International Journal of Mathematical, Engineering and Management Sciences
Vol. 3, No. 3, 258–270, 2018
https://dx.doi.org/10.33889/IJMEMS.2018.3.3-018

SIL Implementation on Safety Functions in Mass Transit System

James Li
Centre of Competence for Mass Transit
AME, Bombardier Transportation, Kingston, Canada
E-mail: james.li@rail.bombardier.com

(Received July 6, 2017; Accepted August 18, 2017)

Abstract
The concept of Safety Integrity Level (SIL) has been developed within different systems of standards (IEC 61508, EN50129 and DEF-STAN 00-56). These standards are applied in different areas: control technology (IEC 61508), railway technology (EN50128 and EN 50129), and defense technology (DEF-STAN-00-56). Nowadays, a lot of the mass transit turnkey projects around the world demand the contractors to follow CENELEC standards and SIL concept for the safety function implementation. Although the concept of SIL is mentioned in these standards, the interpretation of the concept of SIL in these standards is not consistent and unequivocal. This paper is written to elaborate the anomalies of SIL interpretation among these various standards in order for safety engineers to obtain a more detailed view on the concept of SIL over these standards.

Keywords– Safety Integrity Level (SIL), CENELEC Standard, Safety Instrumented System (SIS), Hardware Fault Tolerance (HFT), Common Cause Failure (CCF).

1. Introduction

The CENELEC standard EN50126 have attracted increasingly more widespread attention as international railways applied safety standards since the 1990s. Firstly, EN50126 symbolizes the only international RAMS standard in the railway application. Secondly, the concept behind EN 50126 is not solely task-based but an integrated systematic process, which considers engineering management and quality management, etc. The major property of EN50126 is characterized in the risk-based approach, safety life cycle concept, safety target set-up, and definition of Safety Integrity Level (SIL).

The SIL concept is not very common in the US railway and mass transit industry because of MIL-STD-882, “System Safety Program Requirements”, although a military standard, is the current standard in the rail and mass transit industry for the development of system safety program plans (SSPPs). MIL-STD-882 applies to a system life cycle, as does EN50126, but only addresses safety as opposed to reliability, availability, maintainability and quality. MIL-STD-882 is risk-based as are EN50126, but is not based on SIL. Except for some software integrity levels in IEEE standards, SIL have not been used in the US rail and mass transit industry.

2. Why SIL – History of Safety Integrity Level (SIL)

Since the 1970s, computer technologies have developed rapidly and been utilized in safety critical control applications. However, the software reliability was not feasible to predict the probability or errors in software with any degree of accuracy in a way comparable to the calculation of the probability of failure of electronic hardware on the basis of component failure rates. This eventually led to the development of IEC 61508, the generic international standard for Electrical / Electronic / Programmable Electronic Safety Related Systems, which formed the pattern for the CENELEC standards EN50128 and EN50129 for safety-related systems in railways.

International Journal of Mathematical, Engineering and Management Sciences
Vol. 3, No. 3, 258–270, 2018
https://dx.doi.org/10.33889/IJMEMS.2018.3.3-018

The pioneers leading the way to the development of IEC 61508 use expert judgement to rank the available techniques in order of their effectiveness in ensuring software correctness. Techniques for each stage of the software life cycle were placed in one of four groups ranked in order of increasing effectiveness. The software could be developed to achieve one of four levels of safety integrity by using techniques from the correspondingly ranked group at each stage of the software life cycle.

The principle of achieving levels of safety integrity according to the techniques used in system development was extended to cover protection against errors in design, installation, maintenance, and other systematic errors in electronic systems.

In the continuing development of the SIL concept it was decided to associate a numerical probability value with each SIL. Nonetheless, the linking of each SIL to a specific value of probability is the main source of the anomalies and misuse that has grown around the SIL concept. In all these standards, four safety integrity levels are defined. SIL 4 has the highest level of safety integrity; SIL 1 has the lowest. SIL 0 is used to indicate that there are no safety requirements. Each integrity level is associated with a target probability of failure.

One widely accepted association is shown in Table 1, which is derived from IEC 61508. The low demand column should be used if demands are expected to occur:

- No more than once per year, and
- No more than twice as often as the system is checked out.

Otherwise, use the continuous/high demand column.

Table 1. Safety Integrity Level

Low Demand (Probability of Failure on Demand)	Continuous / High Demand Mode (Dangerous Failure Rate / Hour)	Safety Integrity Level
$\geq 10^{-5}$ to 10^{-4}	$\geq 10^{-9}$ to 10^{-8}	4
$\geq 10^{-4}$ to 10^{-3}	$\geq 10^{-8}$ to 10^{-7}	3
$\geq 10^{-3}$ to 10^{-2}	$\geq 10^{-7}$ to 10^{-6}	2
$\geq 10^{-2}$ to 10^{-1}	$\geq 10^{-6}$ to 10^{-5}	1

3. Different Interpretation of SIL

Since these different standards, IEC61508, EN50126, EN50128, EN50129 or DEF-STAN-00-56 are developed by each individual standard committee, some of them are dedicated to the control technology like IEC61508, some of them are dedicated to the military industry like DEF-STAN-00-56, and others are dedicated to the rail industry like EN50126, EN50128 and EN50129. Consequently, the various standards interpret the meaning of SIL in their own specific way, although the concept of SIL behind IEC61508 and EN50126/128/129 are compatible.

IEC 61508 defines SIL as a discrete level (one out of a possible four) where SIL 4 has the highest level of safety integrity and SIL 1 has the lowest, and it defines safety integrity as the probability of a safety related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time.

EN50126, EN50128 and EN50129 are cautious to avoid mentioning probability in the definition of SIL, which they define as a number, which indicates the required degree of confidence that a system will meet its specified safety functions with respect to systematic failures. EN50126 requires only the existence of SIL. EN50128 is dedicated to software and software SILs without numeric rates, and defined the software SIL as the classification number, which determines the techniques and measures that must be applied to software.

EN50129 defines safety integrity as the ability of a safety-related system to achieve its required safety functions under all the stated conditions within a stated operational environment and within a stated period of time. EN50129 also says "Because it is not possible to assess systematic failure integrity by quantitative methods, safety integrity levels are used to group methods, tools and techniques which, when used effectively, are considered to provide an appropriate level of confidence in the realization of a system to a stated integrity level".

EN50129 reveals the relationship between SIL and Tolerable Hazard Rate (THR) that is the identical concept of Dangerous Failure Rate (DFR) for the continuous mode in IEC61508. Low demand mode is not used by EN50129 to avoid ambiguity in determination of SIL.

EN50129 states that the safety relies both on adequate measures to avoid or tolerate faults (as safeguards against systematic failure) and on adequate measures to control random failures. Measures against both causes of failures should be balanced in order to achieve the optimum safety performance of a system. SILs are used as a means of matching the qualitative approach (to avoid systematic failures) with the quantitative approach (to control random failures).

The overview of these standards emphasizes three aspects in terms of SIL concept:

(a) A target failure rate, which is a maximal rate of dangerous failures of the systems that must not be exceeded (IEC61508, DEF-STAN-00-56 and EN50129).
(b) A set of measures (methods, tools and techniques) that is dedicated to cope with systematic failures (EN50128 and EN50129).
(c) For software, only systematic failures are considered and no target failure rate is considered (EN50128).

4. Safety Instrumented System (SIS)

In IEC61508 a safety instrumented system (SIS) is defined to provide a safety-related function to monitor and maintain the safety of any equipment under its control. In the initial safety analysis such as PHA, SSHA, etc., each hazard is assessed with quantitative and/or qualitative methods to attain the associated risk. The risk is a function of the frequency of occurrence of a hazardous event with the severity of its consequence: Risk = f (severity, frequency). The risk matrix categorizes the risk level and determines the acceptability of risk. For most of the hazards, the hazard severity generally remains unchanged within the initial and final assessment. For instance, a train collision is always assessed as a catastrophic mishap. The effective way to mitigate a hazard to an acceptable level is to reduce the hazardous event frequency to an acceptable one. An SIS is a safety function system implemented to reduce a risk to an acceptable level and the SIL is the safety confidence level assigned to an SIS. For instance, in the mass transit system, the automatic train protection (ATP) system is implemented to prevent trains from the collision, therefore a highest SIL 4 shall be applied to the ATP system. For mass transit trains, emergency braking function is a safety function performed by a train on board brake system to guarantee the safe separation among trains

International Journal of Mathematical, Engineering and Management Sciences
Vol. 3, No. 3, 258–270, 2018
https://dx.doi.org/10.33889/IJMEMS.2018.3.3-018

on the same rail track to avoid collisions. Therefore, emergency braking function shall be applied as SIL 4.

Ideally, an SIS should be a robust hardwire design as its reliability is feasible to verify by calculating the component failure rate to assess the SIL performance. However currently, many of the safety functions performed by SISs are becoming more intelligent and complex. The hardware design approaches using relays and contacts would increase the cumbersomeness of SISs and compromise the operational reliability. The utilization of computer technology in the SISs as well as the software engagement in the safety logic control brings up a new challenge with regards to the quantitative SIL assessment because the software reliability cannot be applied for a quantitative calculation. Therefore, EN50128 copes with software SILs without numeric rates but a set of techniques implemented in the life cycle development, refer to Fig. 1.

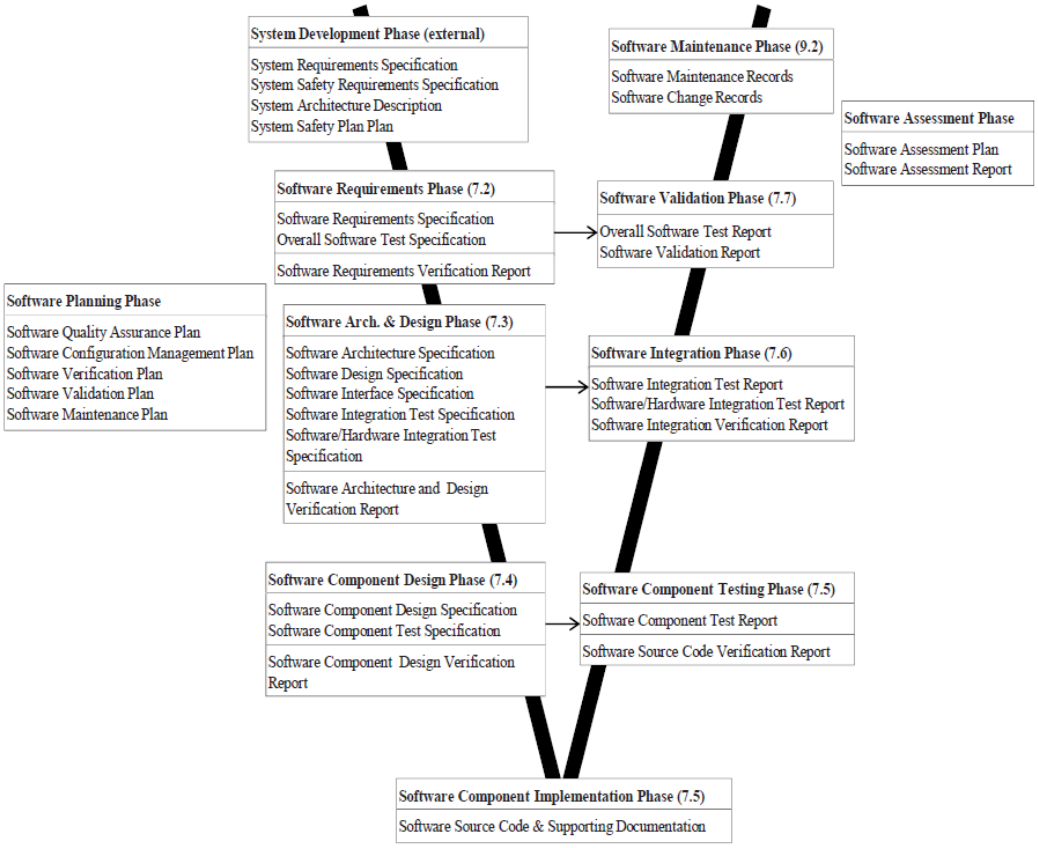

Fig. 1. Software development life cycle in EN50128

5. Safe Failure Fraction (SFF) and Hardware Fault Tolerance (HFT)

In IEC 61508 the concepts of SFF and HFT are introduced as a measure to characterize an SIS and applied in the architecture of the expected SIL.

The failure rate of an SIS is apportioned into safe failure rate (λ_S) and dangerous failure rate (λ_D). The dangerous failure rate is further apportioned into detected dangerous failure rate (λ_{DD}) and undetected dangerous failure rate (λ_{UD}), refer to Fig. 2.

International Journal of Mathematical, Engineering and Management Sciences
Vol. 3, No. 3, 258–270, 2018
https://dx.doi.org/10.33889/IJMEMS.2018.3.3-018

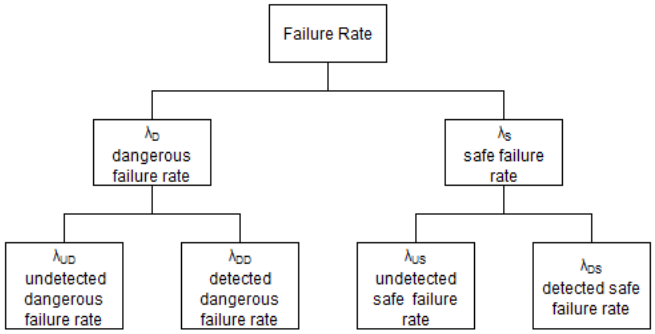

Fig. 2. SIS failure rate apportionment

Safety failure fraction SFF considers the fraction of failures not leading to dangerous ones and is given by:

$$\mathrm{SFF} = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_D} \tag{1}$$

The Hardware Fault Tolerance (HFT) considers the voting of the hardware architecture, which implies how many hardware faults are allowed for system success.

The determination of the maximum allowable safety integrity that can be claimed for the SIS is defined in Table 2.

Table 2. Maximum allowable SIL for a safety function carried out by a type A (B) safety-related element or subsystem

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
< 60%	SIL 1 (not allowed)	SIL 2 (1)	SIL 3 (2)
60% -< 90%	SIL 2 (1)	SIL 3 (2)	SIL 4 (3)
90% -< 99%	SIL 3 (2)	SIL 4 (3)	SIL 4 (4)
≥ 99%	SIL 3 (3)	SIL 4 (4)	SIL 4 (4)

IEC61508 defines a type A that stands for a low complexity system and B for a high complexity system. A low complexity system is characterized by the fact that all failure modes of the SIS are well known, its failed behavior are clearly known and there is a sufficient failure rate to show that the claimed dangerous failure rates are met. A high complexity is present when at least one of these three points is not covered. A safety engineer can use the rule of Table 2 to evaluate the SIL level. For instance, with a 1oo2 SIS type A and an SFF ≥ 99%, the maximum expected SIL is SIL 4.

International Journal of Mathematical, Engineering and Management Sciences
Vol. 3, No. 3, 258–270, 2018
https://dx.doi.org/10.33889/IJMEMS.2018.3.3-018

6. SIL Combining Rules

SIL combining rules elaborate how SISs should be combined to obtain an SIS with an expected SIL. For instance, can a SIL 4 system be constructed from two SIL 2 systems connected in parallel.

Yellow book and DEF-STAN-00-56 have the strictest combining rules for building higher SIL systems from sub-systems of lower SIL by building in back-up or protection functions.

Yellow book and DEF-STAN-00-56 give the following Table 3 for apportion of safety integrity levels. And it also says "The table should not be repeatedly applied to allow a SIL 4 system, say, to be made of many SIL 1 systems" which means the combing rules in Table 3 are not intended to be applied iteratively.

Table 3. Apportionment of safety integrity level

Top Level SIL	SIL of Lower Level Function		Combinator (if present)
	Main	Other	
SIL 4	SIL 4	None	None
	SIL 4	SIL 2	SIL 4
	SIL 3	SIL 3	SIL 4
SIL 3	SIL 3	None	None
	SIL 3	SIL 1	SIL 3
	SIL 2	SIL 2	SIL 3
SIL 2	SIL 2	None	None
	SIL 1	SIL 1	SIL 2
SIL 1	SIL 1	None	None

The combining rules in Table 3 can also be summarized as:

SIL 3 ‖ SIL 3 → SIL 4, SIL 2 ‖ SIL 2 → SIL 3, SIL 1 ‖ SIL 1 → SIL 2, SIL x ‖ SIL y → SIL Max. (x, y). Please note that a SIL > 0 must not be constructed from SIL 0 elements.

Germany standard SIRF has shown a liberal flexibility on the restriction with regards to the SIL AND combination.

For two elements AND combination, the following rules are respected, refer to Fig. 3.

International Journal of Mathematical, Engineering and Management Sciences
Vol. 3, No. 3, 258–270, 2018
https://dx.doi.org/10.33889/IJMEMS.2018.3.3-018

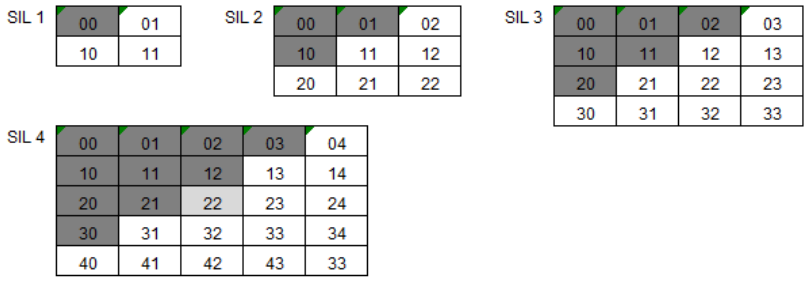

Fig. 3. Two-elements SIL AND combination

The general rule for two elements AND combination is that the claimed SIL can be constructed with sub-systems with lower or equivalent SILs given that the sum of the sub-systems SILs is greater than or equal to the claimed SIL.

According to German standard SIRF, two SIL 2 systems AND combination (connected in parallel) could be constructed to build a SIL 4 at certain conditions in a comparable way that according to Yellow Book and DEF-STAN-00-56 only SIL 3 could be claimed for two SIL2 systems AND combination.

For three elements AND combination, the following rules are respected according to SIRF, refer to Fig. 4.

The general rule for three elements AND combination is that the claimed SIL can be constructed with sub-systems with lower or equivalent SILs given that the sum of the sub-systems SILs is greater than or equal to the claimed SIL.

Another requirement for AND combing rule is the lower sub-system which is constructed to build a system with a higher SIL and should be strictly independent without common cause failures (CFFs). CCFs are multiple failures due to a common cause. CCFs need to be considered when there is a common test, common maintenance, common supplier, or common abnormal environment, etc.

In reference Langerson et al. (2008), a SIL combing method based upon both series and parallel merging rules was introduced according to IEC61508.

IEC61508 use the following merging rules to determine the SIL of each combination:

(a) Series merging rule: for a series structure, the SIL is summarized by the lowest SILs of the subsystem composing the structure, refer to Fig. 5.

International Journal of Mathematical, Engineering and Management Sciences
Vol. 3, No. 3, 258–270, 2018
https://dx.doi.org/10.33889/IJMEMS.2018.3.3-018

SIL 1

000	001
010	011
100	101
110	111

SIL 2

000	001	002
010	011	012
020	021	022
100	101	102
110	111	112
120	121	122
200	201	202
210	211	212
220	221	222

SIL 3

000	001	002	003
010	011	012	013
020	021	022	023
030	031	032	033
100	101	102	103
110	111	112	113
120	121	122	123
130	131	132	133
200	201	202	203
210	211	212	213
220	221	222	223
230	231	232	233
300	301	302	303
310	311	312	313
320	321	322	323
330	331	332	333

SIL 4

000	001	002	003	004
010	011	012	013	014
020	021	022	023	024
030	031	032	033	034
040	041	042	43	044
100	101	102	103	104
110	111	112	113	114
120	121	122	123	124
130	131	132	133	134
140	141	142	143	144
200	201	202	203	204
210	211	212	213	214
220	221	222	223	224
230	231	232	233	234
240	241	242	243	244
300	301	302	303	304
310	311	312	313	314

Fig. 4. Three-elements SIL AND combination

International Journal of Mathematical, Engineering and Management Sciences
Vol. 3, No. 3, 258–270, 2018
https://dx.doi.org/10.33889/IJMEMS.2018.3.3-018

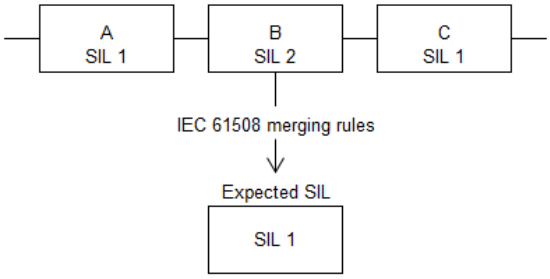

Fig. 5. SIL series merging rule in IEC 61508

(b) Parallel merging rule: the SIL of a parallel structure is given by the SIL of the subsystem with the highest SIL, refer to Fig. 6.

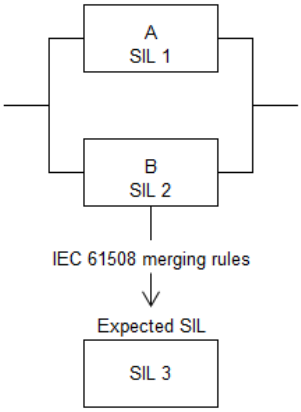

Fig. 6. SIL parallel merging rule in IEC 61508

7. Random Failure Integrity and Systematic Failure Integrity

The differentiation between random failure integrity and systematic failure integrity is not clearly laid out in some of these standards and have resulted in the misuse and misunderstanding of SIL concept in real life practice of safety engineers.

The random failure integrity could be quantified utilizing the hardware component failure rate. However systematic failure integrity is the non-quantifiable part of the safety integrity because systematic faults are caused by human errors in the various stages of the system /subsystem/equipment life cycle such as design errors, which are hardly, predicted quantitatively.

International Journal of Mathematical, Engineering and Management Sciences
Vol. 3, No. 3, 258–270, 2018
https://dx.doi.org/10.33889/IJMEMS.2018.3.3-018

EN50129 clearly says that SILs are concerned with both systematic failure integrity that cannot be assessed by quantitative methods, and random failure integrity that can be assessed by quantitative methods. It is necessary to satisfy both the systematic and the random failure integrity requirements if adequate safety integrity is to be achieved.

Systematic failure integrity is achieved by means of the quality management, safety management and technical safety conditions, refer to Fig. 7. In EN50129, a set of techniques, tools, methods and processes are listed from Table E.1 to E.9 in Annex E; when used effectively, it is considered to provide an appropriate level of confidence in the realization of a system to a stated integrity level.

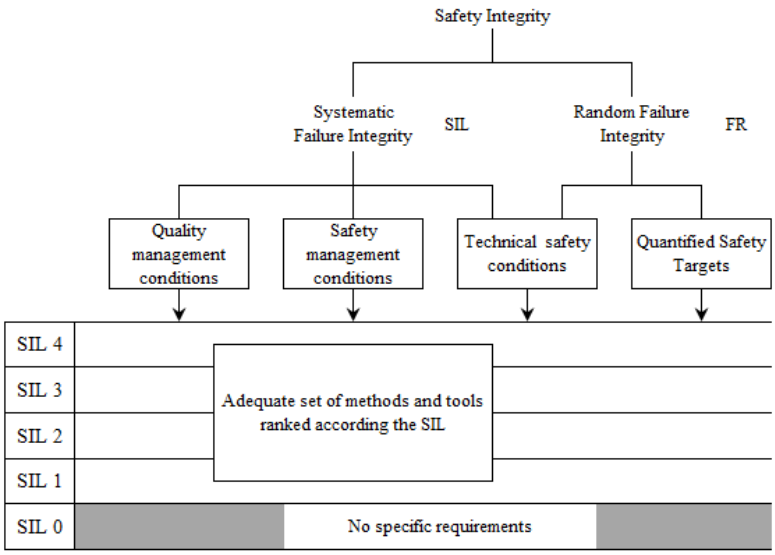

Fig. 7. Relationship between SILs and techniques in EN 50129

8. Probability Failure Performance Analysis

The other fundamental concept besides the safety life cycle in IEC61508 is probability failure performance analysis, which is intended to address hardware random failures to quantify the SIL magnitude levels. IEC 61508 and CENELEC standards (EN50126, EN50128 and EN50129) do not specify how to perform the failure probability analysis. There is no specific requirement that fault trees or Markov models be used. There is only a statement that industry accepted methods shall be used.

A fault tree is one of the commonly applied methods which is utilized in the rail and mass transit industry to predict failure probability or failure frequency for the safety related systems used in safety functions to show sufficient protection against random failures. Fault tree was established in the early 1960's by H. Watson working at Bell Telephone Labs on the launch control system of the Minuteman intercontinental ballistic missile. It is then recognized by Dave Haasl in Boeing as a system safety analysis tool. Now it has become an effective tool widely used in various industries including aircraft, weapons, nuclear power, chemical, robotic and software etc., for system failure

International Journal of Mathematical, Engineering and Management Sciences
Vol. 3, No. 3, 258–270, 2018
https://dx.doi.org/10.33889/IJMEMS.2018.3.3-018

probability analysis. In reference Andrew (2010), a research on methods for predicting a system reliability in terms of the component failure probabilities was introduced.

The typical fault tree structure starts at the top-level system failure and progresses in branches spreading downward developing its causality in terms of lower resolution events until component failure, basic events, appear.

Two types of symbols which appear in the fault tree are “gates” and “events”. Typical event symbols used are ‘basic event’ which usually represents a component failure, and ‘Intermediate event’ which is called a fault. It is important to clearly define each event as a fault or failure so it can be further resolved or be identified as a basic cause. The events in the fault tree are linked using ‘gate’ symbols. The three fundamental logic gates are ‘OR’, ‘AND’ and ‘Voting’. ‘OR’ gate represents output event occurs if at least one of the input events occur; ‘AND” gate represents output event occurs if all input events occur; ‘Voting’ gate indicates at least *m* of the inputs must occur to produce the output event.

To quantify top event system failure, the minimal cut sets should be identified, and the component failure probability should be predicted. Minimal cut sets are defined as a list of minimal (necessary and sufficient) component failed states which cause the system failure. The component failure probability depends upon how the component is maintained and three situations are considered: no repair, repair when the failure occurs (revealed failure), and repair when the failure is discovered (unrevealed failure).

For a ‘no repair’ situation, if a component cannot be repaired then the chances of failure will continue to increase over time. The failure probability, unavailability Q(t), if the component has a constant failure rate, λ, is given by:

$$Q(t) = 1 - e^{-\lambda t} \tag{2}$$

For a ‘revealed failure’ situation, a component failure occurs and the repair can be started immediately. This is unscheduled maintenance, which takes place in response to the component failure occurrence. For a component with constant failure rate, λ, and constant repair rate, μ, the unavailability at time *t* is given by:

$$Q(t) = \frac{\lambda}{\lambda + \mu}(1 - e^{-(\lambda+\mu)t}) \tag{3}$$

For an ‘unrevealed failure’ situation, components are part of standby or safety systems, which only operate under certain conditions then when failures occur they will not be observed. For these types of systems, they must be tested to reveal the failure and so the repair takes place when scheduled tests are carried out. The average unavailability is given by:

$$Q_{AV} = \frac{1}{\theta}\int_0^{\theta}\left(1 - e^{-\lambda t}\right)dt \tag{4}$$

Where θ is the scheduled test interval and λ is the constant failure rate.

International Journal of Mathematical, Engineering and Management Sciences
Vol. 3, No. 3, 258–270, 2018
https://dx.doi.org/10.33889/IJMEMS.2018.3.3-018

The basic mathematic used in the fault tree 'gates' evaluation is Boolean logic which includes Distributive Law (A·(B+C) = A·B+A·C), Identity Absorption Law (A+A=A), Subset Absorption Law (A+A·B=A) and Idempotent Law (A·A=A) etc.

For Common Cause Failures (CCFs), β factor model is used to quantify the probability that a failure cause results in multiple failures. β value ranges from 0.3 to 0.01. For instance, there are three redundant components A, B and C with failure probability $P = 1 \times 10^{-3}$. If these three elements are independent then the failure probability $P(A \cdot B \cdot C) = 1 \times 10^{-9}$; if CCF susceptibilities exist within three components and $\beta = 0.01$ then CCF probability for A, B and C = $P \times \beta = 1 \times 10^{-5}$.

The Markov Model is also a commonly applied method for probability failure performance analysis in the rail and mass transit industry. The term 'Markov Model' is named after the Russian mathematician Andrei Markov (1856 ~ 1922). The Markov model has two characteristics: memory-less and stationary. Memory-less means that the future state of a system depends only upon its current state not upon its past history; stationary means that the probabilities, which govern the transition from state to state remain constant with time. The Markov Model is a powerful reliability analysis tool to evaluate the redundant systems, which have the constant failure rate and repair rate, refer to reference Klion (1997) and MIL-HDBK-338B (2005).

9. Summary

IEC61508 and CENELEC standards EN50126, EN50128 and EN50129 all emphasize the engineering processes to defend against systematic failure. The product safety life cycle process requirements are intended to ensure a sufficient level of the safety integrity against systematic faults. The level of detail and rigor varies with SIL capability rating. SIL concept is widely accepted in the rail and mass transit turnkey projects in the global market except for the countries or regions that already have developed a system of standards like the United States. Nonetheless, the process and documentation production which is strictly required in these standards would increase the complexity of the system design and project cost. The documentation (specification, plan, analysis, report and certification, etc.) development which are recommended in EN50128 and EN50129 for SIL rating is cumbersome which would consume plenty of time and money throughout the project execution, which would impose an adverse impact on the project schedule and cost. The anomalies of SIL interpretation over these various standards also cause misuse in the system safety design implementation. It is more serious that the culture of SIL conformity may inhibit the innovation and continuing use of established systems, although the CENELEC European standards are not intended to be retrospective. Another adverse effect in the SIL concept is that most of these standards distract attention from the aspects of the size, complexity or novelty of the safety system architecture with respect to SIL.

References

Andrews. J. (2010, January). Introduction to fault tree analysis. In *Reliability and Maintainability Symposium (RAMS), 2010 Proceedings – Annual (pp.7-8).* IEEE.

BS EN 50128 *Railway applications – Communications, Signalling and Processing Systems – Software for Railway control and protection systems*, British Standards Institute.

BS EN 50129 *Railway applications – Communications, Signalling and Processing Systems – Safety related electronic systems for signalling*, British Standards Institute.

BS EN50126 *Railway applications – The specification and demonstration of dependability. Reliability, Availability, Maintainability and Safety (RAMS)*, British Standards Institute.

Department of Defense (US), MIL-STD-882: System Safety Program Requirements. 1993 (version C), 2000 (version D).

Engineering Safety Management Issue 3, Yellow Book 3, Volumes 1 and 2, Fundamentals and Guidance (p. 9-3). Published by Railtrack on behalf of the UK rail industry.

IEC 61508, *Functional Safety of Electrical /Electronic / Programmable Electronic Safety Related Systems,* Parts 1-7, International Electro – technical Commission, Geneva, Switzerland (1999-2001).

Klion, J. (1997). System periodically maintenance. In *A Redundancy Notebook (pp.29-88).* Rome Air Development Center Publishing.

Langeron, Y., Barros, A., Grall, A., & Bérenguer, C. (2008). Combination of safety integrity levels (SILs): A study of IEC61508 merging rules. *Journal of Loss Prevention in the Process Industries*, *21*(4), 437-449.

Military Standard (2005). MIL-HDBK-338B Military Handbook Electronic Reliability Handbook, Notice 2 (pp.334-350). Air Force Research Laboratory Information Publishing.

Ministry of Defense (UK), DEF STAN 00-56, *Safety Management Requirements for Defense Systems,* Part 1 and 2, Dec. 1996.