Overview of a Complete Hardware Safety Integrity Verification According to IEC 61508 for the CERN Next Generation of Radiation Monitoring Safety System

Saskia Kristina Hurst
HSE-RP-IL (Radiation Protection), CERN, Switzerland. E-mail: saskia.kristina.hurst@cern.ch

Hamza Boukabache
HSE-RP-IL (Radiation Protection), CERN, Switzerland. E-mail: hamza.boukabache@cern.ch

Daniel Perrin
HSE-RP-IL (Radiation Protection), CERN, Switzerland. E-mail: daniel.perrin@cern.ch

In the framework of the in-house developed CERN Radiation Monitoring Electronic System (CROME), a reliability analysis is necessary to ensure compliance with the legal requirements regarding safety integrity, defined as Safety Integrity Level (SIL) 2 for the Safety Instrumented Functions (SIF) of the system. Given the high expectations for the reliability of the CROME system, its development process is supported by an extensive dependability study according to the IEC 61508 standard. This paper presents the verification of the hardware safety integrity and focuses on one possible approach using the CROME system as an example. The paper exposes the various steps needed to verify the hardware safety integrity, which includes the calculation of the Probability of dangerous Failure per Hour (PFH) and the evaluation of the architectural constraints by calculating the Safe Failure Fraction (SFF) as well as considering the Hardware Fault Tolerance (HFT) of the system. Following the presented approach, these calculations are based on a failure rate prediction with the FIDES standard, a Failure Modes, Effects and Diagnostic Analysis (FMEDA) and a Fault Tree Analysis (FTA). The results of the final CROME system qualification prototype (PQ) show that the hardware safety integrity complies with SIL 2 requirements.

Keywords: safety systems according to IEC 61508, hardware safety integrity verification, SIL, SIF, SIS, FMEDA, FTA, architectural constraints, SFF, HFT, PFH calculation.

1. Introduction & Motivation

Within the Occupational Health & Safety and Environmental Protection Unit (HSE) of CERN, monitoring systems are required to assess radiation risks and control the release of radioactivity. Currently around 800 systems for radiation monitoring are installed on different locations of CERN, mainly at the experiments and access points. Due to the stringent legislation in matters of radiation protection, the radiation monitoring systems need to be able to measure very low radiation levels, very fast ionizing radiation emissions, monitor the ambient dose rate in real-time and generate radiation alarms and interlock signals based on the ambient dose equivalent rate (Boukabache et al. 2016).

As one of the current monitoring systems reaches the end of its lifetime, the Radiation Protection group (RP) is developing a new high performance, cost effective low maintenance radiation monitor for CERN, which will gradually replace it. Given the high expectations for the reliability of the monitoring system, its development process needs to be supported by an extensive dependability study according to the IEC 61508 standard.

2. State of the Art

The IEC 61508 standard gives a guideline on the design of safety-related systems for its whole lifecycle, but leaves the user in choosing appropriate methods in fulfilling the requirements.

This paper is based on the approach Lundteigen and Rausand 2018 and Catelani, Ciani and Luongo 2010a are suggesting for the verification of hardware safety integrity and combining these methods with the calculation of the PFH with fault trees (Belland and Wiseman 2016).

3. The CROME System

The developed radiation monitoring system CROME (CERN RadiatiOn Monitoring Electronic), hereafter referred as CROME system, is capable of measuring very low dose rates down to 50 nSv/h, while being able to track radiation over an extensive range up to nine decades without auto scaling. Due to the timing specificity of the radiations encountered around accelerators, the system has a wide bandwidth, which requires a particularly complex electronics. As a safety system, the CROME system shall trigger visual

Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference
Edited by Piero Baraldi, Francesco Di Maio and Enrico Zio
Published by Research Publishing, Singapore.
ISBN: 978-981-14-8593-0; doi:10.3850/978-981-14-8593-0

and acoustic alarms as well as generate interlock signals used to dump the beams or close the access to areas in order to protect people and the environment.

3.1 *Structure of the CROME System*

The CROME system consists of three main parts, the CROME Measurement and Processing Unit (CMPU), the Alarm Unit (CAU) and the Uninterruptible Power Supply (CUPS). *Figure 1* shows the global structure of the CROME system with its main components, their interconnections and the link to supervision.

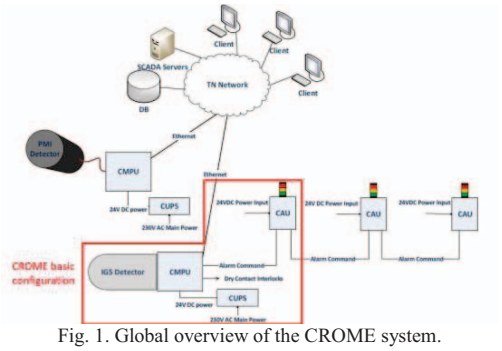

Fig. 1. Global overview of the CROME system.

The core part is the CMPU (see *Figure 2*), which can be either directly attached to a detector (ionisation chamber or neutron counter) or connected to it with a cable. The CMPU is capable of measuring the electrical signal of the detector, calculating the corresponding dose rate and triggering an alarm and/or interlock signal if a defined threshold is exceeded. The CAU (see *Figure 2*) is linked to the CMPU and converts the received signals in visual and acoustic alerts. The CUPS supplies both, the CMPU and CAU with power.

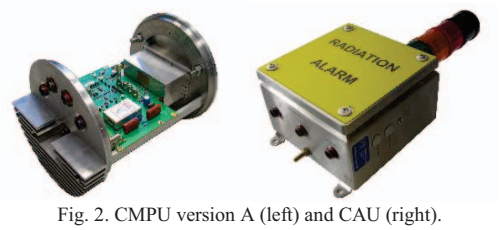

Fig. 2. CMPU version A (left) and CAU (right).

3.2 *Reliability Requirements of the CROME System*

The reliability requirements for the CROME system have been defined in accordance with IEC 60532 standard, which focuses on equipment for radiological protection and especially radiation monitoring systems. The IEC 60532 standard requires Safety Integrity Level 1 (SIL 1) "for equipment intended for the purpose of general area radiological protection" and SIL 2 or SIL 3 if "the equipment is intended to act as an interlock in a safety related protection system, such as personnel access control systems, which prevent human access to areas which can be subject to very high radiation fields" (IEC 2010a). The safety system CROME consists of one Safety Instrumented Function (SIF), which is called "Interlock triggering". The interlock signal is generated by a Field Programmable Gate Array (FPGA) located on the processing board of the CMPU, performing the calculation of the dose rate and its comparison with a pre-set threshold. This signal is transferred to the interlock system through the connecting board of the CMPU. Therefore, the SIL requirement for this function is SIL 2 according to IEC 60532.

The SIL verification is performed for the current prototype PQ in its basic configuration. This implies no chaining of the CROME subsystems, so that the system to be analysed consists of one CMPU directly connected to an ionisation chamber, one CAU and one CUPS (see Figure 3).

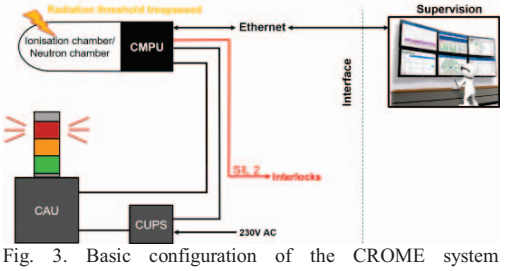

Fig. 3. Basic configuration of the CROME system (Boukabache et al. 2016).

The CROME subsystems consist of several electronic boards with in total around 3000 components (*Figure 4*).

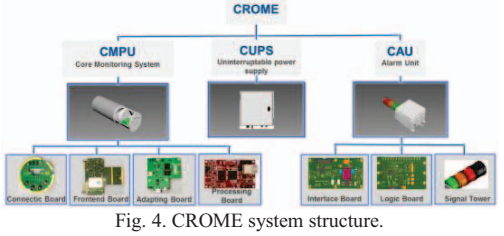

Fig. 4. CROME system structure.

After the reliability analysis of the previous version of the prototype, several components, functions and circuits were modified, as well as

redundancies were added by the board designers, in order to obtain high reliability and the required SIL 2.

4. SIL Verification According to IEC 61508

In this paragraph, a possible general approach for verifying the integrity of hardware safety according to IEC 61508 will be presented in order to demonstrate the approach on the example of the CROME system.

4.1 *IEC 61508 - Overview*

The International Electrotechnical Commission (IEC) is an international standards organisation that publishes international standards for all electronic, electrical and related technologies. The standards have been accepted by governments with the force of law in some countries and are typically cited as best practice. In case of accidents, the standard can be cited in civil cases as a commonly accepted standard of performance (Ingrey, Lerévérend and Dr. Hildebrandt 2007). IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES) is a generic standard, which is applicable to all kinds of industries and covers the general requirements for a Safety Instrumented System (SIS) in all phases of its safety lifecycle. Besides this generic standard, there are application specific standards such as IEC 61511 for the process industry and IEC 62061 for machinery systems. These standards do not only consider functional safety for electronic and electrical components, but also for hydraulic, pneumatic and mechanical components. The IEC 61508 standard is usually used when developing new products and it sets out the requirements for ensuring that systems are designed, implemented, operated and maintained to provide the required SIL. The international standard consists of seven parts. The second part (IEC 61508 – 2) covers specific requirements for safety-related hardware (IEC 2010b). This paper focuses on this part of the standard.

4.2 *Safety Integrity Requirements*

According to IEC 61508, requirements are split into systematic safety integrity requirements, hardware safety integrity requirements and software integrity requirements (Lundteigen and Rausand 2018), as shown in *Figure 5*. To achieve the required SIL, the SIF must meet all safety requirements.

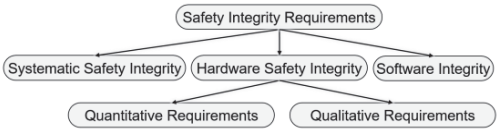

Fig. 5. Safety integrity requirements

Systematic safety integrity aims at avoiding systematic faults during design, installation, operation and maintenance by meeting the requirements of IEC 61508 for hardware and software. Systematic capability indicates the effectiveness of the internal development process and quality system (Lundteigen and Rausand 2018).

Software integrity is covered in IEC 61508 – Part 3 and relates to the safety integrity achieved by having adapted restrictions for application programming methods, tools and associated procedures (Lundteigen and Rausand 2018).

Hardware safety integrity comprises quantitative and qualitative requirements. Quantitative requirements include the Probability of a Failure on Demand (PFD) or Probability of a dangerous Failure per Hour (PFH) calculation and qualitative requirements are related to the architectural constraints that limit the achievable SIL based on Hardware Fault Tolerance (HFT) and the Safe Failure Fraction (SFF) of the sub-system (Lundteigen and Rausand 2006).

The overall safety integrity is always limited by the weakest link principle (the lowest SIL reached by one of the three categories) which is illustrated in *Table 1* (Lundteigen and Rausand 2018).

Table 1. Example for achieving SIL 2.

	SIL1	SIL2	SIL3	SIL4
Systematic safety integrity		x		
Hardware safety integrity			x	
Software integrity			x	
Overall safety integrity		x		

In this example, the overall safety integrity is SIL 2, even if hardware and software integrity are SIL 3, as the weakest link is the systematic safety integrity with a SIL 2.

4.3 *Hardware Safety Integrity*

As mentioned hardware safety integrity is related to random hardware failures and can be split into quantitative and qualitative requirements.

4.3.1 *Quantitative Requirements*

These requirements give quantified evidence that the SIF is able to meet the reliability target. For the validation of the quantitative requirements, either the PFD or the PFH depending on the demand rate on the SIF is used (IEC 2010b). A low demand mode is defined as a demand with a frequency of less than once per year and the PFD needs to be calculated. *Table 2* shows the definition of the SIL depending on the PFD.

Table 2. Definition of SIL according to IEC 61508-2 for a low demand mode.

SIL	Low demand mode (≤ 1 per year): Probability of failure on demand (PFD)
1	$10^{-2} < PFD \leq 10^{-1}$
2	$10^{-3} < PFD \leq 10^{-2}$
3	$10^{-4} < PFD \leq 10^{-3}$
4	$10^{-5} < PFD \leq 10^{-4}$

A high demand mode is defined as a demand with a frequency higher than once a year and a continuous demand as a safety function, which is performed continuously. For both modes, the PFH needs to be calculated. *Table 3* shows the definition of the SIL depending on the PFH.

Table 3. Definition of SIL according to IEC 61508-2 for a high demand/continuous mode.

SIL	High demand/Continuous demand mode: Probability of dangerous failure per hour (PFH)
1	$10^{-6} < PFH \leq 10^{-5}$
2	$10^{-7} < PFH \leq 10^{-6}$
3	$10^{-8} < PFH \leq 10^{-7}$
4	$10^{-9} < PFH \leq 10^{-8}$

The PFD is a measure of probability with consideration of the dangerous, undetectable failure rate (λ_{DU}) and dangerous, detectable failure rate (λ_{DD}), whereas the PFH is a frequency, where only λ_{DU} is considered (Holub and Börcsök 2009; Belland and Wiseman 2016).

4.3.2 *Qualitative Requirements*

Qualitative requirements are often called "architectural constraints" as they give the necessary constraints on the system architecture to ensure sufficient fault tolerance. Architectural constraints also put a limit to the maximum SIL that can be claimed. The reason why architectural constraints are introduced, is to have a sufficiently robust architecture due to the uncertainty in failure rate data or failure modes, non-consideration of systematic failures or unrealistic parameter estimates in the PFH/PFD calculation (Lundteigen and Rausand 2006, IEC 2010b).

Safe Failure Fraction (SFF) and Hardware Fault Tolerance (HFT) are two important parameters regarding the architectural constraints. HFT represents the ability of a functional unit (hardware) to continue to perform a required function in the presence of faults or errors. An HFT of N, for example, means that $N + 1$ faults could cause a loss of the safety function (IEC 2010b).

According to the IEC 61508 standard, failures can be classified according to their effect as *safe* or *dangerous* and be split again into the two categories *detected* or *undetected*. Particular caution applies for *"No effect"* failures, which do not count as safe failures (safe failures are defined as failures that lead to a safe state e.g. a shutdown) and are not considered in the calculation (IEC 2010b).

SFF is the ratio between the sum of the safe failure rate (λ_S) and the detected dangerous failure rate (λ_{DD}) over the sum of the total failure rate (safe and dangerous λ_T).

$$SFF = \frac{\sum \lambda_s + \sum \lambda_{DD}}{\sum \lambda_T} \quad (1)$$

IEC 61508 gives several tables (Route 1H, Route 2H) for the evaluation of the architectural constraints and required HFT according to the SFF of the system. Route 2H can be followed, if failure rates are recorded from field data and there is sufficient confidence in the data, otherwise Route 1H has to be followed. When following Route 1H, the standard gives two tables (*Table 4* and *Table 5*) for Type A components and Type B components. Type A components are defined as simple components, where failure modes are well defined and the behaviour under fault conditions can be completely determined. Type B components in contrast are all components, where those characteristics do not apply (e.g. components that contain software) (IEC 2010b).

Table 4. Route 1H Type A components.

Route 1H type A components			
	Hardware fault tolerance		
Safe failure fraction	0	1	2
<60%	SIL 1	SIL 2	SIL 2
60% - <90%	SIL 2	SIL 3	SIL 3
90% - <99%	SIL 3	SIL 4	SIL 4
99%	SIL 3	SIL 4	SIL 4

Table 5. Route 1H Type B components.

Route 1H type B components			
	Hardware fault tolerance		
Safe failure fraction	0	1	2
<60%	Not allowed	SIL 1	SIL 2
60% - <90%	SIL 1	SIL 2	SIL 3
90% - <99%	SIL 2	SIL 3	SIL 4
99%	SIL 3	SIL 4	SIL 4

4.4 *Approach for the Verification of Hardware Safety Integrity*

In this chapter one way to verify the hardware safety integrity of a SIS is presented. The individual steps are shown in *Figure 6* (Catelani, Ciani and Luongo 2010a).

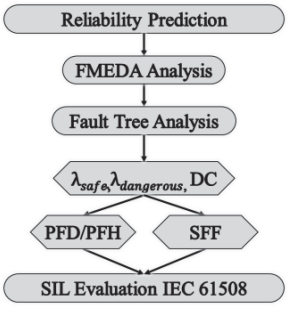

Fig. 6. Steps for the verification of hardware safety integrity (Catelani, Ciani and Luongo 2010a).

The first step of this approach is a reliability prediction for all components that are part of the SIF. The Mean Time To Failure (MTTF) or Failures In Time (FIT) can be estimated by either, using standards, field data or values from the manufacturer calculated through accelerated lifetime tests. These failure rates are the basis for all further calculations.

The second step is a Failure Modes, Effects and Diagnostic Analysis (FMEDA) where the necessary parameters λ_{SD}, λ_{SU}, λ_{DD} and λ_{DU}, which are needed for the calculation of PFH and SFF, are determined. A FMEDA is similar to a Failure Modes and Effects Analysis (FMEA), where all failure modes of each component, their immediate failure effects, failure effects on system level and failure causes are determined. In contrast to a FMEA, a FMEDA does not use a quantitative approach for the determination of critical component failure modes, but additionally considering the failure rate and failure mode probabilities of the components. The failure rates come from the prediction and failure mode probabilities can be obtained from standards or other databases. In a FMEDA the failure rate is divided into λ_{SD}, λ_{SU}, λ_{DD} and λ_{DU} by including the Diagnostic Coverage (DC) (Kim and Kim 2012; Catelani et al. 2010b). The DC is the ratio of the detectable failure rate and the total failure rate:

$$DC\ (safe\ coverage) = \frac{\lambda_{SD}}{\lambda_{SD}+\lambda_{SU}} \quad (2)$$

$$DC\ (dangerous\ coverage) = \frac{\lambda_{DD}}{\lambda_{DD}+\lambda_{DU}} \quad (3)$$

The DC could be given either by the manufacturer on basis of fault insertion tests or field data or estimated from the tables in Annex C of IEC 61508-part 2, which include several components. In this case, the DC was defined on basis of considerations like:

(i) DC = 0%, if the fault is never detected.
(ii) DC = 25%, if the fault is only detected due to maintenance, checks or tests.
(iii) DC = 50%, if the fault is only detected in specific conditions/operation modes.
(iv) DC = 75%, if the main part of the faults is detected.
(v) DC = 100%, if the fault is always automatically detected (Catelani, Ciani and Luongo 2010a).

Table 7 shows an example of a FMEDA for a capacitor from the software ©Isograph.

Table 5. FMEDA of a capacitor in ©Isograph.

Description	Dangerous failure	DC	Effects (immediate)	End Effects	SFF	λ_{DU}
C41 - short (49%)	no	100	No 24V	Unexpected interlock	1	0
C41 - change in value (29%)	no	50	Filter not working properly	Degraded mode	1	0
C41 - open (22%)	no	50	Filter not working properly	Degraded mode	1	0

After the completion of the FMEDA, architectural constraints can be determined by following a four-step procedure.

(i) Assessment and classification of the subsystem components.
(ii) Calculation of the SFF for each component.
(iii) Determination of the achievable SIL of the subsystem.
(iv) Determination of the achievable SIL of the SIF (Lundteigen and Rausand 2006).

In the first step, the subsystem components need to be assessed and classified with respect to their complexity (Type A or Type B). The SFF of each component must be calculated according to Eq. (1). Then the HFT and achievable SIL of the subsystems can be determined by considering redundancies and voting channels in the system architecture. The last step is the determination of the achievable SIL of the system by using merging rules. If subsystems are installed in series the system SIL is restricted by the lowest SIL and if subsystems are installed in parallel the overall SIL is equal to the highest subsystem SIL plus one level (Lundteigen and Rausand 2006).

The PFD or PFH can be calculated by using Fault Tree Analysis (FTA) or Reliability Block Diagrams (RBD) based on the calculated failure rates (λ_{SD}, λ_{SU}, λ_{DD}, λ_{DU}) in the FMEDA (Belland and Wiseman 2016; Innal et al. 2010) Eq. (4) (©Isograph) shows the calculation of the PFD (probability Q):

$$PFD = Q = \lambda_{DU} \cdot \frac{\tau}{2} \cdot \frac{PTC}{100} + \lambda_{DU} \cdot \frac{\sigma}{2} \cdot \left(1 - \frac{PTC}{100}\right) + \lambda_{DU} \cdot MTTR \quad (4)$$

PTC	Proof Test Coverage
τ	Test Interval
σ	Overhaul interval
MTTR	*Mean Time To Repair*

Eq. (5) (©Isograph) shows the calculation of the PFH (frequency ω):

$$PFH = \omega = \lambda_D \cdot (1 - Q) \quad (5)$$

λ_D	Dangerous failure rate

Within the fault trees, the PFH of the system is calculated with Eq. (6) (©Isograph) for OR-gates and Eq. (7) (©Isograph) for AND-gates.

$$\omega_{Sys} = \sum_{i=1}^{n} \omega_i \quad (6)$$

$$\omega_{Sys} = \sum_{j=1}^{n} \omega_j \cdot \prod_{i=1}^{n} Q_i \quad (7)$$

From the results of the fault tree and the architectural constraints, a SIL evaluation can be made according to the presented tables from IEC 61508.

5. SIL Verification of the Hardware Safety Integrity of the CROME System

All mentioned steps have been performed with the software ©Isograph for the defined SIF "Interlock Triggering" with a SIL requirement of SIL 2 for the prototype PQ of the CROME system. This function is under continuous demand and includes the measurement and calculation of the related dose rate, the decision of triggering an interlock signal and the signal transmission to the final elements (Connectic board, frontend board, processing board and adapting board of the CMPU and CUPS). The analysis only considers technical failures of the system, as during normal operation, no human impact on the safety function is possible.

5.1 *Reliability Prediction*

The failure rate prediction for all components was performed according to the FIDES standard. An appropriate life profile has been considered including different phases (winter and summer for CROME systems installed outside), with their ambient/ cycling/ minimum and maximum temperature and relative humidity (FIDES 2010).

5.2 *FMEDA Analysis*

The FMEDA analysis was performed together with the board designers. Each element of the SIF and all its possible failure modes were considered. For every possible component failure mode, the effects on the system and its detectability were defined. Thus, the component failure modes could be separated in safe, dangerous and detectable/undetectable. *Figure 8* shows an excerpt of the FMEDA.

5.3 *PFH Calculation*

The PFH calculation is performed with fault trees, which are based on the FMEDA. The results show that when considering effective automatic diagnostics of the SIF the PFH in failures per million hours (fpmh) is:

$$\text{PFH} = 8.24 \cdot 10^{-8} \text{fpmh}$$

According to *Table 3*, this value is equivalent to SIL 3 ($10^{-8} < PFH \leq 10^{-7}$).

Responsible: HSE-RP	CROME - Failure Modes, Effects and Detectability Analysis (FMEDA)	Date: 14/03/2018
Project: CROME		EDMS NO.: 1935638
Version: V1		Prepared by: Saskia Hurst

ID	Description	Failure modes	Higher effect	End effect	Dangerous failure %	Dangerous coverage %	Safe coverage %	Detected safe failure rate	Undetected safe failure rate	Detected dangerous failure rate	Undetected dangerous failure rate
1.1.1.1.2	Non-polarised Capacitor 470pF 2kV, TDK	(IB) C4, C9 - Short	No 24V_1	Degraded mode CROME	0	0	50	7.35133943503547E-05	7.35133943503547E-05	0	0
		(IB) C4, C9 - Change in value	Filter not working properly	Degraded mode CROME	0	0	50	4.35079272685773E-05	4.35079272685773E-05	0	0
1.1.1.1.3	Polarised Capacitor 22uF 50V, Kemet	(IB) C6 - Short	No 24V	No alert CROME	0	0	100	0.00822833849601834	0	0	0
		(IB) C6 - Change in value	Filter not working properly	Degraded mode CROME	0	0	50	0.00101363590168342	0.00101363590168342	0	0
		(IB) C6 - Open	Filter not working properly	Degraded mode CROME	0	0	50	0.00083475897785693 3	0.00083475897785693 3	0	0
1.1.1.1.4	Non-polarised Capacitor 1uF 50V, Taiyo Yuden	(IB) C8 - Short	No 24V_1	Degraded mode CROME	0	0	100	0.0186375543802391	0	0	0
		(IB) C8 - Change in value	Filter not working properly	Degraded mode CROME	0	0	25	0.00275759733177007	0.0082727919953102	0	0
		(IB) C8 - Open	No 24V_1	Degraded mode CROME	0	0	100	0.00836788155847469	0	0	0
1.1.1.1.5	Single Outputs DCDC Converter, TRACO, THN 20WI Series	(IB) IC8 - Short input	No 24V_1	Degraded mode CROME	0	0	100	0.0593425941574879	0	0	0
		(IB) IC8 - Short output	No 24V_1	Degraded mode CROME	0	0	100	0.0593425941574879	0	0	0
		(IB) IC8 - Open input	No 24V_1	Degraded mode CROME	0	0	100	0.0593425941574879	0	0	0
		(IB) IC8 - Open output	No 24V_1	Degraded mode CROME	0	0	100	0.0593425941574879	0	0	0
		(IB) IC8 - Wrong regulation	No 24V_1	Degraded mode CROME	0	0	75	0.0445069456181159	0.0148356485639372	0	0
1.1.1.1.6	Non-polarised Capacitor 10uF 50V, Taiyo Yuden	(IB) C5 - Short	No 24V_1	Degraded mode CROME	0	0	100	0.0186375543802391	0	0	0
		(IB) C5 - Change in value	Filter not working properly	Degraded mode CROME	0	0	50	0.00551519466354013	0.00551519466354013	0	0

Page 8 of 366

Fig. 8. FMEDA excerpt.

5.4 *Architectural Constraints*

The evaluation of the architectural constraints with the current system structure shows that the requirements for SIL 2 are met. Regarding the architectural constraints, the achievable SIL for the SIF is limited by the lowest achieved SIL of one function. In this case, it is SIL 2 (Current measurement function on the Frontend Board).

An extraction of the results (of relevant functions for the SIF) is presented in *Table 6*.

Table 6. Excerpt architectural constraints.

Board	Functional block	Component type	SFF	HFT	SIL
Connectic board					
	Power supply low voltages	Type A	98%	0	SIL 3
	Output interface interlock	Type A	83%	1	SIL 3
	…				
Frontend board					
	High voltage power supply	Type A	99%	0	SIL 3
	Current measurement	Type B	66%	1	SIL 2
	…				

Table 6 (Continued).

Processing board					
	ZINQ	Type B	100 %	1	SIL 4
	Micro SD card	Type A	81%	0	SIL 2
	…				

Considering both the PFH and the architectural constraints, the hardware safety integrity of the CROME system Prototype PQ conforms to SIL 2.

6. Conclusion & Outlook

The presented methodology is one possible approach for the verification of hardware safety integrity for electronic systems. Based on a reliability prediction and a FMEDA, architectural constraints can be examined and the PFH or PFD can be calculated by fault trees. By comparing the obtained results with the corresponding tables in IEC 61508, a declaration of the reached SIL for hardware safety integrity can be made. For a full SIL verification, it is also necessary to consider systematic safety and software integrity. Only then the overall SIL of the system can be stated.

As an example, the stated approach has been applied to the CROME system. The results show that for the current prototype PQ, architectural constraints, as well as the PFH comply with SIL 2 (SIL 3) requirements and therefore meet the specification. Based on this study, the system will be certified by an authorized certifier.

As a next step reliability testing, including burn-in tests and accelerated lifetime tests, are planned. On the one hand, systematic failures should be eliminated by an adjusted burn-in test procedure for all CROME systems before installation. On the other hand, with accelerated lifetime tests, it is possible to make a PFH estimation from the real failure frequency for comparison with the theoretical approach.

7. Acknowledgements

This work was done within the framework of the CROME Project as part of the CERN HSE RAMSES Program. Many thanks go to Gael Ducos and Michel Pangallo for their active participation in the FMEDA analysis.

References

Boukabache, H., Pangallo, M., Ducos, G., Cardines, N., Bellotta, A., Toner, C., Perrin, D. and Forkel-Wirth, D. (2016, November). Toward a Novel Modular Architecture for CERN Radiation Monitoring. Radiation Protection and Dosimetry. *Volume 173, Issue 1-3*, Pages 240–244

Belland, J. R., Wiseman, D. (2016, January). Using Fault Trees to Analyse Safety-Instrumented Systems. Isograph Inc.

Catelani, M., Ciani, L. and Luongo, V. (2010a, September). The FMEDA Approach to Improve the Safety Assessment According to the IEC 61508. *Microelectronics reliability 50*. 1230-1235

Catelani, M., Ciani, L., Luongo, V. and Singuaroli, R. (2010b, May). Evaluation of the Safe Failure Fraction for an Electromechanical Complex System: Remarks About the Standard IEC 61508. *2010 IEEE Instrumentation & Measurement Technology Conference Proceedings*. 949-953.

FIDES Group. (2010, September). FIDES Guide 2009 Edition A - Reliability Methodology for Electronic Systems. FIDES Group.

Holub, P., Börcsök, J. (2009). Advanced PFH Calculations for Safety Integrity Systems with High Diagnostic. *2009 XXII International Symposium on Information, Communication and Automation Technologies*, 1-8.

Ingrey, A., Lerévérend, P. and Dr. Hildebrandt, A. (2007, April). Manual Safety Integrity Level. Pepperl + Fuchs.

Innal, F., Dutuit, Y., Rauzy, A., Signoret, J.-P. (2010, June). New Insight Into the Average Probability of Failure on Demand and the Probability of Dangerous Failure per Hour of Safety Instrumented Systems. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 224*. 75–86.

International Electrotechnical Commission (IEC) (2010a, August). IEC 60532 - Radiation Protection Instrumentation. IEC.

International Electrotechnical Commission (IEC) (2010b, April). IEC 61508: Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-Related Systems (all parts). IEC.

Kim, B. C., Kim, Y. J. (2012, December). Case Study on the Assessment of SIL Using FMEDA.

Lundteigen, M. A. and Rausand, M. (2006, January). Assessment of Hardware Safety Integrity Requirements.

Lundteigen, M. A. and Rausand, M. (2018, May). Reliability of safety-critical systems. Wiley