XX IMEKO World Congress
Metrology for Green Growth
September 9–14, 2012, Busan, Republic of Korea

FUNCTIONAL SAFETY ASSESSMENT: AN ISSUE FOR TECHNICAL DIAGNOSTICS

Marcantonio Catelani, Lorenzo Ciani, Valentina Luongo

Department of Electronics and Telecommunications, University of Florence,Via S.Marta 3,50139,Florence(Italy)
{marcantonio.catelani, lorenzo.ciani, valentina.luongo}@unifi.it

Abstract: The paper discusses a case study concerning the functional safety assessment based on the evaluation of the Safe Failure Fraction (SFF) for a complex system. Being such evaluation made according to IEC61508 standard, the paper focused on some related ambiguities. The paper is structured in two phases. First, a reliability prediction of each component of the system is implemented and then a Failure Mode and Effect, Diagnostic Analysis (FMEDA) is applied, in order to collect information about failure condition of each component. By using this approach it is possible to study SFF of different complex systems in compliance with qualitative requirements described in the aforementioned standard.

Keywords: Safety Related System; IEC 61508; Safe Failure Fraction; Failure Mode and Effect, Diagnostic Analysis.

1. INTRODUCTION

The standard IEC61508 "Functional Safety of Electrical / Electronic / Programmable Electronic Safety Related System" has been widely accepted and used in many countries and industries because of its contribution in many field of application. A Safety Related System (SRS) is an independent protection layer that implements the required safety function necessary to achieve, or maintain, a safe state of the EUC (Equipment Under Control). It is intended to achieve, on its own or with other E/E/PE SRSs, other technology SRSs or external risk reduction facilities, the necessary safety integrity for the required safety functions [1]. The IEC61508 sets out a generic approach for all safety lifecycle activities (see Figure 1, [1]) for systems comprised of E/E/PE elements that are used to perform safety functions. This unified approach has been adopted in order that a rational and consistent technical policy be developed for all electrically-based safety-related systems. In particular, a Safety Lifecycle can be defined as all necessary activities required during the implementation of all Safety Instrumented Functions, starting from the concept phase of a project until decommissioning of the project when all the Safety Instrumented Functions are no longer available for use.

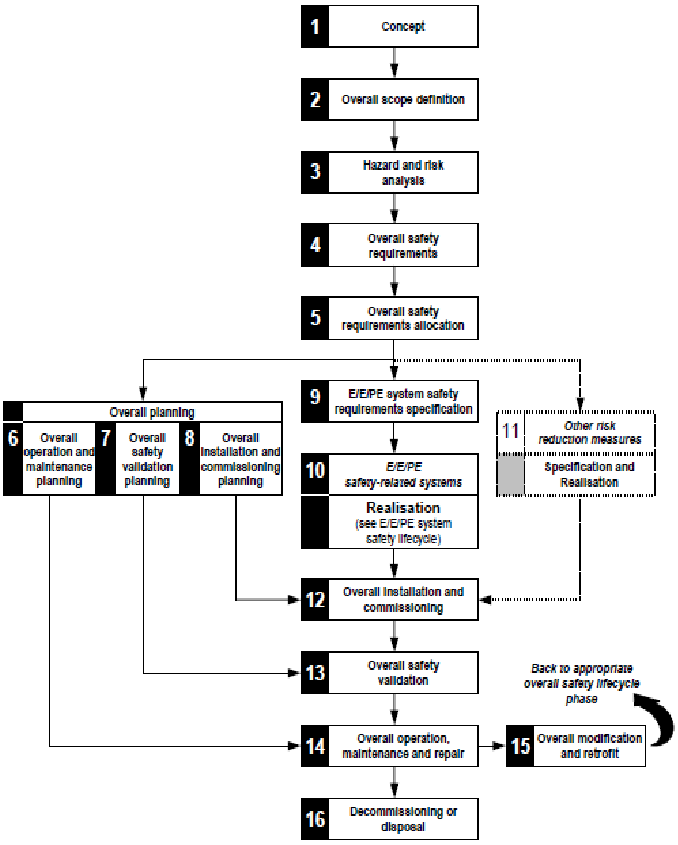

1 Concept
2 Overall scope definition
3 Hazard and risk analysis
4 Overall safety requirements
5 Overall safety requirements allocation
Overall planning
6 Overall operation and maintenance planning
7 Overall safety validation planning
8 Overall installation and commissioning planning
9 E/E/PE system safety requirements specification
10 E/E/PE safety-related systems
Realisation (see E/E/PE system safety lifecycle)
11 Other risk reduction measures
Specification and Realisation
12 Overall installation and commissioning
13 Overall safety validation
14 Overall operation, maintenance and repair
15 Overall modification and retrofit
Back to appropriate overall safety lifecycle phase
16 Decommissioning or disposal

Figure 1. IEC 61508 Overall Safety lifecycle.

Based on the phases recalled in the overall safety lifecycle, the standard provides a guide line for the design, validation and verification of SRSs; it requires to specify a safety function and its safety integrity to be achieved by SRS.

Safety integrity is a fundamental concept in this standard and it is defined as the probability of a SRS satisfactorily performing the required safety functions under all the stated conditions within a specific period of time [1]. There are four distinct level regarding safety integrity called SIL (Safety Integrity Level) from SIL1 to SIL4, where SIL4 is the highest with most stringent requirements. To achieve a specific SIL all the hardware safety integrity requirements must to be met. They are split in quantitative and qualitative requirements [2]. The first one have to be considered to estimate the Probability of Failure on Demand (PFD), that is the average probability of SRS's failure to perform its design function on demand, of each safety function. The qualitative requirements are related, instead, to the architectural constraints that shall be identified. They are a set of requirements that restrict the designer's freedom on the possible configuration of hardware, and limit the achievable SIL based on Hardware Fault Tolerance (HFT) and Safe Failure Fraction of the subsystem [1]. This paper address a case study in calculation of SFF of a complex system and underlines some ambiguities concerning the application of this standard.

2. BASIC CONCEPTS

A Safety Related System shown in Figure 2 consists of three types of elements: sensor or transducer, logic solver (e.g. PLC, micro controller, PLD), actuating items (e.g. valves, brakes).

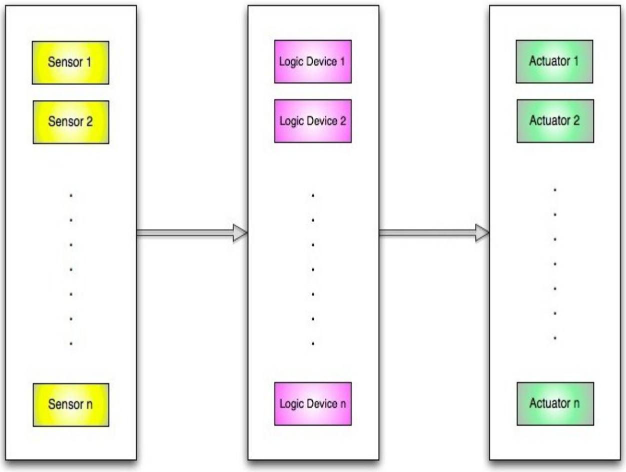


Figure 2. Safety Related System (SRS) block diagram.

The main SRS functions are:

1. when a predefined process demand (deviation) occurs in the EUC, the deviation shall be detected by the SRS sensors, and the required actuating items shall be activated and fulfill their intended functions.

2. the SRS shall not be activated spuriously, that is, without the presence of predefined process demand (deviation) in EUC [3].

The most important concept of this standard is the Safety Integrity Level SIL. As already said, there are four possible discrete level for specifying safety integrity requirements of the safety functions to be allocated to the E/E/PE Safety Related Systems, and they are generally related to complete systems. SIL is connect to the concepts of SFF and HFT. Before defining this parameters, it's useful to classify failures according to their causes and effects.
The type of failures can be classified as:

- Dangerous failures (D). Failures which have the potential to put the safety related system in a hazardous or fail-to-function state.
- Safe failures (S). Failure which does not have the potential to put the safety related system in a hazardous or fail-to-function state .

  Both safe and dangerous failures con be split into: detected and undetected. These are in relation to hardware, revealed or unrevealed, by diagnostic tests, proof-tests, operator intervention or through normal operation.
- Random hardware failures. These are physical failure where the supplied service deviates from the specified service due to physical degradation of the item. They result from one or more of the possible degradation mechanisms in the hardware.
- Systematic failures. These failures are nonphysical failures where the supplied service deviates from the specified service without any physical degradation of the item. The failures related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or manufacturing process, operational procedures or documentation [3].

The SFF is a parameter concerning the fraction of overall hardware failure rate of device considered as safe or detected dangerous failure. It is taken into account when determining the architectural constraints on hardware safety integrity [4].

SFF is defined [3] as the ratio between the sum of safe failures λ_s and detected dangerous failure λ_{dd} with respect to the sum of all possible failure λ_{Tot} (safe and dangerous).

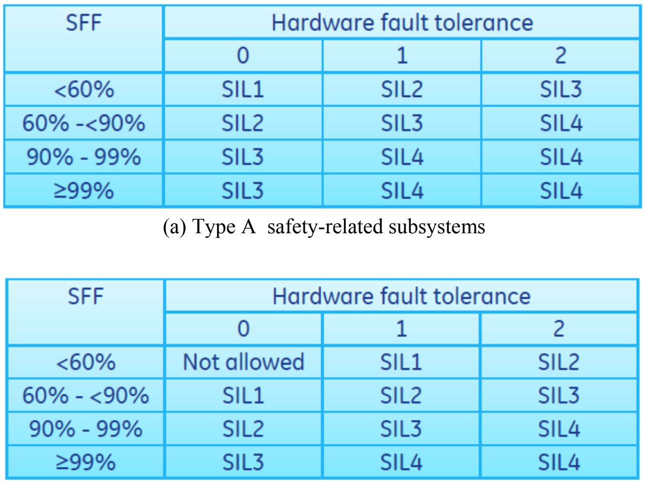
$$SFF = \frac{\sum \lambda_s + \sum \lambda_{dd}}{\sum \lambda_{Tot}} \qquad (1)$$

Two methods can be considered in order to demonstrate if the requirement of SFF has been met: the test method and FMEDA-Failure Mode and Effect, Diagnostic Analysis [5, 6]. Clearly a 60% safe failure fraction could be demonstrated fairly easily. Test would require a sample of only a few failures to reveal 60% or alternatively a FMEDA, addressing blocks of circuitry rather than individual components, would establish if 60% were achieved. Turning to 90% coverage, the test sample would now need to exceed a good number of failures (for reasonable statistical significance) and the FMEDA would require a more detailed approach. For 99% coverage a reasonable sample size would now exceed a major number of failures the test demonstration is likely to be impracticable [7].

The Hardware Fault Tolerance measures the number of fault tolerated before the safety function is affected. A system with HFT of N means that N+1 faults could cause a loss of safety function [8].

The Hardware Fault Tolerance in combination with the Safe Failure Fraction is defined in table I. A "type A" components are described as simple devices with well-known failure modes; the "type B" devices are, instead, complex components with potentially unknown failure modes, i.e., microprocessors, ASICs, etc.

TABLE I. HARDWARE SAFETY INTEGRITY: ARCHITECTURAL CONSTRAINTS



SFF	Hardware fault tolerance		
	0	1	2
<60%	SIL1	SIL2	SIL3
60% -<90%	SIL2	SIL3	SIL4
90% - 99%	SIL3	SIL4	SIL4
≥99%	SIL3	SIL4	SIL4

(a) Type A safety-related subsystems

SFF	Hardware fault tolerance		
	0	1	2
<60%	Not allowed	SIL1	SIL2
60% - <90%	SIL1	SIL2	SIL3
90% - 99%	SIL2	SIL3	SIL4
≥99%	SIL3	SIL4	SIL4

(b) Type B safety-related subsystems

Another important parameter for the evaluation of the SFF is representing by the Diagnostic Coverage (DC). It is defined as the ratio of the detected failure rate with respect to the total failure rate of the component or subsystem as detected by diagnostic tests.

$$DC = \frac{\sum \lambda_{dd}}{\sum \lambda_d} \tag{2}$$

Diagnostic Coverage does not include any faults detected by proof tests (or periodic tests performed to detect failures in a SRS) [1]. The Diagnostic Coverage factor can be calculated by considering which component failure modes are detected by diagnostics. It may be exist for whole or parts of a SIS, for example it may exist for sensor and/or logic solver and/or final elements.

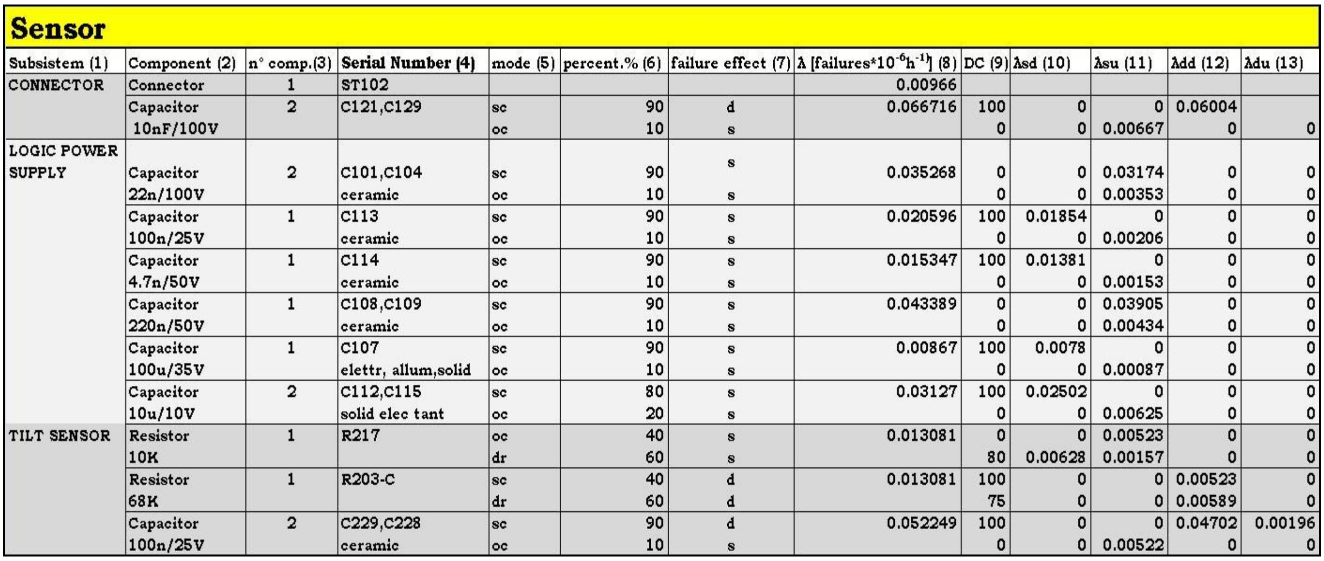
3. PROPOSED APPROACH

To determine the architectural constraints it is necessary to meet the qualitative hardware safety integrity requirements. These requirements are applied in two ways, to specify the required architecture or to verify if a given architecture corresponds to a specified SIL [9]. In either cases, there are some step to follow. First of all the architecture of the system and the complexity of its components have to be described. As shows in Table I, there are two type of components classified according to the knowledge of the failure modes: known (Type A) or unknown (Type B).

The second step consists in SFF evaluation according to Eq. (1); then a distinction in safe and dangerous failure is made. There are many reliability analysis used to accomplish this operation: Fault Tree Analysis (FTA) and the Markov-Chain analysis, failure rate prediction for the individual component and modules and Failure Mode and Effect, Diagnostic Analysis (FMEDA) for all components or for the units of interest.

The final step is to verify the achievable SIL of each subsystem (sensors, logic solvers, actuators). This paper is focused on the methods to achieve the second step and copes with some noticed problems. Our approach is based

TABLE II. AN EXTRACT OF FMEDA ANALYSIS: SENSOR SUB-SYSTEM



Sensor

Subsistem (1)	Component (2)	n° comp.(3)	Serial Number (4)	mode (5)	percent.% (6)	failure effect (7)	λ [failures*$10^{-6}h^{-1}$] (8)	DC (9)	λ_{sd} (10)	λ_{su} (11)	λ_{dd} (12)	λ_{du} (13)
CONNECTOR	Connector	1	ST102				0.00966					
	Capacitor	2	C121,C129	sc	90	d	0.066716	100	0	0	0.06004	
	10nF/100V			oc	10	s		0	0	0.00667	0	0
LOGIC POWER SUPPLY	Capacitor	2	C101,C104	sc	90	s	0.035268	0	0	0.03174	0	0
	22n/100V		ceramic	oc	10	s		0	0	0.00353	0	0
	Capacitor	1	C113	sc	90	s	0.020596	100	0.01854	0	0	0
	100n/25V		ceramic	oc	10	s		0	0	0.00206	0	0
	Capacitor	1	C114	sc	90	s	0.015347	100	0.01381	0	0	0
	4.7n/50V		ceramic	oc	10	s		0	0	0.00153	0	0
	Capacitor	1	C108,C109	sc	90	s	0.043389	0	0	0.03905	0	0
	220n/50V		ceramic	oc	10	s		0	0	0.00434	0	0
	Capacitor	1	C107	sc	90	s	0.00867	100	0.0078	0	0	0
	100u/35V		elettr, allum,solid	oc	10	s		0	0	0.00087	0	0
	Capacitor	2	C112,C115	sc	80	s	0.03127	100	0.02502	0	0	0
	10u/10V		solid elec tant	oc	20	s		0	0	0.00625	0	0
TILT SENSOR	Resistor	1	R217	oc	40	s	0.013081	0	0	0.00523	0	0
	10K			dr	60	s		80	0.00628	0.00157	0	0
	Resistor	1	R203-C	sc	40	d	0.013081	100	0	0	0.00523	0
	68K			dr	60	d		75	0	0	0.00589	0
	Capacitor	2	C229,C228	sc	90	d	0.052249	100	0	0	0.04702	0.00196
	100n/25V		ceramic	oc	10	s		0	0	0.00522	0	0

on the reliability prediction and FMEDA technique being such methods less expensive with respect to the formulas suggested in the standard IEC61508; the advantages can be reached for the case study presented here, in term of cost and time and allow to cover wider reliability configuration classes.

It is important to remember that in the electrical-electronic field, a fundamental role is played by the reliability prediction analysis. It can be performed by using particular data base [10]. Under specified hypotheses, the approach is based on the use of established failure rate models for electrical and electronics components. Failures rates are calculated by gathering different information such as stress, quality, performance, temperature and humidity conditions, operative environment, and so on. The prediction models are not intended to describe the physical behavior of the components or explain their failure mechanisms, but to represent the best estimate based on observed data.

Field data, instead of laboratory data, is a coherent choice in relation with the statistical meaning of the prediction models.

The reliability of electronic components mostly depends on the particular application, (besides being an intrinsic characteristic); thus, knowledge of the real operating conditions is necessary to guarantee accurate reliability prediction [11]. However application specific data is preferred where any error in estimating the probability of failure of a particular component could have a significant impact on the estimation of the SFF.

The failure rates that was generated from a reliability prediction of a prototype of our complex system can be used in the FMEDA. The scope of this method is to identify all the fault states of the component or sub-system under examination. FMEDA con be considered as an extension of the FMEA-Failure Mode and Effect Analysis technique based on the MIL-STD-1629 with additional information [12]. It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, dangerous undetected) in the safety models [13].

The FMEDA is an extremely important step in meeting the requirements of IEC 61508, because the calculation of SFF and DC depend on it. An extract of FMEDA of the equipment under examination, concerning the sensor subsystem components, is shown in Table II. From the first column to the fourth one there is the classification of the element under consideration. Column (1) shows subsystems in which the complex system has been split. Columns (2), (3) and (4) give information about components, the number of them and the name of each component in the part list. For each component of the system all possible failure modes should be considered (column 5). In Table II some failure modes are reported: oc-open circuit, sc-short circuit, dr-drift. The identification of the failure modes can be often difficult to achieve. In fact, failure modes depend on many factors. There is a disagreement between failure modes given from different standard so, even with simple component, such as a resistor, can arise problems of misinterpretations. Column (6) shows the percentages with which failure modes occur and the column (7) denotes the failure effect in safe (s) and dangerous (d). In columns (8) and (9) there are respectively the failure rate achieved from reliability prediction and the Diagnostic Coverage DC. An important issue is that the method shows diagnostics only for known component failure modes. The standard require a division of the failure rate of each component in: probability of safe failure λ_s, and the probability of dangerous failure λ_d and in detected and undetected to indicate the fraction of dangerous failures and safe failures which will be detected or undetected by the diagnostic tests (columns from 10 to 13). The division between safe and dangerous failures can be made in deterministic way for simple components but is otherwise based on engineering choice. The standard advise a division of failure into 50% safe and 50% dangerous. The approach of the standard seems to be ambiguous. This is an important issue because an incorrect division of failure rate cause a wrong value of SFF. In fact increasing the safe failure rates we achieve an increased SFF. It can lead to obtain a not enough robust architecture because with a specific HFT, increasing SFF we have an higher SIL's value. In order to achieve a more careful division between safe and dangerous failures our prototype of the electromechanical complex system has been projected with some diagnostic hardware subsystems.

Another ambiguity of the standard approach is that only random hardware failures are taken into consideration in the SFF calculation, but the Part 2 of the IEC61508 tells us that the target is to be applied equally to random hardware failures and to systematic failures. A solution of this problem is that the reliability prediction is as more carefully as possible.

4. CONCLUSIONS

The role of Safety Related Systems is more and more increased in the last years, and the industries must deal with the standard. In fact, the aim of a SRS is to reduce the risk from a hazardous state of the system under control to a tolerable level.

This paper presents a case study concerning the study of a complex system and, in particular, it describes the way in which the SFF can be achieved with the help of two reliability analysis, reliability prediction and FMEDA.

In both cases some ambiguities have been found. In reliability prediction field data is preferred because any error in estimating the probability of failure could have a significant impact on the estimation of the SFF. In FMEDA analysis is extremely important to predict all possible failure modes and to perform an accurate division between safe and dangerous failures because a simplistic division of failure into 50% safe and 50% dangerous suggested in the IEC61508 could lead to an erroneous value of SFF.

The FMEDA approach proposed in this paper represents a fundamental step in the functional safety assessment and it put in evidence the role that the diagnostic plays in the safety field.

REFERENCES

[1] IEC61508 Electric/Electronic/Programmable Electronic safety-related systems, parts 1–7. Technical report, International Electrotechnical Commission, May 2010.

[2] J.L. Rouvroye, A.C. Brombacher, “New quantitative safety standards: different techniques, different results?”, Elsevier Reliability Engineering and System Safety, vol. 1792, pp.121–125 ,1999.

[3] M.Rausand, A. Høyland,”System Reliability Theory“ 2nd Edition, J.Wiley & Sons, Inc., Hoboken, New Jersey. 2004.

[4] Y.Sato, I. Yoshimura,“Safety Achieved by the Safe Failure Fraction (SFF) in IEC 61508”, IEEE Transactions on Reliability, vol. 57, n.4, December 2008.

[5] M. Catelani, L. Ciani, V. Luongo, R. Singuaroli, “Evaluation of the Safe Failure Fraction for an electromechanical complex system: remarks about the standard IEC61508”, Proc. Of IEEE Instrumentation and Measurement Technology Conference (I2MTC) 2010, pp.949-953, 3-6 May 2010.

[6] M. Catelani, L. Ciani, V. Luongo, “The FMEDA approach to improve the safety assessment according to the IEC61508”, Microelectronics Reliability, Volume 50, Issues 9-11, Pages 1230-1235.

[7] D.J.Smith, K.G. L. Simpson,”Functional Safety” Elsevier Butterworth-Heinemann, 2004.

[8] R.Mariani, G.Boschi, F.Colucci,”Using an innovative SoC-level FMEA methodology to design in compliance with IEC61508”, Design, Automation & Test in Europe Conference & Exhibition, 16-20 April 2007.

[9] M.A.Lundteigen, M.Rausand,”Assessment of Hardware Safety Integrity Requirements” Proceedings of the 30th ESReDA Seminar, Trondheim, Norway, June 07-08, 2006.

[10] Military Handbook 217, Reliability Prediction Of Electronic EauiDment, (Springfield, VA: National Technical Information Services) 1990. MIL-HDBK-2 17F dates fiom January 1990.

[11] J.P.Rooney,The Foxboro Company, Foxborough,“IEC61508: An Opportunity for Reliability”, IEEE Proceedings Annual Reliability And Maintainability Symposium, 2001.

[12] Military Standard 1629, Procedurc;s For Performing A Failure Mode And Effect Analysis For Shiuxard EauiDment, (Springfield, VA National Technical Informatiori Services) 1974.

[13] W.M. Goble, A.C. Brombacher,“Using a failure modes, effects and diagnostic analysis (FMEDA) to measure diagnostic coverage in programmable electronic systems” Elsevier Reliability Engineering and System Safety, 66 (1999) 145–148.