H2020-MSCA-ITN-2018-PETER. Proposal Number 812790

Pan-European Training, research and education on
Electromagnetic Risk management (PETER)

Deliverable 2.1 (D2) - Overview of EMI-Relevant IEC 61508 Techniques & Measures

Hasan Habib[1], Pejman Memar[2], Tim Claeys[1], Jens Vankeirsbilck[2]

Davy Pissoort[1], Jeroen Boydens[2]

[1] Department of Electrical Engineering, KU Leuven Bruges Campus, 8200 Bruges, Belgium

[2] Department of Computer Science, KU Leuven Bruges Campus, 8200 Bruges, Belgium

This project has received funding from the
European Union's EU Framework Programme
for Research and Innovation Horizon 2020
under Grant Agreement No 812790.

Deliverable Number	**D2.1 (D2)**
Deliverable Name	**Overview of EMI-relevant IEC61508 techniques & measures**
Deliverable Duration	April 1, 2019 to October 31, 2020
Due Date of Deliverable	October 31, 2020
Revised Due Date of Deliverable	November 15, 2020
Actual Submission Date	November 10, 2020
Deliverable Lead Partner	KU Leuven
Dissemination Level	Public
Work Package	WP2
No of Pages (Annex not included)	21
Keywords	WP2, EMI, IEC61508 techniques & measures

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

Table of Contents

Table of Figures

List of Tables

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

1. Introduction

This deliverable describes the findings after about one year of research within the PETER project on relevant techniques and measures to manage safety-related risks for systems when these are being affected by electromagnetic disturbances. More precisely, it was studied which techniques and measures described in IEC 61508 - the mother standard of nearly all functional safety standards – are effective to cope with electromagnetic disturbances and/or how these techniques and measures should be adopted to become (more) effective for this purpose.

1.1. Some background on IEC 61508

Experts from academia and industry have been working together for about 20 years to create IEC 61508 [1][2]. IEC 61508 is an international standard published by the International Electrotechnical Communication (IEC) and, as its title states, focuses on the "Functional Safety of Electrical/Electronic/Programmable Electronic (E/E/PE) Safety-Related Systems". IEC 61508 is a basic functional safety standard applicable to all kinds of industry. As such, many other functional safety standards are derived from it.

IEC 61508 defines functional safety as: "that part of the overall safety relating to the EUC (Equipment Under Control) and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities."

IEC 61508 provides a quite large collection of well-proven techniques and measures to reduce the safety-related risks of E/E/PE systems well below the tolerable level [3]. The techniques and measures cover all phases of the safety life cycle, ranging from setting the early requirements of the system until the decommissioning of the system. As such IEC 61508 describes how proper safety-related systems should be designed, developed, operated and maintained. Moreover, the IEC 61508 techniques and measures cover both hardware and software. They comprise, for example, specific procedures to detect errors in signals and data. If such errors would increase the functional safety risk above the tolerable level, the safety-related system should initiate a precautionary procedure and, for example, switch the system to a safe state.

IEC 61508 defines four Safety Integrity Levels (SILs). Each SIL describes the rigor with which the safety-related system should be designed, developed, operated, and maintained. Which SIL applies depends on the evaluation of the consequences of a failing safety-related system. A higher SIL level means a higher probability that the safety-related system will work as expected when needed. SIL1 is the minimum level of protection and SIL4 ensures maximum protection. Table 1 summarizes the targeted confidence levels for each SIL.

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

Table 1 - SIL levels mentioned in IEC 61508 and the associated confidence levels (Table D.1) [3]

SIL	Low demand mode of operation	Number of treated demands		High demand or continuous mode of operation	Hours of operation in total	
	(Probability of failure to perform its design function on demand)	1-$\alpha = 0.99$	1-$\alpha = 0.95$	(Probability of a dangerous failure per hour)	1-$\alpha = 0.99$	1-$\alpha = 0.95$
4	$\geq 10^{-5}$ to $< 10^{-4}$	4.6×10^5	3×10^5	$\geq 10^{-9}$ to $< 10^{-8}$	4.6×10^9	3×10^9
3	$\geq 10^{-4}$ to $< 10^{-3}$	4.6×10^4	3×10^4	$\geq 10^{-8}$ to $< 10^{-7}$	4.6×10^8	3×10^8
2	$\geq 10^{-3}$ to $< 10^{-2}$	4.6×10^3	3×10^3	$\geq 10^{-7}$ to $< 10^{-6}$	4.6×10^7	3×10^7
1	$\geq 10^{-2}$ to $< 10^{-1}$	4.6×10^2	3×10^2	$\geq 10^{-6}$ to $< 10^{-5}$	4.6×10^6	3×10^6
NOTE 1: 1-α represents the confidence level. NOTE 2: See D.2.1 and D.2.3 for prerequisites and details of how this table is derived.						

The standard framework of IEC 61508 is divided into seven parts:

1. General requirements
2. Specific requirements for the electrical, electronic and programmable electronic safety-related systems
3. Software requirements
4. Definitions and abbreviations used throughout the standard
5. Examples of methods for the determination of safety integrity levels
6. Guidelines for specific applications
7. An overview of all techniques and measures

1.2. The increasing importance of EMI for functional safety

All electronic devices are vulnerable to electromagnetic disturbances and, hence, suffer from EMI. EMI will affect the functioning of electronic devices, and in extreme cases, can cause critical failures. In addition, as every electronic device will inevitably create electromagnetic disturbances, the EM environment is getting more 'polluted'. This will only get worse as more wireless communication or high-power switching devices are being used [4].

As every E/E/PE is vulnerable to interference by electromagnetic disturbances, EMI should be considered during the hazard-and-risk analyses as a likely cause of functional safety risks for

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

modern systems. Hence, achieving a sufficiently high level of Electro-Magnetic Compatibility (EMC) plays a vital role to ensure the functional safety of a safety-related system. Figure 1 represents the relationship among EMC, functional safety, and overall safety.

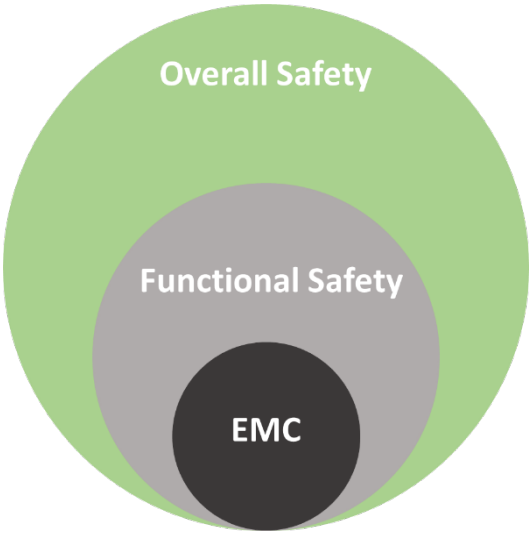

Figure 1 - Relationship among EMC, functional safety, and the overall safety.

Unfortunately, the first and second editions of IEC 61508 only take EMI into account by considering test related to the Electro-Magnetic Compatibility (EMC) Directive. However, it is already known for two decades that it is economically not viable to test all possible states for a modern digital system. Hence, managing the functional safety-related risks due to electromagnetic disturbances should take another approach [5][6], which will be described in this deliverable.

2. So, why is EMC testing insufficient for functional safety?

As stated above, a functional safety assessment should consider should and investigate all possible causes for functional safety risks of the system-at-hand. Although the second edition of IEC 61508 mentions that the occurrence of EMI should be managed for safety reasons, it does not further elaborate on this apart from referring to the EMC Directive and associated test standards.

The EMC Directive 2014/30/EU [7] limits electromagnetic emissions from equipment in order to ensure that, when used as intended, such equipment does not disturb radio and telecommunication, as well as other equipment. The directive also governs the immunity of such equipment to interference and seeks to ensure that this equipment is not disturbed by radio

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

emissions, when used as intended. However, for the purpose of the PETER project and this deliverable, it is important to note that the EMC Directive explicitly states itself that it does not cover safety in Art. (13):

> "This Directive should not deal with the safety of equipment, since that is dealt with by separate Union or national legislation"

The main aim of the CE certification, of which the EMC Directive is a part, is to allow for a single European market into which there are European-wide rules for free circulation of goods.

In order for manufacturers to get presumption-of-compliance to the essential requirements of the EMC Directive, many EMC standards have been developed over the last decades [8]. The main focus of these EMC standards is testing of a final prototype of the product. Unfortunately, for safety-related systems, this approach has several major shortcomings [9]:

1. The common approach in the EMC standards is to test the electronics' immunity against well-prescribed types of electromagnetic disturbances by applying those to a new, perfectly constructed prototype in a benign physical/climatic environment leaving the life cycle (ageing, vibrations, temperature) out of the picture. These tests are based on economic/technical compromises to account for (say) up to 90% of the electromagnetic disturbances that normally occur in the electronics environment.
2. While electromagnetic interference in practice can easily occur together with other foreseeable faults (such as short-circuits, dry joints or out of tolerance components to name a few), these are not addressed in the testing prescribed by the EMC standards.
3. In the immunity tests prescribed in the EMC standards, electromagnetic disturbances are applied one by one. However, in real-life multiple electromagnetic disturbances can occur simultaneously, possibly leading to quite different failure modes.
4. In the real-life environment, there are several reflections from EM disturbances of various devices. These reflections can combine with each other and disturb the system, but they are not considered during tests performed in typical anechoic or semi-anechoic EMC test chamber that is being used.
5. Mitigation techniques in case of failures are typically limited to "hardware-only" solutions (extra shielding, filtering, grounding, etc.)

In [3], an example is given to clearly show that it is economically not viable to prove functional safety of a digital system through testing alone. The example is repeated here.

All digital systems are non-linear, which means that even if it was possible to test 99% of all their possible states, the test results could not be extrapolated to provide any reliable information about the behavior of the remaining 1%.

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

This results in a well-known problem: digital systems can fail in an unpredictable manner as the direct result of untested combinations of perfectly correct input. For example, if a digital system had four inputs each digitized to 8-bit accuracy, plus sixteen binary inputs (either on or off), and all inputs were independent of each other, there would 2^{48} possible combinations of correct inputs, about 2.10^{14}. At 100 nanoseconds per test it would take $2{\cdot}10^{5}$ seconds to test them all – about 2.3 days (if testing 24/7).

Of course, there are many more system states than are required for just the "input space", not least to handle the processing of the input data, and to discover whether EMI could cause an unsafe error or malfunction by immunity testing alone would require each EMC test to be applied in turn to all possible system states. However, limiting our example to the input space alone, when performing a radiated immunity test (e.g. to IEC 61000-4-3) the lowest frequency would be set at the correct level (taking measurement uncertainty into account), and the test would dwell at that frequency while the complete set of correct input states was exercised. For the simple example system above, this would take 2.3 days. Then the test frequency would be stepped 1% higher for another 2.3 days, and 230 such steps would cover one decade of frequency, taking nearly 1.5 years, 24/7. The whole process would then be repeated with three other angles of incidence, and again with 90° antenna polarization.

So even the simple example system discussed earlier would need 12 years of EMC testing (24/7) to perform an IEC 61000-4-3 test covering just one frequency decade, on its "input space" alone.

Assuming all of the digital states (not just input space) could be tested in 5 days, and testing conducted RF immunity on two cable ports from 100kHz to 100MHz; radiated disturbances from 100MHz to 10GHz; EFT/B at four test levels on one cable, and four test levels of ESD on 10 test points would need about 58 years of testing, 24/7.

Of course, this is all a gross simplification: clever testing techniques might be able to be used to reduce the testing time; and it might also be possible to speed up the testing of the system states. Assume that "intelligent" digital testing techniques reduce the number of states to be tested by 10 (without, of course, compromising our design confidence of between 99.99% and 99.99999%); this simple example of a safety-related system could be EMC tested in about 6 years. Although most EMC test laboratories would be very pleased to provide this amount of testing, even if their customers could afford the cost almost no-one could countenance such a long delay in their project.

The above example is possibly unrepresentative of future mass-produced safety-related systems. Assuming this to have eighteen 8-bit digitized monochrome camera inputs, it would have 2^{144} possible input states, which is 2^{103} more than the worked ex-ample above. Even with "intelligent" digital testing techniques giving a 10:1 reduction and just 10 nanoseconds per test, testing its

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

input space alone with just one radiated frequency, one angle of incidence and one antenna polarization would need a dwell time of more than $6 \cdot 10^{26}$ years (24/7).

3. Techniques and measures to ensure the safety of the system

In recent past, several working groups within the IET and the IEEE EMC society have undertaken a goal to develop proper guidance on how to manage functional safety risks due to electromagnetic disturbances. The latest state-of-the-art is described in IEEE 1848-2020 "Standard for Techniques and Measures to Manage Functional Safety and Other Risks with Regard to Electromagnetics Disturbance" [10]. P1848 describes an IEC 61508-inspired risk management approach and provides guidance about assessment, measurement and usage of techniques and measures (T&Ms) to reduce overall functional safety risks with regard to electromagnetic disturbances [11].

IEEE 1848 introduces the concept of EM Resilience. The overall approach of IEEE 1848 is to first minimize possible errors and failures. As there will always be some remaining errors and failures, one must implement ways to detect these errors followed by either a correction or a switch of the system to the safe state

IEEE 1848 lists a quite extensive set of techniques and measures and that help to ensure that a system remains acceptably safe despite unforeseeable EM disturbances. IEEE 1848 links these techniques and measures to the SILs of IEC 61508 by giving a specific recommendation for each technique and measure. These recommendations are shown in Table 2. Based on these recommendations, (independent) assessment of the design can be performed to verify that functional safety risks related to electromagnetic disturbances have been properly managed.

The IEEE 1848 techniques and measures can be divided into three flavours. First, we start with T&Ms for diverse redundancy:

a. Using several detectors for detection of the same information.
b. Using several communication channels to transfer the same data.
c. Storing data in multiple copies.
d. Processing the same data in different processors.
e. Using multiple signals to represent the same information and using it to identify an error.
f. Using voting on the received data to identify the correct information.

Note that the use of diversity is essential to properly manage functional safety risks due to electromagnetic disturbances. Electromagnetic disturbances influence many different components in a system at the same time. A common redundant system has two or more

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

identical sets of hardware and software with the same inputs, and performs the same operations on them. When a malfunction occurs in one of these 'parallel channels', a comparator/voter detects that their outputs no longer agree and triggers appropriate actions to maintain safety. Unfortunately, the malfunctions that an electromagnetic disturbance creates in identical channels can easily be so similar that the comparator/voter cannot tell that there is a problem at all. So, electromagnetically diverse channels are a necessity.

Table 2 - Types of recommendations for different safety integrity levels [12]

HR	the technique or measure is highly recommended for this safety integrity level. If this technique or measure is not used then the rationale behind not using it should be detailed with reference to Annex C during the safety planning and agreed with the assessor.
R	the technique or measure is recommended for this safety integrity level as a lower recommendation to a HR recommendation.
---	the technique or measure has no recommendation for or against being used.
NR	the technique or measure is positively not recommended for this safety integrity level. If this technique or measure is used then the rationale behind using it should be detailed with reference to Annex C during the safety planning and agreed with the assessor.
HR: *Highly Recommended*, R: *Recommended*, ---: *No Recommendation*, NR: *Not Recommended*	

Second, there are various techniques and measures for error detection and correction, including:

a. Using enough redundant data to make the error detectable, i.e. Error Detection Coding (EDC).
b. Using enough redundant data which can remove or allow to remove data with error, i.e. Error Correct Coding (ECC).
c. Self-testing at startup, using simple hardware- or software-based checks.
d. Dynamic hardware- and software-based checks during operation by transmitting pre-determined data and analyzing it at the receiver end.

Third, some techniques and measures aim at managing the influence of electromagnetic disturbances on power supplies:

a. Using in-built comparators to ensure power supply is supplying power within a certain design limit.

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

b. Internal batteries are used for the power supply, and external supplies are used for charging the batteries or external power is always compared with a fixed voltage of batteries.
c. Using multiple power sources and then comparing the voltage difference between them.
d. In case of power failure, the system should first switch to a safe state using batteries to avoid possible system failure.

It is important to note that IEEE 1848 include both software- and hardware-based techniques and measures. Table 3 shows various software-based techniques and measures mentioned in IEC 61508, followed by their recommended usage for a certain SIL level.

Table 3 - Various software-based techniques mentioned in IEC 61508 and their recommended usage for a certain SIL level (Part of table A.2) [12]

Technique and Measures		Ref.	SIL 1	SIL 2	SIL 3	SIL 4
	Architecture and design feature					
1	Fault detection	C.3.1	---	R	HR	HR
2	Error detecting codes	C.3.2	R	R	R	HR
3a	Failure assertion programming	C.3.3	R	R	R	HR
3b	Diverse monitor techniques (with independence between the monitor and the monitored function in the same computer)	C.3.4	---	R	R	---

3.1 Recent research on hardware-based techniques and measures

Several hardware-based techniques and measures are developed to ensure the functional safety of the system. The research leading to this mainly aimed at addressing the challenge on how to apply, in a cost-effective way, electromagnetically diverse channels in a redundant system. The techniques and measures try to improve the Bit-Error-Rate (BER) and decrease the amount of false-negatives when affected by harsh electromagnetic disturbances. This section covers the recent developments in this area.

Degraeve et al. have studied the effectiveness of spatial diversity within redundant channels. In this study, the authors cope with interference caused by strong incident plane waves as well within a reverberation environment [13], [14]. For the latter, a large set of plane waves is used as a source for the analysis. A simple triple-redundant wired communication channel at the

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

printed circuit board level is used as a case study. It is found that using different orientations of the different channels in the redundant system is needed to significantly improve the BER.

In [15], Lannoo et al. studied the use of different termination schemes at the ends of the three redundant channels to check if this could introduce EM-diverse behaviour and positively effect the BER. It was found that different termination schemes do not contribute significantly and that matching all ends of the redundant channels is the best approach.

In [16], Lannoo et al. studied the use of two channels with inverted data. In this approach, opposite bits are transmitted on both channels to transfer the same information. For instance, if '0' in the first channel represents "*low*", '1' also has the same representation (i.e. "*low*") in the second channel. In the case that the received data from both channels do not align, then the voter triggers a warning to put the equipment under consideration (EUC) into a safe state. It was shown that this does not improve the BER a lot compared with the reference, but allows to enable safe actions when anomalies are detected. This is something what a differential pair is not capable of.

In [17] and [18], two other potential methods were investigated, namely time and frequency diversity, respectively. These methods change timing and frequency parameters of the transmission data line coding technique. This changes the sampling position of the induced disturbance voltage and effectively improves the BER response. Both time and frequency diversity have their specific advantages and disadvantages.

The implementation of a matched filter is something that is well known in digital processing, but was never applied to an EM-diversity technique. In [19], the matched filter was first investigated to cope with harsh Continuous Wave (CW) sinusoidal disturbances using a theoretical framework. Next, in [20] the implementation was further expanded to analyse the effect of using a matched filter against possible different phase and amplitude modulated signals. The implementation of the matched filter was altered slightly to be implemented using an oversampling factor of the base communication frequency. This investigation showed positive results.

When using the above described methods, different choices can be made by the voters. This allows to create a system with a higher availability (but also higher safety risks) or a system that could activate safe actions sooner (and has a lower availability). This is described in [21]. In addition, the effectiveness of the voting mechanism versus the matched filter is described in [22]. This shows that a matched filter could be more effective than using voting on the same analogue samples.

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

More recently, Habib et al. have proposed the design of a low-cost EMI detector to detect the occurrence of electromagnetic disturbances in a wired communication channel [23]. In this study, the proposed EMI detector uses an inverted data line pair to transmit the same data. In this setup, one line sends the normal data, and the other line transmits the inverted data. Accordingly, it performs arithmetic operations on received voltages to detect the electromagnetic disturbances and generates a warning when these corrupt the data. This can help the system to trigger a precautionary procedure and switch the system to a safe state. Theoretical simulations are used to validate the findings. It has been shown that the proposed EMI detector can detect the EMI disturbances in most cases.

3.2 Recent research on software-based techniques and measures

From the data communication viewpoint, EMI induces voltages onto communication channels or internal hardware. As a result of that, bit-flips are generated in the transmitted data or the embedded system's hardware. To tackle this problem, various software-based techniques have been developed and used as an extra layer of protection throughout the communication [24]. These techniques include Error Detection and Correction Codes (EDCCs), Control Flow Error (CFE) detection, and Data Flow Error (DFE) detection. In the following section, the recent developments in this area will be covered.

Van Waes et al. have studied the EMI effectiveness of different software-based single-bit error EDCC techniques. EDCCs add redundant information to the original data, which is used during decoding to detect or even correct the corrupted data.

First, the resiliency of Cyclic Redundancy Checks (CRC) has been considered [25]. In this study, they have shown that at some frequencies, the ratio of false negatives (i.e. undetectable invalid data) can rise to 50% of all the received data words. Three techniques, including choosing an appropriate CRC code, choosing a different bit frequency and combining multiple error detection layers, have been proposed to overcome this downside.

Thereafter, the effectiveness of Hamming codes was investigated [26]. The simulations described in [19] showed that under certain conditions, the impact of the introduced overhead cannot be compensated by the single error-correcting capabilities of the Hamming codes. Furthermore, it has been shown that for a specific bit and disturbance frequency and for larger data sets, the use of a Hamming code provides limited to no advantage.

Later, the EMI-resiliency of Data Triple Modular Redundancy (TMR), also called Triplication, was investigated in [27]. The results demonstrated that certain variants of triplication were better equipped to deal with electromagnetic interference than others. However, it has been found

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

when the disturbance frequency equals an integer multiple of the bit frequency, all variants significantly lose their advantages.

Then, the preliminary findings have been extended regarding the effectiveness of a Hamming single error correction code and data triplication, respectively. The authors update those findings by considering the use of overvoltage protection systems [28]. It is found that the EMI-resiliency depends on the ratio between the bit-rate frequency and the disturbance frequency. At a specific ratio, each of the considered EDCCs has an increased vulnerability for false negatives. Finally, the main cause behind that downside were uncovered, which were the repetitive or alternating bit patterns within the codes themselves.

Finally, the insights of [28] have been used to cope with false negatives and find the most EMI-resilient Triplication-based codes. It is found that a code with inversion is significantly more robust to these disturbances [29].

Memar et al. have extended this research horizon by considering multiple-bit error EDCCs. As the first step, the behavior of Primitive Reed-Solomon codes (RSCodes) under harsh EMI has been investigated [30]. Reed-Solomon codes are cyclic, non-binary, and linear block-based error correction codes [31]. They can be used as a forward error correction (FEC) in data communication owing to their strong correction capability. Like other EDCCs, RSCodes also takes advantage of adding redundant information to the original message for recovering the possibly corrupted data. It is found that the EMI-resiliency of RSCodes depends on the ratio among the bit-rate frequency, the disturbance frequency, and the symbol size. This resiliency significantly decreases at a specific ratio where all elements/symbols of a code word turn into an identical value (i.e. repetitive pattern).

In parallel to the mentioned studies, Thati et al. and Vankeirsbilck et al. have studied and proposed various CFE and DFE detection techniques. A CFE occurs when there is an error in the execution order of instructions, a DFE, on the other hand, occurs when the input, intermediate or output data gets corrupted.

In [32], Thati et al. have compared different well-known DFE techniques. These techniques are briefly explained in Table 4. It is concluded that soft error detection using software redundancy (SEDSR) and error detection by duplicated instructions (EDDI) have a better trade-off between fault coverage and overheads than software-implemented fault tolerance (SWIFT), critical block duplication (CBD), and overhead reduction (VAR3+). Furthermore, it is shown that, Error detection by diverse data and duplicated instructions (ED4I) and software approach (SA) had better fault coverage, but at the expense of execution time and code size usage.

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

Table 4 - Brief explanation of the compared techniques in [32]

Technique	Explanation
ED^{4}I	A full code duplication mechanism in which all instructions in the basic blocks are duplicated.
EDDI	A full code duplication mechanism with selective comparison in which all instructions in the basic blocks are duplicated.
SA	It is a full code duplication mechanism with selective comparison. In this mechanism, all instructions in the basic blocks are duplicated as in ED4I and EDDI. However, in SA, comparison instructions must be placed after the last original and duplicated instructions in each basic block to compare their results.
SWIFT	It is a selective instruction-based code duplication technique. This technique is the improved version of EDDI in which all instructions in the basic blocks are duplicated, except store instructions.
VAR3+	A selective instruction-based code duplication technique in which all instructions in the basic blocks, except branch and store instructions, are duplicated.
CBD	A selective code duplication mechanism based on the basic blocks in which critical blocks must be identified in the control flow graph.
SEDSR	This technique is the extended version of CBD in which critical blocks (i.e. blocks with two or more incoming edges) must be identified in the control flow graph.

In [33], Thati et al. have proposed a new approach, called Full Duplication and Selective Comparison (FDSC) technique. FDSC combines the ideas of existing techniques by duplicating the entire codebase and placing comparison instructions in critical basic blocks only. This approach was compared with three established techniques: Error Detection by Diverse Data and Duplicated Instructions (ED^{4}I), Critical Block Duplication (CBD) and Software Implemented Fault Tolerance (SWIFT). The result showed a noticeable increase in fault detection ratio as well as a decrease in code size and execution time overhead.

In another study [34], Thati et al. have developed a new software approach based on instruction level duplication and comparison, called Instruction Level Duplication and Comparison (ILDC), for DFE detection. This approach was implemented in five different case studies. To validate the proposed technique, its fault detection ratio and execution time overhead were measured and compared with the following two existing techniques: overhead reduction (VAR3+) and software-

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

implemented fault tolerance (SWIFT). The results showed that ILDC detects more errors than VAR3+ and SWIFT at a lower over-head.

In [35], Thati et al. have presented another novel software-based approach to counter DFEs, called Selective Duplication and Selective Comparison (SDSC). It is shown that the proposed SDSC technique has a higher error detection ratio with a lower silent data corruption compared to both the Critical Block Duplication (CBD) and near Zero silent Data Corruption (i.e. a mechanism in which the stored values are loaded back from memory and checked against the stored value) techniques, but at the cost of a slightly higher execution time overhead.

To tackle CFEs, Vankeirsbilck et al. [36] have proposed a novel signature monitoring technique called random additive signature monitoring (RASM). This approach uses signature updates with random values as well as optimally placed validity checks to detect inter-block CFEs. It is shown that RASM has a higher detection ratio, lower execution time overhead, and lower code size overhead than the studied approaches.

Moreover, in [37], Vankeirsbilck et al. have proposed a new approach called Random Additive Control Flow Error Detection (RACFED). RACFED extends the functionality of RASM by placing gradual signature updates after each instruction. It is found that RACFED can detect most of the CFEs, while having a lower execution time overhead than the considered existing techniques, i.e. Relationship Signatures for Control Flow Checking (RSCFC) and Software-Implemented Error Detection (SIED).

Later, Thati et al. have proposed a hybrid approach to detect both DFEs and CFEs, called Data and Control Flow Error Detection (DCFED) [38]. DCFED merges the previous developed DFE and CFE detection techniques, i.e. FDSC (i.e. a mechanism in which all basic blocks are duplicated except blocks with only branch instructions) and RACFED, respectively, to create one technique which can detect both data flow and control flow errors. This approach was compared with a similar technique called Software Implemented Error Detection (SIED). The results showed that DCFED achieves a higher error detection ratio.

4. Work in progress to reduce EMI related safety risks

From the beginning of the PETER project, two parallel research paths are being pursued, namely one in hardware (ESR5) and one in software (ESR6).

ESR5's work focuses on the development of an EMI detector with no or a reduced number of false negatives. As it is impossible to restrict electromagnetic disturbances with some specific

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

characteristics, there is a dire need to develop a detector to detect BERs caused by such disturbances. The ongoing work is considering the development of an EMI detector using a differential pair data transmission lines followed by advanced signal processing techniques to detect EMI disturbances in all cases. Current results show that the EMI detector works effectively in most cases except when the distance between a pair of transmission lines is quite large, or the EMI frequency lies in a specific range.

The main goal of ESR6' research is to investigate the EMI-resiliency of EDCCs for multiple-bot errors and to improve their resiliency against electromagnetic disturbances. More specifically, ESR6 considers circumstances where EDCCs are unable to detect the incorrect data; this type of error is defined as a false negative. The behavior of Primitive Reed-Solomon codes has been investigated for the past couple of months. Improving the resiliency of RSCodes against EMI is the next step of this research path.

5. Conclusions

This overview summarized crucial aspects of IEC 61508 concerning EMI relevant techniques. It has been concluded that current EMC testing is largely insufficient to guarantee the safety of safety-related systems. IEEE 1848 desribes techniques and measures to manage functional safety risks with regards to electromagnetic disturbances by making it more resilient for electromagnetc disturbances. This was followed by a description of recent research results on hardware- and software-based techniques and measures. Initial research for enhancing EMI related functional safety includes hardware-based techniques such as spatial and inversion diversity, accompanied by a voter, as well as software-based techniques for investigating the EMI-resiliency of single-bit EDDCs. Current research tries to fill the gap in these domains and improve the effectiveness of utilized systems by focusing on the detection of EMI disturbances followed by precautionary measures and the development of multi-bit EDCCs using e.g. primitive Reed-Solomon codes.

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

References

[1] IEC 61508 “Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-Related Systems (Seven parts).”

[2] R. Bell, “Introduction and Revision of IEC 61508,” in *Advances in Systems Safety*, Springer London, 2011, pp. 273–291.

[3] “IEC 61508 Edition 2.0 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures,” *Int. Electrotech. Comm.*, 2010.

[4] D. Pissoort and K. Armstrong, “Why is the IEEE developing a standard on managing risks due to EM disturbances?,” in *2016 IEEE International Symposium on Electromagnetic Compatibility (EMC)*, 2016, pp. 78–83.

[5] K. Armstrong, “Introduction to EMC for Functional Safety Introduction to EMC for Functional Safety Introduction to EMC for Functional Safety.”

[6] K. Armstrong and C. Com, “KHBO Seminar Oostende 6 February 2013 EMC for Functional Safety Introduction to EMC for Functional Safety,” 2013.

[7] “Directive 2014/30/eu of the European parliament and of the council of 26 february 2014 on the harmonization of the laws of the member states relating to electromagnetic compatibility,” *Off. J. Eur. Union*, 2014

[8] “IEC - Electromagnetic compatibility - EMC Product Standards > Product families for EMC standards.” [Online]. Available: https://www.iec.ch/emc/emc_prod/prod_main.htm. [Accessed: 14-Oct-2020].

[9] K. Armstrong, “EMI and functional safety why traditional immunity testing is inadequate and what should be done instead,” in *17th International Zurich Symposium on Electromagnetic Compatibility, 2006*, 2006, vol. 2006, pp. 469–472, doi: 10.1109/emczur.2006.214973.

[10] K. Armstrong, D. Pissoort, A. Degraeve, and J. Lannoo, “Reducing functional safety and other risks due to EM disturbances: IEEE Standard 1848,” in *2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility, EMC/APEMC 2018*, 2018, pp. 199–204, doi: 10.1109/ISEMC.2018.8393766.

[11] D. Pissoort, J. Lannoo, J. V Waes, A. Degraeve, and J. Boydens, “Techniques and measures to achieve {EMI} resilience in mission- or safety-critical systems,” *IEEE Electromagn. Compat. Mag.*, vol. 6, no. 4, pp. 107–114, 2017, doi: 10.1109/MEMC.0.8272297.

[12] “IEC 61508 Edition 2.0 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements,” *Int. Electrotech. Comm.*, 2010.

This project has received funding from the European Union’s EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

[13] A. Degraeve and D. Pissoort, “Study of the effectiveness of spatially EM-diverse redundant systems under reverberation room conditions,” in *IEEE International Symposium on Electromagnetic Compatibility*, 2016, vol. 2016-Septe, pp. 374–378, doi: 10.1109/ISEMC.2016.7571676.

[14] A. Degraeve and D. Pissoort, “Study of the effectiveness of spatially EM-diverse redundant systems under plane-wave illumination,” in *2016 Asia-Pacific International Symposium on Electromagnetic Compatibility, APEMC 2016*, 2016, pp. 211–213, doi: 10.1109/APEMC.2016.7523012.

[15] J. Lannoo, A. Degraeve, D. Vanoost, J. Boydens, and D. Pissoort. “Study on the use of different transmission line termination strategies to obtain EMI-diverse redundant systems”. In: *2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC)*. 2018, pp. 210–215

[16] J. Lannoo, A. Degraeve, D. Vanoost, J. Boydens, and D. Pissoort, “Effectiveness of inversion diversity to cope with EMI within a two-channel redundant system,” in *2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility, EMC/APEMC 2018*, 2018, pp. 216–220, doi: 10.1109/ISEMC.2018.8393769.

[17] J. Lannoo, J. Van Waes, A. Degraeve, D. Vanoost, J. Boydens, and D. Pissoort. “Effectiveness of Time Diversity to Obtain EMI- Diverse Redundant Systems”. In: *2018 International Symposium on Electromagnetic Compatibility (EMC EUROPE)*. 2018, pp. 288–292

[18] J. Lannoo, D. Vanoost, J. Vanwaes, J. Peuteman, J. Boydens, and D. Pissoort. “Effectiveness of Frequency Diversity to Create EM-Diversity in Triple- Modular Redundant Data Transmission Systems”. In: *IEEE Transactions on Electromagnetic Compatibility* (2020)

[19] J. Lannoo, J. Van Waes, D. Vanoost, J. Boydens, and D. Pissoort. “The Effectiveness of a Matched Filter to Cope with Harsh Continuous Wave EMI”. In: *2019 IEEE International Symposium on Electromagnetic Compatibility, Signal Power Integrity (EMC+SIPI)*. 2019, pp. 35–39

[20] J. Lannoo, T. Claeys, D. Vanoost, J. Van Waes, J. Boydens, and D. Pissoort. “Effectiveness of a Matched Filter to Cope With Harsh Phase and Amplitude Modulated EMI”. In: *IEEE Transactions on Electromagnetic Compatibility* 62.4 (2020), pp. 1582–1590

[21] J. Lannoo, J. Van Waes, D. Vanoost, J. Boydens, and D. Pissoort. “Analysis of Availability and Safety Considerations in EM-Diverse Systems”. In: *2019 International Symposium on Electromagnetic Compatibility - EMC EUROPE*. 2019, pp. 927–932

[22] J. Lannoo, J. Van Waes, D. Vanoost, J. Boydens, and D. Pissoort. “Comparing the Performance of a Matched Filter and Majority Voting to Cope with Harsh Electromagnetic Disturbances”. In: *2020 International Symposium on Electromagnetic Compatibility (EMC EUROPE)*. 2020

This project has received funding from the European Union’s EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

[23] H. Habib, T. Claeys, D. Vanoost, and G. A. E. Vandenbosch, and D. Pissoort, "Development of an EMI Detector Based on an Inverted Data Pair with Reduced Number of False Negatives," in *2020 International Symposium on Electromagnetic Compatibility - (EMC EUROPE)*, 2020.

[24] R. W. Hamming, "Error detecting and error correcting codes," *Bell Syst. Tech. J.*, vol. 29, no. 2, pp. 147–160, 1950.

[25] J. Van Waes, J. Lannoo, A. Degraeve, D. Vanoost, D. Pissoort, and J. Boydens, "Effectiveness of cyclic redundancy checks under harsh electromagnetic disturbances," in *2017 International Symposium on Electromagnetic Compatibility-EMC EUROPE*, 2017, pp. 1–6.

[26] J. Van Waes *et al.*, "Effectiveness of Hamming Single Error Correction Codes under Harsh Electromagnetic Disturbances," in *IEEE International Symposium on Electromagnetic Compatibility*, 2018, vol. 2018-August, pp. 271–276, doi: 10.1109/EMCEurope.2018.8485176.

[27] J. Van Waes, J. Vankeirsbilck, J. Lannoo, D. Pissoort, and J. Boydens, "Effectiveness of data triplication in harsh electromagnetic environments," in *2018 International Symposium on Electromagnetic Compatibility (EMC EUROPE)*, 2018, pp. 266–270.

[28] J. Van Waes, D. Vanoost, J. Vankeirsbilck, J. Lannoo, D. Pissoort, and J. Boydens, "Resilience of Error Correction Codes Against Harsh Electromagnetic Disturbances: Fault Mechanisms," *IEEE Trans. Electromagn. Compat.*, pp. 1–11, Aug. 2019, doi: 10.1109/temc.2019.2931369.

[29] J. Van Waes, D. Vanoost, J. Vankeirsbilck, J. Lannoo, D. Pissoort, and J. Boydens, "Resilience of Error Correction Codes Against Harsh Electromagnetic Disturbances: Fault Elimination for Triplication-Based Error Correction Codes," *IEEE Trans. Electromagn. Compat.*, 2020.

[30] P. Memar, J. Vankeirsbilck, D. Vanoost, D. Pissoort, T. Holvoet, and J. Boydens, "Reed-Solomon Codes Resilience Against Harsh Electromagnetic Disturbances: Fault Mechanisms," 2020.

[31] W. A. Geisel, "Tutorial on Reed-Solomon error correction coding," 1990.

[32] V. B. Thati, J. Vankeirsbilck, N. Penneman, D. Pissoort, and J. Boydens, "CDFEDT: Comparison of data flow error detection techniques in embedded systems: an empirical study," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, 2018, pp. 1–9.

[33] V. B. Thati, J. Vankeirsbilck, N. Penneman, D. Pissoort, and J. Boydens, "An improved data error detection technique for dependable embedded software," in *2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC)*, 2018, pp. 213–220.

[34] V. B. Thati, J. Vankeirsbilck, D. Pissoort, and J. Boydens, "Instruction Level Duplication and Comparison for Data Error Detection: a First Experiment," in *2018 IEEE XXVII International Scientific Conference Electronics-ET*, 2018, pp. 1–4.

[35] V. B. Thati, J. Vankeirsbilck, J. Boydens, and D. Pissort, "Selective Duplication and Selective Comparison for Data Flow Error Detection," in *2019 4th International Conference on System*

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

Reliability and Safety (ICSRS), 2019, pp. 10–15.

[36] J. Vankeirsbilck, N. Penneman, H. Hallez, and J. Boydens, “Random Additive Signature Monitoring for Control Flow Error Detection,” *IEEE Trans. Reliab.*, vol. 66, no. 4, pp. 1178–1192, 2017.

[37] J. Vankeirsbilck, N. Penneman, H. Hallez, and J. Boydens, “Random additive control flow error detection,” in *International Conference on Computer Safety, Reliability, and Security*, 2018, pp. 220–234.

[38] V. B. Thati, J. Vankeirsbilck, D. Pissoort, and J. Boydens, “Hybrid Technique for Soft Error Detection in Dependable Embedded Software: a First Experiment,” in *2019 IEEE XXVIII International Scientific Conference Electronics (ET)*, 2019, pp. 1–4.

This project has received funding from the European Union’s EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/