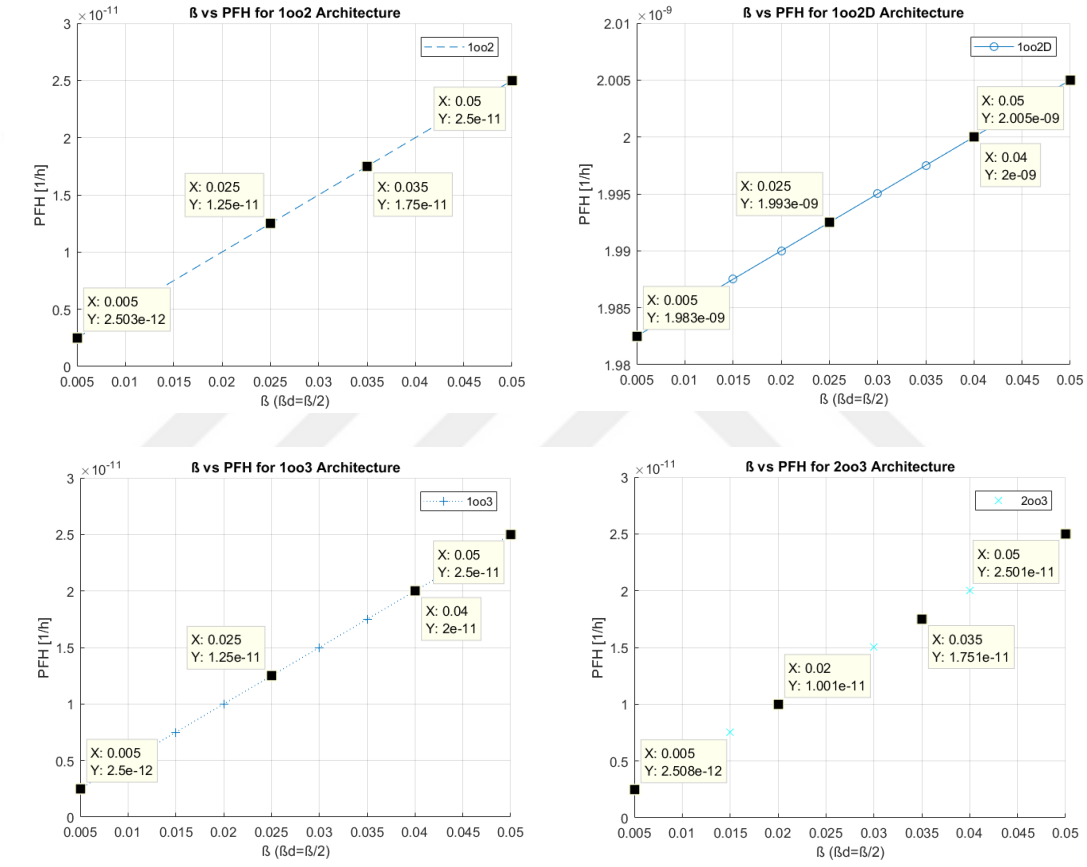


Figure 5.9 The influence of ß for different architectures

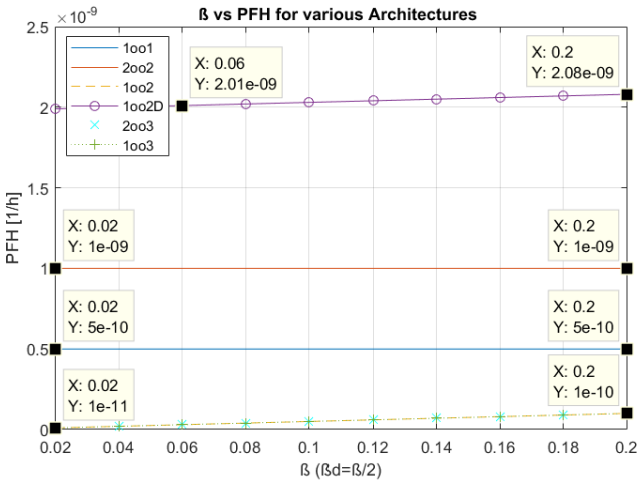


Figure 5.10 Comparison of the influence of ß for different architectures

If K is updated from 0.98 to 0.9999, then the influence of ß on PFH increases as shown below:

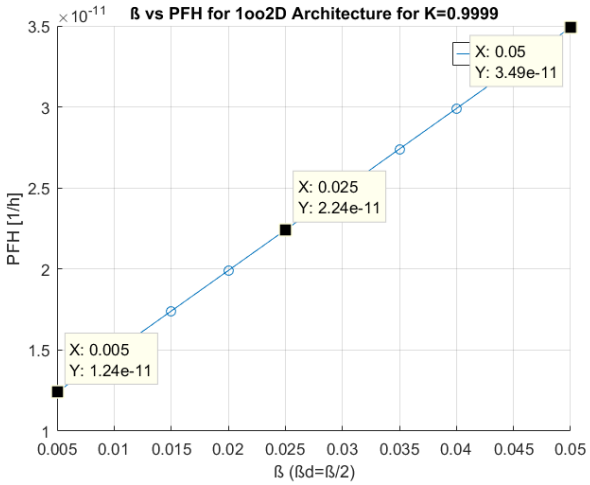


Figure 5.11 The influence of ß for 1oo2D when K is 0.9999.

Deduction:

To make an exhaustive effort for decreasing the ß ten times affects 1oo2 almost linearly such that ten times better PFH can be reached. Similar is also valid for 2oo3 and 1oo3. The effect of ß on 1oo2D is negligible.

B. Influence of $ß_d$

Table 5.7. Parameters used for the analysis of $ß_d$ effect (for ß= 0.02)

λ	$λ_s$	$λ_{sd}$	$λ_d$	$λ_{dd}$	$λ_{du}$	DC	SFF	ß	$ß_d$ (PoI)	MTTR	MRT	K	T1
1E-07	5E-08	4,95E-08	5E-08	4,95E-08	5E-10	0.99	0.995	0.02	0.002<ßd<0.02	8	8	0.98	1

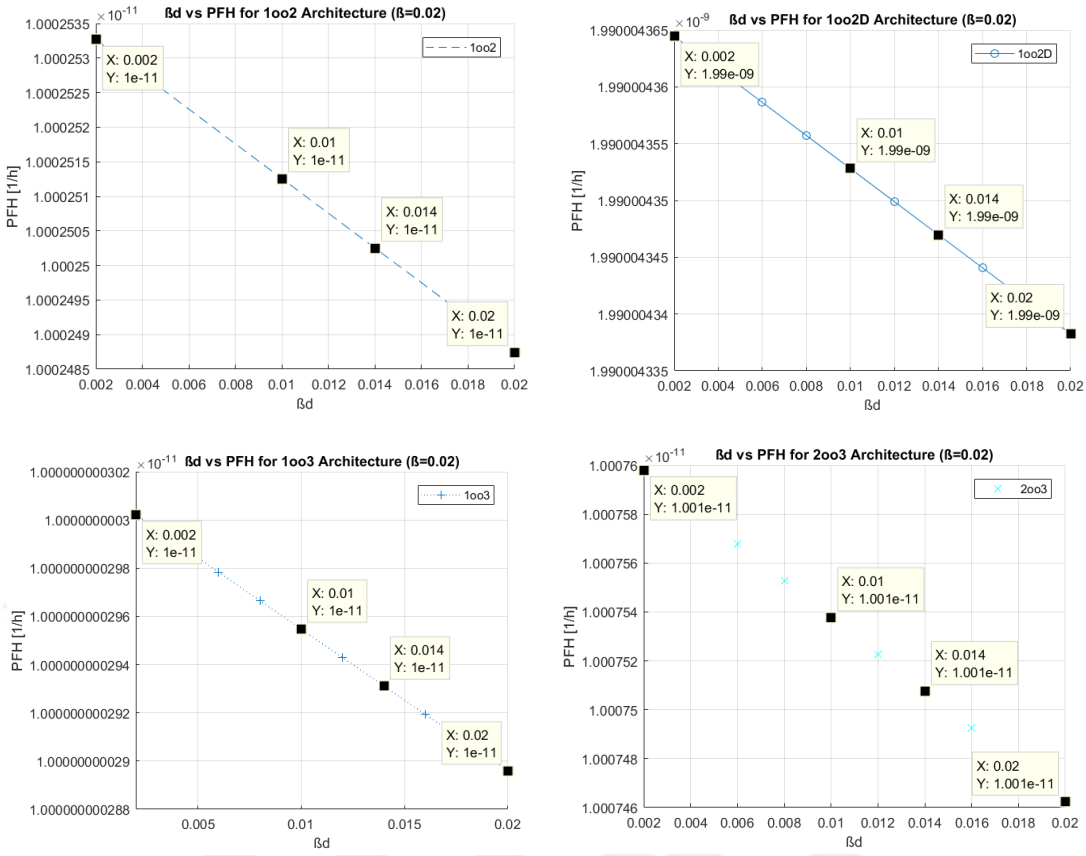


Figure 5.12 The influence of ß for different architectures for ß of 2%

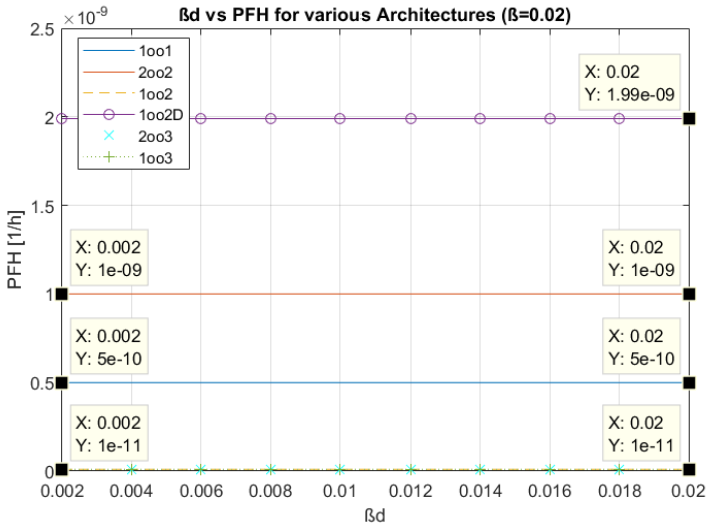


Figure 5.13 Comparison of the influence of $ß_d$ for different architectures for ß of 2%

This part sows whether the effect of $ß_d$ changes if ß value change.

Table 5.8 Parameters used for the analysis of $ß_d$ effect (for ß= 0. 2)

λ	λ_s	λ_{sd}	λ_d	λ_{dd}	λ_{du}	DC	SFF	ß	$ß_d$ (PoI)	MTTR	MRT	K	T1
1E-07	5E-08	4,95E-08	5E-08	4,95E-08	5E-10	0.99	0.995	0.2	0.02<ßd<0.2	8	8	0.98	1

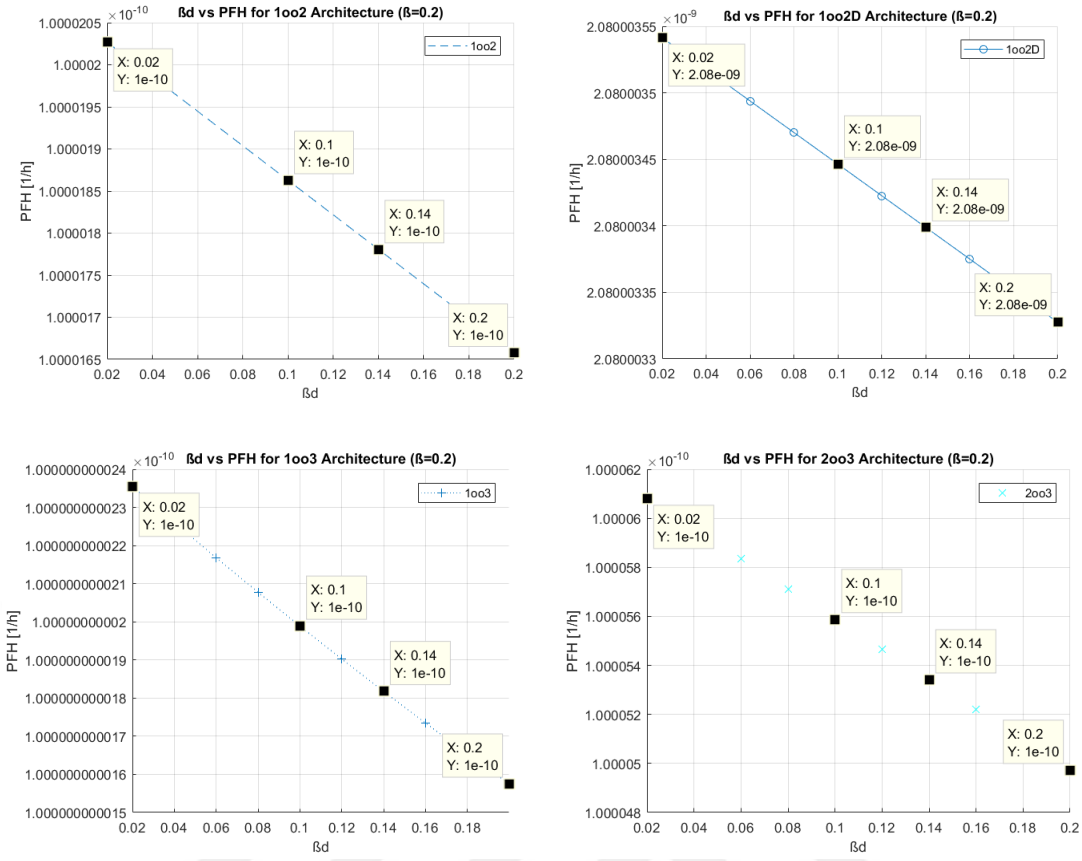


Figure 5.14 The influence of $ß_d$ for different architectures for ß of 20%

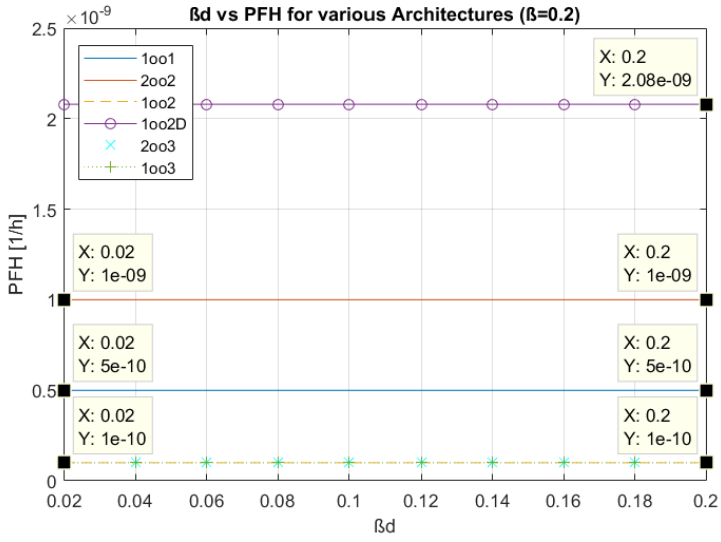


Figure 5.15 Comparison of the influence of $ß_d$ for different architectures for ß of 20%

Deduction:

It is found that an increase in the $ß_d$ does almost not affect the PFH which is very strange, because lots of effort is paid for increasing the diagnostics and the return of this endeavor

is almost zero. As something wrong might be with this formula, it will be researched in next studies.

5.3.3 The Influence of DC

Table 5.9 Parameters used for the analysis of DC

λ	λ_s	λ_{sd}	λ_d	λ_{dd}	λ_{du}	DC (PoI)	SFF	ß	$ß_d$	MTTR	MRT	K	T1
1E-07	5E-08	4,95E-08	5E-08	v	v	0<DC<0.99	v	0.02	0.01	8	8	0.98	1

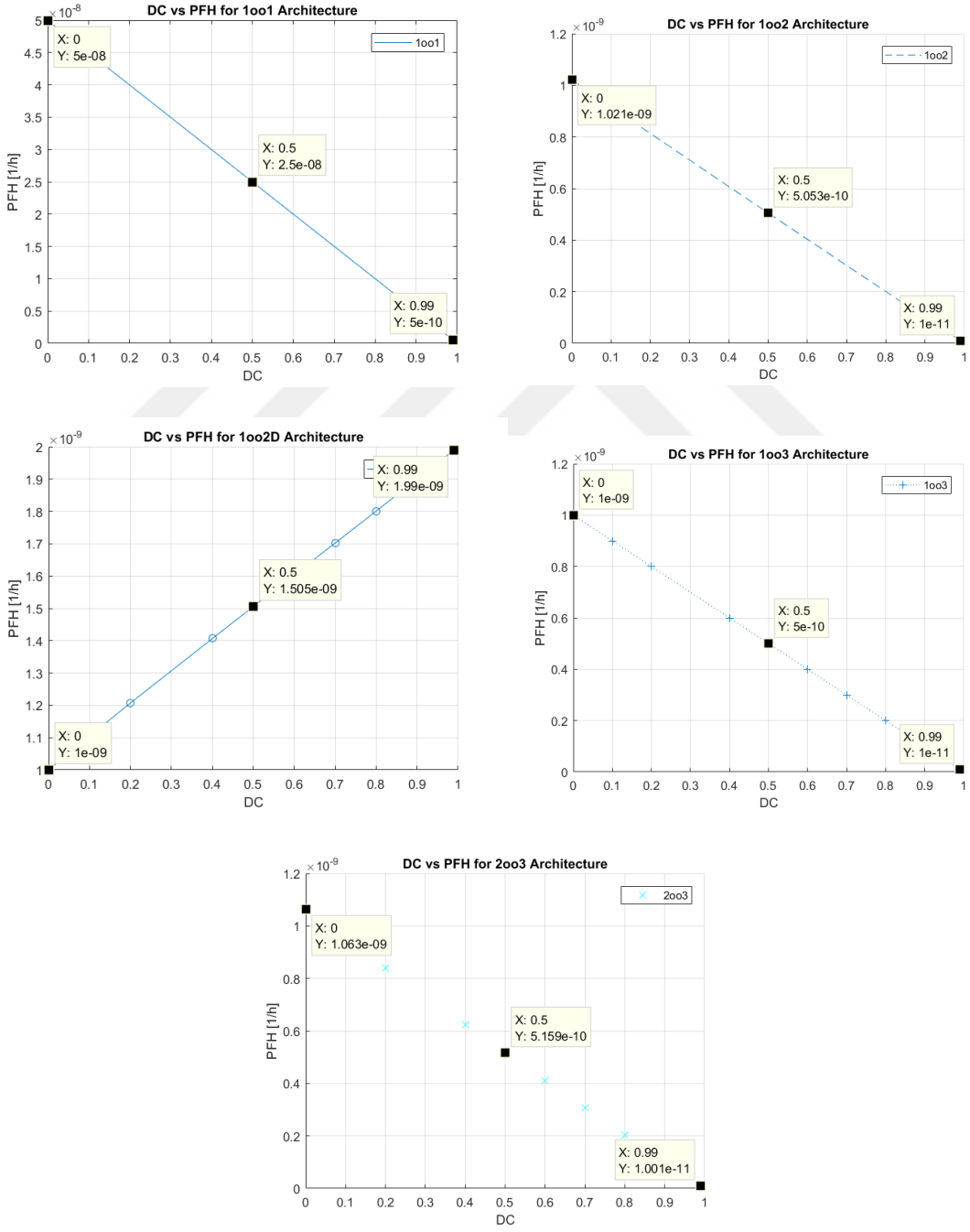


Figure 5.16 The influence of DC for different architectures

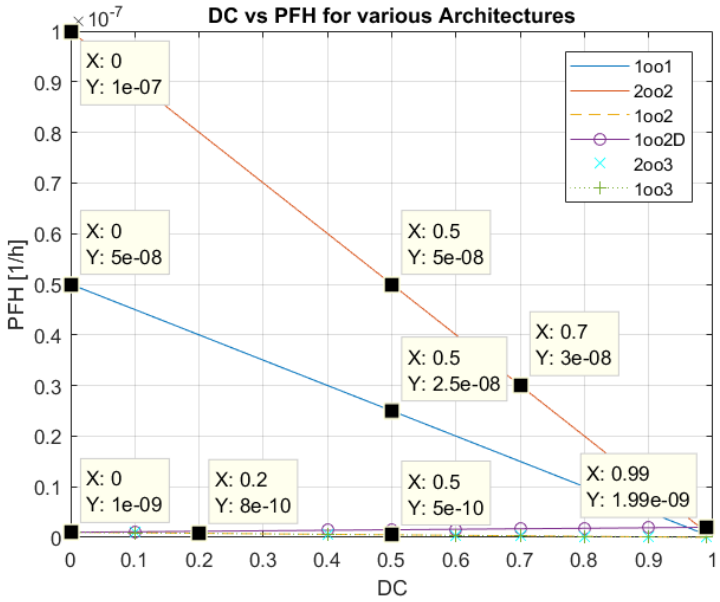


Figure 5.17 Comparison of the influence of DC for different architectures

Deduction:

An increase of DC causes a decrease in the PFH for all architectures except 1oo2D. For 1oo2 and 2oo3, in case the DC is doubled from 0.5 to 0.99, then the PFH falls by half. For 1oo2D, it is found very strange that there is a positive correlation between PFH and DC such that if DC goes up from 0.5 to 0.99, the PFH increases about 33%. The author believes that this is an issue to be considered again in the formulations.

5.3.4 The Influence of MTTR

Table 5.10 Parameters used for the analysis of MTTR

λ	λ_s	λ_{sd}	λ_d	λ_{dd}	λ_{du}	DC	SFF	ß	$ß_d$	MTTR (PoI)	MRT	K	T1
1E-07	5E-08	4,95E-08	5E-08	4,95E-08	5,00E-10	0.99	0.995	0.02	0.01	0<MTTR<1000	8	0.98	1

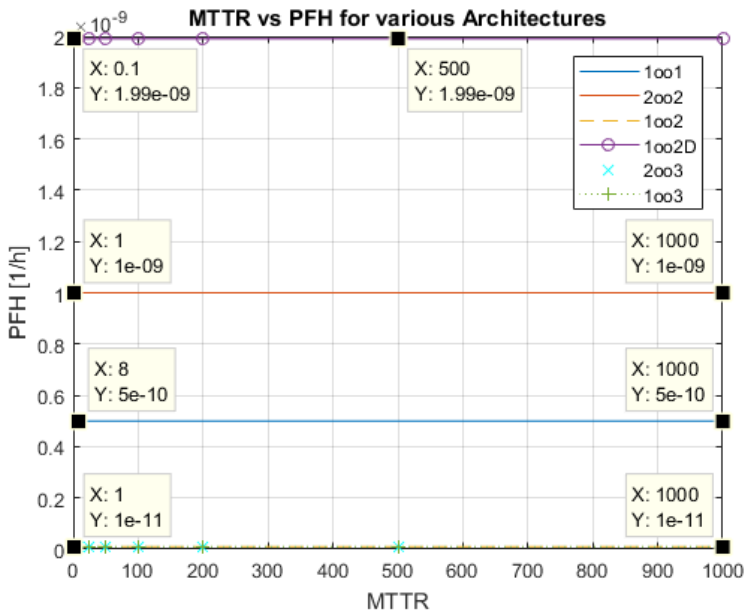


Figure 5.18 Comparison of the influence of DC for different architectures

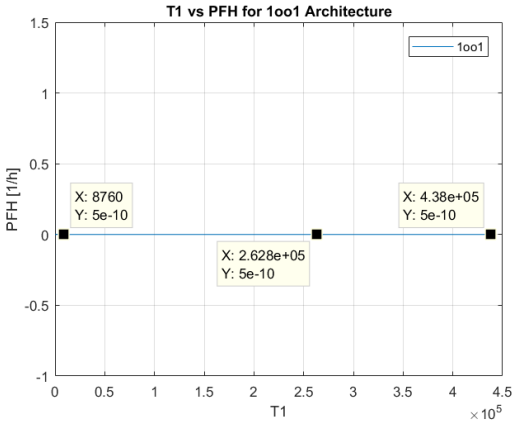
Deduction:

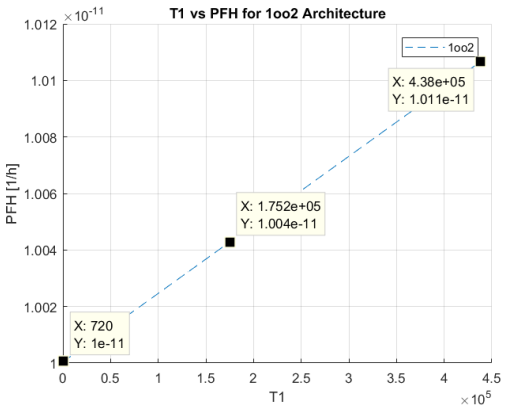
MTTR is usually selected not more than 8 hours. In this simulation, as the affect during the 8 hours was found as none, the time range is changed up to1000 hours. Even in this case, for all architecture, the MTTR has almost no impact on the PFH.

5.3.5 The Influence of T1

Table 5.11 Parameters used for the analysis of K

λ	λ_s	λ_{sd}	λ_{sl}	λ_{dd}	λ_{du}	DC	SFF	ß	$ß_d$	MTTR	MRT	K	T1 (PoI)
1E-07	5E-08	4,95E-08	5E-08	4,95E-08	5,00E-10	0.99	0.995	0.02	0.01	8	8	0.98	1/(365.24)<T1<50





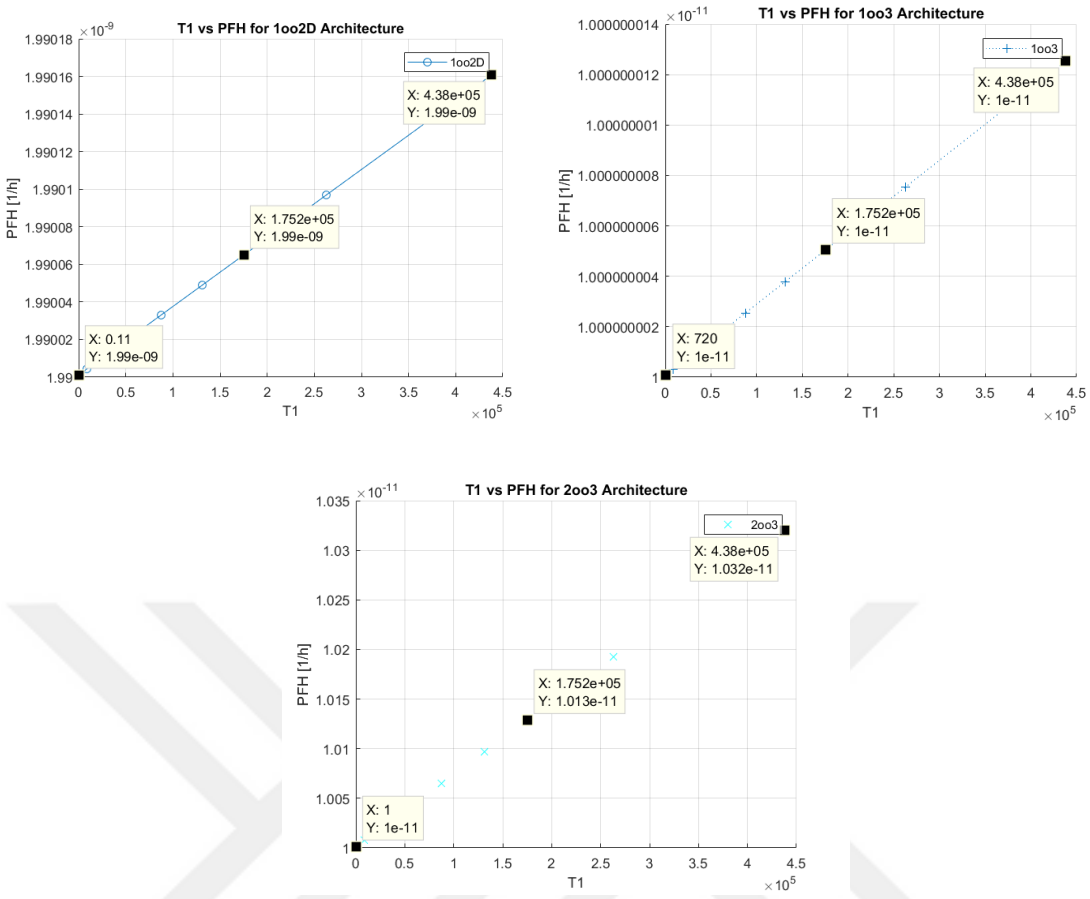


Figure 5.19 The influence of T_1 for different architectures

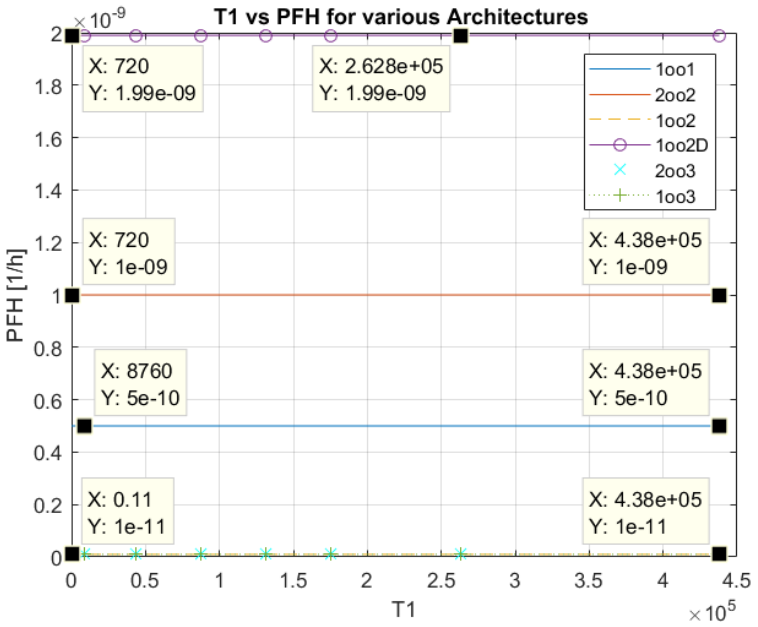


Figure 5.20 Comparison of the influence of T_1 for different architectures

Deduction:

T1 can be selected from one day to many years according to the type of the unit. For vital computers it is usually the life time such as 20 years. However, for both very short and very long time, the T1 does almost not affect PFH.

5.3.6 The Influence of K

Table 5.12 Parameters used for the analysis of K

λ	λ_s	λ_{sd}	λ_d	λ_{dd}	λ_{du}	DC	SFF	ß	$ß_d$	MTTR	MRT	K (PoI)	T1
1E-07	5E-08	4,95E-08	5E-08	4,95E-08	5,00E-10	0.99	0.995	0.02	0.01	8	8	0.1<K<0.999	1

IEC 61508-6 [2], B.3.2.2.4, notes that the parameter K will need to be determined by an FMEA. If K is variated from 0.98 to 1 (practically not possible, but for the purpose of analyzing the theoretical limit), its influence can be noticed more clearly.

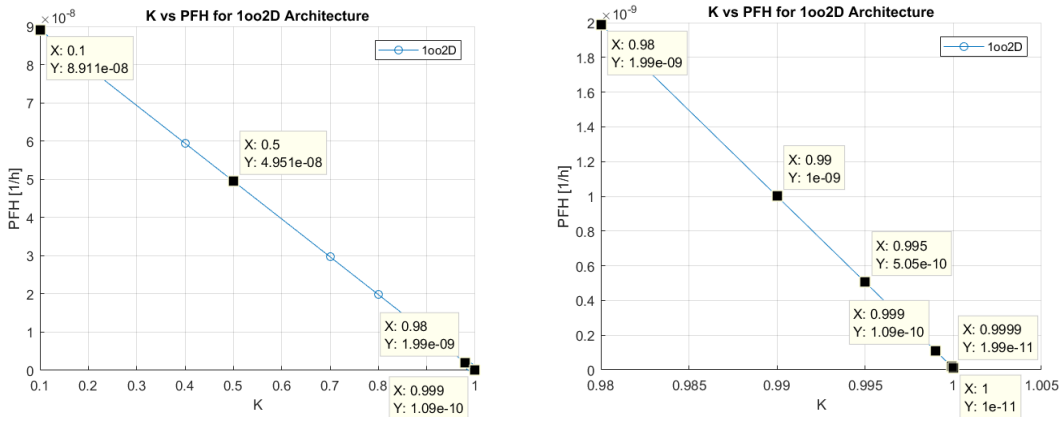


Figure 5.21 Comparison of the influence of T_1 for different architectures

Deduction:

The parameter K has an important impact on the PFH. If it is increased from 0.95 to 0.99, five times better PFH can be obtained. And if it changes from 0.98 to 0.99, then two times, if from 0.98 to 0.999, then twenty times and if from 0.98 to 0.9999, then hundred times lower PFH could be obtained.

5.3.7 Route Map with regards to the Parameters

1. Decrease λ as much as possible - for each potential architecture. A linear relationship with a slope 1 is valid.
2. Decrease common cause factor, namely ß as much as possible - for 1oo2, 1oo3, 2oo3 architectures, approximately ten times better ß results in ten times better

PFH; however the effect for 1oo2D is very limited such that ten times better ß results in two times better PFH.

3. The effect of detecting the common cause failures, namely $ß_d$ has almost no effect on PFH for any architecture, hence do not spend much effort to detect common cause failures.
4. Increase DC for all architectures except 1oo2D. For 1oo2 and 2oo3, in case the DC is doubled from 0.5 to 0.99, then the PFH falls by half. For 1oo2D, if DC goes up from 0.5 to 0.99, the PFH increases about 33%.
5. Do not perform much effort to decrease MTTR for the safety performance as it has almost no effect on PFH for any architecture.
6. Similar to the case with MTTR, do not perform much effort to decrease T1 for the safety performance as it has almost no effect on PFH for any architecture.
7. If 1oo2D is chosen, then increase K. If K changes from 0.98 to 0.9999, then hundred times better PFH could be resulted.

Note that these clauses are valid in case ß factor is used. If this is not the case, other simulations are needed.

For decrease λ, following items can be performed:

- Reducing stress on parts
- Selecting higher quality parts
- Using multiplicative adjustment factor
- Using additive adjustment factor,
- Considering duty cycle,
- Using different reliability calculation handbooks like Telcordia[90], MIL-HNDBK- 217FN2 [91], 217 Plus [92] etc. and choose best,

There are differences between results of various methodologies because of assumptions and data they use. While the selection of the handbook is usually given in the tender specifications, the table below shows how different the results can be seemed when using different handbooks. In safety calculations, usually no handbook is asked by the customers. This means that in case the reliability is calculated by using the best model resulting the lowest λ value, the safety calculations will directly be affected in the same way as shown in the previous section with the simulations.

Table 5.13 Failure rate comparison in /million hours] of different handbooks for a board [92]

Environment	Ground Benign				Ground Fixed			
Temperature	10 Deg. C		70 Deg. C		10 Deg. C		70 Deg. C	
Stress	10%	50%	10%	50%	10%	50%	10%	50%
ALCATEL	6.59	10.18	13.30	19.89	22.08	29.79	32.51	47.27
Bellcore Issue 4	5.72	7.09	31.64	35.43	8.56	10.63	47.46	53.14
Bellcore Issue 5	8.47	9.25	134.45	137.85	16.94	18.49	268.90	275.70
British Telecom HDR4	6.72	6.72	6.72	6.72	9.84	9.84	9.84	9.84
British Telecom HDR5	2.59	2.59	2.59	2.59	2.59	2.59	2.59	2.59
MIL-HDBK-217 E Notice 1	10.92	20.20	94.37	111.36	36.38	56.04	128.98	165.91
MIL-HDBK-217 F Notice 1	9.32	18.38	20.15	35.40	28.31	48.78	45.44	79.46
MIL-HDBK-217 F Notice 2	6.41	9.83	18.31	26.76	24.74	40.15	73.63	119.21
217Plus Version 2.0		0.28		4.89		0.51		6.04
RIAC data		3.3						

Main reliability models are described in the next section.

CHAPTER 6

RELIABLITY CALCULATION

To calculate safety parameters, firstly reliability calculations should be done. Therefore, this section firstly gives some historical information and then explains reliability calculations before performing the reliability calculations.

6.1 History

The importance of reliability is noticed several decades ago. In [93], it is stated that the first predictive reliability models appeared while Wernher von Braun, one of the most famous rocket scientists, was working on the V1 missile in Germany when the rockets were found to be having poor reliability for which the team worked based on the principle that a chain is no stronger than its weakest link. It continues that failures were observed with not only the weakest part but also with remaining components. The team later consulted a mathematician, Eric Pernchka, who came up with a concept which says 'if the survival probability of an element is 1/x, survival probability of system of n such similar components will be $1/x^n$, which forms the basis for the reliability of series system [94]. The concepts of reliability developed slowly until World War II. During the War, over 50 % of the defense equipment was found to be failed state in storage; it was due to electronic system failure and in particular because of vacuum tube failures.

First pioneers showed up in 1950s where Reliability was born as a branch of engineering in USA. In 1952 the Department of Defense (DOD) and the American electronic industry created the Advisory Group on Reliability of Electronic Equipment (AGREE) of which report suggested modularity in design, reliability growth and demonstration tests to improve reliability and also a classical definition of reliability [93]. This period witnessed the first conference on 'quality control and reliability' and the first journal in the area 'IEEE Transaction on Reliability' by the Institute of Electrical and Electronics Engineers

[93]. Today, this science continuous to develop with updates to modelling and math behind the models. This is also an inevitable need science there arise new components, the models of components can change or better components are in production lines, hence the reliability science shall be adapted to this development.

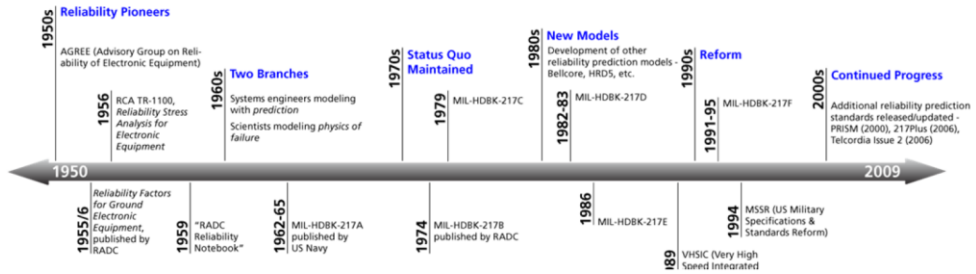


Figure 6.1 Historical development of reliability prediction analyses [95]

6.2 Prediction Methodology, Handbooks and Modelling Considerations

For reliability prediction, following procedure can be applied in a systematic way:

- System definition,
- Identification of the model purpose,
- Handbook selection for prediction,
- Subsystems definition,
- Assemblies definition,
- Components definition,
- Calculation,
- Results generation,
- Reviewing and analyzing the results,
- Collect data from the field,
- Updating results according to the data from the field.

6.2.1 Handbooks

In today's reliability world, there exist several handbooks. The calculation model is usually selected based on the parts in the system and customer/system requirements. For example, Telcordia is usually accepted in telecommunication industry while MIL-HDBK-217 FN2 is widely used in military projects. The following table derived from [96] notes the most significant characteristic features of the handbooks used for reliability modelling.

Table 6.1 Handbook Characteristics [96]

Model	**Description**
MIL-HDBK-217	MIL-HDBK-217 models are based on various publications of MIL-HDBK-217, Military Reliability Prediction of Electronic Equipment. This standard, the original for reliability predictions, provides component models for nearly every conceivable type of electronic device. Accepted and known worldwide, it is used by commercial companies and the defense industry. MIL-HDBK-217 models support the ability to perform parts count and parts stress predictions. Both F Notice 1 and 2 are supported. Information about entering part parameters for this model appears in "MIL-HDBK-217 Part Parameters" on page 10-322.
217Plus	The 217Plus model is based on RIAC-HDBK-217Plus, Handbook of 217Plus Reliability Prediction Models. This standard was published in May 2006 by the Reliability Information Analysis Center (RIAC), a Department of Defense Information Analysis Center sponsored by the Defense Technical Information This model supersedes the PRISM model. It now incorporates all of the major component categories found in MIL-HDBK-217 models and supports both parts count and parts stress predictions. Information about entering part parameters for this model appears in "217Plus Part Parameters" on page 10-514.
Telcordia	Telcordia models are based on various issues of the Telcordia document, Reliability Prediction Procedure for Electronic Equipment, Technical Reference SR-332. Prior issues, known as Bellcore models, were developed by AT&T Bell Lab, who modified MIL-HDBK-217 models to better reflect the failure rates that AT&T

Table 6.1 Handbook Characteristics [96] (cont'd)

Telcordia (cont'd)	Bell Lab equipment was experiencing in the field. Like MIL-HDBK-217 models, these models include the ability to perform parts count or parts stress predictions. The Prediction module supports Telcordia Issues 1, 2, and 3 as well as Bellcore Issues 4, 5, and 6. Unless a significant difference exists between Telcordia and Bellcore models, Telcordia is used generically to refer to all models. These models support various calculation methods that take into account burn-in, laboratory, and/or field data. For more information, see "Telcordia Calculation Methods" on page 10-25. Because of the popularity of these calculation methods with commercial companies, the Prediction module supports using them with all but a FIDES, IEC TR 62380, or RDF 2000 model. Information about entering part parameters for Telcordia and prior Bellcore models appears in "Telcordia Part Parameters" on page 10-367. NOTE: Telcordia Issue 3, released in September 2010, replaces Telcordia Issue 2, released in September 2006. Both of these issues include support of a user-definable upper confidence interval, calculation of a mean failure rate and standard deviation failure rate for each part, and new part categories and subcategories. For information about fields specific to these last two issues, see "Telcordia Issue 3 and Issue 2 Fields" on page 10-381.
IEC TR 62380 RDF 2000	The IEC TR 62380 model is based on the IEC TR 62380 standard, Reliability Data Handbook - Universal Model for Reliability Prediction of Electronic Components, PCBs, and Equipment Reliability Data Handbook – Universal Model for Reliability Prediction of Electronic Components, PCBs, and Equipment, published by the International Electrotechnical Commission (IEC). This model has only a few numeric differences from the earlier RDF 2000 model, which is based on the UTE C 80-810 standard published by the Union Technique de l'Electricite et de la Communication. Both models use cycling profiles and their applicable phases as a

Table 6.1 Handbook Characteristics [96] (cont'd)

IEC TR 62380 RDF 2000 (cont'd)	basis for failure rate calculations. These models, which replaced the earlier CNET 93 model, cannot be mixed with other models or use methods supplied by other models. The IEC TR 62380 or RDF 2000 model can only be selected for the top-most assembly. In this case, any model override selections that might exist for lower-level assemblies are ignored. Information about entering part parameters for these models appears in "IEC TR 62380/RDF 2000 Part Parameters" on page 10-429.
Mechanical	The Mechanical model is based on the Handbook of Reliability Prediction Procedures for Mechanical Equipment, Document No. NSWC-98/LE1. Developed under the direction of the United States Navy, this model supports failure rate calculations for various types of mechanical devices, including springs, bearings, seals, motors, brakes, clutches, and many more. This standard is the only one of its kind. For more information, see "Mechanical Model" on page 10-545.
NPRD and EPRD	While NPRD and EPRD Libraries are not calculation models, they supply failure rates for thousands of parts. If the model you have selected does not support a failure rate calculation for a particular part, you can search the NPRD and EPRD Libraries to see if they contain failure rates for this part. For more information, see "NPRD and EPRD Libraries" on page 10-45.
PRISM	The PRISM model is based on the PRISM methodology, which was released in March 2000. It deviates from traditional reliability prediction methodologies by allowing you to factor in component, assembly, and system test data. It also addresses system level design and manufacturing processes to refine the system prediction. In addition, component and system assessment models address not only operational aspects but also non-operational and/or dormant aspects of a part or system. Because its component models are based on

Table 6.1 Handbook Characteristics [96] (cont'd)

PRISM (cont'd)	failure rate data recorded in failures per million calendar hours, the failure rate units for this model uses failures per million calendar hours rather than failures per million operating hours. Information about entering part parameters for this model appears in "PRISM Part Parameters" on page 10-522.
Siemens SN 29500 v1	The Siemens SN 29500 model is based on IEC 61709, Electronic Components - Reliability - Reference Conditions for Failure Rates and Stress Models for Conversion. It provides frequently updated failure rate data at reference conditions as well as parts count and parts stress predictions. The reference conditions adopted by this model are typical for the majority of applications of components in systems. If operating conditions differ significantly from reference conditions, this model supports converting the failure rate data at the reference conditions to actual operating conditions. Information about entering part parameters for this model appears in "Siemens Part Parameters" on page 10-528.

6.2.2 Reliability Modelling Considerations

When analysed the models, it can be concluded that the calculations are based on specified considerations. These could be condensed as quality, environment, types, life data availability and stress elements. As these are important parameters for the safety calculations, too which is the aim of this study, these factors are detailed in below.

i. Quality Levels

Quality level is a measure of the manufacturer's production and test procedures as well as the quality controls in place and the scales for quality levels vary significantly from one model to another [45].

ii. Environment

The environment is a very important parameter for the calculations. However, the environments are not same at each handbook. Moreover, some handbooks like IEC TR 62380 or Siemens do not use environments but rather mission phase and/or cycling

information. The environment factor is also a criteria to select the handbook such that if there is a need for a special environment which is not supported by a handbook, then it is inevitable to switch to another handbook. A concrete example can be given for the naval environment which is not supported by Telcordia. Then, it is not convenient to use Telcordia for a naval system. The following table provides the environments available for MIL-HDBK-217, Telcordia, and Bellcore. Next, environments for 217 Plus Parts Stress and PRISM are given.

Table 6.2 Environments for MIL-HDBK-217, Telcordia, and Bellcore

Airborne	Ground	Naval	Other
• AIC, AC – Airborne, Inhabit Cargo, Commercial • AIF – Airborne, Inhabit Fighter • ARW – Airborne, Rotary Winged • AUC – Airborne, Uninhab Cargo • AUF – Airborne, Uninhab Fighter	• GB, GC – Ground, Benign, Controlled • GF, CU – Ground, Fixed, Uncontrolled • GF1, Ground Fixed, Controlled • GM – Ground Mobile • GM2 – Mobile Acutely • GMS – Ground Missile Silo	• NS – Naval Sheltered • NS2 – Naval Sheltered, Common • NSB – Naval Submarine • NU – Naval Unsheltered	• MF – Missile Flight* • ML – Missile Launch • MP – Mobile Shoulder • SF, SC – Space Flight, Commercial

Table 6.3 Environments for 217 Plus Parts Stress and PRISM

Airborne	Ground	Naval
• A – Airborne • AF – Airborne, Fixed Wing • AFI – Airborne, Fixed Wing, Inhabited • AFU – Airborne, Fixed Wing, Uninhabited • AM – Airborne, Missile • AMF – Airborne, Missile, Flight • AML – Airborne, Missile, Launch	• G – Ground • GM – Ground, Mobile • GMH – Ground, Mobile, Heavy Wheeled • GMH,CM – Ground, Mobile, Heavy Wheeled, Chassis Mounted • GMH,EC – Ground, Mobile Heavy Wheeled, Engine Compartment • GMH–EM Ground, Mobile, Heavy Wheeled, Engine Mounted	• Naval • NSB, Naval, Shipboard • NSC, S – Naval, Shipboard, Sheltered • NSC, U – Naval, Shipboard, Unsheltered

Table 6.3 Environments for 217 Plus Parts Stress and PRISM (cont'd)

• AR – Airborne, Rotary Wing • ARI – Airborne, Rotary Wing, Inhabited • ARU – Airborne, Rotary Wing, Uninhabited • AS – Airborne, Space	• GMH,IPC – Ground, Mobile, Wheeled • Instrument Panel Closed • GMH,IPO – Ground, Mobile, Heavy Wheeled, • Instrument Panel Open • GMH,ITRU – Ground, Mobile, Heavy Wheeled, Trunk • GML – Ground, Mobile, Light Wheeled • GML,CM – Ground, Mobile, Light Wheeled, Chassis Mounted • GML–EC – Ground, Mobile, Light Wheeled, Engine Compartment • GML–EM – Ground, Mobile, Light Wheeled, Engine Mounted • GML–IPC – Ground, Mobile, Light Wheeled, Instrument Panel Closed • GML,IPO – Ground, Mobile, Light Wheeled, Instrument Panel Open • GML,TRU – Ground, Mobile, Light Wheeled, Trunk • GMP – Ground, Man Pack • GMT – Ground, Mobile, Tracked • GS – Ground, Stationary • GSI – Ground, Stationary, Indoors • GSO – Ground, Stationary, Outdoors	• NSM – Naval, Submarine

iii. Tpyes

The type of the part is a criteria for all the models as it influences the required parameters for the calculation. For instance, the technology type, quality level, number of gates, pins, package type and years in production are asked when modelling with MIL-HDBK-217 FN2 parts stress for IC/Logic, CGA or ASIC. And Telcordia Issue 3 asks quality level, technology type and number of gates for the same category. Another issue to be considered is that some element types are not supported by one handbook while it can be

supported in another one. For instance, laser is supported by MIL-HDBK-217 FN2, but not in Telcordia Issue 3.

iv. Life Data Availability

Field data or data received in laboratory tests are enabling to adjust the predicted failure rates. This is not available for some methods like MIL-HDBK-217, while some like 217Plus support these adjustments.

v. Stress

There are two ways two calculate reliability prediction, one is parts count, and the other is parts stress. While the former is used at early phases, the latter is used later when the design is maturated so that there are more available data for the components such that more precise calculations can be performed. Parts count method uses generic failure rates and typical stress levels. On the other hand, electrical and temperature stresses shall be specified exactly when using parts stress method. The method is also used to update the design according to the results, for instance the duty cycle can be updated for some components to lessen the stress.

vi. Failure Rate Adjustments

The λ that a system has in the field might be better or worse than the base failure rate, which is the resulted value of the calculation. Multiplicative and additive adjustment factors can be used with any model as provided on 10-23 of [96]. However, according to the author of this thesis, the multiplicative factors can be misused therefore, they are somehow questionable. Process grades, Bayesian analysis, and predecessor analysis are enabled in Telcordia calculation methods, and 217Plus and PRISM can be used for adjustments to the base failure rates. It is also possible to re-use the rates calculated by a handbook for the calculation with another book. It is mentioned in [96] that Telcordia calculation methods can be used for burn-in, laboratory, and/or field data to adjust base failure rates calculated by a MIL-HDBK-217 model.

6.2.3 Calculation with Selected Handbooks

In this section, an introductive information is provided to explain the basic calculation methods. The whole model information and the other models and their information are to be found in the relevant handbook.

Taking into account the effect of using different handbooks on the λ which affects directly the PFH, two different handbooks are selected in this thesis so that the effect of the handbook selection can be seen concretely and making possible to reach low PFH values of safety functions for a system which is the main aim of this study. The selected handbooks are MIL-HDBK-217 FN2 and 217 Plus. MIL-HDBK-217 is selected since it is the most accepted and widely method around the technical world. Secondly, 217 Plus is selected since 217Plus is becoming more and more popular in the last years since the methodology is developed by the RIAC to fill the void left after MIL-HDBK-217 was no longer scheduled to be updated and it is chosen for several civil projects.

A. Calculation Description for MIL-HDBK-217 FN2

MIL-HDBK-217 FN2 [91] explains the equation for a typical example of the type of model used for most other part types as one for discrete semiconductors:

$\lambda_p = \lambda_b \, \pi_T \, \pi_A \, \pi_R \, \pi_S \, \pi_C \, \pi_Q \, \pi_E$

λ_p is the part failure rate,

λ_b is the base failure rate usually expressed by a model relating the influence of electrical and temperature stresses on the part,

π_E = and the other π factors modify the base failure rate for the category of environmental application and other parameters that affect the part reliability

π_E and π_Q factors are used in most all models and other π factors apply only to specific models. The applicability of π factors is identified in each section of the handbook. Below, a calculation model is described.

Calculation Model for Microcircuits, Gate/Logic Arrays and Microprocessor

A description is provided after the classification as below:

5.1 MICROCIRCUITS, GATE/LOGIC ARRAYS AND MICROPROCESSORS

DESCRIPTION
1. Bipolar Devices, Digital and Linear Gate/Logic Arrays
2. MOS Devices, Digital and Linear Gate/Logic Arrays
3. Field Programmable Logic Array (PLA) and Programmable Array Logic (PAL)
4. Microprocessors

The equation is given as following:

$\lambda_p : (C_1\pi_T + C_2\pi_E)\pi_Q \, \pi_L$ [fpmh]

where:

C_1 : Die Complexity Failure Rate

π_T : Temperature Factor

C_2 : Package Failure Rate

π_E : Environment Factor

π_Q : Quality Factor

π_L : Learning Factor

If the component is “Digital and Linear Gate/Logic Array”, then “the Die Complexity Failure Rate – C_I” is given as follows:

Table 6.4 Bipolar, digital and linear gate/logic array die complexity failure rate-C_1

Digital		Linear		PLA/PAL	
No. Gates	C_1	No. Transistors	C_1	No. Gates	C_1
1 to 100	.0025	1 to 100	.010	Up to 200	.010
101 to 1,000	.0050	101 to 300	.020	201 to 1,000	.021
1,001 to 3,000	.010	301 to 1,000	.040	1,001 to 5,000	.042
3,001 to 10,000	.020	1,001 to 10,000	.060		
10,001 to 30,000	.040				
30,001 to 60,000	.080				

If the type is not “Digital and Linear Gate/Logic Array”, then other tables provided in the book are to be taken into account. For the other parameters, another the table below is given as

Table 6.5 All other model parameters

All Other Model Parameters

Parameter	Refer to
π_T	Section 5.8
C_2	Section 5.9
π_E, π_Q, π_L	Section 5.10

For instance, for π_T the section 5.8 provides the following table:

Table 6.6 Temperature factor for all microcircuits π_T

	TTL, STTL, ASTTL, CML, HTTL, FTTL, DTL, ECL	BiCMOS, LSTTL, LTTL, ALSTTL	IIL, ISL	Digital MOS, VHSIC CMOS	Linear (Bipolar & MOS)	Memories (Bipolar & MOS), MNOS	GaAs MMIC	GaAs Digital
Ea(eV) → T_J (°C)	.4	.5	.6	.35	.65	.6	1.5	1.4
25	.10	.10	.10	.10	.10	.10	3.20E-09	1.00E-08
30	.13	.14	.15	.13	.15	.15	8.40E-09	2.50E-08
35	.17	.19	.21	.16	.23	.21	2.10E-08	5.90E-08
40	.21	.25	.31	.19	.34	.31	5.20E-08	1.40E-07
45	.27	.34	.43	.24	.49	.43	1.30E-07	3.10E-07
50	.33	.45	.61	.29	.71	.61	2.90E-07	6.80E-07
55	.42	.59	.85	.35	1.0	.85	6.70E-07	1.50E-06
60	.51	.77	1.2	.42	1.4	1.2	1.50E-06	3.10E-06
65	.63	1.0	1.6	.50	2.0	1.6	3.20E-06	6.40E-06
70	.77	1.3	2.1	.60	2.8	2.1	6.80E-06	1.30E-05
75	.94	1.6	2.9	.71	3.8	2.9	1.40E-05	2.50E-05
80	1.1	2.1	3.8	.84	5.2	3.8	2.90E-05	4.90E-05
85	1.4	2.6	5.0	.98	7.0	5.0	5.70E-05	9.40E-05
90	1.6	3.3	6.6	1.1	9.3	6.6	1.10E-04	1.70E-04
95	1.9	4.1	8.5	1.3	12	8.5	2.10E-04	3.20E-04
100	2.3	5.0	11	1.5	16	11	4.00E-04	5.80E-04
105	2.7	6.2	14	1.8	21	14	7.50E-04	1.00E-03
110	3.2	7.5	18	2.1	28	18	1.40E-03	1.80E-03
115	3.7	9.2	23	2.4	35	23	2.40E-03	3.10E-03
120	4.3	11	28	2.7	45	28	4.30E-03	5.30E-03
125	5	13	35	3.1	58	35	7.50E-03	9.00E-03
130	5.8	16	44	3.5	73	44	1.30E-02	1.50E-02
135	6.7	19	54	3.9	92	54	2.20E-02	2.40E-02
140	7.7	23	67	4.4	120	67	3.70E-02	3.90E-02
145	8.8	27	82	5.0	140	82	6.10E-02	6.30E-02
150	10	32	100	5.6	180	100	1.00E-01	1.00E-01
155	11	37	120	6.3	220	120	1.60E-01	1.60E-01
160	13	43	150	7.0	270	150	2.60E-01	2.40E-01
165	15	50	180	7.8	330	180	4.10E-01	3.70E-01
170	16	59	210	8.7	400	210	6.40E-01	5.70E-01
175	18	68	250	9.6	480	250	9.90E-01	8.50E-01

Table 6.6 Temperature factor for all microcircuits π_T (cont'd)

$$\pi_T = .1 \exp\left(\frac{-Ea}{8.617 \times 10^{-5}}\left(\frac{1}{T_J + 273} - \frac{1}{298}\right)\right)$$ Silicon Devices

$$\pi_T = .1 \exp\left(\frac{-Ea}{8.617 \times 10^{-5}}\left(\frac{1}{T_J + 273} - \frac{1}{423}\right)\right)$$ GaAs Devices

E_a = Effective Activation Energy (eV) (Shown Above)
T_J = Worse Case Junction Temperature (Silicon Devices) or Average Active Device Channel Temperature (GaAs Devices). See Section 5.11 (or Section 5.12 for Hybrids) for T_J Determination.

NOTES:
1. $T_J = T_C + P\theta_{JC}$
   T_C = Case Temperature (°C)
   P = Device Power Dissipation (W)
   θ_{JC} = Junction to Case Thermal Resistance (°C/W)
   θ_{JC} should be obtained from the device manufacturer, MIL-M-38510, or from the default values shown in Section 5.11 for the closest equivalent device.
2. Use Digital MOS column for HC, HCT, AC, ACT, C and FCT technologies.
3. Table entries should be considered valid only up to the rated temperature of the component under consideration.

B. Calculation Description for 217 Plus

In this section, 217 Plus calculation method is described utilizing its standard [92]. There are two primary elements to 217Plus, component reliability prediction models and system-level models. A system failure rate estimate is first made by using the component models to estimate the failure rate of each component. This is the traditional methodology used in many reliability predictions, and represents the reliability predictions, i.e., a reliability estimate that is made before empirical data or detailed assessments are available. This prediction is then modified in accordance with system level factors, which account for non-component, or system level, effects. This is an example of a reliability "assessment", in which the process and design factors are assessed. Finally, the prediction and assessment are combined with empirical data to form the reliability "estimate" of the product, which is the best estimate of reliability based on all analysis and data available to the analyst.

The basis for the 217Plus methodology is the component reliability models, which estimate a system's reliability by summing the predicted failure rates of the constituent components in the system. This estimate of the system reliability is further modified by the application of "System-Level" factors, called Process Grade Factors (PGF).

The premise of traditional methods of reliability predictions, such as MIL-HDBK-217, is that the failure rate of a product or system is primarily determined by the components comprising it. Historically, a significant number of failures also stem from non-component causes such as design deficiencies, manufacturing defects, inadequate requirements, induced failures, etc., that have not been explicitly addressed in prediction methods.

The data in Figure below, contains the nominal percentage of failures attributable to each of eight identified predominant failure causes based on data collected by the RIAC. The data in this figure represents nominal percentages. The actual percentages can vary significantly around these nominal values.

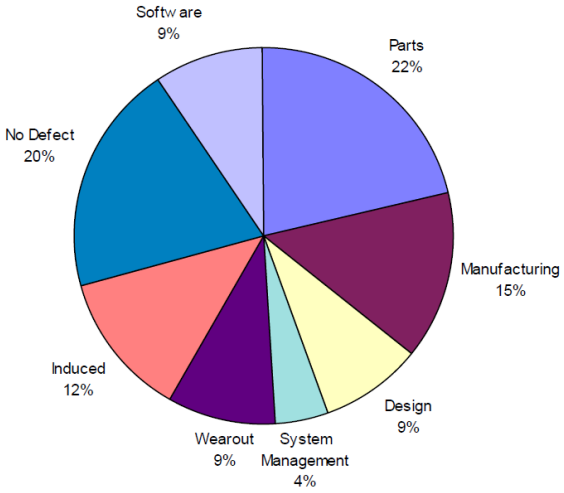


Figure 6.2 Failure Cause Distribution of Electronic Systems [92]

These process grades correspond to the degree to which actions have been taken to mitigate the occurrence of product or system failure due to these failure categories. Once the base estimate is modified with the process grades, the reliability estimate is further modified by empirical data taken throughout item development and testing. This modification is accomplished using Bayesian techniques that apply the appropriate weights for the different data elements. Advantages of the 217Plus methodology are that it uses all available information to form the best estimate of field reliability, it is tailorable, it has quantifiable confidence bounds, and it has sensitivity to the predominant product or system reliability drivers. The methodology represents a holistic approach to predicting, assessing and estimating product or system reliability by accounting for all primary factors that influence the inability of an item to perform its intended function. It factors in all available reliability data as it becomes available on the program. It, thus, integrates test and analysis data, which provides a better prediction foundation and a means for estimating variances from different reliability measures.

The fundamental 217Plus failure rate model for a system is as follows:

$$\lambda_p = \lambda_{IA} (\Pi_P + \Pi_D + \Pi_M + \Pi_S + \Pi_I + \Pi_N + \Pi_W) + \lambda_{SW} \quad (6.1)$$

The sum of the Pi-factors in the parenthesis represents the cumulative multiplier that accounts for all of the processes used in system development and sustainment. The sum of these values is normalized to unity for processes that are considered the mean of industry practices. The individual model factors are:

λ_p : Predicted failure rate of the product or system (in failures per million calendar hours)

λ_{IA} : Initial assessment of the failure rate based on component failure rate estimates

Π_P : Parts process multiplier

Π_D : Design process multiplier

Π_M : Manufacturing process multiplier

Π_S : System management process multiplier

Π_I : Induced process multiplier

Π_N : No-defect process multiplier

Π_W : Wearout process multiplier

λ_{SW} : Software failure rate prediction

Additional factors included in the model account for the effects of infant mortality, environment, and reliability growth. Since each of these factors does not influence all of the factors in the above equation, they are applied selectively to the applicable factors. For example, environmental stresses will generally accelerate part defects and manufacturing defects to failure. These additional factors are normalized to unity under average conditions, so that the value inside the parenthesis is one under nominal conditions and for nominal processes.

$$\lambda_p = \lambda_{IA} (\Pi_P \Pi_{IM} \Pi_E + \Pi_D \Pi_G + \Pi_M \Pi_{IM} \Pi_E \Pi_G + \Pi_S \Pi_G + \Pi_I + \Pi_N + \Pi_W) + \lambda_{SW} \quad (6.2)$$

Π_{IM}: Infant mortality factor

Π_{IM}: Environmental factor

Π_G: Reliability growth factor

The initial assessment of the failure rate, λ_{IA}, is the seed failure rate value, which is obtained by using the 217Plus component reliability prediction models, along with other available data. This failure rate is then modified by the Pi-factors that account for specific processes used in the design and manufacture of the product or system, along with the environment, reliability growth and infant mortality characteristics of the item. The above failure rate expression represents the total failure rate of the system, which includes "induced" and "no defect found" failure causes. If the inherent failure rate is desired, then the "induced" and "no defect found" Pi-factors should be set to zero, since they represent operational and non-inherent failure causes.

For grading factors, Table 7.2-23 shall be filled out. It asks for instance, “What is the % of team members having relevant product experience (thresholds at 25, 50%)?” and according the answer, there is a factor. The questions are grouped as Design, Manufacturing, Part Quality, System Management, CND, Induced, Wearout, Growth.

6.2.4 Conversion

In case the reliability data is already provided for an element or equipment, there is a need to adapt it to the operating conditions where the system/subsystem will be operated. For this cause, conversion factors have been created for the temperature and environment. As mentioned in [97] most COTS item predictions are expressed with 30 degrees C and Ground Benign environments. The below tables show the conversion factors for different temperature and environment.

Table 6.7 Temperature factor for all microcircuits [98]

From Temperature °C \ To Temperature °C	10	20	30	40	50	60	70	80	90	100
10	X	0.9	0.8	0.8	0.7	0.5	0.4	0.3	0.2	0.1
20	1.1	X	0.9	0.9	0.7	0.6	0.5	0.4	0.2	0.2
30	1.2	1.1	X	1.0	0.8	0.7	0.5	0.4	0.3	0.2
40	1.3	1.2	1.0	X	0.8	0.7	0.6	.04	0.3	0.2
50	1.5	1.4	1.2	1.2	X	0.8	0.7	0.5	0.3	0.2
60	1.9	1.7	1.6	1.5	1.2	X	0.8	0.6	0.4	0.3
70	2.4	2.2	1.9	1.8	1.5	1.2	X	0.7	0.5	0.3
80	3.3	3.0	2.7	2.6	2.1	1.7	1.4	X	0.7	0.4
90	4.9	4.5	4.0	3.8	3.2	2.5	2.0	1.5	X	0.6
100	7.7	7.0	6.3	6.0	5.0	4.0	3.2	2.3	1.6	X

Table 6.8 Environment conversion [98]

To From	217 ⇒	GB	GF	GM	NS	NU	AIC	AIF	AUC	AUF	ARW	SF
217 ⇓	SD-18 ⇓⇒	Protected	-	-	Normal	Severe	Normal	-	Severe	Severe	Severe	-
GB	Protected	X	0.5	0.2	0.3	0.1	0.3	0.2	0.1	0.1	0.1	1.1
GF	-	2.0	X	0.4	0.6	0.3	0.6	0.4	0.2	0.1	0.2	2.0
GM	-	5.0	2.5	X	1.4	0.7	1.4	0.9	0.6	0.3	0.5	5.0
NS	Normal	3.3	1.7	0.7	X	0.5	1.0	0.7	0.4	0.2	0.3	3.3
NU	Severe	10.0	3.3	1.4	2.0	X	2.0	1.4	0.9	0.5	0.7	10.0
AIC	Normal	3.3	1.7	0.7	1.0	0.5	X	0.7	0.4	0.2	0.3	3.3
AIF	-	5.0	2.5	1.1	1.4	0.7	1.4	X	0.6	0.4	0.5	5.0
AUC	Severe	10.0	5.0	1.7	2.5	1.1	2.5	1.7	X	0.6	0.8	10.0
AUF	Severe	10.0	10.0	3.3	5.0	2.0	5.0	2.5	1.7	X	1.4	10.0
ARW	Severe	10.0	5.0	2.0	3.3	1.4	3.3	2.0	1.3	0.7	X	10.0
SF	-	0.9	0.5	0.2	0.3	0.1	0.3	0.2	0.1	0.1	0.1	X

CHAPTER 7

PTC WINDCHILL TOOL

This sections aims to introduce the readers the tool which is used for reliability analyses in this study with the guidance provided in [96]. The development of the tools goes beyond 1986 where Innovative Software Designs is incorporated to pursue its goal of producing a set of superior, user-friendly reliability analysis software tools by combining expertise in reliability analysis with expertise in software engineering. For reliability calculations, the tool PTC Windchill is used. PTC Windchill Quality Solutions is a completely integrated set of software tools for analyzing product performance, reliability, and safety. Recognized for its user-friendly, state-of-the-art features, it offers all of the tools described in the following table in a unique, fully integrated framework. In addition to supplying an intuitive interface for data entry, it provides easy-to-use wizards for importing, exporting, filtering, graphing, and reporting on your data. Providing unparalleled customer satisfaction, PTC Windchill Quality Solutions is an industry standard for QLM (quality lifecycle management) analyses.

7.1 Modules

Table 7.1 Modules and Their Usage

Tool	**Description**
PTC Windchill Markov	Models a wide array of complex, state dependent systems. This broad analysis tool calculates reliability results for varied systems, especially those with sequence dependencies. Markov analysis assesses dynamic system behavior. A Markov diagram, which is also known as a state transition diagram, represents the system as a set of random variables and their interdependencies.

Table 7.1 Modules and Their Usage (cont'd)

PTC Windchill Prediction	Predicts the likely failure rates of components and/or systems. Predictions are based on statistically developed models that compute failure rates based on component and environmental parameters.
PTC Windchill RBD	Assesses reliability metrics of complex systems that employ redundancy and other methods to increase reliability. This module is a complete tool for the evaluation of block diagrams and phase diagrams, offering sophisticated optimization and simulation techniques to model system reliability. It can take maintenance, repair resource, capacity, downtime, and spares information into account and optimize maintenance intervals and the number of repair resources and onsite and offsite spares. When possible, PTC Windchill RBD analytically analyzes the system to compute failure rate, MTBF (mean time between failures), reliability, availability, unreliability, and unavailability. When configuration complexities make analytical analysis impossible, a built-in Monte Carlo simulation engine is used. This module supports many advanced capabilities that are unavailable in typical tools for evaluating block diagrams. Besides supporting maintenance data, it supports capacity, cost analysis, imperfect maintenance, repair resources, spares, downtime, cost calculations, and optimizations for maintenance intervals, repair resources, and spares. The RBD module also supports phase diagrams, which model the operation of subsystems and components in specific mission phases of a phase-based system.
PTC Windchill Event Tree	Identifies all possible causes of a system failure and/or all possible events that can occur in the system to determine the probability of a particular event's occurrence based on the events leading up to it.
PTC Windchill FMEA	Establishes the effects of various failure modes on a system and gauges how critical the effects of these failures are on the system.
PTC Windchill FTA	Establishes the effects of various failure modes on a system and gauges how critical the effects of these failures are on the system.
PTC Windchill ALT	Uses life stress models to extrapolate the test data from a small sample of overstressed products to predict the reliability of the product at normal stress levels
PTC Windchill FRACAS	Records and analyzes significant incident information so that effective correction actions are quickly identified, implemented, and verified.

Table 7.1 Modules and Their Usage (cont'd)

PTC Windchill LCC	Evaluates the total lifetime cost of the system, factoring in metrics such as failure rates and repair costs.
PTC Windchill Maintainability	Estimates the MTTR (mean time to repair) for various components to aid in the development of maintenance plans for the system.
PTC Windchill Weibull	Forecasts failures based on samples of actual field data. This general statistical tool assesses failure rate distributions, optimization techniques, and predictive analyses.

7.2 File Types

A Project is a group of files that is treated as a single entity to simplify setup and management. A Project contains one or more System files and all necessary support files. A System file stores all of the data to analyze for a particular system. The System file, which is split either horizontally (default) or vertically, displays the panes in which you record and track data. When multiple panes are present, tabs are shown. You quickly activate a window by clicking its tab. In addition to storing the data to analyze, a System file stores calculation options and results. The panes shown in the System file depend on the modules selected for use in your current session.

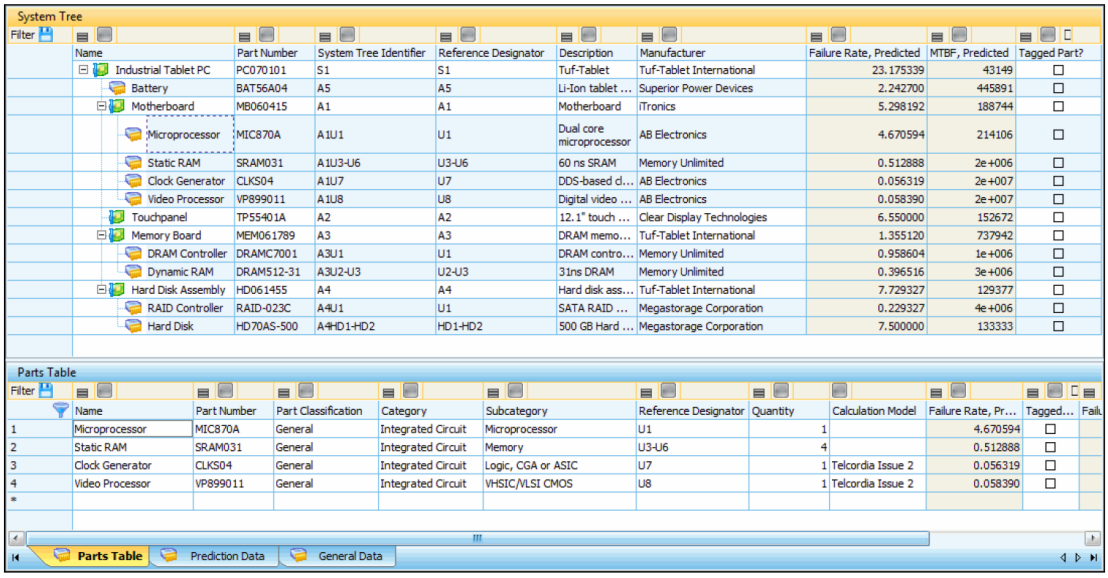


Figure 7.1 File Types

The support files for a module are available only when the module is in use. Some examples of support files are Alert, Assembly Library, Report Design, Table Format etc.

7.3 General Part Categories and Subcategories

When inserting a part in the System Tree Items table or Parts Table, part classification, category, and subcategory must be selected. Then parameters based on the selected calculation model are provided.

Table 7.2 Capacitor Part Category

Capacitor Subcategory	217	217Plus	PRISM	Telcordia	HRD5	IEC TR 62380/ RDF 2000	299B	299C	Siemens	FIDES 2004
Air Trimmer, Variable (CT)	X	X	X	X	X	X		X	X	
Button Mica (CB)	X	X	X	X	X		X	X	X	
Ceramic, Variable (CV)	X	X	X	X	X	X	X*	X	X	
Chassis Mount, Elec, Alum (CU, CUR)	X	X	X	X	X	X	X	X	X	X
Chip, Ceramic (CDR)	X	X	X	X	X	X	X	X		X
Chip, Elec (CWR)	X	X	X	X	X	X	X	X	X	
Chip, Silicon				X**						
Feed Through, Paper (CZ, CZR)	X	X	X	X	X	X	X	X	X	
General Ceramic (CK, CKR)	X	X	X	X	X	X	X	X	X	X
Glass (CY, CYR)	X	X	X	X	X		X	X	X	
Lead Mount, Elec, Alum (CE)	X	X	X	X	X	X	X	X	X	X
Metallized Paper-Plastic (CH, CHR)	X	X	X	X	X	X	X	X	X	
Mica (CM, CMR)	X	X	X	X	X		X	X	X	
MOS				X**						
Nonsolid, Elec, Tant (CL, CLR, CRL)	X	X	X	X	X		X	X	X	X
Other, Variable		X	X		X			X	X	
Paper (CA, CP)	X	X	X	X	X	X	X	X		
Paper-Plastic (CQ, CQR, CPV)	X	X	X	X	X	X	X	X	X	
Piston, Variable (PC)	X	X	X	X	X	X	X	X	X	
Plastic (CFR)	X	X	X	X	X	X	X	X	X	
Solid, Elec, Tant (CSR)	X	X	X	X	X	X	X	X	X	X
Super Metallized Plastic (CRH)	X	X	X	X	X	X	X	X	X	
Temp Compensat, Ceramic (CC, CCR)	X	X	X	X	X	X	X	X	X	X
Vacuum, Variable or Fixed (CG)	X			X	X	X		X		

* The Parts Count method supports this part, but the Parts Stress method does not.

** Supported only by Telcordia Issue 2.

Table 7.3 Connection Part Category

Connection Subcategory	217	217Plus	PRISM	Telcordia	HRD5	IEC TR 62380/ RDF 2000	299B	299C	Siemens	FIDES 2004
Board with Plated Thru Holes	X	X			X		X	X		X
General	X	X		X	X	X	X	X	X	X
IC Socket	X			X	X			X		
Other Connection	X	X					X	X	X	
PCB Edge	X	X		X	X	X	X	X		X
SMT Interconnect Assy	X	X			X			X		

Table 7.4 Inductor Part Category

Inductor Subcategory	217	217Plus	PRISM	Telcordia	HRD5	IEC TR 62380/ RDF 2000	299B	299C	Siemens	FIDES 2004
Chip								X		
Coil	X	X		X	X	X	X	X	X	X
Transformer	X	X		X	X	X	X	X	X	X

Table 7.5 Integrated Circuit Part Category

Integrated Circuit Subcategory	217	217Plus	PRISM	Telcordia	HRD5	IEC TR 62380/ RDF 2000	299B	299C	Siemens	FIDES 2004
Bubble Memory	X	X	X							
Custom					X					
EEPROM	X	X	X	X	X	X	X	X	X	X
GaAs Digital	X	X	X	X	X	X				
GaAs MMIC	X	X	X	X	X	X		X	X	
Linear	X	X	X	X	X	X	X	X	X	X
Logic, CGA or ASIC	X	X	X	X	X	X	X	X	X	X
Memory	X	X	X	X	X	X	X	X	X	X
Microprocessor	X	X	X	X	X	X	X	X	X	X
PAL, PLA	X	X	X	X	X	X	X	X		X
SAW - Surface Acoustic Wave	X						X	X	X	
VHSIC/VLSI CMOS	X	X	X	X	X					

7.3.1 Mechanical Part Category

This model is based on the Handbook of Reliability Prediction Procedures for Mechanical Equipment [99]. The Mechanical model was developed under the direction of the United States Navy and is the only standard of its kind. It supports failure rate calculations for various mechanical part, including springs, bearings, seals, motors, brakes, clutches, and many more. Regardless of the calculation model selected, when a Mechanical Part category/subcategory combination is selected, the Mechanical model is used for the part. Following tables are given in [99] for mechanical reliability prediction.

Table 7.6 Miscellaneous Part Category

Miscellaneous Subcategory	217	217Plus	PRISM	Telcordia	HRD5	IEC TR 62380/ RDF 2000	299B	299C	Siemens	FIDES
Antenna, Loop							X	X		
Antenna, Telescopic							X	X		
Battery				X		X	X	X		X*
Ceramic Resonator				X	X	X		X	X	X
Computer Subsystem				X						
COTS Board										X*
Crystal Resonator					X	X	X	X	X	X
Delay Line				X			X	X		
Display						X				X
Electric Bell							X	X		
Electric Cable							X	X		
Fan										X*
Ferrite Device, Microwave	X			X		X	X	X		
Filter	X				X	X	X	X	X	
Fuse	X			X	X	X	X	X	X	X*
Gas Discharge Tube					X					
Gyroscope				X				X		
Heater				X			X	X		
Incandescent Lamp	X			X	X		X	X	X	
Laser	X							X		

Table 7.6 Miscellaneous Part Category (cont'd)

Miscellaneous Subcategory	217	217Plus	PRISM	Telcordia	HRD5	IEC TR 62380/ RDF 2000	299B	299C	Siemens	FIDES
LCD						X				X
Load, Dummy or Microwave	X			X			X	X		
Loudspeaker							X	X		
Keyboard										X*
Meter	X			X	X			X		
Microphone							X	X		
Microwave Element	X			X	X	X	X	X		
Neon Lamp	X			X			X	X	X	X
Oscillator				X	X	X		X	X	
Piezoelectric Component (Transducer, Sensor)									X	
Power Module or Supply				X**						
Quartz Crystal	X			X		X	X	X	X	X
Quartz Filter						X	X	X	X	
RF or Microwave Passive Device				X**					X	
Surge Arrestor									X	
Termination	X									
Thermal-Electric Cooler				X		X		X		
Thermal Sensitive Component								X		
Tube	X						X	X		

* Supported only by FIDES 2009 models.

** Supported only by Telcordia Issue 2.

Table 7.7 Optical Device Category

Optical Device Subcategory	217	217Plus	PRISM	Telcordia	HRD5	IEC TR 62380/ RDF 2000	299B	299C	Siemens	FIDES 2004
Amplifiers				X*					X	
Coupler / Splitter				X				X	X	
Detector, Isolator, Emitter	X	X		X	X	X	X	X	X	X

Table 7.7 Optical Device Category (cont'd)

Optical Device Subcategory	217	217Plus	PRISM	Telcordia	HRD5	IEC TR 62380/ RDF 2000	299B	299C	Siemens	FIDES 2004
Dispersion Compensating Module				X*					X	
Fiber Optic Item	X			X*					X	
Laser Diode	X			X*	X	X			X	
Laser Module				X				X	X	
Modulator				X*					X	
Optical Switch				X*					X	
Optical Wavelength Locker				X*						
Other Optical Module or Device		X		X	X	X			X	
Power Coupler / Divider (Tap)				X*				X		
Receiver Module				X*						
Transceiver				X*					X	
Transponders				X*					X	
Wavelength Division Multiplexer				X				X	X	

Table 7.8 Relay Part Category

Relay Subcategory	217	217Plus	PRISM	Telcordia	HRD5	IEC TR 62380/ RDF 2000	299B	299C	Siemens	FIDES 2004
Automotive								X	X	
Contactor	X			X		X	X	X	X	
Dry Circuit	X					X	X	X	X	
Electronic Time Delay, Non-Thermal	X	X				X	X	X		
General Purpose	X	X		X		X	X	X	X	X
High Speed	X					X	X	X		
High Voltage	X					X	X	X	X	X
Latching	X			X		X	X	X		
Low Power	X						X	X	X	X
Medium Power	X					X	X	X	X	X

Table 7.8 Relay Part Category (cont'd)

Relay Subcategory	217	217Plus	PRISM	Telcordia	HRD5	IEC TR 62380/ RDF 2000	299B	299C	Siemens	FIDES 2004
Medium Power	X					X	X	X	X	X
Mercury				X		X		X	X	
Polarized	X					X	X	X		
Reed, Dual In Line	X	X		X	X	X		X	X	
Sensitive	X					X	X	X	X	
Solid State, Time Delay	X	X		X		X	X	X		
Thermal, Bimetal	X	X		X		X	X	X		

Table 7.9 Resistor Part Category

Resistor Subcategory	217	217Plus	PRISM	Telcordia	HRD5	IEC TR 62380/ RDF 2000	299B	299C	Siemens	FIDES 2004
Accurate, WW (RB, RBR)	X	X	X	X	X	X	X	X	X	X
Carbon, Var NonWW (RV)	X	X	X	X	X	X	X	X	X	
Chassis Mount, WW Power (RE, RER)	X	X	X	X	X	X	X	X	X	X
Composition (RC, RCR)	X	X	X	X	X	X	X	X		
Film (RL, RLR, RN, RNR, RM)	X	X	X	X	X	X	X	X	X	X
Film, Power (RD)	X		X	X	X	X	X	X	X	X
Film, Var NonWW (RVC)	X	X	X	X	X	X	X	X	X	X
General		X							X	
Glass Glazed, Var							X	X	X	
Lead Mount, WW Power (RW, RWR)	X	X	X	X	X	X	X	X	X	X
Lead Screw, Var WW (RT, RTR)	X	X	X	X	X		X	X	X	
Network Film (RZ)	X	X	X	X	X	X	X	X	X	X
Organic Solid, Var							X	X	X	
Power, Var WW (RP)	X	X	X	X	X		X	X	X	X
Precision, Var NonWW (RQ)	X	X	X	X	X	X	X	X	X	

Table 7.10 Rotating Device Part Category

Rotating Device Subcategory	217	217Plus	PRISM	Telcordia	HRD5	IEC TR 62380/ RDF 2000	299B	299C	Siemens	FIDES 2004
Motor	X			X	X		X	X		
Other	X			X	X		X	X		

Table 7.11 Semiconductor Part Category

Semiconductor Subcategory	217	217Plus	PRISM	Telcordia	HRD5	IEC TR 62380/ RDF 2000	299B	299C	Siemens	FIDES 2004
Alphanumeric Display	X			X	X		X	X		
Diode	X	X	X	X	X	X	X	X	X	X
GaAs FET	X	X	X	X	X	X	X	X	X	
HBT				X*						
Microwave Diode	X	X	X	X	X	X	X	X	X	X
Microwave Power Transistor	X			X	X	X	X	X	X	
Microwave Transistor	X	X	X	X	X	X			X	
Si FET	X	X	X	X	X	X	X	X	X	X
Thyristor	X	X	X	X	X	X	X	X	X	X
Transistor	X	X	X	X	X	X	X	X	X	X
Unijunction Transistor	X	X	X	X	X	X	X	X		

* Supported only by Telcordia Issue 3.

Table 7.12 Software Part Category

Software Subcategory	217	217Plus	PRISM	Telcordia	HRD5	IEC TR 62380/ RDF 2000	299B	299C	Siemens	FIDES 2004
217Plus Software		X								
PRISM Software			X							
RADC Toolkit Software	When the Software subcategory is selected, the reliability of the software component is calculated using the software reliability equation from the *The Rome Laboratory Reliability Engineer's Toolkit*, April 1993 issue, page 124-125. For descriptions of the parameters required by this equation, see "General Software Model" on page 10-580.									

Table 7.13 Switching Device Part Category

Switching Device Subcategory	217	217Plus	PRISM	Telcordia	HRD5	IEC TR 62380/ RDF 2000	299B	299C	Siemens	FIDES 2009
Basic Sensitive	X	X				X	X	X		
Circuit Breaker	X			X				X		
Keyboard						X				
Other	X*	X			X				X	
Rocker or Slide	X*	X		X	X	X				
Rotary	X	X		X	X	X	X	X		X
Thumbwheel	X	X			X	X	X	X		
Toggle or Pushbutton	X	X		X	X	X	X	X		X

* This part is not supported by the Parts Count method in FN1.

7.4 Stress Parameters

The failure equations that a calculation model provides for a part require that certain stress parameters are entered, namely Voltage Parameters, Power Parameters, Current Parameters, and Temperature Parameters.

Table 7.14 Voltage Parameters

Parameter	Type	Description
Applied DC Voltage	Real (Volts)	The DC voltage (VDC) applied to the capacitor.
AC RMS Voltage	Real (Volts)	The AC RMS voltage (VAC) applied to the capacitor.
Operating Voltage	Real (Volts)	The description depends on the part type. • For diodes, the reverse diode voltage. • For transistors, the applied Vce (Voltage, Collector to Emitter). • For relays, the reverse relay voltage. • For resistors, the operating maximum voltage.
Rated Voltage	Real (Volts)	The description depends on the part type. • For capacitors, the rated voltage (VDC) of the device. • For diodes, transistors, and resistors, the rated voltage specified by the manufacturer.
Voltage Ratio	Real	Generally, this field is left at #.#. For most parts, the voltage ratio is calculated as follows: Voltage Ratio = (Operating Voltage / Rated Voltage) * 100 For capacitors, the voltage ratio is calculated as follows: Voltage Ratio = [(√2 * AC RMS Voltage + Applied DV Voltage) / Rated Voltage] * 100 If you enter a value for this parameter, this value is used in place of a computed voltage ratio. When prediction calculations run, all parts with entered or calculated voltage ratios over 100 are flagged as overstressed parts. Overstressed parts appear in red in the System Tree Items table and Parts Table by default. Under **Display** in the Options window, the color in which to display overstressed parts is specified. For more information, see "Display User Options" on page 1-317.

Table 7.15 Power Parameters

Parameter	Type	Description
Operating Power or Power Dissipation	Real (Watts)	The operating power of the device in the circuit. This parameter is used in temperature calculations. For more information, see "Temperature Parameters" on page 10-318.
Power Rating	Real (Watts)	The rated power of the device. **NOTE:** Power rating is a derating parameter. Under **Prediction** in the Project properties, **Show derating fields on Part Data form** controls whether the Derating Parameters box appears on the right side of the Prediction Data pane. For more information, see "Derating Parameters" on page 10-116.
Required Power	Real (Watts)	The required power output of the device.
Power Ratio	Real	Generally, this field is left at #.#. The power ratio is calculated as follows: Power Ratio = (Operating Power / Rated Power) * 100 If you enter a value for this parameter, this value is used in place of a calculated power ratio.

Table 7.16 Current Parameters

Parameter	Type	Description
Operating Current	Real (Amps)	The operating load stress of the device in the circuit.
Rated Current	Real (Amps)	The maximum rated current of the device with a resistive load.
Current Ratio	Real	Generally, this field is left at #.#. The current ratio is calculated as follows: Current Ratio = (Operating Current / Rated Current) * 100 If you enter a value for this parameter, this value is used in place of a calculated current ratio.
Rated Forward Current	Real (Amps)	The maximum rated forward rms current of the device.
Forward Peak Current	Real (Amps)	The peak forward current of the device.
Peak Current	Real (Amps)	The peak current that the device experiences.

- **Comprehensive Temperature Parameters**

The following table describes the comprehensive parameters that can appear for calculating the junction temperature of a part during operation.

Table 7.17 Temperature Parameters

Parameter	Type	Description
Initial Temp Rise	Real (Degrees C)	The rise in temperature between the operating temperature of the assembly and the location specified for thermal resistance units. The operating temperature is initially defined in the Calculation Data pane when the assembly is inserted. Normally, the operating temperature is the ambient temperature of the surrounding air, but it can also be a board temperature, the temperature of the heat sink rails, or any other specified temperature.

Table 7.17 Temperature Parameters (cont'd)

Parameter	Type	Description
Operating Power or Power Dissipation	Real (Watts)	The power dissipation of the device in watts, which is normally available in the manufacturer's databook. Be sure to use the actual rated (rather than maximum rated) power dissipation. For integrated circuits and semiconductors, operating power can generally be calculated as: Operating Power = Icc * Vcc + Iol * Vol Where each of the parameters above are found in the databook tables.
Thermal Resistance	Real (Degrees C/Watts)	The resistance to the movement of temperature between the junction and the location specified for thermal resistance. When a device is operating, it generates heat at its junction. This heat is transmitted through the device to its surface and is then dissipated into the air (or into a heat sink). The lower the thermal resistance, the easier it is for the heat to escape or dissipate. Thermal resistance, which is often referred to as ThetaJC, is generally found in the manufacturer's databook.
Junction-	Text	The location at which thermal resistance values are recorded. This field is not used in any temperature calculations. It is a five-character text field that is used for informational purposes only. Thermal resistance can be specified as Junction-Case, Junction-Air, Junction-Board, or whatever. If thermal resistance is being specified as Junction-Case, entering `Case` in this field points out that the thermal resistance value is the actual resistance to temperature movement between the device junction and the device case. Because consistent use of the same location for all thermal resistance values is assumed, you do not have to use this field to specify the location. You can use this field to enter any information you want.
Junction-	Text	The location at which thermal resistance values are recorded. This field is not used in any temperature calculations. It is a five-character text field that is used for informational purposes only. Thermal resistance can be specified as Junction-Case, Junction-Air, Junction-Board, or whatever. If thermal resistance is being specified as Junction-Case, entering `Case` in this field points out that the thermal resistance value is the actual resistance to temperature movement between the device junction and the device case. Because consistent use of the same location for all thermal resistance values is assumed, you do not have to use this field to specify the location. You can use this field to enter any information you want.
Temperature Rise	Real (Degrees C)	The rise in temperature between the operating temperature and the junction. When this field is left at `#.#`, the temperature rise is calculated using the values specified for the initial temperature rise, power dissipation, and thermal resistance: Temperature Rise = Initial Temperature Rise + Power Dissipation * Thermal Resistance If you enter a value for this parameter, this value is used in place of a calculated temperature rise. To calculate the junction temperature of the device, the temperature rise (whether calculated or entered) is added to the operating temperature. If you prefer, you can directly enter the value to use for the junction temperature for **Junction Temp Override**. For components inside a hybrid, if the temperature rise from case to junction cannot be determined, use the following defaults: • Integrated.Circuits: 10 degrees C • Transistors: 25 degrees C • Diodes: 20 degrees C

Table 7.17 Temperature Parameters (cont'd)

Parameter	Type	Description
Junction Temp Override	Real (Degrees C)	Generally this field is left at #.# so that the junction temperature is calculated. If you enter a value for this parameter, this value is used in place of a calculated junction temperature. (Perhaps you want to use the temperature value obtained from an infrared scanner or a thermal engineer.) Using this method, changes to the subassembly temperature or to factors contributing to the temperature rise are not taken into account.
Minimum Temp Rating	Real (Degrees C)	The minimum rated lower limit operating temperature for a semiconductor. This field is shown for several semiconductor subcategories when the 299B or 299C model selected is selected. It is not required by the 299C model when **Foreign** is selected.
Maximum Rated Temperature	Real (Degrees C)	The maximum junction temperature, which is normally available in the manufacturer's databook. For silicon integrated circuits, the stated maximum junction temperature is normally 175 degrees C. The device is flagged as overstressed if the sum of the temperature rise and subassembly temperature is greater than the maximum junction temperature.

Basic Temperature Parameters

The following table describes the basic parameters that appear for calculating the junction temperature of many different parts during operation.

Table 7.18 Basic Temperature Parameters

Parameter	Type	Description
Temperature Rise	Real (Degrees C)	The rise in temperature between the operating temperature and the case. If you enter a value for this parameter, this value is added to the operating temperature. If you prefer, you can directly enter the value for the case temperature for **Case Temp Override**. However, when you enter an override value, any changes to the subassembly temperature or to factors contributing to the temperature rise are not taken into account.
Temp Override *OR* Case Temp Override	Real (Degrees C)	Generally this field is left at #.# so that the case temperature is calculated. If you enter a value for this parameter, this value is used in place of a calculated temperature rise. (Perhaps you want to use the temperature value obtained from an infrared scanner or a thermal engineer.) Using this method, changes to the subassembly temperature or to factors contributing to the temperature rise are not taken into account.
Max Junction Temp	Real (Degrees C)	The maximum junction temperature, which is normally available in the manufacturer's databook. The part is flagged as overstressed if the sum of the temperature rise and subassembly temperature is greater than the maximum junction temperature. This field is shown only for certain types of capacitors and resistors.

7.5 The Standard ANSI/VITA 51.1-2008

Reliability engineers continue to use MIL-HDBK-217F Notice 2 to perform failure rate predictions, however it has not been updated recently while there are many new developments in the industry that are not accounted for, so engineers adjust the models in MIL-HDBK-217F Notice 2 for newer technologies, use different defaults for unknown stress conditions, and make differing assumptions of quality and complexity factors for COTS items to reach more realistic values. But using different methods yields in incomparable results. ANSI/VITA [97] is American National Standard for reliability prediction MIL-HDBK-217 subsidiary specification and provides defaults and methods to adjust the models in MIL-HDBK-217F Notice 2 for standardization of the inputs to the MIL-HDBK-217F Notice 2 calculations to give results that are more consistent.

Data sources are cited where the specified default value is based on field data or test data analysis. Source data that was used to derive the specified factor is provided in the VITA 51 website, and links provided in the electronic version of this document. In some cases, the default value is based on engineering judgment, and this is noted where applicable. To be conservative, PiQ's based on engineering judgement were generally set higher than the PiQ's that were derived from field or test data.

CHAPTER 8

THE ARCHITECTURE

Considering the simulations results in the chapter and after observing the most used architectures in the ERTMS ETCS and CBTC domain, it is decided to go further on the two architectures, namely 2oo3 and 1oo2D.

A design can also support these two architectures, though the development might become more complex for the engineers.

8.1 HW Architectures and Algebraic Formulations

The new generation Ethernet communication supports 10 Gbit/s, therefore the cross channel communication of safe processor units can be realized this way on the backplane. Usually, PCIe serial communical supports 8 Bbit/s and with four of them communication speed of 32 Gbit/s can be reached. However, safe codes are relative low such as 512 Kbyte, therefore backplane Ethernet can fulfill the needs.

A simplified block diagram of the system for the Safety Critical Computer (SCC) is shown below where analog cards etc. are not specified explicitly.

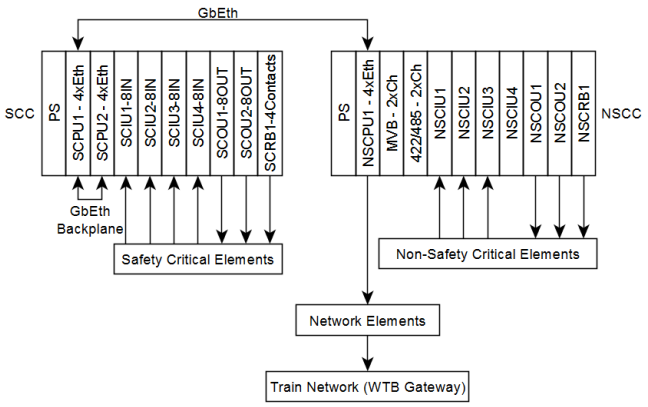


Figure 8.1 Safety Critical Computer Architecture

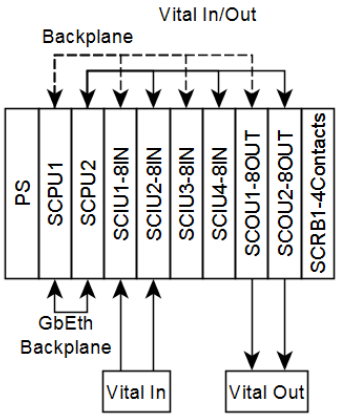


Figure 8.2 Safety Critical IN/Out Mechanism

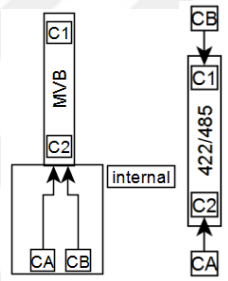


Figure 8.3 MVB and RS 422/485 Structure

Note that for MVB, CA and CB are redundant channels, connected internally. MVB communication is ear-to-ear communication. RS 422 is point to point, RS 485 is bus connection. The channels are independent from each other.

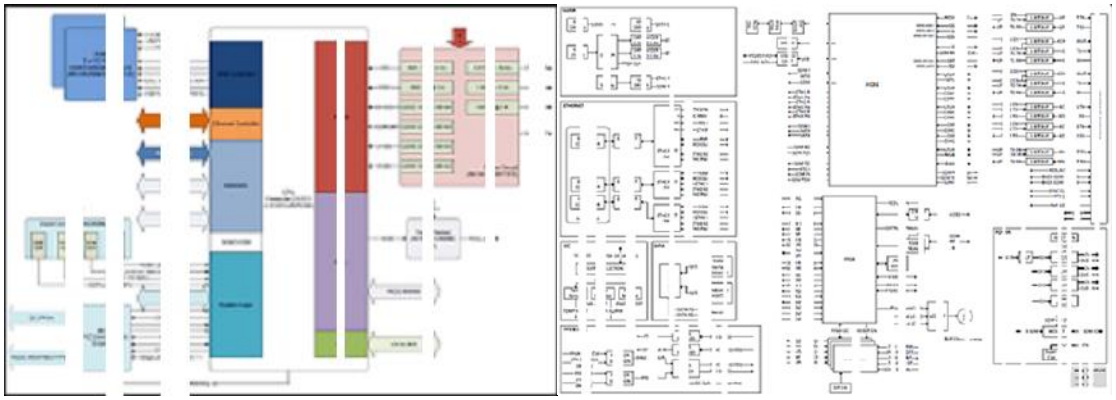


Figure 8.4 Safety Critical Computers

CHAPTER 9

THE CALCULATION

9.1 Reliability Calculation

In this part, the calculation windows are placed. 217PLUS Calculation Data Screen View in PTC Windchill Tool is shown below.

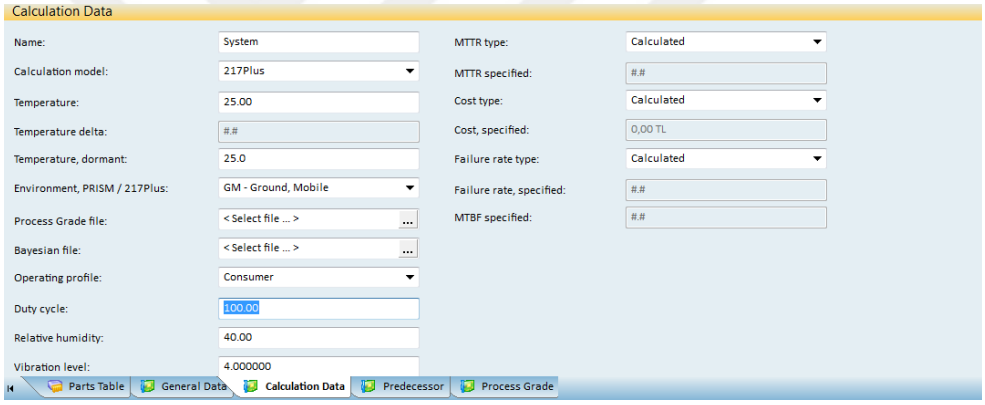


Figure 9.1 Data Screen View

The screen view in PTC Windchill tool of process grade values used for 217PLUS calculations is provided below.

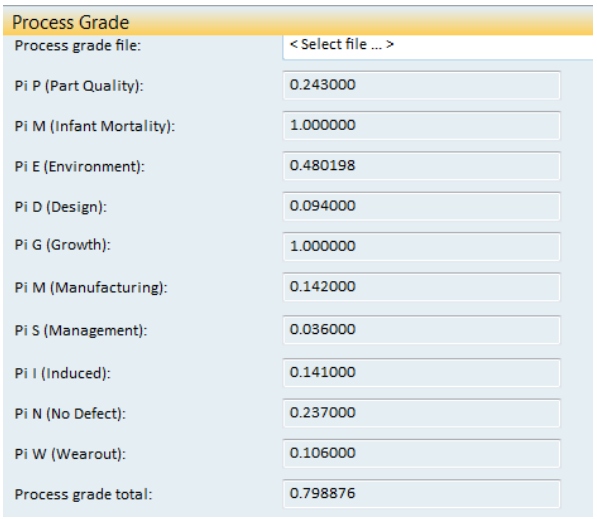


Figure 9.2 217 Plus Data Screen View in PTC Windchill Tool

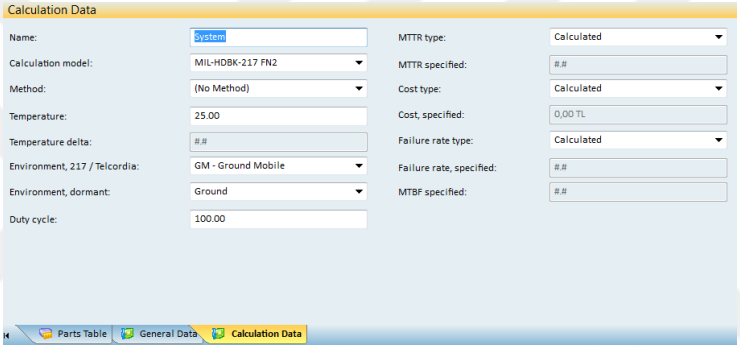


Figure 9.3 MIL-HDBK-217FN2 Calculation Data Screen View in PTC Windchill Tool

9.1.1 Safety Critical Processor Unit (SCPU) -1

Failure rate of the processor for different junction temperatures are provided by the company as given below.

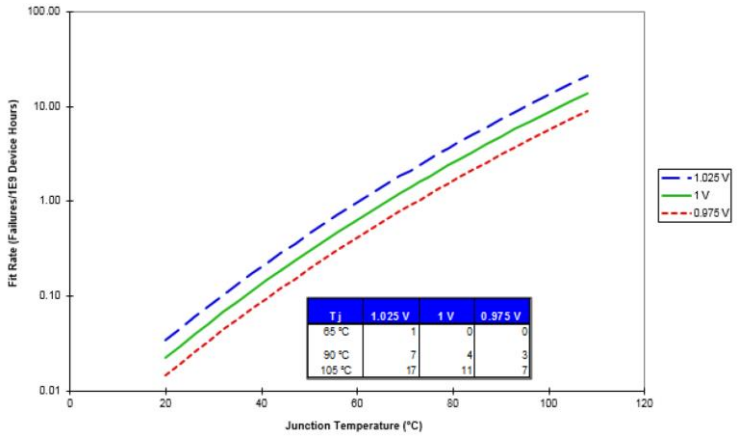


Figure 9.4 Failure Rate of the Processor (data converted using conversion tables)

9.1.1.1 SCPU-1 MIL-HDBK-217FN2 Parts Stress Calculation Results, Duty Cycle 100%

The bill of materials are given in the Appendix A.1. The report of the reliability prediction analysis according to the methods explained previous chapters is given below. The results show that the failure rate is less than 3 per million hours for the temperature 25 ^{o}C, Ground Mobile environment and the MTBF is about 350.000 hours.

Table 9.1 SCPU-1 MIL-HDBK-217FN2 prediction results for parts stress, DC 100%

System Tree Summary

File Name: [illegible]
System: System
Ref Des:
Description:

Failure Rate: [illegible]
MTBF Total: [illegible]
Temperature: 25
Environment: GM - Ground Mobile

Name	Part Number	Ref Des	Quantity	Failure Rate	MTBF
[illegible]	System		1	[illegible]	[illegible]
[illegible]	[illegible]		2	[illegible]	[illegible]
CAP 47U [illegible]	[illegible]		2	0.013300	75,330,525
RESIST THFM SMD 0R 5% 0.063W	5305-4056-0000		2	0.000006	3,295,045,116
RESIST THFM SMD 100R 5% [illegible]	5305-4056-1001		2	0.001352	750,645,133
RESIST THFM SMD 1K 5% 1/16W	5305-4056-1002		1	[illegible]	3,521,400,426
RESIST THFM SMD 1K 5% 1/16W	5305-4056-1002		2	0.001306	725,181,427
RESIST THFM SMD 1K 5% 1/16W	5305-4056-1002		2	0.000600	1,403,023,076
RESIST THFM SMD 10K 5% 1/16W	[illegible]		1	[illegible]	[illegible]
RESIST THFM SMD 10K 5% 1/16W	[illegible]		1	[illegible]	[illegible]
RESIST THFM SMD 2K2 5% 0.063W	5305-4056-2202		4	[illegible]	[illegible]
[illegible]	[illegible]		1	[illegible]	[illegible]
RESIST THFM SMD 4K7 5% 1/16W	[illegible]		1	[illegible]	[illegible]
RESIST THFM SMD 4K7 5% 1/16W	[illegible]		2	[illegible]	[illegible]
RESIST THFM SMD 4K7 5% 1/16W	5305-4056-4702		31	[illegible]	52,083,421
RESIST THFM SMD 100K 1% 1/16W	5305-4074-1004		5	[illegible]	[illegible]
RESIST THFM SMD 10R %1 1/16W	[illegible]		6	[illegible]	[illegible]
RESIST THFM 0402 1100 1% 1/16W 50V	[illegible]		1	0.000024	[illegible]
RESIST THFM SMD 1K5 %1 1/16W	5305-4074-1502		1	[illegible]	[illegible]
RESIST THFM 0402 200R 1% 50V	[illegible]		1	[illegible]	[illegible]
[illegible] 0402 [illegible] %1 1/16W 50V	[illegible]		24	[illegible]	[illegible]
[illegible] 0402 [illegible] %1 1/16W 50V	[illegible]		1	[illegible]	[illegible]
[illegible] 0402 [illegible] %1 1/16W 50V	[illegible]		1	[illegible]	[illegible]
[illegible] 1%	[illegible]		[illegible]	[illegible]	[illegible]

Page 1 of 1

Print Date: [illegible]
Print Time: [illegible]

Table 9.1 SCPU-1 MIL-HDBK-217FN2 prediction results for parts stress, DC 100% (cont'd)

Name	Part Number	Ref Des	Quantity	Failure Rate	MTBF
KEMET STD CER 0402 1% 50V 6.8pF LF	MC-0000-0138		2	0.019682	50,805,807
KEMET X7R 0603 470N %10 25V	MC-0000-0464		1	0.008850	113,009,249
CAP X7R 0402 3N3 10% 50V	MC-0000-0463-3101		1	0.002706	369,583,599
CAP X7R 0402 3N3 10% 50V	MC-0000-0463-3101		2	0.005524	181,025,725
CAP X7R 0402 3N3 10% 50V	MC-0000-0463-3101		3	0.008287	120,677,292
FILTRE PRT BEAD 0603 %25 0R30 BLM18A LF	MC-0000-0160-1000		1	0.000224	4,460,625,000
TD SVR MC34VR500V1ES	MC-0000-1694		1	0.172039	5,812,946
TD CER 6V8C0388P4CE	ARCE 15-0000-1445		1	0.191673	5,217,739
TD MPU 5V0100V760B P6A4C3E	MC-0000-1698		1	0.460030	2,448,751
KRISTAL FUND 26M 18A 8PF 20PPM	MC-0000-0862		1	0.272565	3,668,854
CAP CER SMD 100N 10% 16V 402	MC-0000-0363		3	0.013137	76,119,019
CAP CER SMD 100N 10% 16V 402	MC-0000-0363		53	0.231253	4,324,372
CAP CER SMD 18N 10% 25V 402	MC-0000-0437		3	0.009156	109,217,395
CAP CER SMD 4U7 %10 10V 805	MC-0000-0439		1	0.005362	186,494,368
CAP CER SMD 4U7 %10 10V 805	MC-0000-0439		1	0.005603	178,445,528
CAP CER SMD 4U7 %10 10V 805	MC-0000-0439		7	0.043240	23,123,237
CAP CER SMD 4U7 %10 10V 805	MC-0000-0439		2	0.010740	93,113,905
CAP CER SMD 22U %10 10V 1210	MC-0000-0429		8	0.048930	20,434,354
CAP CER SMD 22U %10 10V 1210	MC-0000-0429		18	0.081076	18,375,148
CAP CER SMD 1N 10% 25V 402	MC-0000-0430		1	0.002597	385,089,905
CAP CER SMD X5R 220N %10 6.3V	MC-0000-0787		1	0.006036	165,657,125
CAP CER SMD 2U2 10% 25V 0805	MC-0000-0731		3	0.021581	46,339,110
CAP CER SMD 2U2 10% 25V 0805	MC-0000-0731		1	0.007282	137,312,198
CAP CER SMD 2U2 10% 25V 0805	MC-0000-0731		2	0.014581	68,556,555
CAP CER SMD 2U2 10% 25V 0805	MC-0000-0731		5	0.036715	27,232,305
CAP CER SMD 10U %10 6.3V 0805 LF	MC-0000-0760		1	0.013729	72,836,539
CAP CER SMD X5R 220N %10 6.3V	MC-0000-0787		1	0.006036	165,657,125
CAP CER SMD 2U2 10% 25V 0805	MC-0000-0731		3	0.021581	46,339,110
CAP CER SMD 2U2 10% 25V 0805	MC-0000-0731		1	0.007282	137,312,198
CAP CER SMD 2U2 10% 25V 0805	MC-0000-0731		2	0.014581	68,556,555
CAP CER SMD 2U2 10% 25V 0805	MC-0000-0731		5	0.036715	27,232,305
CAP CER SMD 10U %10 6.3V 0805 LF	MC-0000-0760		1	0.013729	72,836,539

Page #: 2

Print Date: 10.04.15
Print Time: 03:08

9.1.1.2 SCPU-1 MIL-HDBK-217FN2 Parts Stress Calculation Results, Duty Cycle 75% (06-24:00 operating hours)

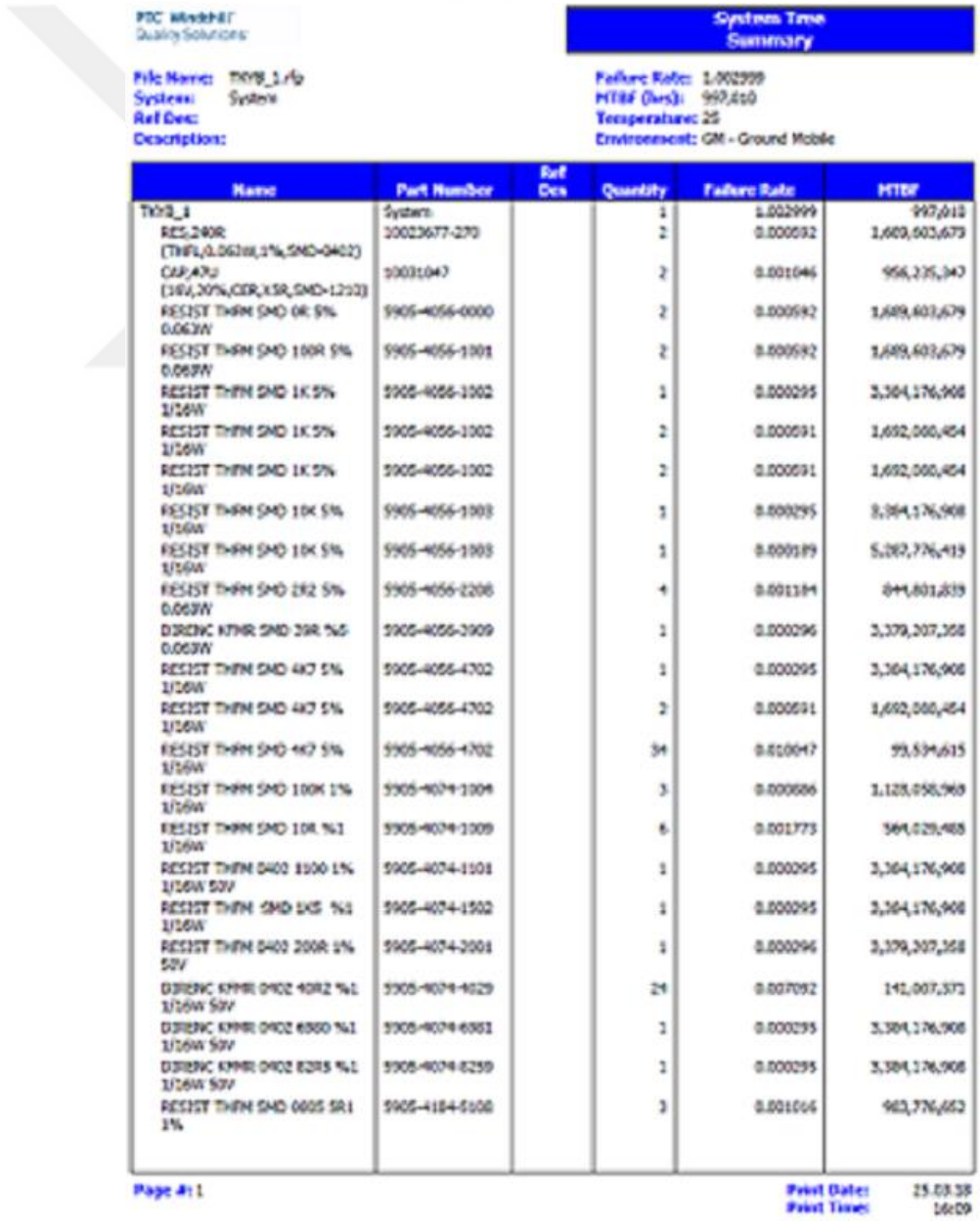
The mission term of the applications are usually not 100%. Consider a car, a plane or a train; these vehicles do not working every minute, therefore it is beneficial to consider these when performing calculations. The results for 75% DC show that the failure rate is

less than 2.5 per million hours for the temperature 25 ^{o}C, Ground Mobile environment and the MTBF is about 450.000 hours.

9.1.1.3 SCPU-1 217 PLUS Parts Stress Calculation Results, DC 100%

One important parameter on the reliability prediction results is the method, i.e. the handbook used as detailed in the previous sections. Accordingly, all the calculations are performed with respect to another handbook, namely 217Plus developed by the RIAC. The results show that the failure rate is about than 1 per million hours for the temperature 25 ^{o}C, Ground Mobile environment and the MTBF is about 1000.000 hours.

Table 9.2 SCPU-1 217Plus prediction results for parts stress, DC 100%



System Tree Summary

File Name: THYB_1.rlb
System: System
Ref Des:
Description:

Failure Rate: 1.002999
MTBF (hrs): 997,010
Temperature: 25
Environment: GM - Ground Mobile

Name	Part Number	Ref Des	Quantity	Failure Rate	MTBF
THYB_1	System		1	1.002999	997,010
RES,240R (THFI,0.063W,1%,SMD=0402)	10023677-270		2	0.000592	1,689,603,679
CAP,47U (16V,20%,CER,X5R,SMD=1210)	10031047		2	0.001046	956,235,347
RESIST THFM SMD 0R 5% 0.063W	5905-4056-0000		2	0.000592	1,689,603,679
RESIST THFM SMD 100R 5% 0.063W	5905-4056-1001		2	0.000592	1,689,603,679
RESIST THFM SMD 1K 5% 1/16W	5905-4056-1002		1	0.000295	3,384,176,908
RESIST THFM SMD 1K 5% 1/16W	5905-4056-1002		2	0.000591	1,692,088,454
RESIST THFM SMD 1K 5% 1/16W	5905-4056-1002		2	0.000591	1,692,088,454
RESIST THFM SMD 10K 5% 1/16W	5905-4056-1003		1	0.000295	3,384,176,908
RESIST THFM SMD 10K 5% 1/16W	5905-4056-1003		1	0.000189	5,282,776,419
RESIST THFM SMD 2R2 5% 0.063W	5905-4056-2208		4	0.001184	844,801,839
DIRENC KTHR SMD 29R %5 0.063W	5905-4056-2909		1	0.000296	3,378,207,358
RESIST THFM SMD 4K7 5% 1/16W	5905-4056-4702		1	0.000295	3,384,176,908
RESIST THFM SMD 4K7 5% 1/16W	5905-4056-4702		2	0.000591	1,692,088,454
RESIST THFM SMD 4K7 5% 1/16W	5905-4056-4702		34	0.010047	99,534,615
RESIST THFM SMD 100K 1% 1/16W	5905-4074-1004		3	0.000886	1,128,058,969
RESIST THFM SMD 10R %1 1/16W	5905-4074-1009		6	0.001773	564,029,485
RESIST THFM 0402 100R 1% 1/16W 50V	5905-4074-1101		1	0.000295	3,384,176,908
RESIST THFM SMD 1K5 %1 1/16W	5905-4074-1502		1	0.000295	3,384,176,908
RESIST THFM 0402 200R 1% 50V	5905-4074-2001		1	0.000296	3,378,207,358
DIRENC KMRI 0402 40R2 %1 1/16W 50V	5905-4074-4029		24	0.007092	141,007,371
DIRENC KMRI 0402 6R65 %1 1/16W 50V	5905-4074-6651		1	0.000295	3,384,176,908
DIRENC KMRI 0402 82R5 %1 1/16W 50V	5905-4074-8259		1	0.000295	3,384,176,908
RESIST THFM SMD 0805 5R1 1%	5905-4184-5108		3	0.001016	983,776,662

Page #: 1

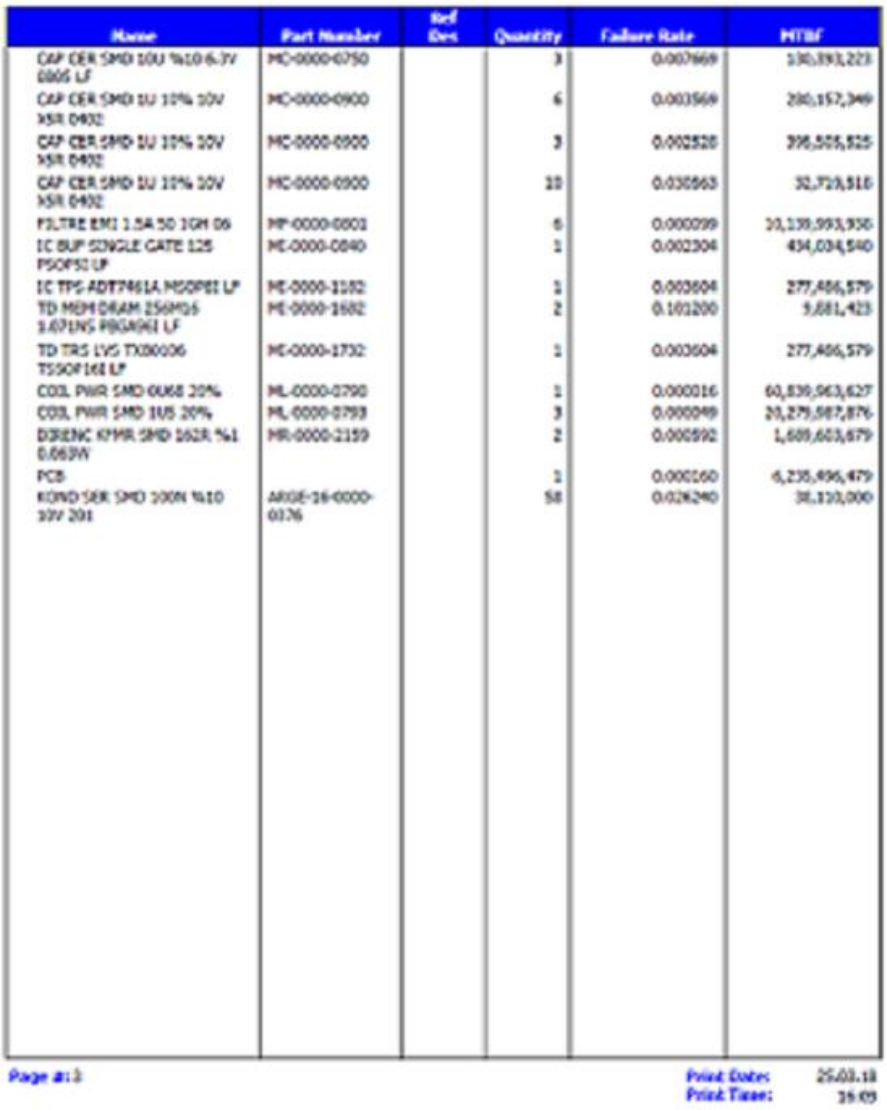
Print Date: 25.03.18
Print Time: 16:09

Table 9.2 SCPU-1 217Plus prediction results for parts stress, DC 100% (cont'd)

Name	Part Number	Ref Des	Quantity	Failure Rate	MTBF
KOND STD COG 0402 1% 50V 6.8pF LF	5910-0166-6130		2	0.000692	1,444,048,320
KOND X7R 0603 470% %10 25V	5910-0454-7002		1	0.000411	2,433,654,780
CAP X5R 0402 3N3 10% 50V	5910-0463-3101		1	0.000381	2,626,268,162
CAP X5R 0402 3N3 10% 50V	5910-0463-3101		2	0.000737	1,356,923,854
CAP X5R 0402 3N3 10% 50V	5910-0463-3101		3	0.001107	903,358,682
FILTER FRT BEAD 0603 %25 OR3R BLM18A LF	5915-1160-1000		1	0.001445	692,867,336
TD SVR MC34VR500V1E5	MI-0000-1894		1	0.003604	277,406,579
TD CDR 6V49205BFAGE	ARGE-15-0000-1445		1	0.003604	277,406,579
TD MPU LS1021AXN7MQB FBGA525I	MI-0000-1898		1	0.400200	2,498,751
KRISTAL PUMD 25M 1N4 8PF 20PPM	MP-0000-0062		1	0.272565	3,668,850
CAP CER SMD 100N 10% 10V 402	MC-0000-0563		3	0.007621	131,214,504
CAP CER SMD 100N 10% 10V 402	MC-0000-0563		53	0.026465	34,968,796
CAP SER SMD 10N 10% 25V 402	MC-0000-0427		3	0.001129	885,948,634
CAP SER SMD 4U7 %10 10V 805	MC-0000-0428		1	0.000577	1,732,814,933
CAP SER SMD 4U7 %10 10V 805	MC-0000-0428		1	0.001752	570,914,668
CAP SER SMD 4U7 %10 10V 805	MC-0000-0428		7	0.024272	41,196,437
CAP SER SMD 4U7 %10 10V 805	MC-0000-0428		2	0.001270	787,463,504
CAP SER SMD 22U %10 10V 1210	MC-0000-0429		8	0.004065	245,906,275
CAP SER SMD 22U %10 10V 1210	MC-0000-0429		10	0.004749	210,577,852
CAP SER SMD 1N 10% 25V 402	MC-0000-0430		1	0.000452	2,212,425,397
CAP SER SMD X5R 220N %10 6.3V	MC-0000-0707		1	0.000840	1,191,140,902
CAP CER SMD 2N2 10% 25V 0805	MC-0000-0711		3	0.001282	779,823,739
CAP CER SMD 2N2 10% 25V 0805	MC-0000-0711		1	0.000604	1,655,902,000
CAP CER SMD 2N2 10% 25V 0805	MC-0000-0711		2	0.000870	1,149,888,827
CAP CER SMD 2N2 10% 25V 0805	MC-0000-0711		5	0.051445	19,438,380
CAP CER SMD 100 %10 6.3V 0805 LF	MC-0000-0750		1	0.013455	74,322,594

Page #:2 Print Date: 25.03.10
Print Time: 16:09

Table 9.2 SCPU-1 217Plus prediction results for parts stress, DC 100% (cont'd)



Name	Part Number	Ref Des	Quantity	Failure Rate	MTBF
CAP CER SMD 10U %10 6.3V 0805 LF	MC-0000-0750		3	0.007869	130,393,223
CAP CER SMD 1U 10% 10V X5R 0402	MC-0000-0900		6	0.003569	280,157,349
CAP CER SMD 1U 10% 10V X5R 0402	MC-0000-0900		3	0.002520	396,505,525
CAP CER SMD 1U 10% 10V X5R 0402	MC-0000-0900		10	0.030863	32,719,516
FILTRE EMI 1.5A 50 1GH 06	MF-0000-0001		6	0.000099	10,139,993,936
IC BUF SINGLE GATE 125 PSOP5I LF	ME-0000-0840		1	0.002304	434,034,540
IC TPS ADT7461A MSOP8I LF	ME-0000-1182		1	0.003604	277,486,579
TD MEM DRAM 256M16 1.07INS FBGA96I LF	ME-0000-1682		2	0.101200	9,881,423
TD TRS LVS TX30006 TSSOP16I LF	ME-0000-1732		1	0.003604	277,486,579
COIL PWR SMD 0068 20%	ML-0000-0790		1	0.000016	60,839,963,627
COIL PWR SMD 1U5 20%	ML-0000-0793		3	0.000049	20,279,987,876
DIRENC KMR SMD 162R %1 0.063W	MR-0000-2159		2	0.000592	1,689,603,679
PCB			1	0.000160	6,235,496,479
KOND SER SMD 100N %10 10V 201	ARGE-16-0000-0176		58	0.028240	35,410,000

Page #: 3 Print Date: 25.03.18 Print Time: 19:09

9.1.1.4 SCPU-1 MIL-217 PLUS Parts Stress Calculation Results, DC 75%

The results for 75% DC show that the failure rate is about 0.99 per million hours for the temperature 25 ºC, Ground Mobile environment and the MTBF is a little more than 1.000.000 hours. If it is compared to the handbook MIL-217-FN2, the change in DC does not affect much the failure rate when using the handbook 217 Plus.

9.1.2 SCPU -2

9.1.2.1 SCPU-2 MIL-HDBK-217FN2 Parts Stress Calculation Results, DC 75%

Failure rate of the second used processor for different temperatures are provided by the company as given below.

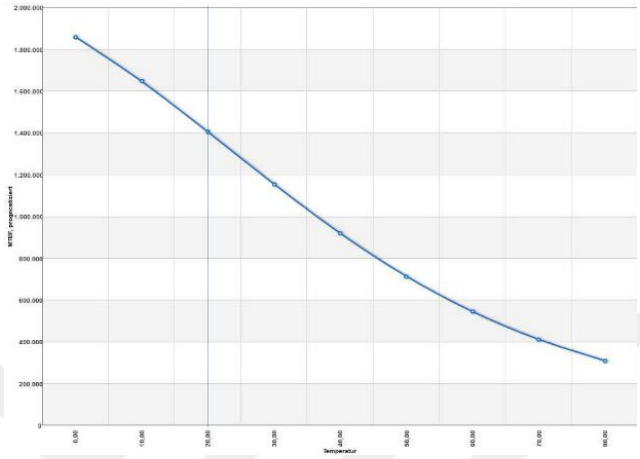
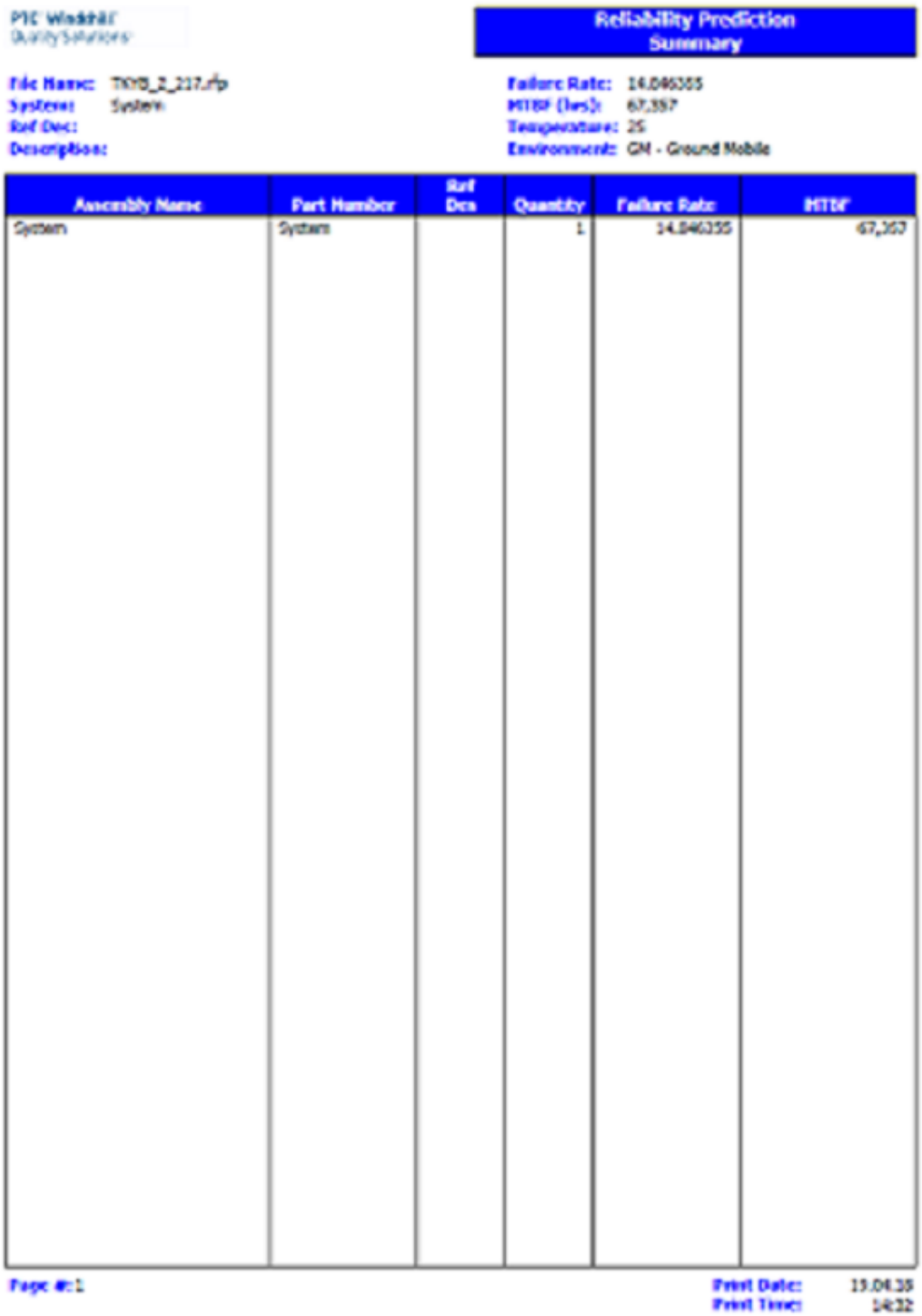


Figure 9.5 MTBF vs. Temperature of the second CPU

The results for the second SCPU show that the failure rate is less than 16 per million hours for the temperature 25 ºC, Ground Mobile environment and the MTBF is a little more than 65000 hours.

Table 9.3 SCPU-2 MIL-HDBK-217FN2 results for parts stress, DC 75%



PTC Windchill
Quality Solutions

Reliability Prediction Summary

File Name: TKYB_2_217.rlp
System: System
Ref Doc:
Description:

Failure Rate: 14.046355
MTBF (hrs): 67,357
Temperature: 25
Environment: GM - Ground Mobile

Assembly Name	Part Number	Ref Des	Quantity	Failure Rate	MTBF
System	System		1	14.046355	67,357

Page #: 1

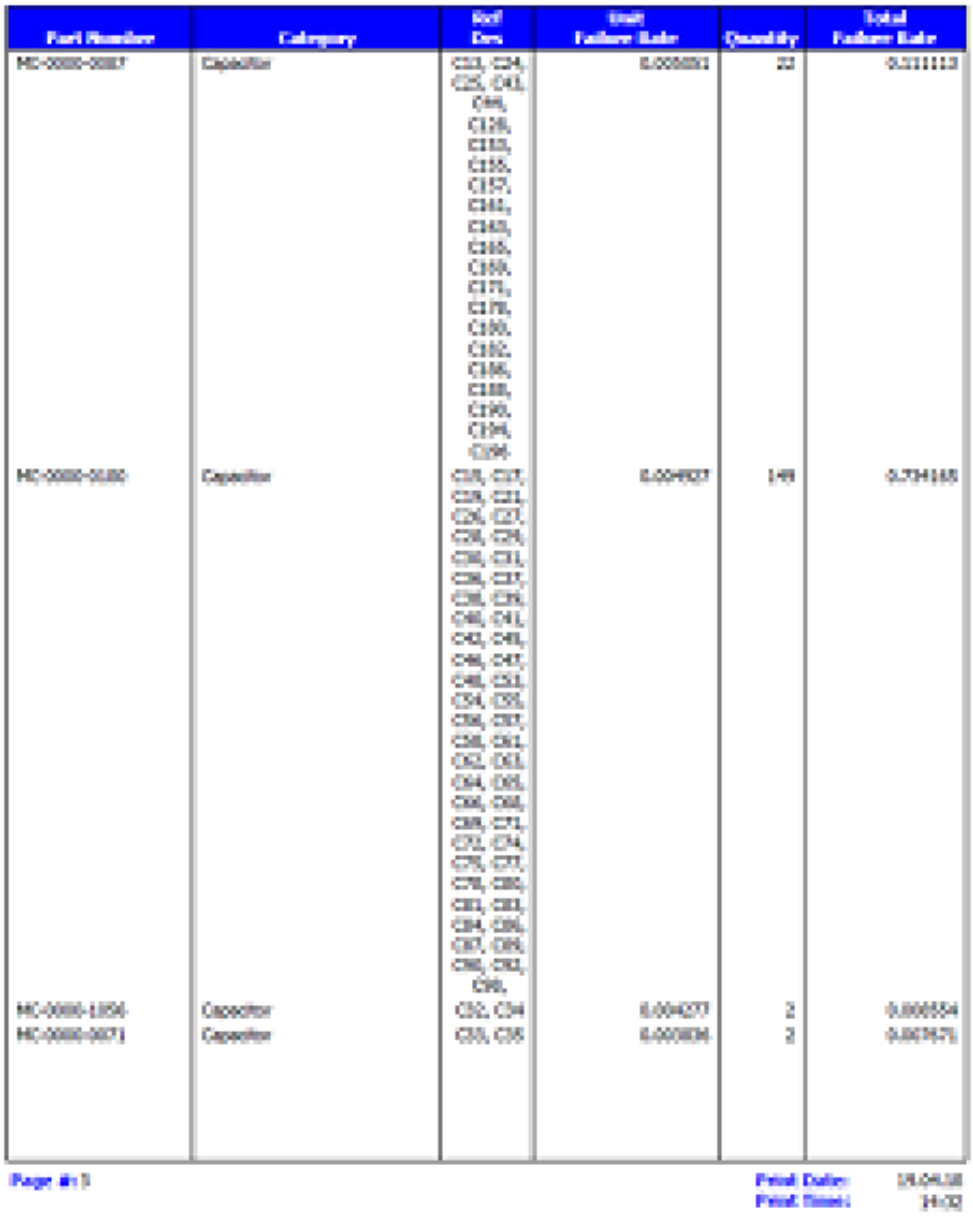
Print Date: 15.04.15
Print Time: 14:32

Table 9.3 SCPU-2 MIL-HDBK-217FN2 results for parts stress, DC 75% (cont'd)

Part Number	Category	Ref Des	Unit Failure Rate	Quantity	Total Failure Rate
MP-0041-0001	Connection	BOARD1	0.030150	1	0.030150
ARGS V17 0021 0021	Integrated Circuit	BOARD2	2.678571	1	2.678571
MB-0003-1215	Integrated Circuit	BOARD3	1.875000	1	1.875000
MC-0003-0429	Capacitor	C1, C2, C4, C5, C6, C7, C206, C208	0.012423	8	0.099384
MC-0003-0016	Capacitor	C3, C104, C105, C108, C111, C116, C124, C126	0.010810	8	0.086480
MC-0003-1196	Capacitor	C8, C14, C15, C18, C20, C49, C85, C153, C189, C215, C245, C259, C327, C373, C391, C392, C396, C553, C554	0.011570	19	0.219824
MC-0003-0076	Capacitor	C9	0.075056	1	0.075056
MC-0003-0177	Capacitor	C10	0.006610	1	0.006610
MC-0003-0176	Capacitor	C11	0.007825	1	0.007825
MC-0003-0098	Capacitor	C12, C205, C210	0.003649	3	0.010947

Print Date: 10.04.10
Print Time: 14:10

Table 9.3 SCPU-2 MIL-HDBK-217FN2 results for parts stress, DC 75% (cont'd)



Part Number	Category	Ref Des	Unit Failure Rate	Quantity	Total Failure Rate
MC-0000-0087	Capacitor	C11, C24, C25, C41, C44, C125, C133, C135, C137, C141, C143, C145, C159, C172, C178, C180, C182, C186, C188, C190, C194, C196	0.000051	22	0.111113
MC-0000-0100	Capacitor	C10, C17, C18, C21, C26, C27, C28, C29, C30, C31, C36, C37, C38, C39, C40, C41, C42, C43, C46, C47, C48, C53, C54, C55, C56, C57, C58, C61, C62, C63, C64, C65, C66, C68, C69, C71, C72, C74, C75, C77, C78, C80, C81, C83, C84, C86, C87, C89, C95, C92, C96,	0.004937	149	0.734165
MC-0000-1056	Capacitor	C32, C94	0.004277	2	0.008554
MC-0000-0071	Capacitor	C33, C35	0.003836	2	0.007671

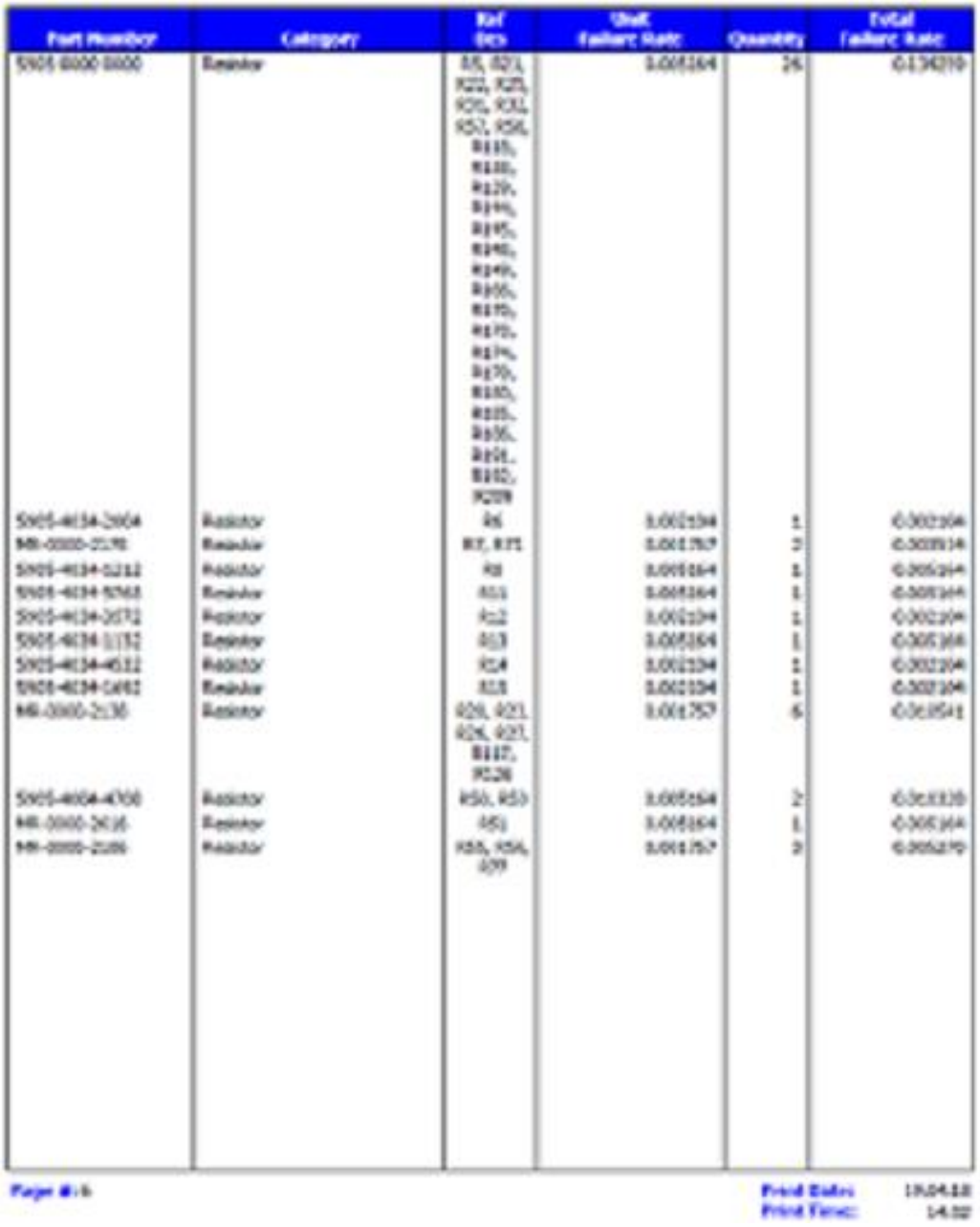
Print Date: 18.04.18
Print Time: 14:02

Table 9.3 SCPU-2 MIL-HDBK-217FN2 results for parts stress, DC 75% (cont'd)

Part Number	Category	Ref Des	Unit Failure Rate	Quantity	Total Failure Rate
5910-8450-0072	Capacitor	C51, C52, C58, C60, C67, C70, C71, C76, C79, C82, C88, C88	0.009905	12	0.118855
10072720	Capacitor	C84	0.012401	1	0.012401
5910-8451-0095	Capacitor	C93, C94, C95, C96, C97	0.009219	5	0.031095
MC-0000-0061	Capacitor	C112, C119	0.010471	2	0.020942
5910-7451-0091	Capacitor	C129, C130, C158, C168, C172, C183, C191, C197	0.009219	8	0.073752
MC-0000-0064	Capacitor	C145, C151, C175	0.009091	3	0.027272
MC-0000-0030	Capacitor	C211	0.009455	1	0.009455
MC-0000-0073	Capacitor	C222, C226, C227	0.010199	3	0.030596
5910-8000-2702	Capacitor	C254	0.009091	1	0.009091
10012990	Semiconductor	D1	0.004823	1	0.004823
MO-0000-0155	Optical Device	D5, D16, D20, D24, D27	0.002161	5	0.010807
MO-0000-0152	Optical Device	D3, D10, D11, D12, D13, D19, D21, D22, D23, D25, D26	0.002161	11	0.023776
MT-0000-0001	Semiconductor	D6, D7	0.014618	2	0.029235
MT-0000-0000	Semiconductor	D8, D15, D17	0.014618	3	0.043853
MT-0000-0412	Semiconductor	D9, D14, D18	0.014618	3	0.043853
5952-9900-0358	Inductor	F1, F2, F3, F4, F5, F6	0.009219	6	0.055312
ML-0000-0004	Inductor	F7, F12, F14, F15, F16	0.009219	5	0.046091
ML-0000-0008	Inductor	F8	0.009219	1	0.009219

Page #: 4 Print Date: 19.04.18
Print Time: 14:32

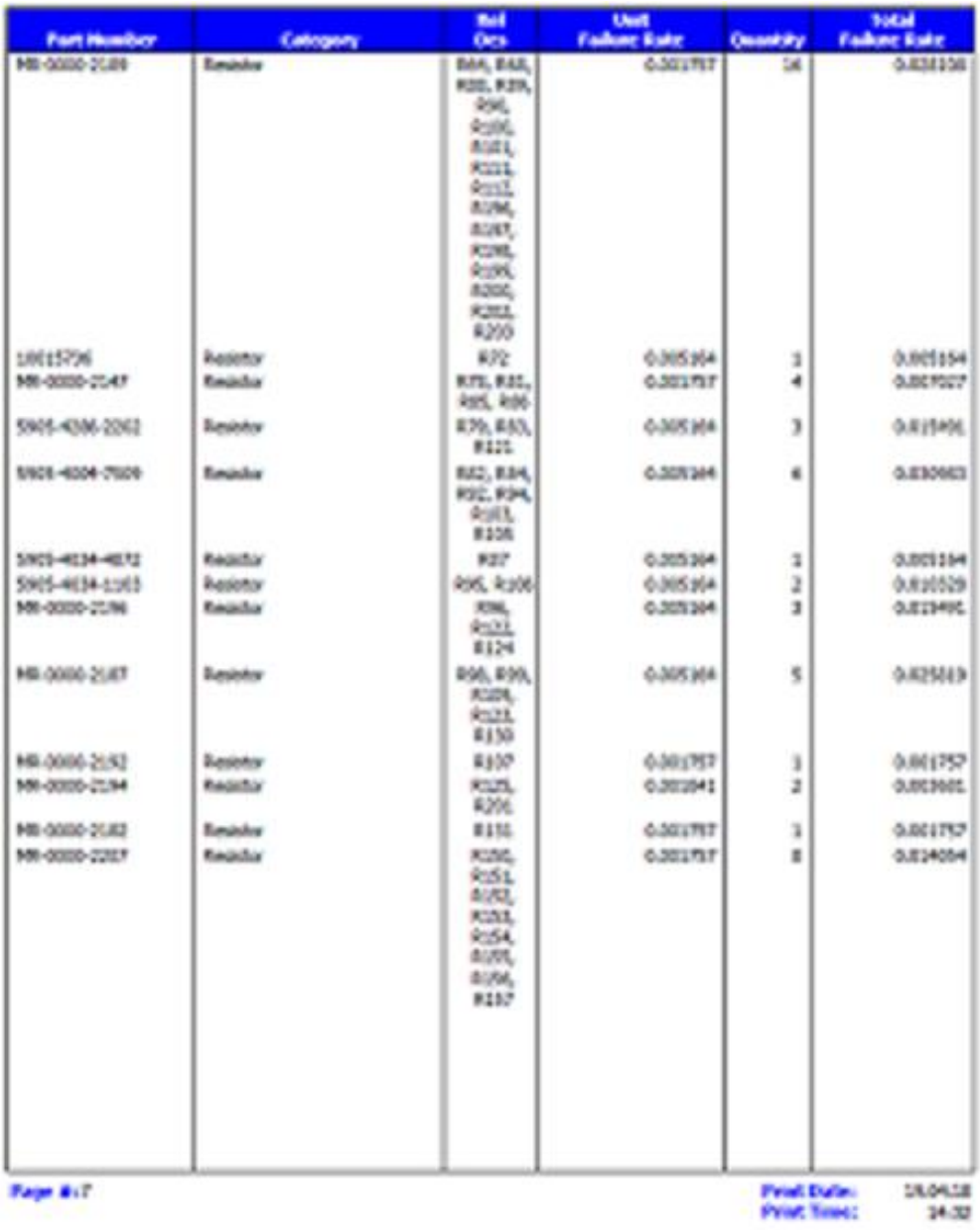
Table 9.3 SCPU-2 MIL-HDBK-217FN2 results for parts stress, DC 75% (cont'd)



Part Number	Category	Ref Des	Unit Failure Rate	Quantity	Total Failure Rate
5905-8000-0000	Resistor	R5, R21, R22, R25, R26, R32, R57, R58, R115, R118, R129, R144, R145, R148, R149, R155, R170, R171, R174, R179, R180, R185, R186, R191, R192, R209	0.005164	26	0.134210
5905-4034-2604	Resistor	R6	0.001594	1	0.001594
MR-0000-2178	Resistor	R7, R71	0.001757	2	0.003514
5905-4034-5212	Resistor	R8	0.005164	1	0.005164
5905-4034-5763	Resistor	R11	0.005164	1	0.005164
5905-4034-2671	Resistor	R12	0.001594	1	0.001594
5905-4034-1152	Resistor	R13	0.005164	1	0.005164
5905-4034-4512	Resistor	R14	0.001594	1	0.001594
5905-4034-5492	Resistor	R15	0.001594	1	0.001594
MR-0000-2136	Resistor	R20, R21, R24, R27, R117, R128	0.001757	6	0.010541
5905-4004-4700	Resistor	R50, R53	0.005164	2	0.010328
MR-0000-2618	Resistor	R51	0.005164	1	0.005164
MR-0000-2186	Resistor	R55, R56, R99	0.001757	3	0.005270

Print Date: 19.04.18
Print Time: 14.02

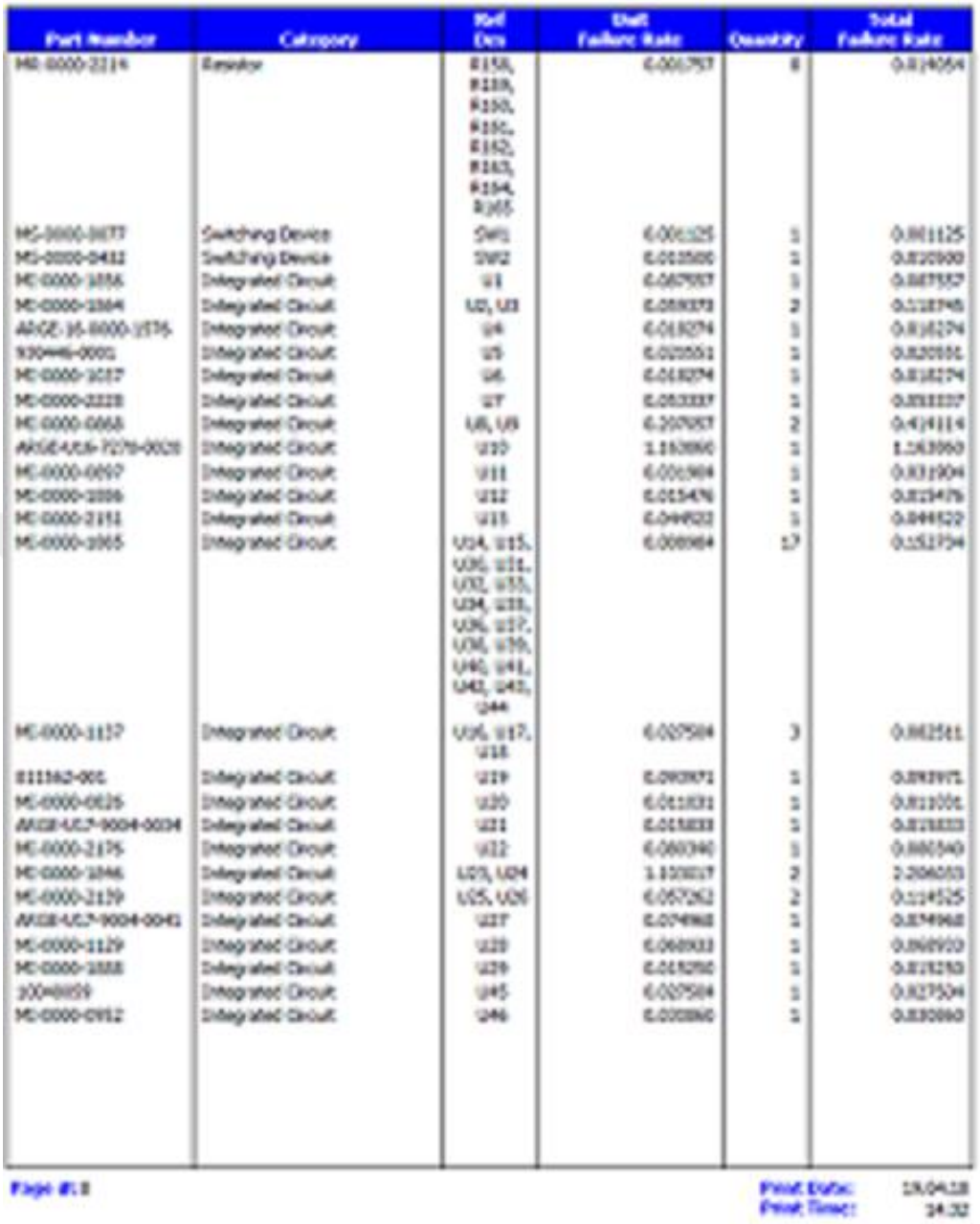
Table 9.3 SCPU-2 MIL-HDBK-217FN2 results for parts stress, DC 75% (cont'd)



Part Number	Category	Ref Des	Unit Failure Rate	Quantity	Total Failure Rate
MB-0000-2189	Resistor	R66, R68, R88, R89, R96, R100, R101, R111, R112, R186, R187, R188, R189, R200, R203, R210	0.001757	16	0.028108
10015726	Resistor	R72	0.005364	1	0.005364
MB-0000-2147	Resistor	R75, R81, R85, R86	0.001757	4	0.007027
5905-4586-2202	Resistor	R79, R83, R121	0.005364	3	0.016091
5905-4604-7509	Resistor	R82, R84, R92, R94, R103, R108	0.005364	6	0.032183
5905-4634-4872	Resistor	R87	0.005364	1	0.005364
5905-4634-1103	Resistor	R95, R106	0.005364	2	0.010729
MB-0000-2196	Resistor	R98, R113, R124	0.005364	3	0.016091
MB-0000-2187	Resistor	R99, R90, R109, R123, R150	0.005364	5	0.026819
MB-0000-2192	Resistor	R107	0.001757	1	0.001757
MB-0000-2194	Resistor	R125, R206	0.002041	2	0.003601
MB-0000-2182	Resistor	R151	0.001757	1	0.001757
MB-0000-2207	Resistor	R150, R151, R152, R153, R154, R155, R156, R157	0.001757	8	0.014054

Page #:7 Print Date: 18.04.18 Print Time: 14:32

Table 9.3 SCPU-2 MIL-HDBK-217FN2 results for parts stress, DC 75% (cont'd)



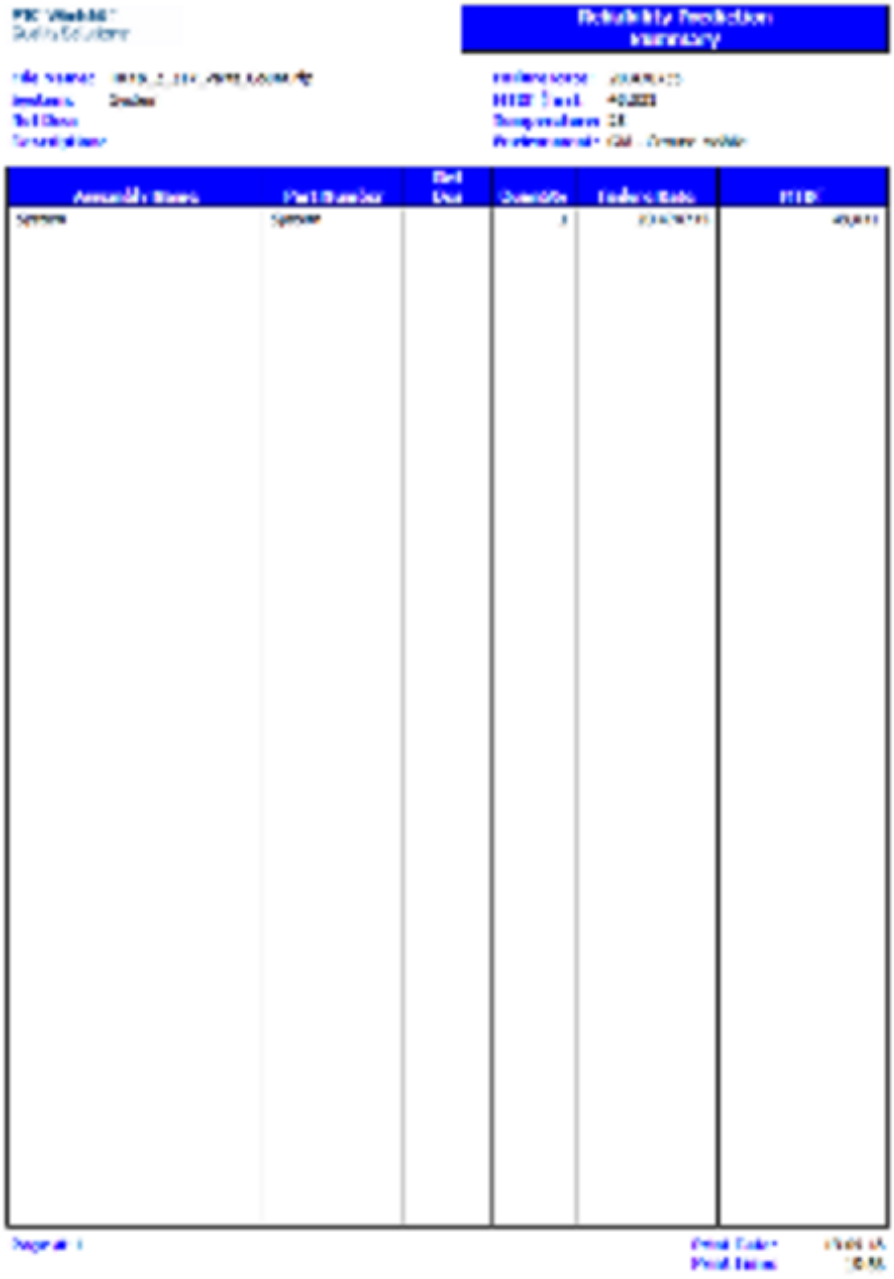
Part Number	Category	Ref Des	Unit Failure Rate	Quantity	Total Failure Rate
MI-0000-2214	Resistor	R158, R159, R160, R161, R162, R163, R164, R165	0.000757	8	0.006056
MC-0000-0677	Switching Device	SW1	0.001125	1	0.001125
MS-0000-0412	Switching Device	SW2	0.010500	1	0.010500
MI-0000-1056	Integrated Circuit	U1	0.067557	1	0.067557
MI-0000-1064	Integrated Circuit	U2, U3	0.059373	2	0.118746
AVGE-J6-0000-J376	Integrated Circuit	U4	0.018274	1	0.018274
930446-0001	Integrated Circuit	U5	0.020551	1	0.020551
MI-0000-1017	Integrated Circuit	U6	0.018274	1	0.018274
MI-0000-2228	Integrated Circuit	U7	0.033337	1	0.033337
MI-0000-0668	Integrated Circuit	U8, U9	0.207057	2	0.414114
AVGE-U16-P270-0020	Integrated Circuit	U10	1.163060	1	1.163060
MI-0000-0697	Integrated Circuit	U11	0.031904	1	0.031904
MI-0000-1006	Integrated Circuit	U12	0.013476	1	0.013476
MI-0000-2191	Integrated Circuit	U13	0.044522	1	0.044522
MI-0000-1065	Integrated Circuit	U14, U15, U16, U31, U32, U33, U34, U35, U36, U37, U38, U39, U40, U41, U42, U43, U44	0.008984	17	0.152734
MI-0000-1157	Integrated Circuit	U16, U17, U18	0.027504	3	0.082511
811362-001	Integrated Circuit	U19	0.093971	1	0.093971
MI-0000-0025	Integrated Circuit	U20	0.011031	1	0.011031
AVGE-U17-9004-0034	Integrated Circuit	U21	0.015833	1	0.015833
MI-0000-2175	Integrated Circuit	U22	0.080340	1	0.080340
MI-0000-1046	Integrated Circuit	U23, U24	1.103017	2	2.206033
MI-0000-2179	Integrated Circuit	U25, U26	0.057262	2	0.114525
AVGE-U17-9004-0041	Integrated Circuit	U27	0.074968	1	0.074968
MI-0000-1129	Integrated Circuit	U28	0.060933	1	0.060933
MI-0000-1088	Integrated Circuit	U29	0.018250	1	0.018250
300-8859	Integrated Circuit	U45	0.027504	1	0.027504
MI-0000-0912	Integrated Circuit	U46	0.030060	1	0.030060

Page #:8 Print Date: 18.04.28
Print Time: 14:32

9.1.2.2 SCPU-2 MIL-HDBK-217FN2 Parts Count Calculation Results, DC 75%

The method parts count is used when the design is not fixed. In this case, not all the parameters are known in the design, and the reliability engineers can provide a light to the design engineers. The results for the second SCPU show that the failure rate is less than 21 per million hours for the temperature 25^{o}C, Ground Mobile environment and the MTBF is a little more than 47000 hours for the DC 75%.

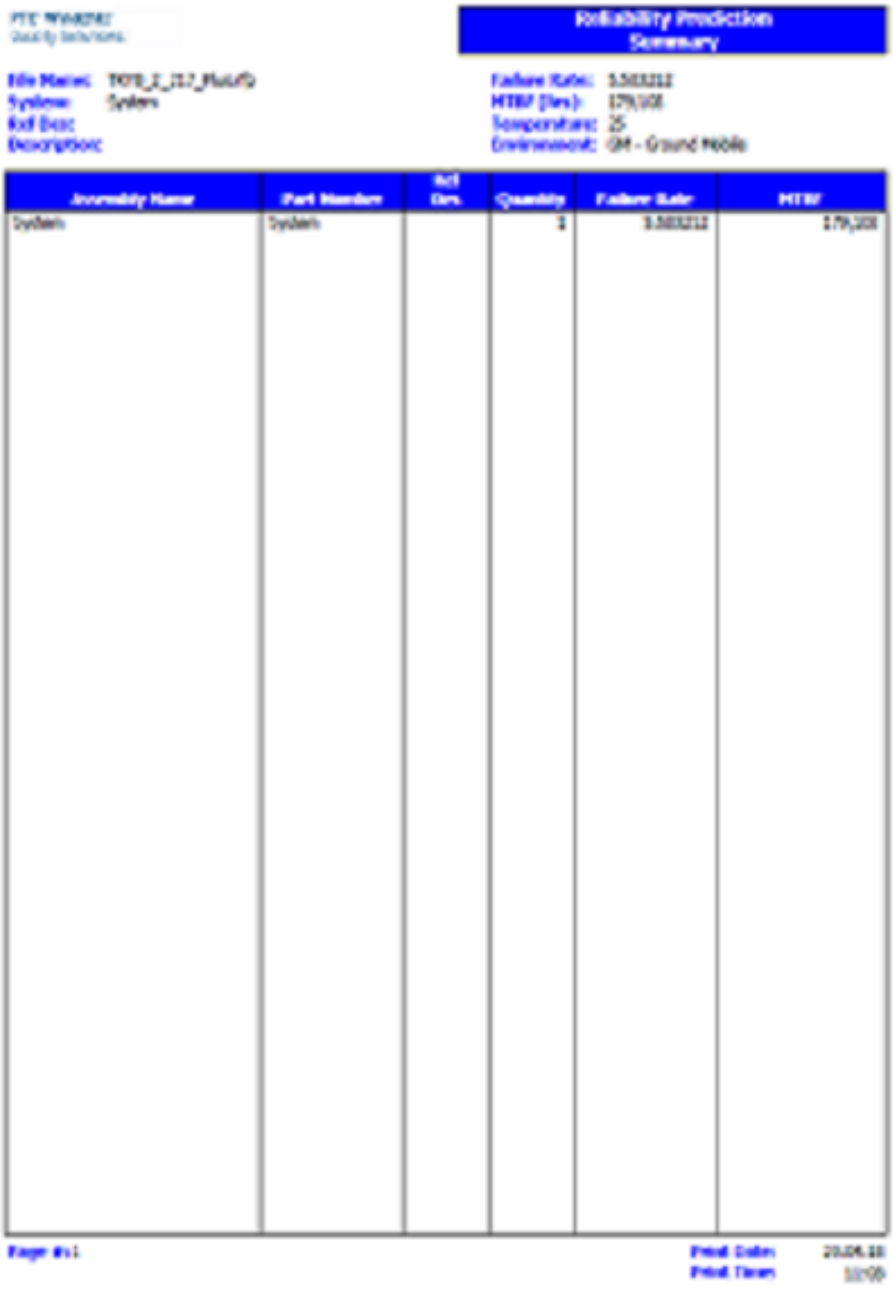
Table 9.4 SCPU-2 MIL-HDBK-217FN2 results for parts count, DC 75%



9.1.2.3 SCPU-2 217 PLUS Parts Stress Calculation Results, DC 75%

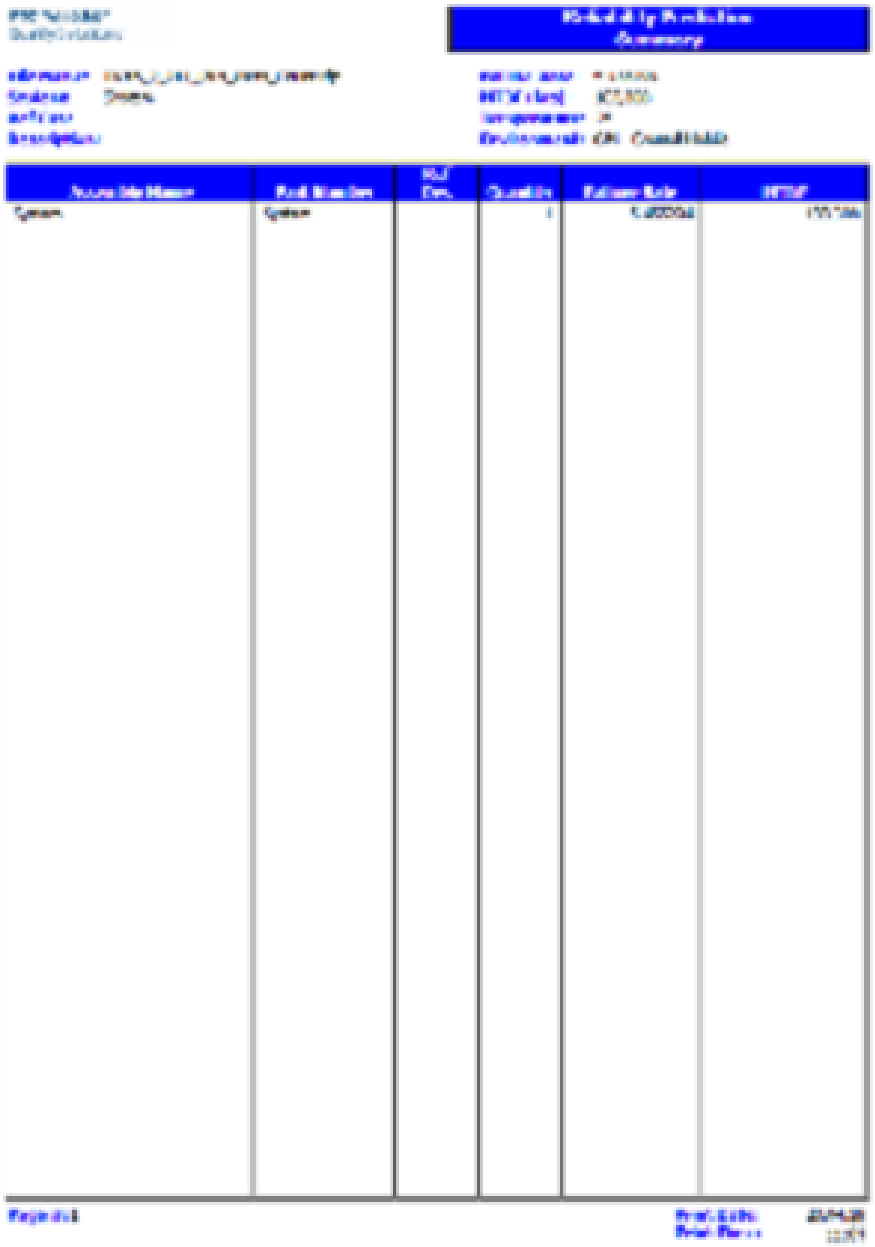
The calculations for the second SCPU show that the failure rate is less than 6 per million hours for the temperature 25ºC, Ground Mobile environment and the MTBF is a little more than 170000 hours for the DC 75% and parts stress method.

Table 9.5 SCPU-2 217Plus results for parts stress, DC 75%



9.1.2.4 SCPU-2 217 PLUS Parts Count Calculation Results, DC 75%

Table 9.6 SCPU-2 217Plus results for parts count, DC 75%



9.1.3 Reliability Calculation Results Summary

To have overall view of the different reliability prediction results following table is prepared.

Table 9.7 Reliability prediction results

Handbook	**217FN2**	**217FN2**	**217FN2**	**217FN2**	**217 Plus**	**217 Plus**	**217 Plus**	**217 Plus**
Method	Parts Count	Parts Count	Parts Stress	Parts Stress	Parts Count	Parts Count	Parts Stress	Parts Stress
Duty Cycle	100%	75%	100%	75%	100%	75%	100%	75%
Failure Rate [pmh] SCPU-1	3.405003	2.625682	2.881366	2.204989	0.87494	0.87494	1.002999	0.999608
Failure Rate [pmh] SCPU-2	26.780473	20.478735	19.446899	14.846355	5.455294	5.455294	5.695245	5.583212
MTBF [h] SCPU-1	293,685.50	380,853.43	347,057.61	453,517.00	1,142,935.52	1,142,935.52	997,009.97	1,000,392.15
MTBF [h] SCPU-2	37,340.64	48,831.14	51,422.08	67,356.60	183,308.18	183,308.18	175,585.07	179,108.37

The table below shows the comparison of results. It can firstly be concluded that 217 plus give more optimistic results about 2.5 times, secondly DC is an important parameter such that it affects 1.3 for the handbook MIL-217-FN2, thirdly the parts counts results are pessimistic than the parts stress method a s it takes worse case scenarios, and this difference is sharper for 217 Plus.

Table 9.8 Reliability prediction results comparison table

SCPU-1 and SCPU-2	**Handbook comparison**	**DC comparison for 217 FN2**	**Parts Count 75% vs Parts Stress 75% for 217 FN2**	**Parts Count 75% vs Parts Stress 75% for 217Plus**
Failure Rate [pmh] SCPU-1	2.205853695	1.306748469	1.190791428	3.293215535
Failure Rate [pmh] SCPU-2	2.659106443	1.309877003	1.379377969	3.564775611

9.2 Safety Calculation

9.2.1 Safety Calculations With Respect to IEC 61508 [2] Formulas

According to the IEC 61508 [2], following algebraic formula should be used when using 1oo2 system architecture.

$$PFH_G = 2\big((1-\beta_{\mathrm{D}})\big)\lambda_{\mathrm{DD}} + (1-\beta)\lambda_{\mathrm{DU}}(1-\beta)\lambda_{\mathrm{DU}}t_{CE} + \beta\lambda_{\mathrm{DU}} \qquad (9.1)$$

$$t_{ce} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \quad (9.2)$$

The common cause failure evaluation with respect to the international safety standard is given below.

Table 9.9 Dependant Failure Scoring Table

Item	subsystem		Evaluated	
	X_LS	Y_LS	X_LS	Y_LS
Separation/segregation				
Are all signal cables for the channels routed separately at all positions?	1.5	1.5	0	0
Are the logic subsystem channels on separate printed-circuit boards?	3.0	1.0	3	1
Are the logic subsystems physically separated in an effective manner? For example, in separate cabinets.	2.5	0.5	1	0.2
If the sensors/final elements have dedicated control electronics, is the electronics for each channel on separate printed-circuit boards?				
If the sensors/final elements have dedicated control electronics, is the electronics for each channel indoors and in separate cabinets?				
Diversity/redundancy				
Do the channels employ different electrical technologies for example, one electronic or programmable electronic and the other relay?	8.0		0	
Do the channels employ different electronic technologies for example, one electronic, the other programmable electronic?	6.0		0	
Do the devices employ different physical principles for the sensing elements for example, pressure and temperature, vane anemometer and Doppler transducer, etc?				
Do the devices employ different electrical principles/designs for example, digital and analogue, different manufacturer (not re-badged) or different technology?				
Is low diversity used, for example hardware diagnostic tests using the same technology?	2.0	1.0	2	1
Is medium diversity used, for example hardware diagnostic tests using different technology?	3.0	2.0	0	0
Were the channels designed by different designers with no communication between them during the design activities?	1.5	1.5	1.5	1.5
Are separate test methods and people used for each channel during commissioning?	1.0	0.5	1	0.5
Is maintenance on each channel carried out by different people at different times?	3.0		3	
Complexity/design/application/maturity/experience				
Does cross-connection between channels preclude the exchange of any information other than that used for diagnostic testing or voting purposes?	0.5	0.5	0.5	0.5
Is the design based on techniques used in equipment that has been used successfully in the field for > 5 years?	0.5	1.0	0	0
Is there more than 5 years experience with the same hardware used in similar environments?	1.0	1.5	0.5	0.5
Is the system simple, for example no more than 10 inputs or outputs per channel?		1.0		0
Are inputs and outputs protected from potential levels of over-voltage and over-current?	1.5	0.5	1.5	0.5
Are all devices/components conservatively rated (for example, by a factor of 2 or more)?	2.0		0.5	
Assessment/analysis and feedback of data				
Have the results of the failure modes and effects analysis or fault-tree analysis been examined to establish sources of common cause failure and have predetermined sources of common cause failure been eliminated by design?		3.0		1
Were common cause failures considered in design reviews with the results fed back into the design? (Documentary evidence of the design review activity is required.)		3.0		1
Are all field failures fully analyzed with feedback into the design? (Documentary evidence of the procedure is required.)	0.5	3.5	0	0
Procedures/human interface				
Is there a written system of work to ensure that all component failures (or degradations) are detected, the root causes established and other similar items inspected for similar potential causes of failure?		1.5		1.5
Are procedures in place to ensure that: maintenance (including adjustment or calibration) of any part of the independent channels is staggered, and, in addition to the manual checks carried out following maintenance, the diagnostic tests are allowed to run satisfactorily between the completion of maintenance on one channel and the start of maintenance on another?	1.5	0.5	1.5	0.5
Do the documented maintenance procedures specify that all parts of redundant systems (for example, cables, etc.) intended to be independent of each other, are not to be relocated?	0.5	0.5	0.5	0.5
Is all maintenance of printed-circuit boards, etc. carried out off-site at a qualified repair centre and have all the repaired items gone through a full pre-installation testing?	0.5	1.0	0.5	1
Does the system have low diagnostic coverage (60 % to 90 %) and report failures to the level of a field-replaceable module?	0.5		0	
Does the system have medium diagnostics coverage (90 % to 99 %) and report failures to the level of a field-replaceable module?	1.5	1.0	0	0
Does the system have high diagnostics coverage (>99 %) and report failures to the level of a field-replaceable module?	2.5	1.5	2.5	1.5
Do the system diagnostic tests report failures to the level of a field-replaceable module?				
Competence/training/safety culture				
Have designers been trained (with training documentation) to understand the causes and consequences of common cause failures?	2.0	3.0	1	1.5
Have maintainers been trained (with training documentation) to understand the causes and consequences of common cause failures?	0.5	4.5	0.2	2
Environmental control				
Is personnel access limited (for example locked cabinets, inaccessible position)?	0.5	2.5	0.5	2.5
Is the system likely to operate always within the range of temperature, humidity, corrosion, dust, vibration, etc., over which it has been tested, without the use of external environmental control?	3.0	1.0	3	1
Are all signal and power cables separate at all positions?	2.0	1.0	2	1
Environmental testing				
Has the system been tested for immunity to all relevant environmental influences (for example EMC, temperature, vibration, shock, humidity) to an appropriate level as specified in recognized standards?	10.0	10.0	1	1
SUM			27.2	21.7
S = X +Y			48.9	
S_D = X(Z+1)+Y			76.1	
Z			1	

Table 9.10 Value of Z – programmable electronics

Diagnostic coverage	Diagnostic test interval			
	Less than 1 min	Between 1 min and 5 min	Greater than 5 min	Evaluated
≥ 99 %	2.0	1.0	0.0	5 min --> 1.0
≥ 90 %	1.5	0.5	0.0	
≥ 60 %	1.0	0.0	0.0	

Table 9.11 Calculation of $ß_{int}$ and $ß_{Dint}$

Score (S or S_D)	Logic subsystem	Sensors or final elements	Evaluated S	Evaluated S_D
120 or above	0.50%	1%		
70 to 120	1%	2%		76.1 --> 0.02
45 to 70	2%	5%	48.9--> 0.02	
Less than 45	5%	10%		

Table 9.12 Calculation of ß for systems with levels of redundancy greater than 1oo2

Calculation of β for systems with levels of redundancy greater than 1oo2						Evaluated	β	$β_D$
MooN		N						
		2	3	4	5			
M	1	$β_{int}$	0,5 $β_{int}$	0,3 $β_{int}$	0,2 $β_{int}$	1oo2	0.02	0.02
	2	-	1,5 $β_{int}$	0,6 $β_{int}$	0,4 $β_{int}$			
	3	-	-	1,75 $β_{int}$	0,8 $β_{int}$			
	4	-	-	-	2 $β_{int}$			

Table 9.13 Resulted safety Calculation

Component	ß	ßd	λ	DC	λs	λd	λsd	λdd	λdu	SFF
	%	%	FIT	%	FIT	FIT	FIT	FIT	FIT	%
Channel A			2,204.9890	99.00	881.9956	1,322.9934	873.1756	1,309.7635	13.2299	99.400
Channel B			14,846.36	99.00	5,938.5420	8,907.8130	5,879.1566	8,818.7349	89.0781	99.400
Common Cause Fractions	2.00	2.00						101.2850	1.0231	

Accordingly, the PFH of SCL (Safety Critical Logic) for MIL HDBK 217 FN2, Parts Stress and DC 75% is found as 1.46E-09 [1/h]. The result is calculated as 4.61E-10 [1/h] for 217 Plus.

9.2.2 Safety Calculations With Respect to Conventional Markov Model

For the quantitative part of the safety, despite EN 50129 [17] defines some basic formulation concerning safety calculations regarding railway domain, IEC 61508 [2] provides formulas for quantitative analyses with respect to several architectures, however there is neither information nor reference about how these formulas are derived. Moreover, the formulas are only relevant for the homogenous configurations, i.e. in case the design utilizes diversity, the formulas are not applicable. Fuqua [20] explains Markov model from the reliability perspective, however no common cause faults (CCFs) are considered in this study. Kim et al. [21] analyses triple modular and dual system with

Markov model where all the modules are same and no CCF is considered for safety calculation. Chen et al [22] gives Markov state transition for homogenous redundant system without considering CCF. Zhang et al [23] apply Markov model to IEC 61508 [2] to analyze availability of systems with self-diagnostic components, but no diverse design is considered neither CCF is involved as stated in the paper. Considering the studies, it is revealed that a comprehensive study is lacking for the safety analyses of diverse system with consideration of common cause failures.

Markov model for 1oo2 used in the literature and in the industry is illustrated in this section. As expressed above, no exhaustive model is provided for the safety calculations considering the CCF and diverse design including all possible states. In [25], a Markov model is created as shown in and relevant formulas are provided. However, same as in the standard IEC 61508 [2] no diverse design is taken into account. Moreover, the transitions between states do not cover every possible condition.

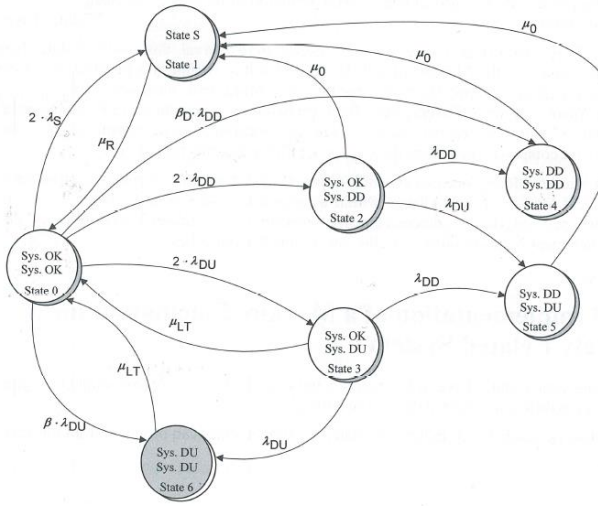


Figure 9.6 Markov model for 1oo2 architecture [25]

For the conventional approach where the new defined states are not provided, the result is calculated as 7.15E-09 [1/h]. It is 1.44E-09 [1/h] for 217 Plus.

9.2.3 Safety Calculation With Respect to Augmented Markov Model

The proposed model differs from the current models in given in IEC 61508 [2] and from the literature references given in previous chapter in several perspectives that are described below. Firstly, it places diverse design, which results in more states, but gives results that are more correct. It takes into account all possible transitions and states including safe failures and safe common cause failures, both detected and undetected. In

addition, new states such as “OK-SD”, “OK-DU&DD”, “OK-DU&SD” are defined of which detailed list is given in the fallowing part. Moreover, special attention is paid to the detected faults, which is one of the main contribution of this study. In case there is a DD transition while the unit is at DU state, the unit shall transit to DU&DD state. Similar is also valid for SD transition at DU state where the unit will transit to DU&SD state. In the current studies, these conditions are overlooked, however they are crucial since when these conditions are occurred, then the system will not go a failure state in case of the second unit fails undetected or a CCF happens, but the system will go to FS state as the fault is detected. By this way, a better safety performance is reached. On the other hand, if there exists a SU failure while the unit is at DU state, this will not change the safety performance since the failure is not detected and no counter-measure can be applied for safety. Moreover, indicating SU faults in different states are important for reliability and availability analyses, since in case of their occurrence, the system cannot perform its intended function, but this state does not cause a dangerous result. Thereof, to avoid state explosion, SU faults are shown in FS state. In case, there exist SU fault, the system moves to FS state, however, in any other case such as while the system is at OK-DU state, if SU occurs, the system cannot transform to FS since there is DU fault. CCF for safe failures are also required, because in previous studies the safe failures are simply added, however it is not correct since after adding failure rates, the CCF shall be subtracted, i.e. $AUB=A+B-(A\cap B)$, otherwise it would be considered two times in a wrong way. As in the dangerous failures, two different CCF are defined for the safe failures, namely safe detected and safe undetected.

For modelling, it is assumed that there is only one transition at a time step. 9. If DD occurs, the system will be placed into the state in such a short time that the probability of occurrence of other failures can be ignored. Furthermore, commenting the proof test interval T_1 is substantial, since if there are proof tests, it is impossible to state that the system is as new as once it was at the beginning of its mission-life. Dogruguven & Ustoglu (2018) shows that the contribution of a T_1 has relative low influence on the safety performance when compared to other parameters such as λ or DC, hence in this paper, T_1 has selected equal to life time of the system. For both items, rate for proof test and repair are set same. At the end of lifetime, the system can be shut down safely and therefore it will transit to the safe state. To evaluate safe CCF, the ratio λ_d / λ_s is considered. Likewise, for the ratio of detected safe CCF to undetected, the ratio β and β_D are used.

At first, possible states considering the explanations are defined along with the status of the modules in 1oo2 Architecture. The state of interest is the state where both units are failed, namely P14.

Table 9.14 Resulted States For 1oo2 Architecture

C1	C2	State	C1	C2	State
OK	OK	**P0**	SD	DD	**P19**
OK	DD	**P1**	SD	DU	**P20**
OK	DU	**P2**	SD	SD	**P21**
OK	SD	**P3**	SD	DU&DD	**P22**
OK	DU&DD	**P4**	SD	DU&SD	**P23**
OK	DU&SD	**P5**	DU&DD	OK	**P24**
DD	OK	**P6**	DU&DD	DD	**P25**
DD	DD	**P7**	DU&DD	DU	**P26**
DD	DU	**P8**	DU&DD	SD	**P27**
DD	SD	**P9**	DU&DD	DU&DD	**P28**
DD	DU&DD	**P10**	DU&DD	DU&SD	**P29**
DD	DU&SD	**P11**	DU&SD	OK	**P30**
DU	OK	**P12**	DU&SD	DD	**P31**
DU	DD	**P13**	DU&SD	DU	**P32**
DU	DU	**P14**	DU&SD	SD	**P33**
DU	SD	**P15**	DU&SD	DU&DD	**P34**
DU	DU&DD	**P16**	DU&SD	DU&SD	**P35**
DU	DU&SD	**P17**	FS		**P36**
SD	OK	**P18**			

Afterwards, the possible next different states are evaluated.

Table 9.15 States For 1oo2 Architecture

First State			Possible Diff. Next State			
State	C1	C2	C1	C2	State	Tr
P0	OK	OK	OK	DD	P1	λ_{2IDD}
P0			OK	DU	P2	λ_{2IDU}
P0			OK	SD	P3	λ_{2ISD}
P0			DD	OK	P6	λ_{1IDD}
P0			DU	OK	P12	λ_{1IDU}
P0			SD	OK	P18	λ_{1ISD}
P0			DU	DU	P14	λ_{CDU}
P0			DD	DD	P7	λ_{CDD}
P0			SD	SD	P21	λ_{CSD}
P0			FS		P36	$\lambda_{1SU} + \lambda_{2SU} - \lambda_{CSU}$
P1	OK	DD	FS		P36	μ_{OFS}
P2	OK	DU	OK	OK	P1	μ_{PR}
P2			OK	DU&DD	P4	λ_{2IDD}
P2			OK	DU&SD	P5	λ_{2ISD}
P2			DD	DU	P8	λ_{1IDD}
P2			DU	DU	P14	$\lambda_{1IDU} + \lambda_{CDU}$
P2			SD	DU	P20	λ_{1ISD}
P2			DD	DU&DD	P10	λ_{CDD}
P3	OK	SD	FS		P36	μ_{OFS}
P4	OK	DU&DD	FS		P36	μ_{OFS}
P5	OK	DU&SD	FS		P36	μ_{OFS}
P6	DD	OK	FS		P36	μ_{OFS}
P7	DD	DD	FS		P36	μ_{OFS}
P8	DD	DU	FS		P36	μ_{OFS}
P9	DD	SD	FS		P36	μ_{OFS}
P10	DD	DU&DD	FS		P36	μ_{OFS}
P11	DD	DU&SD	FS		P36	μ_{OFS}
P12	DU	OK	DU	DD	P13	λ_{2IDD}
P12			DU	DU	P14	λ_{2IDU}
P12			DU	SD	P15	λ_{2ISD}
P12			OK	OK	P0	μ_{PR}
P12			DU&DD	OK	P4	λ_{1IDD}
P12			DU&SD	OK	P5	λ_{1ISD}
P13	DU	DD	FS		P36	μ_{OFS}
P14	DU	DU	OK	OK	P0	μ_{PR}
P14			DU	DU&DD	P16	λ_{2IDD}
P14			DU	DU&SD	P17	λ_{2ISD}
P14			DU&DD	DU	P26	λ_{1IDD}
P14			DU&SD	DU	P32	λ_{1ISD}
P15	DU	SD	FS		P36	μ_{OFS}
P16	DU	DU&DD	FS		P36	μ_{OFS}
P17	DU	DU&SD	FS		P36	μ_{OFS}
P18	SD	OK	FS		P36	μ_{OFS}
P19	SD	DD	FS		P36	μ_{OFS}
P20	SD	DU	FS		P36	μ_{OFS}
P21	SD	SD	FS		P36	μ_{OFS}
P22	SD	DU&DD	FS		P36	μ_{OFS}
P23	SD	DU&SD	FS		P36	μ_{OFS}
P24	DU&DD	OK	FS		P36	μ_{OFS}
P25	DU&DD	DD	FS		P36	μ_{OFS}
P26	DU&DD	DU	FS		P36	μ_{OFS}
P27	DU&DD	SD	FS		P36	μ_{OFS}
P28	DU&DD	DU&DD	FS		P36	μ_{OFS}
P29	DU&DD	DU&SD	FS		P36	μ_{OFS}
P30	DU&SD	OK	FS		P36	μ_{OFS}
P31	DU&SD	DD	FS		P36	μ_{OFS}
P32	DU&SD	DU	FS		P36	μ_{OFS}
P33	DU&SD	SD	FS		P36	μ_{OFS}
P34	DU&SD	DU&DD	FS		P36	μ_{OFS}
P35	DU&SD	DU&SD	FS		P36	μ_{OFS}
P36	FS		OK	OK	P0	μ_{FSR}

Note that the blank cells show the same as above content. After having analysed, it is found that there are some states, which cannot be possible to be reached such as the state P22.

Table 9.16 Reachability Table

Root State	Final State	P12	P13	-	P30	P16	P36
P12	P0	P0	P14	-	P31	P17	P36
P14	P0	P2	P14	P14	P32	P18	P36
P36	P0	P12	P14	-	P33	P19	P36
P0	P1	P13	P15	-	P34	P20	P36
P2	P1	P14	P16	-	P35	P21	P36
P0	P2	P14	P17	P0	P36	P22	P36
P0	P3	P0	P18	P1	P36	P23	P36
P2	P4	-	P19	P3	P36	P24	P36
P12	P4	P2	P20	P4	P36	P25	P36
P2	P5	P0	P21	P5	P36	P26	P36
P12	P5	-	P22	P6	P36	P27	P36
P0	P6	-	P23	P7	P36	P28	P36
P0	P7	-	P24	P8	P36	P29	P36
P2	P8	-	P25	P9	P36	P30	P36
-	P9	P14	P26	P10	P36	P31	P36
P2	P10	-	P27	P11	P36	P32	P36
-	P11	-	P28	P13	P36	P33	P36
P0	P12	-	P29	P15	P36	P34	P36
						P35	P36

Therefore, these are reduced and finally the following table is obtained.

Table 9.17 Final States for 1oo2 Architecture

C1	C2	First State	Next State	Tr	C1	C2	First State	Next State	Tr
OK	OK	S0	S1		OK	DU&SD	S5	S21	μ_{OFS}
					DD	OK	S6	S21	μ_{OFS}
					DD	DD	S7	S21	μ_{OFS}
				λ_{2IDD}	DD	DU	S8	S21	μ_{OFS}
		S0	S2	λ_{2IDU}	DD	DU&DD	S9	S21	μ_{OFS}
		S0	S3	λ_{2ISD}	DU	OK	S10	S11	λ_{2IDD}
		S0	S6	λ_{1IDD}			S10	S12	λ_{2IDU}
		S0	S10	λ_{1IDU}			S10	S13	λ_{2ISD}
		S0	S16	λ_{1ISD}			S10	S0	μ_{PR}
		S0	S12	λ_{CDU}			S10	S4	λ_{1IDD}
		S0	S7	λ_{CDD}			S10	S5	λ_{1ISD}
		S0	S18	λ_{CSD}	DU	DD	S11	S21	μ_{OFS}
		S0	S21	$\lambda_{1SU} + \lambda_{2SU} - \lambda_{CSU}$	DU	DU	S12	S0	μ_{PR}
OK	DD	S1	S21	μ_{OFS}			S12	S14	λ_{2IDD}
OK	DU	S2	S1	μ_{PR}			S12	S15	λ_{2ISD}
							S12	S19	λ_{1IDD}
							S12	S20	λ_{1ISD}
		S2	S4	λ_{2IDD}	DU	SD	S13	S21	μ_{OFS}
		S2	S5	λ_{2ISD}	DU	DU&DD	S14	S21	μ_{OFS}
		S2	S8	λ_{1IDD}	DU	DU&SD	S15	S21	μ_{OFS}
		S2	S12	$\lambda_{1IDU} + \lambda_{CDU}$	SD	OK	S16	S21	μ_{OFS}
		S2	S17	λ_{1ISD}	SD	DU	S17	S21	μ_{OFS}
		S2	S9	λ_{CDD}	SD	SD	S18	S21	μ_{OFS}
OK	SD	S3	S21	μ_{OFS}	DU&DD	DU	S19	S21	μ_{OFS}
OK	DU&DD	S4	S21	μ_{OFS}	DU&SD	DU	S20	S21	μ_{OFS}
					FS		S21	S0	μ_{FSR}

The generalized transition table for the Markov model is illustrated below. Note that a special transition naming is used between states. Like Hungarian notation for clarifying the variable notation, this naming is very helpful to understand and implement any state machine approach such as Petri nets, Markovian model. The transition starts with lower case “t”, then the number showing the root state comes, hereafter and underscore “_” and finally the final state number. The implementation of the model is structured in this way, and then the transitions are assigned to special values such as “t0_21=$\lambda_{1SU} + \lambda_{2SU} - \lambda_{CSU}$”.

Table 9.18 Generalized transition table for the Markov model

C1	C2	First State	Next State	Tr	Tr in Matlab	Transition General	Outside From the State
OK	OK	**S0**	**S1**	λ_{2IDD}	l2idd	t0_1	-(t0_1+t0_2+t0_3+t0_6+t0_10+t0_16+t0_12+t0_7+t0_18+t0_21)
		S0	**S2**	λ_{2IDU}	l2idu	t0_2	
		S0	**S3**	λ_{2ISD}	l2isd	t0_3	
		S0	**S6**	λ_{1IDD}	l1idd	t0_6	
		S0	**S10**	λ_{1IDU}	l1idu	t0_10	
		S0	**S16**	λ_{1ISD}	l1isd	t0_16	
		S0	**S12**	λ_{CDU}	lcdu	t0_12	
		S0	**S7**	λ_{CDD}	lcdd	t0_7	
		S0	**S18**	λ_{CSD}	lcsd	t0_18	
		S0	**S21**	$\lambda_{1SU} + \lambda_{2SU} - \lambda_{CSU}$	l1su+l2su-lcsu	t0_21	
OK	DD	**S1**	**S21**	μ_{DFS}	mofs	t1_21	-(t1_21)
OK	DU	**S2**	**S1**	μ_{PR}	mpr	t2_1	-(t2_1+t2_4+t2_5+t2_8+t2_12+t2_17+t2_9)
		S2	**S4**	λ_{2IDD}	l2idd	t2_4	
		S2	**S5**	λ_{2ISD}	l2idd	t2_5	
		S2	**S8**	λ_{1IDD}	l1idd	t2_8	
		S2	**S12**	$\lambda_{1IDU} + \lambda_{CDU}$	l1idu+lcdu	t2_12	
		S2	**S17**	λ_{1ISD}	l1isd	t2_17	
		S2	**S9**	λ_{CDD}	lcdd	t2_9	
OK	SD	**S3**	**S21**	μ_{DFS}	mofs	t3_21	-(t3_21)
OK	DU&DD	**S4**	**S21**	μ_{DFS}	mofs	t4_21	-(t4_21)
OK	DU&SD	**S5**	**S21**	μ_{DFS}	mofs	t5_21	-(t5_21)
DD	OK	**S6**	**S21**	μ_{DFS}	mofs	t6_21	-(t6_21)
DD	DD	**S7**	**S21**	μ_{DFS}	mofs	t7_21	-(t7_21)
DD	DU	**S8**	**S21**	μ_{DFS}	mofs	t8_21	-(t8_21)
DD	DU&DD	**S9**	**S21**	μ_{DFS}	mofs	t9_21	-(t9_21)
DU	OK	**S10**	**S11**	λ_{2IDD}	l2idd	t10_11	-(t10_11)
		S10	**S12**	λ_{2IDU}	l2idu	t10_12	-(t10_12)
		S10	**S13**	λ_{2ISD}	l2isd	t10_13	-(t10_13)
		S10	**S0**	μ_{PR}	mpr	t10_0	-(t10_0)
		S10	**S4**	λ_{1IDD}	l1idd	t10_4	-(t10_4)
		S10	**S5**	λ_{1ISD}	l1isd	t10_5	-(t10_5)
DU	DD	**S11**	**S21**	μ_{DFS}	mofs	t11_21	-(t11_21)
DU	DU	**S12**	**S0**	μ_{PR}	mpr	t12_0	-(t12_0)
		S12	**S14**	λ_{2IDD}	l2idd	t12_14	-(t12_14)
		S12	**S15**	λ_{2ISD}	l2isd	t12_15	-(t12_15)
		S12	**S19**	λ_{1IDD}	l1idd	t12_19	-(t12_19)
		S12	**S20**	λ_{1ISD}	l1isd	t12_20	-(t12_20)
DU	SD	**S13**	**S21**	μ_{DFS}	mofs	t13_21	-(t13_21)
DU	DU&DD	**S14**	**S21**	μ_{DFS}	mofs	t14_21	-(t14_21)
DU	DU&SD	**S15**	**S21**	μ_{DFS}	mofs	t15_21	-(t15_21)
SD	OK	**S16**	**S21**	μ_{DFS}	mofs	t16_21	-(t16_21)
SD	DU	**S17**	**S21**	μ_{DFS}	mofs	t17_21	-(t17_21)
SD	SD	**S18**	**S21**	μ_{DFS}	mofs	t18_21	-(t18_21)
DU&DD	DU	**S19**	**S21**	μ_{DFS}	mofs	t19_21	-(t19_21)
DU&SD	DU	**S20**	**S21**	μ_{DFS}	mofs	t20_21	-(t20_21)
FS		**S21**	**S0**	μ_{FSR}	mfsr	t21_0	-(t21_0)

In following, transition matrix is created with the generalized illustration.

Table 9.19 Generalized transition matrix

Root State	Final State	Transition General	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
S10	**S0**	t10_0	0	0	0	0	0	0	0	0	0	0	t10_0	0	t12_0	0	0	0	0	0	0	0	0	t21_0
S12	**S0**	t12_0																						
S21	**S0**	t21_0																						
S0	**S1**	t0_1	t0_1	0	t2_1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S2	**S1**	t2_1																						
S0	**S2**	t0_2	t0_2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S0	**S3**	t0_3	t0_3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S2	**S4**	t2_4	0	t0_3	0	0	0	0	0	0	0	0	t10_4	0	0	0	0	0	0	0	0	0	0	0
S10	**S4**	t10_4																						
S2	**S5**	t2_5	0	0	t2_5	0	0	0	0	0	0	0	t10_5	0	0	0	0	0	0	0	0	0	0	0
S10	**S5**	t10_5																						
S0	**S6**	t0_6	t0_6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S0	**S7**	t0_7	t0_7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S2	**S8**	t2_8	0	0	t2_8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S2	**S9**	t2_9	0	0	t2_9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S0	**S10**	t0_10	t0_10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S10	**S11**	t10_11	0	0	0	0	0	0	0	0	0	0	t10_11	0	0	0	0	0	0	0	0	0	0	0
S0	**S12**	t0_12	t0_12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S2	**S12**	t2_12	0	0	t2_12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S10	**S12**	t10_12	0	0	0	0	0	0	0	0	0	0	t10_12	0	0	0	0	0	0	0	0	0	0	0
S10	**S13**	t10_13	0	0	0	0	0	0	0	0	0	0	0	t11_13	0	0	0	0	0	0	0	0	0	0
S12	**S14**	t12_14	0	0	0	0	0	0	0	0	0	0	0	0	t12_14	0	0	0	0	0	0	0	0	0
S12	**S15**	t12_15	0	0	0	0	0	0	0	0	0	0	0	0	t12_15	0	0	0	0	0	0	0	0	0
S0	**S16**	t0_16	t0_16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S2	**S17**	t2_17	0	0	t2_17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S0	**S18**	t0_18	t0_18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S12	**S19**	t12_19	0	0	0	0	0	0	0	0	0	0	0	0	t12_19	0	0	0	0	0	0	0	0	0
S12	**S20**	t12_20	0	0	0	0	0	0	0	0	0	0	0	0	t12_20	0	0	0	0	0	0	0	0	0
S0	**S21**	t0_21	t0_21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S1	**S21**	t1_21	t1_21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S3	**S21**	t3_21	0	0	0	t3_21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S4	**S21**	t4_21	0	0	0	0	t4_21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S5	**S21**	t5_21	0	0	0	0	0	t5_21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S6	**S21**	t6_21	0	0	0	0	0	0	t6_21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S7	**S21**	t7_21	0	0	0	0	0	0	0	t7_21	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S8	**S21**	t8_21	0	0	0	0	0	0	0	0	t8_21	0	0	0	0	0	0	0	0	0	0	0	0	0
S9	**S21**	t9_21	0	0	0	0	0	0	0	0	0	t9_21	0	0	0	0	0	0	0	0	0	0	0	0
S11	**S21**	t11_21	0	0	0	0	0	0	0	0	0	0	0	t11_21	0	0	0	0	0	0	0	0	0	0
S13	**S21**	t13_21	0	0	0	0	0	0	0	0	0	0	0	0	0	t13_21	0	0	0	0	0	0	0	0
S14	**S21**	t14_21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	t14_21	0	0	0	0	0	0	0
S15	**S21**	t15_21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	t15_21	0	0	0	0	0	0
S16	**S21**	t16_21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	t16_21	0	0	0	0	0
S17	**S21**	t17_21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	t17_21	0	0	0	0
S18	**S21**	t18_21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	t18_21	0	0	0
S19	**S21**	t19_21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	t19_21	0	0
S20	**S21**	t20_21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	t20_21	0

Transition matrix for in-to and out-from the states is shown below.

Table 9.20 Final in and out states

State	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
S0	-(t0_1+t0_2+t0_3+t0_6+t0_10+t0_16+t0_12+t0_7+t0_18+t0_21)	0	0	0	0	0	0	0	0	0	t10_0	0	t12_0	0	0	0	0	0	0	0	0	t21_0
S1	t0_1	-(t1_21)	t2_1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S2	t0_2	0	-(t2_1+t2_4+t2_5+t2_8+t2_12+t2_17+t2_9)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S3	t0_3	0	0	-(t3_21)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S4	0	t0_3	0	0	-(t4_21)	0	0	0	0	0	t10_4	0	0	0	0	0	0	0	0	0	0	0
S5	0	0	t2_5	0	0	-(t5_21)	0	0	0	0	t10_5	0	0	0	0	0	0	0	0	0	0	0
S6	t0_6	0	0	0	0	0	-(t6_21)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S7	t0_7	0	0	0	0	0	0	-(t7_21)	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S8	0	0	t2_8	0	0	0	0	0	-(t8_21)	0	0	0	0	0	0	0	0	0	0	0	0	0
S9	0	0	t2_9	0	0	0	0	0	0	-(t9_21)	0	0	0	0	0	0	0	0	0	0	0	0
S10	t0_10	0	0	0	0	0	0	0	0	0	-(t10_11+t10_12+t10_13+t10_0+t10_4+t10_5)	0	0	0	0	0	0	0	0	0	0	0
S11	0	0	0	0	0	0	0	0	0	0	t10_11	-(t11_21)	0	0	0	0	0	0	0	0	0	0
S12	t0_12	0	t2_12	0	0	0	0	0	0	0	t10_12	0	-(t12_0+t12_14+t12_15+t12_19+t12_20)	0	0	0	0	0	0	0	0	0
S13	0	0	0	0	0	0	0	0	0	0	t10_13	0	0	-(t13_21)	0	0	0	0	0	0	0	0
S14	0	0	0	0	0	0	0	0	0	0	0	0	t12_14	0	-(t14_21)	0	0	0	0	0	0	0
S15	0	0	0	0	0	0	0	0	0	0	0	0	t12_15	0	0	-(t15_21)	0	0	0	0	0	0
S16	t0_16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-(t16_21)	0	0	0	0	0
S17	0	0	t2_17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-(t17_21)	0	0	0	0
S18	t0_18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-(t18_21)	0	0	0
S19	0	0	0	0	0	0	0	0	0	0	0	0	t12_19	0	0	0	0	0	0	-(t19_21)	0	0
S20	0	0	0	0	0	0	0	0	0	0	0	0	t12_20	0	0	0	0	0	0	0	-(t20_21)	0
S21	t0_21	t1_21	0	t3_21	t4_21	t5_21	t6_21	t7_21	t8_21	t9_21	0	t11_21	0	t13_21	t14_21	t15_21	t16_21	t17_21	t18_21	t19_21	t20_21	-(t21_0)

A similar work is realized for the 217 Plus calculation, however it is not necessary to show this as twice in this study, since the method followed is the same.

The analysis according to the new proposed Markov Analysis gives the PFH of SCL (Safety Critical Logic) for MIL HDBK 217 FN2, Parts Stress and DC 75% as 4.24E-10 [1/h]. It is 1.34E-10 [1/h] for 217 Plus.

Table 9.21 Resulted safety Calculation

Model	**IEC 61508**		**Conventional Markov Model**		**Proposed Model**	
Method	217FN2 DC 75%	217 Plus DC 75%	217FN2 DC 75%	217 Plus DC 75%	217FN2 DC 75%	217 Plus DC 75%
Failure Rate SCCU [1/h]	1.46E-09	4.61E-10	7.15E-09	1.44E-09	4.24E-10	1.34E-10

The outcomes for the SCC show that the proposed model conducts 3.44 times better PFH than the IEC 61508 [2] standard and 16.86 times better than the conventional Markov model in the literature for the reliability prediction with respect to MIL-HDBK-217FN2 and DC 75%.

9.3 A Further Improvement of the PFH

It is defined in IEC 61508-6 [2] that the diagnostic testing functions which continuously compares the operation of the PE system with predefined states may be thought of as an additional, and partially diverse, channel running in parallel with the PE system. Further, cross monitoring between channels also can be carried out for revealing non-simultaneous common cause failures where systems remain in the same state for long periods. With PE system technology, cross monitoring may be carried out with a high repetition frequency. Regarding this information, an FTA can be drawn as fallows. Here, instead of Markov, FTA is selected, because in other case, various parameters should be defined, however to evaluate the correctness of these parameters would be disputable.

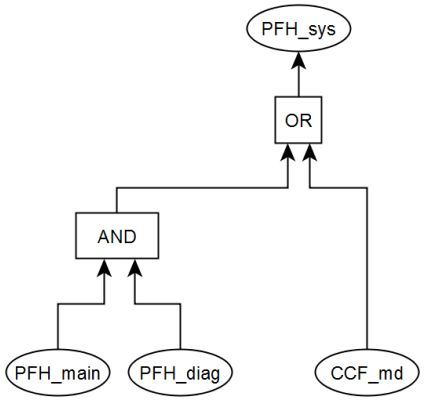


Figure 9.7 Consideration of diagnostic as diverse channel

The use of FTA will show worst-case scenario, since no segregation between safe and unsafe faults are evaluated, instead all faults are assumed dangerous and undetected which results in worst-case scenario.

Table 9.22 Further improved PFH

Model / Failure Rates	Initial PFH		Common Cause Failure	Improved PFH
IEC 61508	217FN2	1.46E-09	2.92E-11	2.92E-11
	217 Plus	4.61E-10	9.22E-12	9.22E-12
Conventional Markov Model	217FN2 DC 75%	7.15E-09	1.43E-10	1.43E-10
	217 Plus	1.44E-09	2.88E-11	2.88E-11
Proposed Model	217FN2 DC 75%	4.24E-10	8.48E-12	8.48E-12
	217 Plus DC 75%	1.34E-10	2.68E-12	2.68E-12

9.4 Safety-Related Communication and Its Calculation

As the safety critical system consists of not only computing unit but also other components, safety related communication should be designed between them. For instance, Figure 9.8 illustrates an overview for a communication inside on-board, between on-board and trackside and inside trackside.

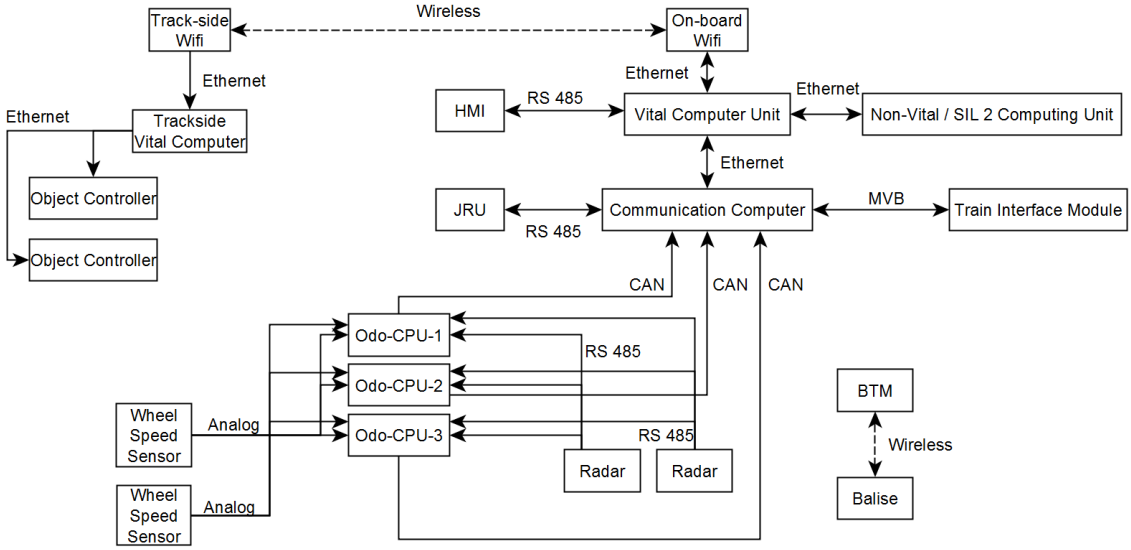


Figure 9.8 Communication System

For instance, the communication between HMI and Vital Computer is to be SIL 4 due to arguments mentioned previously in this study. In this case, a safe communication shall be built between these constituents. The standard [19] defines threats and defences for a safe communication as in Table 9.23.

Table 9.23 Threats/Defences matrix [19]

Threats	Defences							
	Sequence number	Time stamp	Time-out	Source and destination identifiers	Feed-back message	Identification procedure	Safety code	Cryptographic techniques
Repetition	X	X						
Deletion	X							
Insertion	X			X [a]	X [b]	X [b]		
Re-sequence	X	X						
Corruption							X [c]	X
Delay		X	X					
Masquerade					X [b]	X [b]		X [c]

[a] Only applicable for source identifier.
Will only detect insertion from invalid source.
If unique identifiers cannot be determined because of unknown users, a cryptographic technique shall be used, see 7.3.8.

[b] Application dependent.

[c] See 7.4.3 and Clause C.2.

For such a communication, sequence numbering can be used against repetition, deletion, insertion and resequencing while time stamp could be utilized against delay. A safety code is needed for corruption and it has be designed. No measure against masquerade are needed to be taken according to the category definition Table 9.24 and category threat matrix.

Table 9.24 Categories of transmission systems [19]

Category	Main characteristics	Example transmission systems
Category 1	Designed for known and fixed maximum number of participants. All properties of the transmission system are known and invariable during the lifetime of the system. Negligible opportunity for unauthorised access.	Close air-gap transmission (e.g. track balise to train antenna). Proprietary serial bus internal to the safety-related system (e.g. PROFIBUS, CAN, MVB (multi purpose vehicle bus defined by IEC)). Industry-standard LAN connecting different equipment (safety-related and non safety-related) within a single system, subject to fulfilment and maintenance of the preconditions.
Category 2	Properties are unknown, partially unknown or variable during the lifetime of the system. Limited scope for extension of user group. Known user group or groups. Negligible opportunity for unauthorised access (networks are trusted). Occasional use of non-trusted networks.	Proprietary serial bus internal to the safety-related system (e.g. PROFIBUS, MVB), but with the possibility that the transmission system could be reconfigured or substituted by another transmission system during the lifetime. Industry-standard LAN connecting different systems (safety-related and non safety-related) within a controlled and limited area. WAN belonging to the railway, connecting different systems (safety-related and non safety-related) at various locations. Switched circuit in public telephone network, used occasionally and at unpredictable times (e.g. dial-up remote diagnostic of an interlocking system). Leased permanent point-to-point circuit in public telecom network. Radio transmission system with restricted access (e.g. use of wave guides or leaky cables with a link budget limiting the possibility of reception to a close transceiver only, or using a proprietary scheme of modulation, impossible to reproduce with off the shelf or affordable lab equipment).
Category 3	Properties are unknown, partially unknown or variable during the lifetime of the system. Unknown multiple users groups. Significant opportunity for unauthorised access.	Packet switched data in public telephone network. Internet. Circuit switched data radio (e.g. GSM-R). Packet switched data radio (e.g. GPRS). Short range broadcast radio (e.g. Wi-fi). Radio transmission systems without restrictions.

Table 9.25 Threat/Category relationship [19]

Category	Repetition	Deletion	Insertion	Re-sequence	Corruption	Delay	Masquerade
Cat. 1	+	+	+	+	++	+	-
Cat. 2	++	++	++	+	++	++	-
Cat. 3	++	++	++	++	++	++	++

Key

- \- Threat can be neglected.
- \+ Threat exists, but rare; weak countermeasures sufficient.
- ++ Threat exists; strong countermeasures required.

NOTE This matrix of threats is only a guide – analysis will always be necessary to determine whether countermeasures are required and to what degree. Each threat will be dependent on network type, application and configuration.

A model of the telegram including safety code to be created is shown in Figure 9.9.

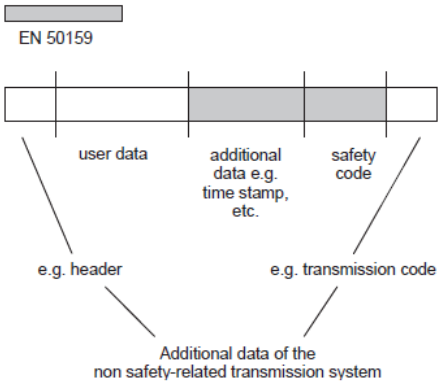


Figure 9.9 Model of message representation within the transmission system [19].

For the length of the safety code following formulas are given in this standard.

$$R_{H1} + R_{H2} + R_{H3} \leq R_H \tag{9.1}$$

$$R_{HW} \times p_{US} \times k_1 = R_{H1} \tag{9.2}$$

$$p_{UT} \times p_{US} \times f_w = R_{H2} \tag{9.3}$$

$$k_2 \times p_{US} \times \frac{1}{T} = R_{H3} \tag{9.4}$$

$$k_1 \geq n \times m \tag{9.5}$$

Because it cannot be assumed that the failure is random, it is necessary to take into account a safety margin m in the factor k_1 and therefore k_1 is recommended to be calculated as above. The factor m represents the safety margin with $m \geq 5$. The maximum frequency of wrong messages f_W can be estimated by the worst-case estimation as below.

$$f_W = f_M \tag{9.6}$$

The maximum value of p_{UT} may be estimated as

$$p_{UT} = 2^{-b} \tag{9.7}$$

$k_2 = 10^{-4}$ can be taken as mentioned in the standard.

For the maximum probability for undetected errors of the safety code with c digits the estimation is given as:

$$p_{US} = 2^{-c} \tag{9.8}$$

If other codes are used, e.g. a combination of two codes, the worst case blocks error probability using the model of “binary symmetric channel" should be taken. Binary

symmetric channel means with probability p a received bit is falsified (0→1 and 1→0). Each bit is independent from each other.

According to the formulas and assumption, the hazard rate of the communication between VCU and DMI will be calculated below where the CRC number is selected as 64 bit.

R_{HW} is assumed considering the reliability calculations in this thesis and number of consecutive corrupted messages until the safe fallback state is entered is selected 4. Cycle time between two consecutive messages is selected as 50 milliseconds. T can be calculated as n times cycle time.

$$R_{HW} = 1\mathrm{E} - 6 \tag{9. 9}$$

$$p_{US} = 2^{-64} = 5.42101\mathrm{E} - 20 \tag{9.10}$$

$$1\mathrm{E} - 6 \times (5.42101\mathrm{E} - 20) \times 4 = 1.08E - 24 = R_{H1} \tag{9.11}$$

$$\mathrm{b} = -1 \tag{9.12}$$

$$\mathrm{f}_M = \frac{1}{50}\mathrm{x}1000\mathrm{x}\,3600 = \frac{72000}{h} = \mathrm{f}_W \tag{9.13}$$

$$0.5 \times (5.42101\mathrm{E} - 20) \times 72000 = 1.95156\mathrm{E} - 15 = R_{H2} \tag{9.14}$$

$$10^{-4} \times 2^{-64} \times 18000 = 9.75782\mathrm{E} - 20 = R_{H3} \tag{9.15}$$

$$R_{H\_total} = R_{H1} + R_{H2} + R_{H3} = 1.95\mathrm{E} - 15\ [1/\mathrm{h}] \tag{9.16}$$

Note that if c is 48, R_{H_total}= 1.28E-10 [1/h] and if c is 32, R_{H_total}= 8.38E-06 [1/h]. Considering these results and THR allocation discussed at the beginning of this study, 64 bit CRC is chosen for the safe communication between DMI and VCU.

CHAPTER 10

RESULTS AND DISCUSSION

In this dissertation, quantitative and qualitative methods to design mission critical safe and reliable controller with very low average frequency of a dangerous failure are researched. For a safety related system, firstly the system under development shall be cognized precisely to set correct RAMS requirements. Thereof, characteristics of the application domain are analysed at the beginning of this thesis. It has been compared and showed that there are inconsistencies in the international standards, directives, harmonization requirements, tender documents and assessment sector. This issue is discussed in [100], which is published by the author in the scope of this thesis. Accordingly, the quantitative requirement for the THR is derived taking into account different approaches. Hereafter, the THR is allocated to subsystems including mission critical safe computer platform.

After THR apportionment, the certification procedure is explained in this study, since there are many actors and there are so many unknown points for the procedure. This part provides to the reader to make sense of the complex procedures. To be able to come to the quantitative calculations, RAMS background is prepared including with the details of the dependant failures. These chapters are essential and distilled in a form as a report utilizing several resources for understanding the specific application domain railway and generic application of RAMS.

Developing safety critical systems require long years of planned investments, broad theoretical knowledge and domain experience. Data interchange between CPUs, synchronization, computation speed and diagnostic measures shall exhaustively be evaluated along with the effects of the parameters used in the reliability and safety calculations ex tunc. Therefore, following THR apportionment, this study focuses on the effects of calculation parameters for different architectures. Special attention is paid for

the architecture 1oo2D regarding its model and normative definition. In this part, a new architecture with its definition is proposed. It has also been revealed that there are correlations between some parameters, which seem independent from each other. An advising route map is created newly to observe what kind of methods can be applied to decrease the hazard rates. The results are published in [101].

Since calculation of safety parameters can only be performed after reliability analyses, these analyses are realized before safety evaluations. The reliability analyses are explained and discussed exhaustively in chapter RELIABLITY CALCULATION. Their correctness is crucial for the correctness of the safety parameters as safety parameters are derived from reliability parameters. Afterwards, information about the tool that is utilized for the reliability calculation is given.

Subsequently, an innovative generic calculation model is proposed to respond to the challenging quantitative requirements for the safety critical computer designed with state of the art technology. The proposed model differs from the current models in several ways such as defining new states as explained in chapter “Safety Calculation”. The results of the proposed model are compared with the current models and with the international safety standard. It has been proven that the proposed model conducts 3.44 times better PFH than the IEC 61508 [2] standard and 16.86 times better than the conventional Markov model in the literature for the reliability prediction with respect to MIL-HDBK-217FN2 and DC 75%. The innovative model is published in [102]. Further researches after augmented Markovian modelling are realized for the purpose of increase the safety performance. Consequently, a PFH of 2.18E-12 [1/h] for the safety computer platform could be reached. This value is close to CBTC requirement PFH_{COBC} that is allocated as 1,125E-12 [1/h] and ERTMS requirement PFH_{EOBC} that is found as 1E-12 [1/h] in the second part of this study. At this stage, there are two options to cover the requirements exactly. The first option is to enhance the reliability of the safety platform, which can be realized by re-consideration of the route map in [101]. The second option is to re-allocate the safety requirement to the subsystems, which would result better safety performance requirements for the remaining parts of the safety critical functions given in the aforementioned section.

In addition to the exhaustive quantitative work, the qualitative aspects for the safety critical system development process are examined in the scope of this study since the safety case which is subject to the safety certification contains safety management part

beside technical safety report. The safety management plays a major role to keep the tough safety critical development process under control by avoiding systematic faults. Setting up correct organizational structure as well as applying Verification & Validation (V&V) concepts, which are two fundamental elements of safety management, in an accurate way are therefore inevitable. In this context, the paper [103] discusses railway safety management in terms of organizational structure and V&V with regards to the current normative status with its drawbacks. Proposals are provided for an updated organization and more harmonized V&V concepts including relations with safety management and quality assurance by sharing practical experiences.

Finally, the main international functional safety standard IEC 61508 [2] and its railway derivations EN 50126 [16], 50128 and 50129, which are followed during the development of a safety critical system or product are evaluated in [104]. Although being developed for long years, when used these norms, it has been revealed that there are still several inconsistencies. The existence of these inconsistencies is possible, since there are too much data and too many requirements. With this study, it is aimed to support the enhancements of these detailed international norms for better understanding utilizing practical experience. Failure and hazard analysis methods, subjective approaches that result in unequal market competition for techniques and measures in standards, tool usage, common cause failure scoring table, SIL 0 SW, single faults, the planning phase of the development, the relation between RAM and Safety are main topics of this publishing.

REFERENCES

[1] European Commission (EC), (2014). EU Transport In Figures, EU Recommendations commission, Publication No: 63317, Brussels.

[2] IEC 61508, (2010). Functional safety of electrical/ electronic/programmable electronic safety related systems, IEC, Geneva.

[3] Leveson, N. (2011). Engineering a Safer World. MIT press, Cambridge.

[4] Smith, D.J., (2001). Reliability, Maintainability and Risk, Sixth Edition, Butterworth-Heinemann, Oxford.

[5] Murthy, D., Rausand, M., Østeras, T., (2008). Product reliability: specification and performance. Springer, London.

[6] Official Journal of the European Union, EU Recommendations commission, (2014). Recommendation of 5 December 2014 on matters related to the placing in service and use of structural subsystems and vehicles under Directives 2008/57/EC and 2004/49/EC of the European Parliament and of the Council, (355), 5 December 2014, 59-77.

[7] IEC 62061, (2005), Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems, IEC, Geneva.

[8] ISO 26262 (2011). Road Vehicles – Functional Safety, Part 1-10, ISO, Geneva.

[9] IEC 61511 (2003). Functional Safety: Safety Instrumented systems for the Process Industry Sector, Part 1-3, IEC, Geneva.

[10] IEC 62425 (2007). Railway Applications – Communication, Signalling and Processing Systems - Safety Related Electronic Systems for Signalling. IEC, Geneva.

[11] IEC 61513 (2004). Nuclear Power Plants – Instrumentation and Control for Systems Important to Safety - General Requirements for Systems. IEC, Geneva.

[12] IEC 60601 (2009). Medical electrical equipment, IEC, Geneva.

[13] Sklet, S. (2006). Safety barriers: Definition, classification, and performance. Journal of Loss Prevention in the Process Industries, 19:494–506.

[14] BSI, (2007). Occupational health and safety management systems – Requirements. OHSAS 18001, London.

[15] Ministry of Labour and Social Security Publication, (2016). Occupational Safety And Health Profile Turkey, Publication Number: 62, Ankara.

[16] CENELEC, (1999). EN 50126 Railway Applications – The specification and demonstration of Reliability, Availability and Safety (RAMS), CENELEC, Brussels.

[17] CENELEC, (2003). EN 50129 Railway Applications – Communications, signalling and processing systems - Safety related electronic systems for signalling, CENELEC, Brussels.

[18] CENELEC, (2011). EN 50128 Railway Applications Communications, signalling and processing systems – Software for railway control and protection systems, CENELEC, Brussels.

[19] CENELEC, (2010). EN 50159 Railway Applications Communications, signalling and processing systems – Safety-related communication in transmission systems, CENELEC, Brussels.

[20] Fuqua, N.B., (2003). "The Applicability of Markov Analysis Methods to Reliability, Maintainability, and Safety", Selected Topics in Assurance Related Technologies by Reliability Analysis Center (RIAC), 10(2):1-8.

[21] H. K. Kim, H. T. Lee and K. S. Lee., (2005). "The design and analysis of AVTMR (all voting triple modular redundancy) and dual-duplex system", Reliability Engineering and System Safety, 88(3): 291-300.

[22] X. Chen, G. Zhou, Y. Yang and H. Huang, (2013). "A newly developed safety-critical computer system for China metro", IEEE Transactions on Intelligent Transportation Systems, 14(2): 709-719.

[23] Zhang, T. Long, W., Sato, Y., (2003). "Availability of systems with self-diagnostic components - applying Markov model to IEC 61508-6", Reliability Engineering and System Safety, 80: 133-141.

[24] Börcsök, J., (2007). Functional Safety. Hüthig GmbH & Co. KG, Heidelberg.

[25] Börcsök, J., Schaefer, S., (2007). "Estimation and Evaluation of Common Cause Failures", IEEE Second International Conference on Systems, 22-28 April 2007, Martinique.

[26] RELEX, (2003). Reliability: A Practitioner's Guide, Intellect, London.

[27] Ugljesa, E. and Börcsök, J., (2009). "Evaluation of sophisticated hardware architectures for safety applications", XXII International Symposium on Information, Communication and Automation Technologies, 19-31 October 2009, Sarajevo.

[28] Dorra, M., Reinert, D., (2013). "Quantitative Analysis of Complex Electronic Systems using Fault Tree Analysis and Markov Modelling", STSARCES Standards for Safety Related Complex Electronic Systems Project, Berufsgenossenschaftliches Institut für Arbeitssicherheit, St. Augustin.

[29] Smith, D.J., Simpson, K.G. (2004). Functional Safety, Elsevier Butterworth-Heinemann, Oxford.

[30] Beugin, J. et al., (2007). "A SIL quantification approach based on an operating situation model for safety evaluation in complex guided transportation systems. Reliability Engineering and System Safety", 92:1686-1700.

[31] Misumi, Y., Sato Y., (1999). “Estimation of average hazardous-event-frequency for allocation of safety-integrity levels”, Reliability Engineering and System Safety, 66:135-144.

[32] Tang, L., (2015). Reliability assessments of railway signaling systems: A comparison and evaluation of approaches, Master Thesis, Norwegian University of Science and Technology, Department of Industrial Economics and Technology Management, Trondheim.

[33] UNISIG, (2015). SUBSET 091 Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2, UNISIG, v.3.4.0.

[34] King, A.G., (2014). “SIL determination: Recognising and handling high demand mode scenarios”, Process Safety and Environmental Protection, 92:324-328.

[35] Smith, S., Gruhn, P., (1995). “The primary integrity parameters - Design parameters for safety systems”, ISA Transactions, 34:311-318.

[36] Liu, Y., Rausand, M., (2016). “Proof-testing strategies induced by dangerous detected failures of safety-instrumented systems”, Reliability Engineering and System Safety, 145:366-372.

[37] Ilavsky, J., Rastocny, K., Zdansky, J., (2013). “Common-cause failures as major issue in safety of control systems”, Information And Safety-Related Systems, 11:86-93.

[38] Hokstad, P., Corneliussen, K., (2004). “Loss of safety assessment and the IEC 61508 standard”, Reliability Engineering and System Safety, 83: 111–120.

[39] IEEE 1474.1, (2004). IEEE Standard for Communications-Based Train Control (CBTC), IEEE, New York.

[40] Lundteigen, M.A. et al., (2009). “Integrating RAMS engineering and management with the safety life cycle of IEC 61508”, Reliability Engineering and System Safety, 94:1894–1903.

[41] UNIFE European Rail Industry, ERTMS in brief - ERTMS European Rail Traffic Management System, http://www.ertms.net/?page_id=40, 06 July 2017.

[42] European Commission, Mobility and Transport, ERTMS- History of ERTMS, https://ec.europa.eu/transport/modes/rail/ertms/general_information/history_ertms_en, 06 July 2017.

[43] UNISIG, (2014). SUBSET 026 System Requirements Specification, UNISIG, v.3.4.0.

[44] ERA, Set of specifications # 2 (ETCS baseline 3 and GSM-R baseline 1), http://www.era.europa.eu/core-activities/ertms/pages/set-of-specifications-2.aspx, 09 July 2017.

[45] ERA, List of supporting informative specifications - Set of specifications # 3, http://www.era.europa.eu/Core-Activities/ERTMS/Pages/List-of-supporting-informative-specifications---Set-of-specifications-3.aspx, 09 July 2017.

[46] ERA, Supporting Documents, http://www.era.europa.eu/Core-Activities/ERTMS/Pages/List-of-supporting-documents.aspx, 09 July 2017.

[47] UNISIG, (2014). SUBSET 088 ETCS Application Level 2 - Safety Analysis, UNISIG, v.3.5.4.

[48] ERA, Report on the certification of ERTMS equipment http://www.era.europa.eu/Document- Register/Documents/Report%20ERTMS%20Certification%20vers%201.0%20(2011).pdf, 09 July 2017.

[49] Stanley P. et al., (2011). ETCS For Engineers, First Edition, TZ-Verlag & Print GmbH., Roßdorf.

[50] TÜV Nord, (2013). Functional Safety Training Notes, Hamburg.

[51] The European Commission, (2013). Official Journal of the European Union, Common safety method for risk evaluation and assessment No 402/2013, Brussels.

[52] Farooq, J., & Soler, J. (2017). "Radio communication for Communications-Based Train Control (CBTC): A tutorial and survey", IEEE Communications Surveys and Tutorials, 19:1377-1402.

[53] AIChE, (1985). Guidelines for Hazard Evaluation Procedures, Third Edition, New York.

[54] UNISIG, (2016). SUBSET 118 Functional Safety Analysis of ETCS DMI for ETCS Auxiliary Hazard, UNISIG, v.1.3.0.

[55] IEC 61882 (2001). Hazard and operability studies (HAZOP studies), Application guide, IEC, Geneva.

[56] IEC 61025, (2006). Fault tree analysis (FTA), IEC, Geneva.

[57] Turkish State Railways (TCDD), (2014). Konya–Karaman Signalling and Telecommunication Project Technical Tender Specifications, Ankara.

[58] Blaauboer, M. et al., (2013). "Reducing Life Cycle Costs of main line interlockings", Signal+Draht, 105:30–32.

[59] Ankara Metropolitan Municipality, (2008). Ankara Metro Electro-Mechanic Works Technical Tender Specification, Ankara.

[60] International Union of Railways (UIC), (2007). Generic requirements deliverable D.1.1 – Signaling Glossary in Integrated European Signalling System (INESS), 218575, Paris.

[61] CENELEC, (2007). PD CLC/TR 50126-2: Guide to the application of EN 50126-1 for safety, CENELEC, Brussels.

[62] ISO 8402, (1994). Quality management and quality assurance – Vocabulary, ISO, 2nd Edition.

[63] USA Department of Defense, (1995). MIL-STD-721C NOTICE 2 Military Standard: Definitions Of Terms For Reliability And Maintainability, USA Department of Defense, Washington DC.

[64] Oedewald, P., Gotcheva, N., (2015). "Safety culture and subcontractor network governance in a complex safety critical project, Reliability Engineering and System Safety", 141:106–114.

[65] Goble, M.W., (2010). Control Systems Safety Evaluation and Reliability, Third Edition, ISA, NC.

[66] Birolini, A., (2007). Reliability Engineering Theory and Practice, Fifth edition, Springer, Berlin.

[67] CENELEC, (2006). EN 61165 Application of Markov Techniques, CENELEC, Brussels.

[68] USA Department of Defense, (1996). MIL HDBK 472 Military Standardization Handbook: Maintainability Prediction, USA Department of Defense, Washington DC.

[69] Rausand, M., (2004). System Reliability Theory, John Wiley & Sons, Inc., Hoboken, New Jersey.

[70] Hauge, S. et al, (2015), Common Cause Failures In Safety Instrumented Systems – ß Factors and Equipment Specific Checklists Based on Operational Experience, SINTEF, Trondheim.

[71] Humphrey, R. A. (1987). Assigning a numerical value to the beta factor common cause evaluation. Reliability '87. Proceedings paper 2C, April 1987, Birminghom.

[72] Fleming, K.N., (1987), Parametric Models For Common Cause Failure Analysis, Advanced Seminar on Common Cause Failure Analysis in Probabilistic Safety Assessment, 16-19 November 1987, Ispra.

[73] Apostolakis, G., and P. Moieni, (1986), "On the Correlation of Failure Rates," Reliability Data Collection and Use in Risk and Availability Assessment, Fifth EUREDATA Conference, 9-11 April 1986, Heidelberg.

[74] Paula, H. M., (1986), "Comments on - On the Analysis of Dependent Failures in Risk Assessment and Reliability Evaluation", Nuclear Safety, 27 (2): 210-212.

[75] Apostolakis, G., and P. Moieni, (1987), "The Foundations of Models of Dependence in Probabilistic Safety Assessment", Reliability Engineering, 18:177-195.

[76] Mosleh, A., (1986), "Hidden Sources of Uncertainty: Judgment in Collection and Analysis of Data", Nuclear Engineering and Design, 93(2):187-193.

[77] NUREG/CR 6268, (2007), Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding, U.S. Nuclear Regulatory Commission Office of Nuclear Regulatory Research, NUREG/CR, Rev I, Washington DC.

[78] Zitrou A., Bedford T., Walls L., (2004). "Developing Soft Factors Inputs to Common Cause Failure Models", Probabilistic Safety Assessment and Management, 14-18 June 2004, Berlin.

[79] Mosleh, A., and N. O. Siu, (1987), "A Multi-Parameter, Event-Based Common-Cause Failure Model", Proceedings of the Ninth International Conference on Structural Mechanics in Reactor Technology, 17-21 August 1987, Lausanne.

[80] OLF 070, (2004). Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry, OLF 070, Trondheim.

[81] National Aeronautics and Space Administration (NASA), 2002. Probabilistic Risk Assessment Procedures for NASA Managers and Practioners, Washington DC.

[82] Hauge, S., (2010). PDS Data Handbook Reliability Data for Safety Instrumented Systems, SINTEF, Trondheim.

[83] Brand, V.P., (1996). IPM3.1: A pragmatic approach to dependent failures assessment for standard systems. AEA Technology, Warrington.

[84] ISO 14224 (2016). Petroleum, petrochemical and natural gas industries collection and exchange of reliability and maintenance data for equipment. ISO, Geneva.

[85] Vesely, W. E., (1977). "Estimating Common Cause Failure Probabilities in Reliability and Risk Analyses: Marshall-Olkin Specializations," Nuclear Systems Reliability Engineering and Risk Assessment, 15: 314-341.

[86] IEC 61165, (2006) Application of Markov techniques, IEC, Geneva.

[87] IEC 60300, (2007) Dependability management – Part 3-2: Application guide – Collection of dependability data from the field, IEC, Geneva.

[88] Karydasa, D.M., Brombacherb A.C., (1999). "Reliability certification of programmable electronic systems", Reliability Engineering and System Safety, 66:103-107.

[89] Hokstad, P. (2005). Probability of Failure on Demand (PFD) – the formulas of IEC 61508 with focus on the 1oo2D voting, ESREL, 27-30 June 2005, Gdansk.

[90] Telcordia Technologies, (2006). SR-332 Reliability Prediction Procedure for Electronic Equipment, Telcordia Technologies, Issue 2, Piscataway NJ.

[91] USA Department of Defense, (1995). MIL HDBK 217 FN2 Military Handbook Reliability Prediction of Electronic Equipment, USA Department of Defense, Washington DC.

[92] Reliability Information Analysis Center, (2010). Reliability Modeling - The RIAC Guide to Reliability Prediction, Assessment and Estimation, Quanterion Solutions Inc., New York.

[93] Verma, A.K., Ajit, S., Karanki, D.R, (2016). Reliability and Safety Engineering, Second Edition, Springer, Piscataway.

[94] Villemeur, A (1992). Reliability, maintainability, and safety assessment, Vol 1. Methods and techniques. New York.

[95] Akers, J.B., Bowman, K.M, (2013). Advanced Windchill Prediction 10.2 Training Manual, PTC Inc, Needham.

[96] PTC Inc., (2015). Reference Guide PTC Windchill Quality Solutions™ 11.0, Needham.

[97] USA Department of Defense, (2008). ANSI/VITA 51.1, American National Standard for Reliability Prediction MIL-HDBK-217 Subsidiary Specification, USA Department of Defense, Washington.

[98] Reliability Analysis Center (RAC), (1988), Reliability Toolkit: Commercial Practices Edition Quanterion Solutions Inc., New York.

[99] Naval Surface Warfare Center (NSWC), (2011). Handbook of Reliability Prediction Procedures for Mechanical Equipment, NSWC, Revision A, Maryland.

[100] Dogruguven, E.H., Ustoglu, I., (2018). "SIL Attachment Paradigm from the Perspective of Quantitative Hazard Rates, Control in Transportation Systems, IFAC PapersOnLine", 6-8 June 2018, Savona.

[101] Dogruguven, E.H., Ustoglu, I., (2018). “Selecting correct architecture for mission critical safe control systems”, ESREL Safety and Reliability – Safe Societies in a Changing World, 17-21 June 2018, Trondheim.

[102] Dogruguven, E.H., Ustoglu, I., (2018). “Enhancement of Full Coverage Markov Model for Diverse Systems with Common Cause Failures”, CEIT 2018, 25-27 October 2018, Istanbul, in press.

[103] Dogruguven, E.H., Ustoglu, I., (2018). “Harmonizing normative organizational structures and certification & validation concepts for safety critical generic projects”, ESREL Safety and Reliability – Safe Societies in a Changing World, 17-21 June 2018, Trondheim.

[104] Dogruguven, E.H., Ustoglu, I., (2018). “An Evaluation of Safety Standards of E/E/PES Systems Regarding Information Consistency & Enhancement Proposals”, RAMS 2019, 28-31 January 2019, Florida, in press.

APPENDIX-A

BILL OF MATERIAL

Board Station BOM file

date : June 17:48:44

ORDER AMOUNT COMP CODE

1 1 board

---

2 2 1xx23xy7270 RESISTOK240R R159 R160 bw02 -- -- 5,625 xa -> 7,6 yw

---

3 2 1xbw7 CAPACITOK47u XZ72 XZ73 1210_0H107 -- open , . -- 1,35 V

---

4 2 59bwxxxx RESISTOK0 R2bs R284 bw02 -- , . -- 69 xa -> 476,1 uW

---

5 2 -1xx1 RESISTOK1xx R149 R150 bw02 -- , . -- 11 xa -> 12,1 yw

---

---

6 5 59bw-4bw6-1xx2 RESISTOK1K R270 R271 R276 bw02 . (R270,271) -- R270,271 -> 1,8 xa -> 3,24 yw

R277 R411 |- R411 -> 1,32 xa -> 1,7424 yw

|- R276,277 -> 3,3 xa -> 10,89 yw

---

7 2 59bw-4bw6-1xx3 RESISTOK10K R303 R3bw bw02 -- R303 -> . / R3bw -> , .

-- 330 uA -> 1,089 yw

---

8 4 59b-2208 RESISTOK2.2 R108 R109 R110 bw02 -- , . -- 18 xa -> 712 uW

R111

---

9 1 59bw-3909 RESISTOK39R R155 bw02 -- , . -- 1xx uA -> 390 nW

---

10 37 59bwbw6-4702 RESISTOK4.7K R163 R164 R175 bw02 . -- R175 -> 287 uA -> 387 uW

R176 R177 R178 |- R358,359 -> 382 uA -> 689 uW

R179 R180 R181 |- -> 702 uA -> 2,31 yw

R182 R1bs R184

R185 R186 R188

R189 R190 R191

R210 R212 R213

R214 R215 R216

R217 R218 R219

R220 R221 R222

R223 R224 R358

R359 R364 R365

R366

---

11 3 59bw074-1xx4 RESISTOK1xxK R85 R86 R87 bw02
. -- 33 uA -> 108,9 uW

---

12 6 59bw4074-1xx9 RESISTOK10 R438 R439 R440 bw02
-- , . -- 165 uA -> 272 nW

R441 R442 R443

---

13 1 59bw40741101 RESISTOK110 R117 bw02
-- -- 1xx uA -> 1,1 uW

---

14 1 59bw0741502 RESISTOK1.5K R408 bw02
-- -- 1,32 xa -> 2,6 yw

---

15 1 59bk4074-2xx1 RESISTOK2xx R291 bw02
-- -- 2xx uA -> 8 uW

---

16 24 59bk407k4029 RESISTOK40.2 R26 R27 R28 R29 bw02 -- -- 33 xa -> 45 yw

R30 R31 R32 R33

R34 R35 R36 R38

R39 R40 R41 R42

R43 R44 R45 R46

R47 R48 R49 R50

---

17 1 59bk407k6981 RESISTOK698 R137 bw02 -- -- 2xx uA -> 27,6 uW

---

18 1 59bk407k8259 RESISTOK82.5 R120 bw02 -- -- 1xx uA -> 825 nW

---

19 3 59bk418k5108 RESISTOK5.1 R131 R132 R133 08bw -- , .-- 69 xa -> 24,6 yw

---

20 2 5910-0166-8130 CAPACITOK6.8p XZ56 XZ57 bw02 -- open , .-- 3,3V

---

21 1 5910-bw5k7082 CAPACITOK470n C146 0603 -- -- 1,0V

---

22 5 5910-bw63-3101 CAPACITOK3.3n XZbs XZ84 XZ85 bw02 -- open , .-- XZbs -> 3,3V / XZ84 -> 1,0V

XZ86 XZ87 |- XZ85,286,287 -> 1,35V

---

23 1 5915k160kxx0 0R38, 0R38 EB2 0603 -- , .-- 0,155 A -> 16,8175 yw (7xx mOhm DCR)

---

24 1 NNk5-xxxxk444 MC34VR5xxV1ES TD11 QFN56_HS -- --

---

25 1 NNk5-xxxxk445 6V492bwBNLGI TD22 VFQFPN48_HS -- --

---

26 1 NNk5-99xxpx19 LS1021AXN7KQB_DDR_CONTROLLER TD2 PBGA525 -- --

---

27 1 NNk6-xxxx-0173 25MHZ K2 XTAL_FUND_32X25MM_JA4 -- --

---

28 58 NNk6-xxx0376 CAPACITOK1xxn C147 C148 C149 0201_IPC -- open , .-- 1,0 V

C150 C151 C152

C153 C154 C155

C156 C157 C158

C159 C160 C161

C162 C163 C164

C165 C166 C1xy

C168 C169 C170

C171 C172 C173

C174 C175 C176

C177 C178 C179

C180 C181 C182

C1bs C184 C185

C186 C187 C188

C189 C190 C191

C192 C193 C194

C195 C196 C197

C198 C199 XZxx

C431 C432 C433

C434

---

29 56 MC-xxx0363 CAPACITOK1xxn XZ97 XZ98 XZ99 bw02 -- open , . -- C409,410,411,412,413,414,415,416,417,

C3xx C301 C302 -- C418,419,420,421,424,425,426,427,428,

C303 C3bw C3bw -- C429,430,503 -> 3,3 V

C306 C307 C308 |- -> 1,35 V

C315 C316 C317

C318 C319 C320

C321 C322 C323

C324 C325 C326

C327 C328 C329

C330 C4bw C4bw

C409 C410 C411

C412 C413 C414

C415 C416 C417

C418 C419 C420

C421 C422 C423

C424 C425 C426

C427 C428 C429

C430 C499 C502

C503 C5bw

---

30 3 MCxxxx-bw27 CAPACITOK10n C641 C642 C643 bw02 -- open , .-- 0,xy5V

---

31 11 MC-xxxbw28 CAPACITOK4.7u C607 C608 C609 08bw -- open , .-- C607 -> 1,2V

C610 C611 C612 |- C608 -> 2,5V

C613 C614 C615 |- C609,610,611,612,613,614,615 -> 3,3V

C616 C617 |- C616,617 -> 1,35V

---

32 18 Mxxxx-bw29 CAPACITOK22u C707 C708 C709 1210_0H106 -- open , .-- C707,708,709,710,719,720,745,746 -> 1,35V

C710 C711 C712 |- C7011,712,713,714,715 -> 1,0V

C713 C714 C715 |- C716,717,718,726,727 -> 1,0V

C716 C717 C718

C719 C720 C726

C727 C745 C746

---

33 1 Mxxx-bw30 CAPACITOK1n C653 bw02 -- open , .-- 3,3V

---

34 1 MCxxx-0707 CAPACITOK220n C89 bw02 .-- 1,2 V

---

35 11 MCxxxx-0711 CAPACITOK2.2u C70 C71 C72 C73 08bw .-- C70,72,73 -> 1,0V

C74 C75 C85 C86 |- C71 -> 3,3V

C87 XZ82 Cbs6 |- C74,75 -> 1,35V

---

36 4 MCxxx-0750 CAPACITOK10u C541 C542 C543 08bw .-- C541 -> 3,3V

C544 |- C542,543,544 -> 1,8V

---

37 19 Mxxx-09xx CAPACITOK1u C1 XZ C3 C4 C31 bw02 .-- C1,2,3,4,38,59, -> 1,35V

C32 C33 C34 C35 |- C40,41,42 -> 1,8V

C36 C37 C38 C39 |- C31,32,33,34,35,36,37,39,2219 -> 3,3V

C40 C41 C42 C59

C60 XZ219

---

38 6 MFpxxx-0801 180, 180 EB7 EB8 EB9 EB10 0603 -- , .-- 0.32 A -> 9,216 yw (90 mOhm DCR)

EB20 EB21

---

39 1 MIxxx-0840 74LVC1G125DCK TD36 PSOP5 -- --

---

40 1 MIxxxxk182 ADT7461A TD33 MSOP8I -- --

---

41 2 MIxxxk682 MT41K256M16HA_107 TD6 TD7 FBGA96_HA -- --

---

42 1 MIxxk732 TXB0106PWR TD16 PDS0_G16 -- --

---

43 1 MLxxx-0790 INDUCTOK0.68uH L11 2525 -- .-- 4.5 A -> 111.375 yw (5,5 mOhm DCR)

---

44 3 ML-x0793 INDUCTOK1.5uH L4 L5 L6 2525 -- .-- 2.5 A -> 93,75 yw (15 mOhm DCR)

---

45 2 MR-xxxx2159 RESISTOK162 R78 R79 0603 -- -- 1.35 V -> 11.25 yw

CURRICULUM VITAE

PERSONAL INFORMATION

Name Surname : Ersin Hasan DOĞRUGÜVEN

Date of birth and place :14.07.1985, İstanbul

Foreign Languages :German, English

E-mail :ehdogruguven@aselsan.com.tr

EDUCATION

Degree	Department	University	Date of Graduation
Master	Mechanical Engineering	İTÜ	2012
Undergraduate	Control Engineering	İTÜ	2009
High School		İstanbul Erkek Lisesi	2004

WORK EXPERIENCE

Year	Corporation/Institute	Enrollment
2016-	ASELSAN INC.	Senior Expert System Design Engineer, Technical Manager

2013-2016	Private Company	R&D Chief, Head of Signaling
2009-2013	TÜBİTAK	Expert Researcher

PUBLISHMENTS

Conference Papers

1. Dogruguven, E.H., Ustoglu, I., (2018). "Selecting Correct Architecture For Mission Critical Safe Control Systems", ESREL Safety and Reliability – Safe Societies in a Changing World, 17-21 June 2018, Trondheim.

2. Dogruguven, E.H., Ustoglu, I., (2018). "Harmonizing Normative Organizational Structures And Certification & Validation Concepts For Safety Critical Generic Projects", ESREL Safety and Reliability – Safe Societies in a Changing World, 17-21 June 2018, Trondheim,

3. Dogruguven, E.H., Ustoglu, I., (2018). "SIL Attachment Paradigm from the Perspective of Quantitative Hazard Rates", Control in Transportation Systems, IFAC PapersOnLine, 6-8 June 2018, Savona.

4. Dogruguven, E.H., Ustoglu, I., (2018). "Enhancement of Full Coverage Markov Model for Diverse Systems with Common Cause Failures", CEIT 2018, 25-27 October 2018, Istanbul, in press.

5. Dogruguven, E.H., Ustoglu, I., (2018). "An Evaluation of Safety Standards of E/E/PES Systems Regarding Information Consistency & Enhancement Proposals", RAMS 2019, 28-31 January 2019, Florida, in press.

6. Dogruguven, E.H., Acarman, T., (2012). "Proposal of Regenerative Braking Algorithm to Maximize Energy Transfer and to Enhance Yaw Stability". IEEE International Conference on Vehicular Electronics and Safety, 24-27 July 2012, Istanbul.

AWARDS

1. TÜBİTAK scholarship for the R&D Project Sliding Mode Control for Hybrid Electric Vehicles