Pan-**E**uropean **T**raining, research and education on **E**lectromagnetic **R**isk management (PETER)

Deliverable 4.2 – Flow diagram for an EMI-aware safety case

Authors:

Mohammad Tishehzan[1], Dr Mark Nicholson [1], Dr John F. Dawson [2]
Dr Davy Pissoort[3]

[1] Department of Computer Science, University of York, York, UK

[2] Department of Electronic Engineering, University of York, York, UK

[3] Department of Electrical Engineering, KU Leuven Bruges Campus, 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. 812.790

Deliverable Number	**D4.2 (D6) – updated version**
Deliverable Name	**Flow diagram for an EMI-aware safety case**
Deliverable Duration	April 1, 2019 to May 31, 2021
Due Date of Deliverable	May 31, 2021
Actual Submission Date	**June 8, 2021**
Deliverable Lead Partner	University of York
Dissemination Level	Public
Work Package	WP4
No of Pages	29
Keywords	WP4, EMI, Safety case

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

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 Figures

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

The occurrence of Electromagnetic Interference (EMI) in electrical and electronic devices may cause a wide range of degradations in the performance and functionality of systems. There has been a large body of standards applied to different systems and devices to demonstrate the Electromagnetic Compatibility (EMC) for them. However, compliance with those standards does not imply that a system's functionality is adequately safe once exposed to any and all kinds of Electromagnetic Disturbances (EMD). The majority of EMC-related standards heavily rely on EMC testing, and the performance of devices is monitored in a limited number of scenarios that do not cover all possible situations during the system's operation. Therefore, replacing the traditional approach with a more robust and yet cost-effective risk-based approach is essential.

Applying a risk-based approach necessitates considering EMI as a cause of system failure from the earliest phases of the system engineering lifecycle. Generally, it includes understanding the electromagnetic environment that the system is intended to operate in, analysing and reducing the contribution of EMI to system safety risks and verifying and validating the final product so that it can be certified/approved for release to service. Once released to service, the required EMI-related activities during operation of the system should be considered. In other words, it is essential to have a comprehensive procedure to make sure that EMI issues have been taken into account during the system lifecycle and the related safety risks are identified and diminished to an acceptable degree. Increasing test levels based on accurate risk identification of the EM environment (risk-based EMC) was an initial attempt to achieve safety. However, due to the limitations of this approach, the idea of EM resilience has been developed.

Different safety standards such as IEC 61508 [1] and ARP 4754 (and ARP 4761) [2], [3] provide an overall safety lifecycle that should be followed along with the system lifecycle. They include general guidelines and requirements to ensuring safety in each phase of the lifecycle. However, they do not explicitly describe how to address the contribution of EMI to system safety. In order to provide more apparent EMI safety requirements, the IEC 61000-1-2 [4] has been published based on IEC 61508 methodology. Moreover, the newly published IEEE 1848 [5] gathered some techniques and measures that can be applied to increase the system's resilience against EMI.

A widely recognised practice for demonstrating the safety properties of the system to the different stakeholders is to develop a safety case for the system. A safety case employs clear and comprehensible arguments to show that the given evidence meets applicable safety requirements in the related context. An EMI-aware safety case provides evidence and arguments about how the evidence demonstrates the system is acceptable safe despite potential EMI caused by internal or external sources of electromagnetic disturbances. An EMI-aware safety case can ease the system's integration, particularly in modular systems, where

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/

there are concerns about the compatibility of the elements. It would also facilitate the certification process through its structured argumentation.

Developing an EMI-aware safety case brings EMC/EMI engineering, Safety engineering and Systems engineering together and requires an interdisciplinary collaboration (see Figure 1). In this deliverable, an overview of argumentation about safety against EMI is presented. The contribution of different EMI related activities during the lifecycle to develop the safety case is investigated, and the overall EMI-aware safety case development process leading to EMI-aware safety case is provided.

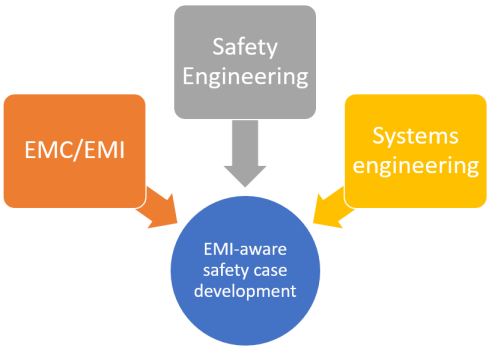

Figure 1- Developing an EMI-aware safety case requires interdisciplinary collaboration

The deliverable is organised as follows: section 2 comprises the introduction of systems engineering and associated safety processes and the safety case approach. In section 3, the argumentation about safety against EMI is investigated, and the workflow for producing a safety case is presented in section 4. Then, the application of the workflow in the maritime context is discussed in section 5. Finally, in section 6, future required works for expanding the workflow are noted.

2. Systems Engineering and Associated Safety Assurance Process (SAP)

Systems engineering is a cross-practice discipline that has evolved to manage the complexities of processes and systems by implementing systematic methodologies to the entire lifecycle of a system [6]. One of the primary targets of system engineering is to assure that the defined functional and non-functional (e.g. safety) requirements of a system are satisfied during the development and operation stages of a system. Hence, the safety process of a system has consistent interaction with the development steps of a system which also continues during the post-release period. In this section, the process of system engineering and system safety engineering is discussed, and the Safety Case approach, which is a highly practised approach for demonstrating safety, is explained.

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/

2.1. Systems Engineering and SAP Workflow

The guidelines and standards in different industries propose a system lifecycle that fits better the processes of that industry. Despite the differences between details of their defined steps, the overall path of steps is relatively similar. For instance, the ARP 4754a development process of a system is illustrated in Figure 2. It starts from concept development and planning at the earliest phases of the lifecycle and then continues with defining top-level functions and requirements, allocation of functions and decomposition of the requirement into the lower levels and realisation of the system during design and implementation steps.

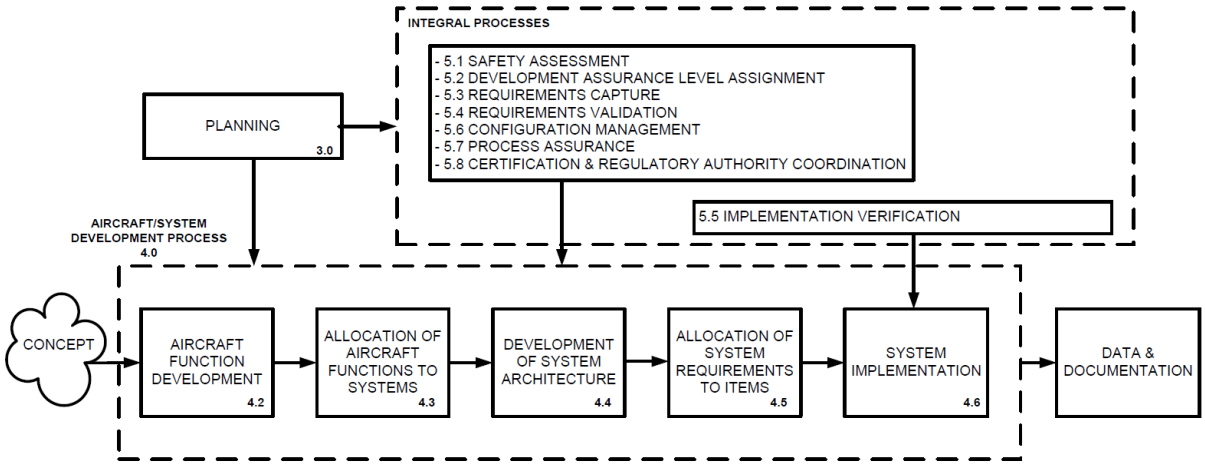

Figure 2- System development process model of ARP 4754a [2]

The interaction of the Safety Assurance Process (SAP) with the development steps is illustrated in Figure 3. In ARP guidelines, four main safety steps in each development level (aircraft, system and item level) are considered, including all essential safety activities during the development process. Functional Hazard Analysis (FHA) examines the system functions to discover functional failures and classifies them based on their associated hazards. FHA receives the functions defined in the development process and feeds the architecture development process at each level with safety objectives.

Once the system architecture is provided, Preliminary System Safety Assessment (PSSA) exploits the system architecture and failure conditions provided by FHA to establish safety requirements and perform an early assessment on the architecture to investigate whether it can meet safety objectives associated with each failure conditions. It also updates the failure conditions list and provides feedback on the architecture for the development process. This process repeats iteratively until the architecture meets all safety objectives (see Figure 4). During PSSA, various types of safety analysis methods (FTA, FMEA, etc.) can be applied. The choice of these methods depends on the context of the system and the applicability of them. In general, PSSA has the highest contribution to the safety assessment of the system prior to the implementation phase.

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/

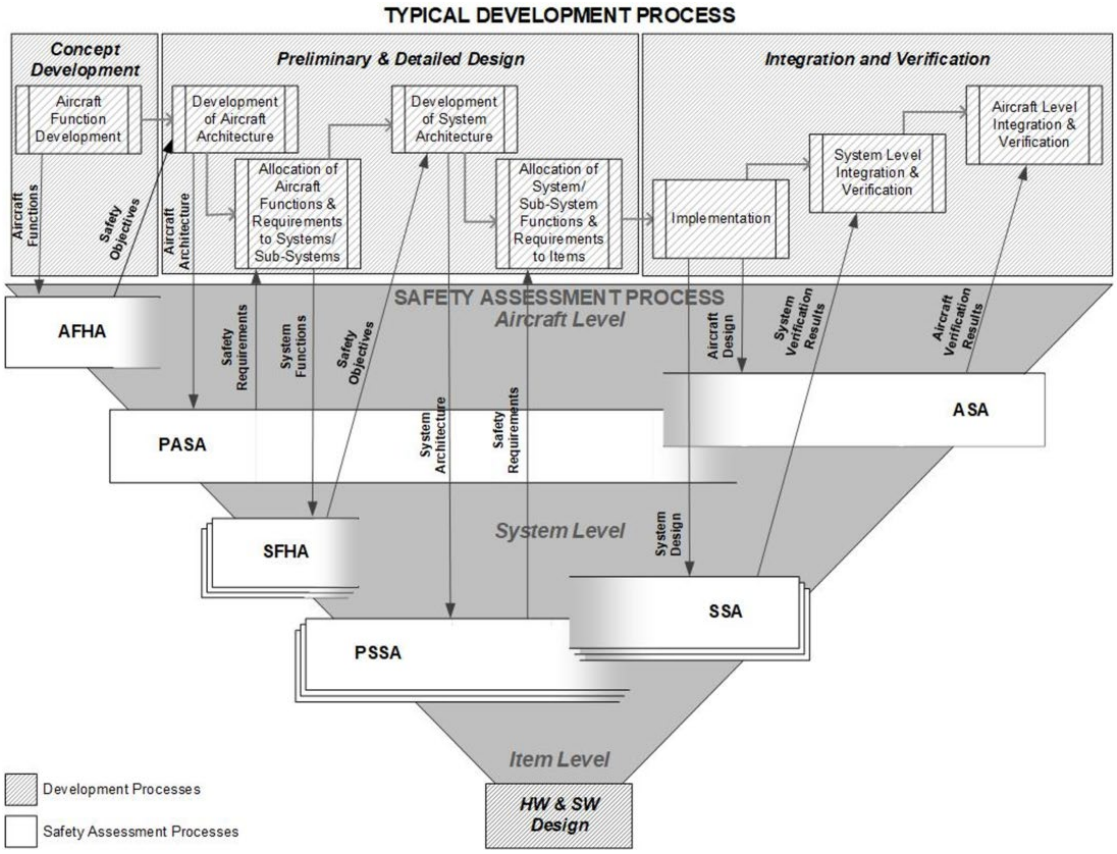

Figure 3- Interaction between Safety Assurance Process and system development [3]

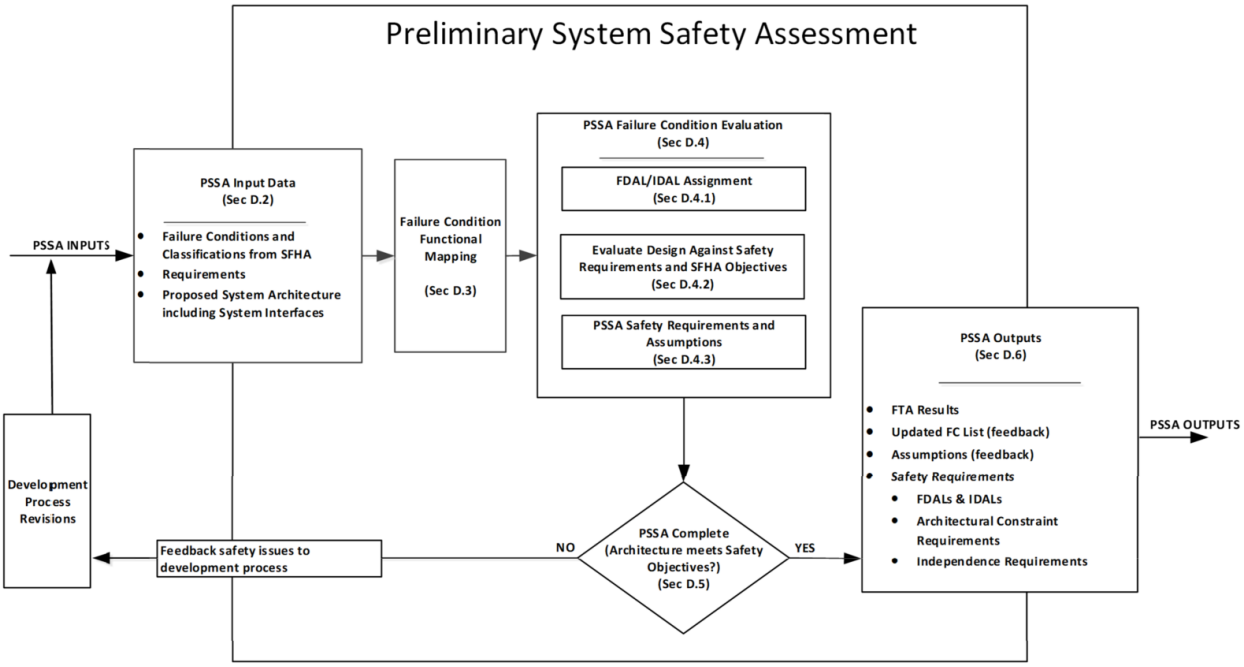

Figure 4- Flow diagram of PSSA process [3]

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 system is implemented, System Safety Assessment (SSA) investigates the system to verify that the safety requirements produced during PSSA are satisfied. If satisfaction is achieved, the results are fed into general verification of the system development. In contrast, a lack of satisfaction leads to feedback for system modification. The last safety process of the ARP guidelines is Common Cause Analysis (CCA), which investigates the dependencies between functions to identify Common Cause Failures (CCFs). This process is performed as a series of activities during PSSA and SSA.

It is noted that, although the classification of these safety processes may differ between safety standards, the essence of safety activities is similar. For instance, the PSSA can be considered equivalent to risk analysis and requirement identification and allocation steps in IEC 61508 standard.

2.1.1. Reasoning about safety achievement

The safety processes presented in the standards and guidelines reflect the steps that developers are required to follow to assess the system's safety. However, reasoning about how to implement the process and define the top-level safety objectives which demonstrate the achievement of safety in a system have been not presented by standards. Therefore, researchers and experts in different fields have been developing frameworks suitable for their context and compatible with controlling standard and processes for demonstrating safety achievement. For instance, [7] proposed a layered safety argumentation model for the automotive industry, which applies to the functional safety standard for vehicles.

Another approach for argumentation about safety is called the 4+1 principles of safety which was initially developed for software safety based on common safety standards [8], [9]. The principles provide a big picture of how safety assurance is achieved regardless of details provided in different standards and can be integrated into various contexts. These Principles are as follow:

Principle 1 - Software safety requirements shall be defined to address the software contribution to system hazards

Principle 2 - The intent of the software safety requirements shall be maintained throughout requirements decomposition

Principle 3 - Software safety requirements shall be satisfied

Principle 4 - Hazardous behaviour of the software has been identified and mitigated

Principle 4+1 - The confidence established in addressing the software safety principles shall be commensurate to the contribution of the software to system risk

Applying these principles is a potential approach for argumentation about safety in the EMI context. Therefore, in section 3, the applicability of them to EMI is discussed.

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/

2.2. Safety Cases

The safety case idea is rooted in the goal-based approach toward achieving safety. In this approach, safety should be demonstrated by reducing the risk to a tolerable level. The concept of a safety case can be defined as following [10]:

'A safety case should communicate a clear, comprehensible and defensible argument that a system is acceptable safe to operate in a particular context'

Every safety case comprises three elements: Objective, Argument and Evidence. The argument provides the reasoning behind the achievement of the Objective by considering the appropriate evidence. (see Figure 5)

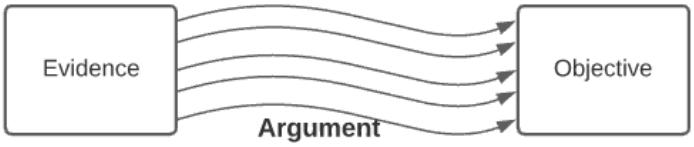

Figure 5- Argument answers the question 'How does the provided evidence lead to the achievement of the Objective?'

The Objective is a claim about the system that needs to be supported. It could be a requirement, a defined characteristic of the system, a safety goal, etc. The supporting evidence includes analysis results, tests and other clues that back up the argument that the case is based on. All three elements are required in a safety case as an argument without proper evidence is not cogent and does not lead to an acceptance that the Objective is met. Vice versa, achieving an Objective supported by evidence without proper argument is vague and requires explanation to be understood. Since the applied tools for providing the evidence, the rationale of the argument and Objective validity may include uncertainty and errors, it is required that the confidence within safety case's elements be evaluated. The 'Confidence Case' [11] is provided to demonstrate how confident we are in the elements of the safety case.

The scope of the safety case has to be determined from the early phases of development. The boundaries of the system, the operational use, and the environmental conditions of the system affect the scope of the safety case. Hence, it is essential to make sure that the scope of the safety case is monitored and controlled during development and operation. Furthermore, in cases where there are various interacting safety case arguments (known as modules [12]), the interfaces between the safety case modules that could be used for integration into a modular safety case must be defined.

A Safety Case is a live artefact that develops incrementally during the development and operation phases of the lifecycle. It should reflect the reasoning and activities that have been undertaken for identifying hazards, determining correct requirements and acceptable risk level, reducing the safety risks to the acceptable level and maintaining the safety argument

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/

during the operation. A safety case has a hierarchical structure. The defined top-level goal is broken down into sub-goals by appropriate arguments. These sub-goals are broken down again, and this process continues until the sub-goals could be supported by evidence directly (Figure 6).

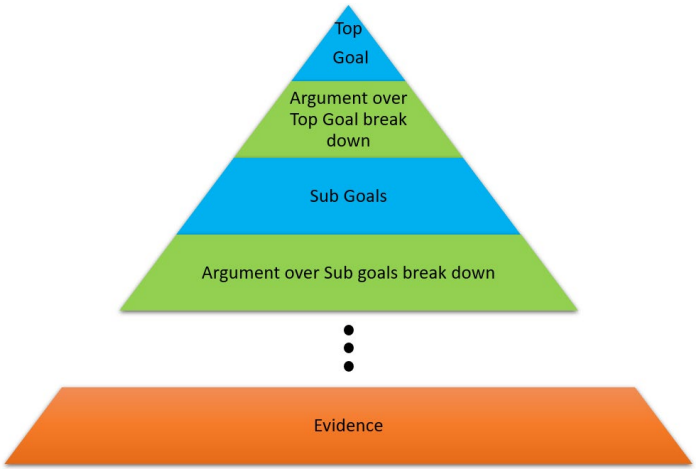

Figure 6- The hierarchical structure of the safety case

There are several ways for illustrating the argumentation in the safety case. The most simple ones are explaining them in a free text or a tabular structure. However, applying these methods may lead to ambiguity and difficulties in communication between stakeholders. Besides, traceability between safety case elements can also be problematic. Thus, graphical methods are preferred for safety argumentation. One such method, the Goal Structuring Notation (GSN), is a graphical argumentation tool that explicitly connects the safety case elements and provides a comprehensible structure for argumentation [13]. In the next part, GSN is briefly explained.

2.2.1. Goal Structuring Notation (GSN)

GSN facilitates demonstrating the interaction between safety objectives, arguments and evidence through a set of graphical elements and consequently better projection of argumentation. The primary elements of GSN can be introduced as follows:

Goal:

A claim about the system that needs to be supported. A goal could be a specified requirement, target or constraint.

Strategy:

The reasoning behind how do the goals break down into sub-goals. It is the nature of argument which connects different levels of goals.

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/

Solution:

The solutions are the items of evidence provided to support the claims. A solution could be the results of tests, analysis or a reference.

Context:

The contextual information about a goal, strategy, or solution essential to be considered is presented as a context in GSN. A context can be a reference, statement, or information about the system, environment, or requirements.

Assumption and Justification:

In some cases defining goals, reasoning behind an argument or using a piece of evidence requires some assumptions or justification. In GSN, this information could be presented via Assumption or Justification elements.

The relationship between the GSN elements can be divided into two categories. If there is a causal relationship between elements and the support of an element is required for another one, the '**SupportedBy**' link (A solid arrow) can be used. Once there is a contextual relationship between elements, the '**InContextOf**' link (A hollow arrow) will be applied

In Figure 7, the GSN elements and relationships are illustrated.

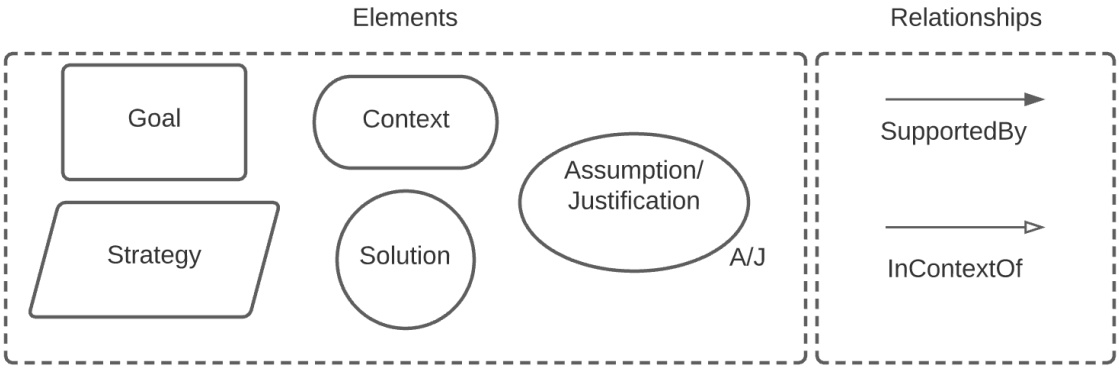

Figure 7- GSN elements and relationships

An argument used in a safety case can be reused and instantiated into another safety case. **Safety Case Patterns** provides a suitable level of abstraction and allow exploiting successful argument in multiple safety cases. Patterns could help to describe and use general principles, structures and processes for common problems in various contexts [14].

Although GSN primarily has been used for illustrating safety cases, it can also be exploited as a tool for demonstrating the technical documentation of standards and guidelines. For instance, in [15], the application of GSN in demonstrating compliance to EMC directive standards has been investigated for the first time. This study comprises two use cases: EMC assurance case for equipment tested in the EMC lab and in-situ EMC testing of large machines.

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/

3. EMI-aware safety cases

EMI can be considered a cause for many emergent failures and hazardous conditions. In some cases identifying EMI as the initial event in the failure propagation chain is not straightforward. Susceptibility to EMI arises from deficits in the architecture and design, and since EMI could affect simultaneously multiple elements and functions, it may be classified as a potential source for systematic common cause failures.

Multiple activities, including risk analysis and testing, are performed during the lifecycle. Nonetheless, there is no unique existing line of reasoning regarding safety against EMI. Argumentation about EMI related processes are the backbone of demonstrating safety and thus the EMI-aware safety case. In this section, the evolution of argumentation about functional safety in regards to EMI from risk-based EMC to EM resilience has been discussed. Then, in section 4, an overview of EMI-related activities in the lifecycle into the reasoning about safety and safety case development is explained.

3.1. Argumentation about safety against EMI

Traditionally, there has been a misinterpretation about achieving functional safety against EMI by showing compliance with harmonised EMC standards and European EMC directive [16]. Although these standards provide a baseline for the performance of the equipment, they are not intended to provide safety [17] or to provide evidence for safety assurance. Hence, there has been a gap between EMC performance processes and safety processes.

3.1.1. Previous IET guideline and IEC 61000-1-2

In order to fill this gap, the first guideline to provide confidence about functional safety regarding EMI have been developed [18]. Moreover, by considering [18] and IEC 61508 lifecycle, a particular workflow for the EMC for functional safety has been published by the IET [19]. In this approach, the worst-case scenarios for intersystem and intrasystem EM interaction are identified, and a specification for the system is created. Based on the created specification, EMC techniques are included in the design process, and the verification and validation plan is prepared. After system realisation, the V/V process is performed, and the system enters the operational phase. Eventually, the workflow proposed a list of activities for maintenance of the system. It is noted that the drawbacks of this approach led to publishing further IET guidelines [20] by focusing on EM resilience for achieving safety which is discussed in the following subsection of this deliverable.

Although the guideline does not explicitly provide argumentation about achieving safety, it can be inferred that EMC can be controlled for functional safety by following the identified workflow steps (see Figure 8). Accordingly, the top-level argument of the guideline is depicted in Figure 9. The top-level goal is achieved by ensuring that all the external EM threats and 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/

severity of all hazards caused by the EM threats are identified during risk analysis. Besides, the effects of internal components' emissions are also determined. Another argument over the design phase can be identified, which defines three goals that require addressing (G5, G6 and G7). The level of EM risks should be reduced during design to an acceptable level determined by the Safety Integrity Level (SIL). Furthermore, producing the V/V plan and also performing it should be demonstrated.

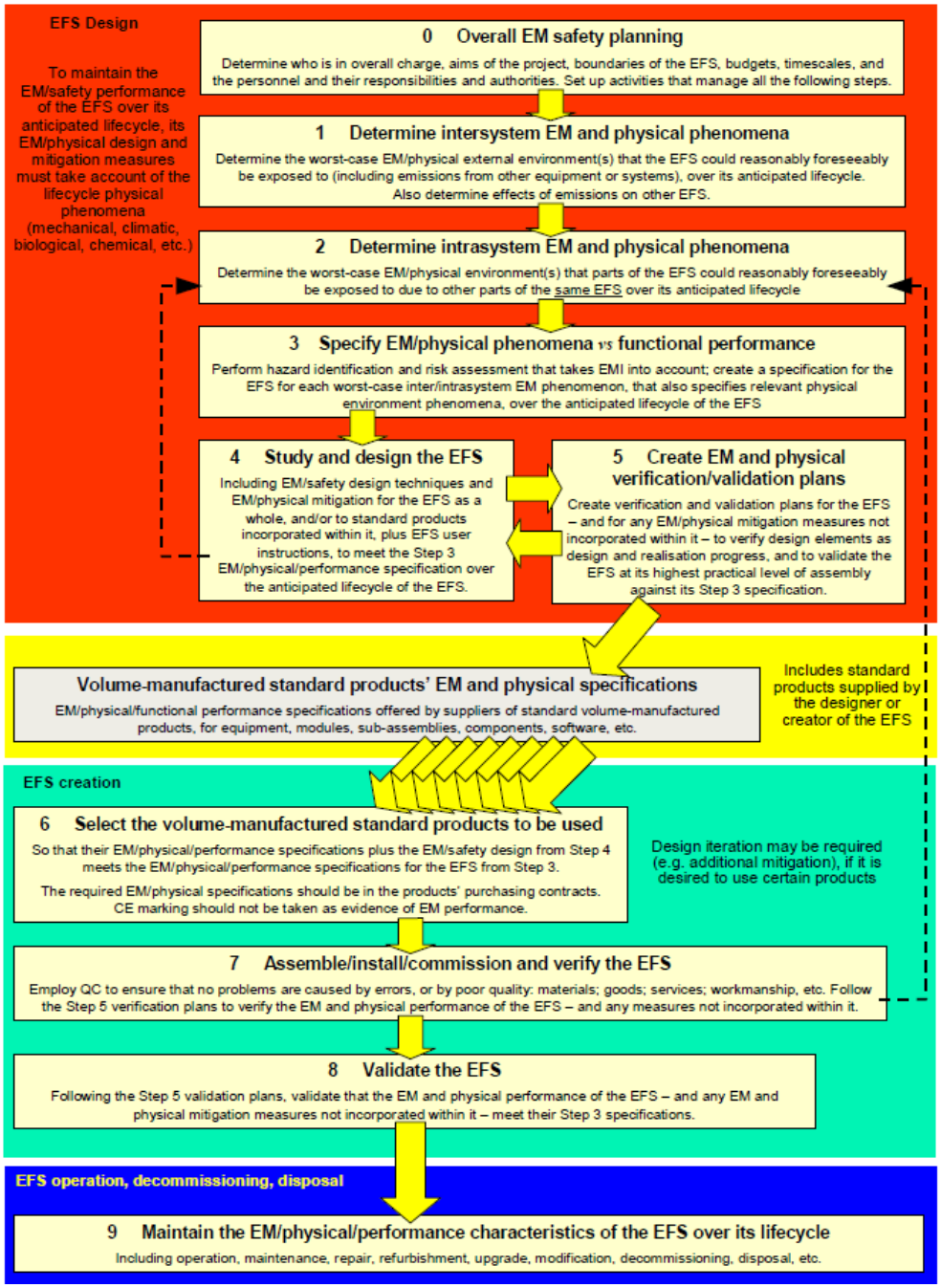

Figure 8- EMC for functional safety in IET guide [14]

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/

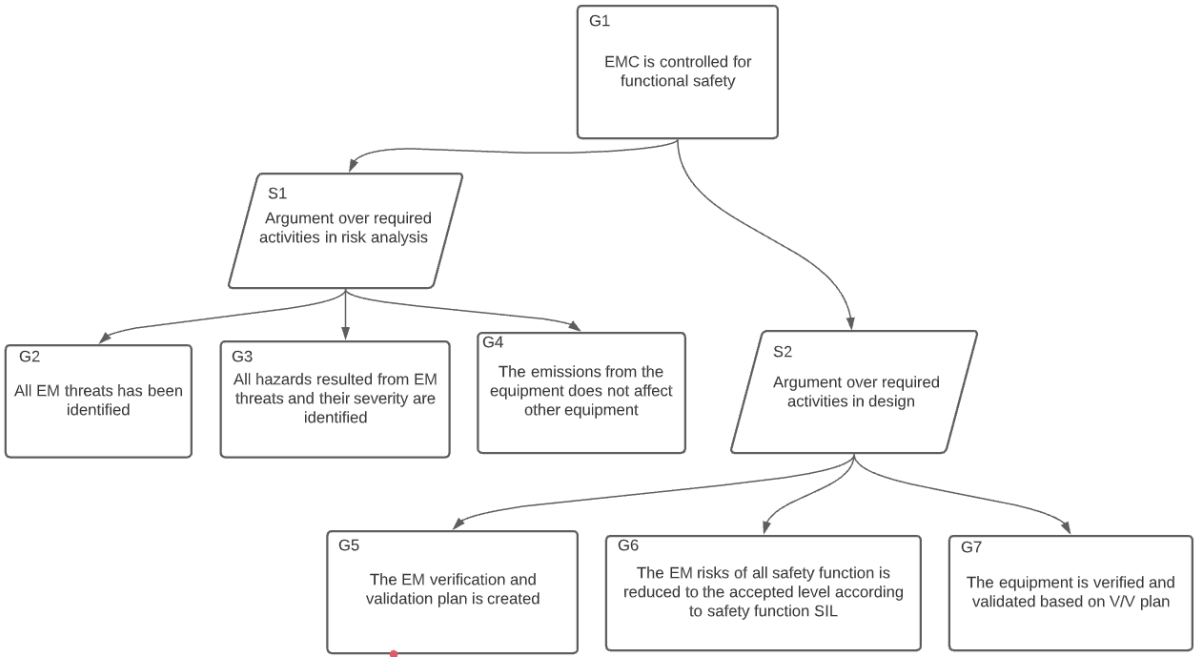

Figure 9- Top-level argument based on [13] and [14]

In 2016, IEC 61000-1-2 was published, which provides one methodology for the achievement of functional safety with regard to EM phenomena [4]. This standard proposes a process to be followed simultaneously to processes of IEC 61508 (see Figure 10). The standard considers four aspects related to EMI:

- Electromagnetic Environment
- Design and integration in equipment and system level
- Verification/Validation
- Immunity testing

It is noted that the standard does not include any activity for the operational phase. The standard states some actions and argues that by undertaking them, functional safety regarding EMI would be achieved. Therefore, the top-level argumentation of the standard is illustrated in Figure 11.

The key part of the IEC 61000-1-2 is considering the output of the electromagnetic environment assessment in the system safety requirement specification and provision of the test plan based on the most severe electromagnetic environment regardless of the Safety Integrity Level of the system, which is determined during the IEC 61508 process. Therefore, the standard suggests an additional procedure of immunity testing for safety with specific pass criteria called 'Defined State (DS)', which can be determined according to the system safety requirement specification. Alternatively, the standard suggests that DS criteria can be considered equal to criteria A (no degradation of performance or loss of function is allowed

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 equipment is used as intended) in the normal immunity tests. The difference between the normal immunity test and the safety immunity test is called the test margin.

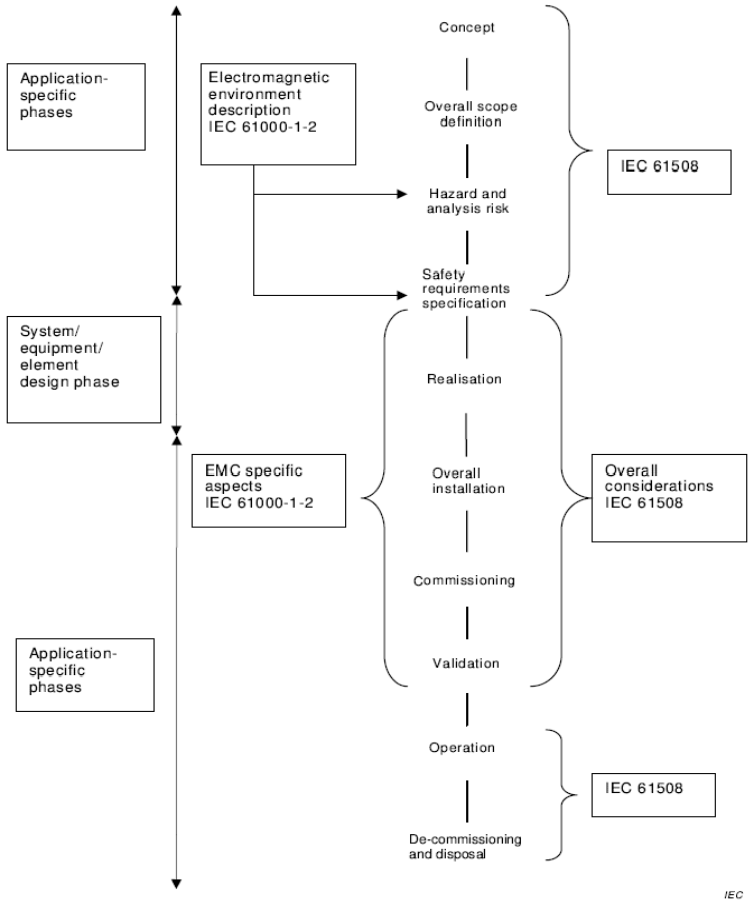

Figure 10- The IEC 61000-1-2 activities during IEC 61508 lifecycle [4]

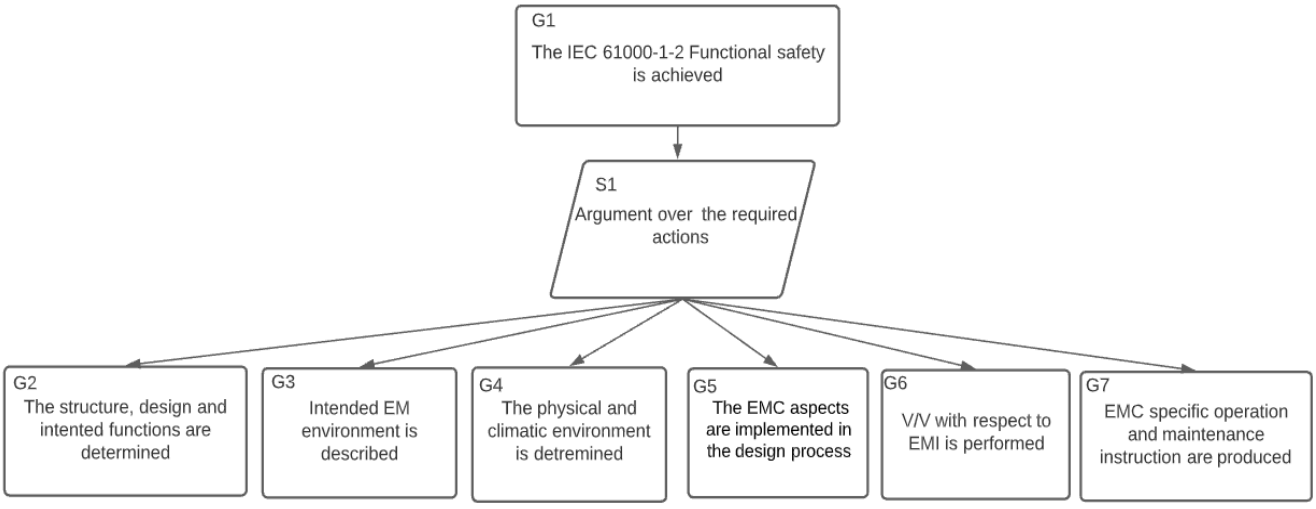

Figure 11- The top argument of IEC 61000-1-2

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/

3.1.2. Electromagnetic Resilience

The argumentation for achieving safety according to [4], [19] relies on having a comprehensive specification of the environment and increasing immunity tests levels. In [21] and [22], it is discussed that due to rapid changes in technologies, the electromagnetic environment is becoming more complex; hence, the exact specification of the EM environment may not be achieved. Furthermore, performing immunity test for functional safety when there could be numerous different test plans will be overwhelming. Consequently, it is argued that following the previous method may not be sufficiently targeted to secure functional safety.

To overcome these issues, the IET published a new guide for functional safety in regards to EMI [20] and introduced the Electromagnetic Resilience idea, where the goal is increasing tolerance of the system once exposed to electromagnetic disturbances. In order to achieve electromagnetic resilience, it is suggested that the techniques and measures (T&Ms) mentioned in IEC 61508 be tailored to become suitable for failures arising from EMI. Based on this idea, the IEEE 1848 [5] provides a list of T&Ms to be applied during the lifecycle. Similar to IEC 61508, the standard assigns an importance level to each T&M according to the Function's SIL of the system. The importance level determines whether applying the T&M is Mandatory, Highly Recommended, Recommended or Not Recommended. Some of these T&Ms may be applied during design for other purposes based on IEC 61508 recommendation, but they are also effective against EMI [23].

The top-level argument in this approach is depicted in Figure 12. Besides applying T&Ms, the approach necessitates good EMC engineering during design. Good EMC engineering comprises considering the traditional EMC rule of thumbs, the design and installation guidelines noted in standards, mitigation techniques like shielding, filtering, etc. Furthermore, complying with normal EMC standards is another goal in this approach. These standards ensure that the system's emission is controlled during operation, and a minimum level of immunity is achieved.

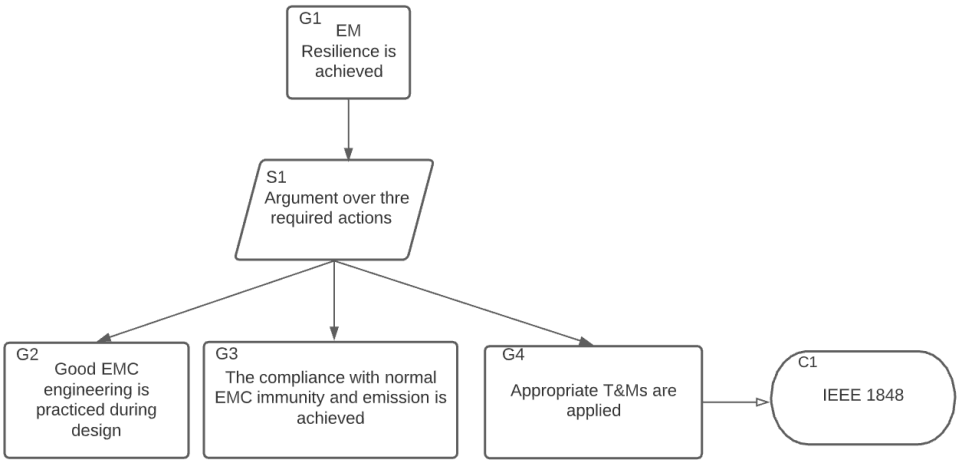

Figure 12- Top-level argument of [11]

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 approach recommends the general process of IEC 61508 for developing and operating phases but does not introduce an EMI specific workflow to follow. Moreover, it is not clear how the contribution of each T&M in the EMI risk reduction can be evaluated and the confidence in them be assessed.

3.1.3. 4+1 software safety principles applicability in EMI

Assuring the safety of a system requires reasoning and justifications based on the essence and characteristics of that system. However, often argumentations about safety are similar in a different context and only need to be tailored to fit better into that context and its aspects. In [8] and [9], the main principles for justifying the safety of software are presented. These principles are extracted based on the requirements that implicitly exist in safety standards such as IEC 61508 and ISO 26262. Therefore, they can be adapted in other contexts like demonstrating safety against EMI. They are called '4+1 principles' since they consist of four principles that justify a safe system and one more principle that addresses the confidence when enforcing and assuring those four principles. Ultimately, by addressing these principles, the safety of the system could be demonstrated. The interpretation of these principles in the EM risk management are investigated in the [24] and are called '4+1 Principles of EM Risk Management'. In this section, these principles and how they may contribute to demonstrate safety regarding EMI are explained.

Principle 1- EM [Safety] risk requirements shall be defined to address the contribution of EMDs to system hazards

This principle requires that all risks arising from software be identified and appropriate requirements for managing those risks be defined. In the case of EMI related risks, the steps of the process that controls system development should reflect that sources of EM and associated EMI risks are identified, and related requirements are defined. This principle inherently consists of two claims that must be addressed (see Figure 13). Indicating this principle can be done during environment assessment and EM requirement specification and further in risk assessment of the system architecture. Indeed, one can argue that identifying all risks may not be possible as specifying the electromagnetic environment consists of a high level of uncertainty. However, by considering only the foreseeable part of the electromagnetic totality of the environment, this issue can be addressed. This topic will be explained in the following section.

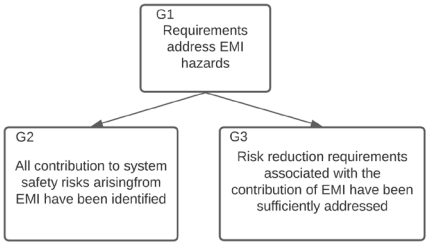

Figure 13- Principle 1 of the safety against EMI

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/

Principle 2- The intent of the EM [safety] risk requirements shall be maintained throughout requirements decomposition

This principle focuses on traceability and keeping the essence of the high-level requirement during decomposition of them into lower-level requirements as the design progresses. The EMI related requirements derived from environment assessment, risk analysis and managerial requirements derived from regulation comprise the high-level EM requirement, and the design decision for realisation and implementation can be considered low-level EMI requirements (see Figure 14).

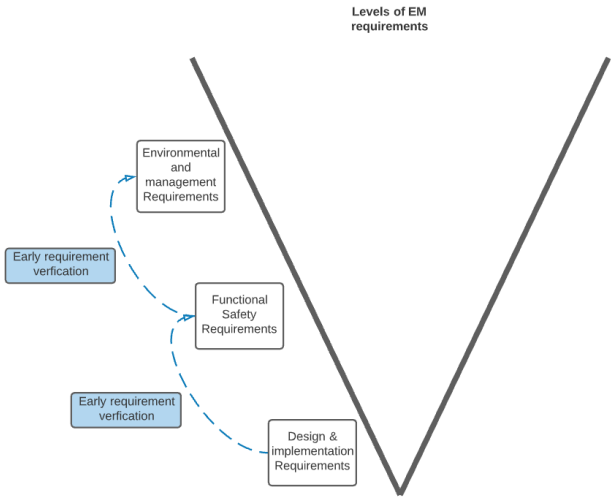

Figure 14- Levels of EM related requirements

The EMI workflow should indicate that the reasoning of EM management and environment-derived requirements can be identified in lower-level requirements. The principle can be demonstrated by employing early verification activities in the lifecycle [25]. Early verification enables not only principle 2 but helps to make sure correct requirements are identified (a part of principle 1 argument) and prevents costly reworks due to incorrect requirements specification in later development phases.

Principle 3- EM [safety] risk requirements shall be satisfied. Satisfaction of the correct defined requirements during verification and validation phases is the concept of principle 3. This principle can be demonstrated by providing evidence produced by tests, analysis or reusing trustable evidence.

Principle 4- Emergent hazardous behaviour of the system due to EMDs shall be identified and mitigated

This principle focuses on identifying unanticipated hazardous behaviour that emerged during the design process. This principle can be demonstrated by assuring that there is no error in the design process and that additional requirements are defined to mitigate any identified unanticipated behaviour [8].

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 principle affects the EMI related processes in two ways. First, unidentified or uncontrolled emission of the system's components can be considered emergent hazardous behaviours that arise from errors during the design or implementation of the system. Therefore, the defined requirements regarding the emission of the component and activities for demonstrating components' compliance with emission standards are related steps to principle 4. Moreover, the design decisions that may lead to an increase in the system's susceptibility can be regarded as emergent hazardous behaviour. This kind of EMI error is often more challenging to be managed as the causal design decisions are usually rooted in other functional and safety requirements and constraints (for instance, using redundancy or a voting system with similar technologies). One of the factors that may cause an increased likelihood of the emerging issues is that EMI related requirements to mitigate these kinds of hazardous decisions can not be defined early in the process (see Figure 15). Nevertheless, demonstrating principle 4 regarding EMI can be done by verifications during design and implementation phases. Monitoring regimes can also be defined to prompt reassessment or rework as required during the operational phases of the system lifecycle.

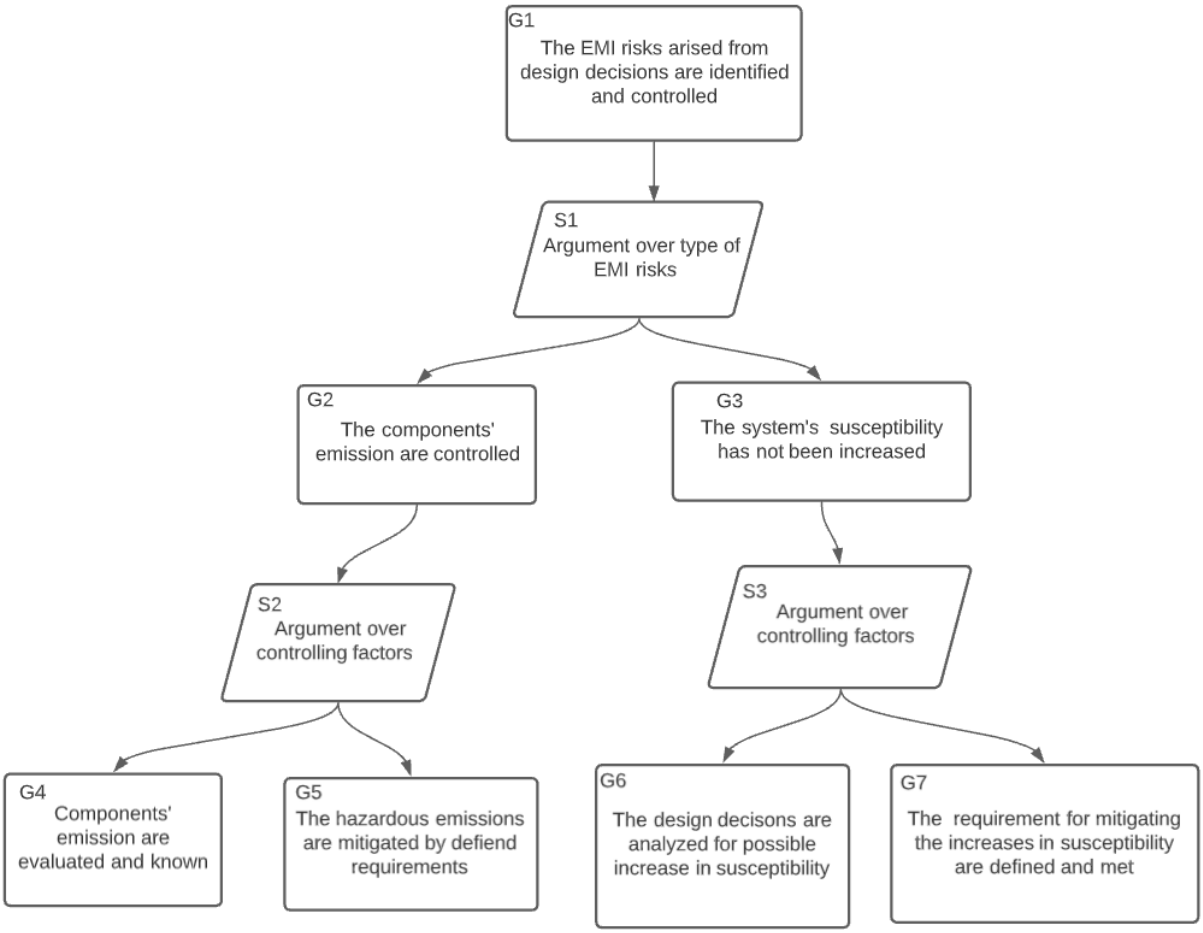

Figure 15- demonstrating principle 4 in regards to EMI hazards

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/

Principle 4+1 - The confidence established in addressing the EM [safety] risk principles shall be commensurate to the contribution of the EMD to the system [safety] risk

This principle focuses on determining and evaluating an acceptable degree of confidence within the demonstration of the four principles. The necessary rigour is determined by the safety integrity level of the concerned functions. In order to find out whether the provided evidence guarantees the required level of confidence, the appropriateness and trustworthiness of them should be assessed [8]. This principle covers all four main principles and their contribution to demonstrating safety during development phases. For instance, the argument over determining the boundary of the foreseeable electromagnetic environment, the required effort for increasing immunity, and the confidence in the provided evidence which supports the safety claims indicate the contribution of this principle.

3.1.4. The relationship between argumentations

In this section, the evolution of reasoning about the achievement of safety with regards to EMI has been discussed. The shortcomings of the IEC 61000-1-2 about having an exact specification of the environment and relying on test margins for providing safety promoted the idea of increasing the system's resilience by applying related techniques and measures. However, in this argumentation, there are some ambiguities around determining confidence in the processes. 4+1 principles provide a universal and systematic argumentation towards achieving safety and can be used to improve the reasoning behind mentioned approaches. For instance, each of the introduced EM related T&Ms can be used as an argument for establishing the safety principles.

In the next section, an overview of an EMI-aware safety workflow that can lead to achieving safety by demonstrating the safety principles is presented.

4. Workflow for developing and maintaining an EMI-aware safety case

An EMI-aware safety case is a live artefact that is incrementally developed during the lifecycle. The related activities that populate the EMI-aware safety case start from producing the EM plan and continue during the operation for maintenance and monitoring purposes. Figure 16 illustrates the general EMI activities workflow and its relationship with safety case development. Defining safety case goals starts from EM planning and continues through lifecycle as new requirements may be defined in each phase, including during operation. As the system goes through the development lifecycle, consequent safety case development activities start to evolve. By increasing the information about the environment and identifying foreseeable associated risks, the strategy for demonstrating safety and required confidence can be determined. During design and verification, evidence is provided gradually, and 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/

proposed safety case can be evaluated. Finally, upgrading the system and functional or environmental changes during operation effect, and maintenance of, safety case.

During the development phases, different kind of electromagnetic requirements can be defined based on the origin of the requirement (source of requirement elicitation), the level of development that the requirement is identified at and should be met and the concept of that requirement. In the case of EMI, three kinds of requirements can be identified (see Figure 17).

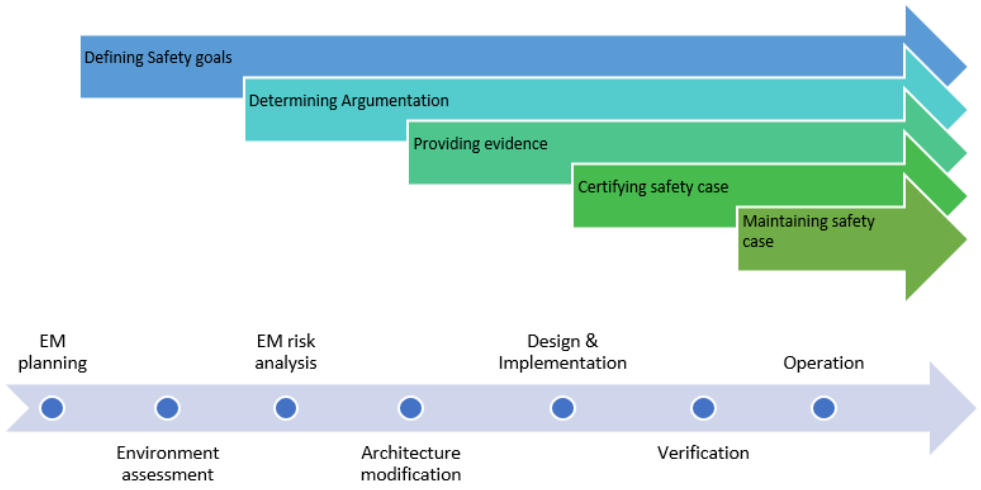

Figure 16- Relationship between EMI workflow and safety case development

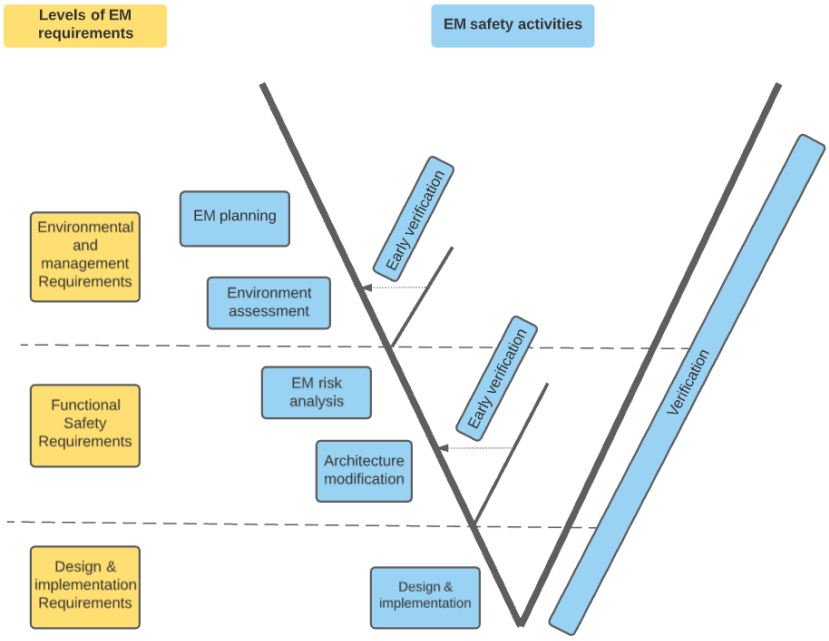

Figure 17- EM activities and related requirements in V diagram of development phases

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/

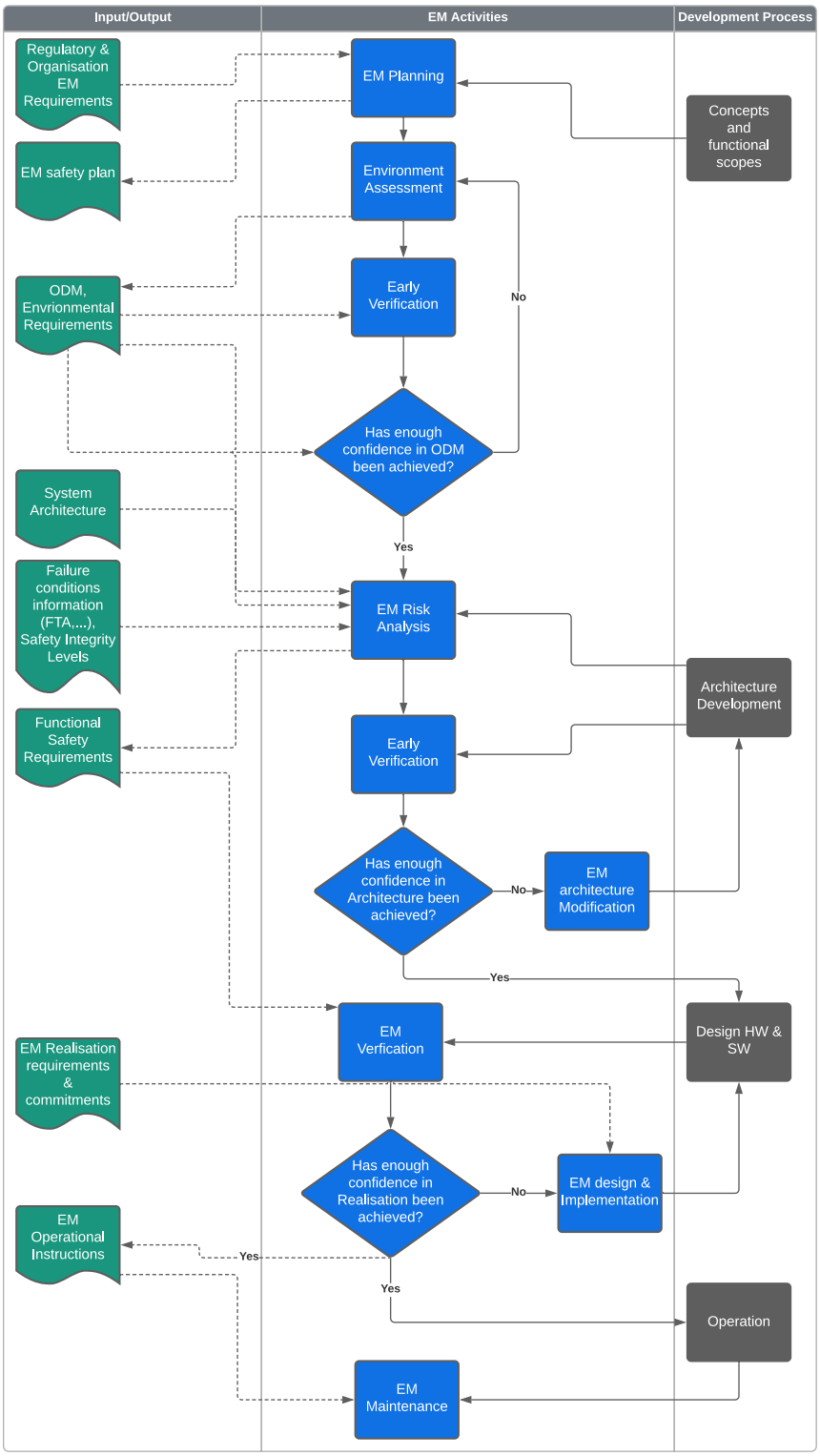

Figure 18- Flow Diagram of EM activities and their interactions with the development process to Achieve EM Resilience

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/

The top-level requirements are derived from organisational and regulatory necessities. They include the required EM and safety standards and guidelines that the system should comply with and any specific EM-related requirement asked for by the stakeholders. Moreover, the requirements derived from external environment assessment such as totality of foreseeable electromagnetic fields, climate, etc., and physical consideration of the system can be considered the Environment and management requirements. These requirements are identified during EM planning and environment assessment, which are often performed at early development phases and considered as the input for system structure development. It is essential to verify these requirements as early as possible, as these requirements and assumptions comprise the intent of lower-level requirements and modification of them in later phases leads to costly and challenging system changes. Once the system's structure is provided, EM risk analysis of the architecture generates functional safety requirements, which comprises required risk reduction, the information for architecture modification, and operational instructions on the system's behaviour. The design and implementation requirements are the lowest-level EM-related requirements that comprise the design commitments and the system's installation instructions. The flow diagram of all EM safety activities and their interactions with the development process is illustrated in Figure 18. The flow diagram also indicates the input and output artefacts of the activities with dotted arrows.

Eventually, the safety goals, arguments, and evidence provided from workflow's steps should indicate that the 4+1 principles have been demonstrated. In the following sub-sections, the overview of the phases is explained. It is noted that the details of the steps will be published in further disseminations.

4.1.1. EM Planning

EM planning is the first phase of the safety workflow regarding EMI, which comprises the requirement elicitation from regulators and other stakeholders (e.g. the required complying standards). Moreover, it includes determining responsibilities between involved development and safety parties in the project. The EM safety plan and the management requirements are the outputs of this step.

4.1.2. Environment Assessment

Analysing the electromagnetic environment where the system is intended to operate, is a vital part of the workflow. This step identifies the totality of the foreseeable electromagnetic environment that comprises the Operational Domain Model (ODM) of the system. An ODM includes the environmental conditions in which the system should be designed to be resilient in. The developer must be able to demonstrate safety for operation in it. It should be noted that the ODM does not include all the environmental conditions that the system may encounter. The ideal model is to include all the foreseeable electromagnetic environment scenarios into the ODM. However, some involved factors such as type of the system's functions, deficiency in the environmental analysis process, and the limitation of the system's monitoring devices or immunity capability may lead to defining a more restricted ODM than

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/

the foreseeable environment. In other words, once the safety case developer could not argue or provide enough confidence about the system's immunity in all of the foreseeable environment, the ODM will be restricted (see Figure 19). These identified restrictions will lace operational restriction on the system so that adherence to them can be ensured.

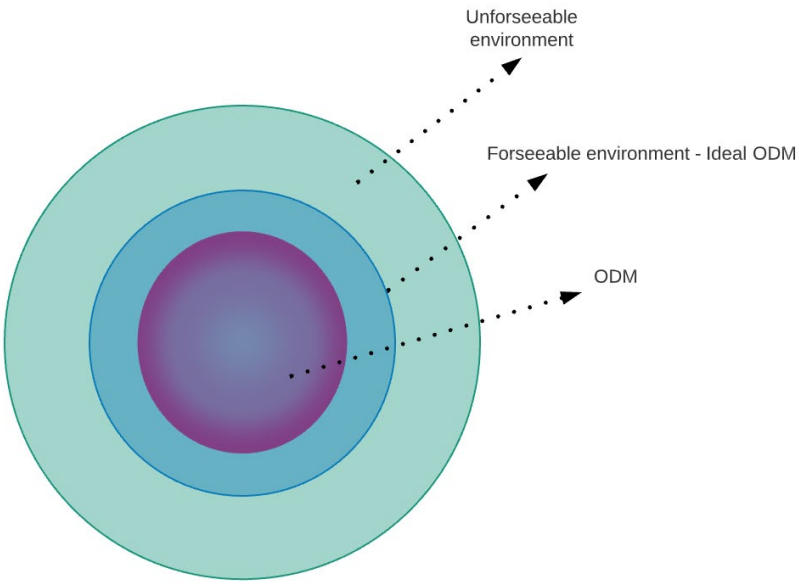

Figure 19- The conceptual diagram of the electromagnetic environment and ODM

Identifying the ODM helps to define the requirements and safety goals, provide the verification plan and determine the thresholds for EMI monitoring and detection systems. The ODM is a dynamic artefact as the system undergoes the development phases, the internal electromagnetic emission of the selected components will alter the ODM boundaries.

4.1.3. EM risk Analysis

Once the architecture of the system and results of the functional hazard analysis (e.g. Failure conditions, Fault Tree Analysis, etc.) are provided, the EMI risk analysis should be performed to identify systems vulnerabilities. Both deductive and inductive approaches need to be applied. In the deductive approach, the result of FTAs, including different cut sets and Functional Failure Sets (FFSs), are investigated to identify how much EM resilience is required for each component in the FFs according to the safety integrity level of the functions. Moreover, by applying Electromagnetic Topology (EMT) based analysis methods [26] and other inductive methods such as FMEA, the impact of the sources defined in the ODM on the components is investigated to identify the susceptibilities of the components and possible common cause failures. The output of this step includes functional safety requirements and required information for architecture modification.

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/

4.1.4. Architecture Modification

The results of EM risk analysis may lead to modification of the architecture. The architecture modification and EM risk analysis processes are iterative and continue until the satisfaction of all defined requirements has been verified during the early verification (see Figure 17 and Figure 18), and some of the required evidence and undeveloped arguments in the safety case become available. Operational procedures such as monitoring systems, hazard mitigation and Maintenance instructions are determined as functional safety requirements in this development phase. Moreover, applying most techniques and measures for increasing EM resilience and reducing the risk can be performed in architecture modification.

4.1.5. Design and Implementation

During development, the design commitments derived from upper-level requirements and EMC design knowledge should be considered as input for the process. Moreover, non-technical EM related aspects such as EM consideration of different technologies can be considered in the design and decision on the COTS. The process of evaluating the compatibility of the in-house and Commercial Off The Shelf (COTS) components should be performed at this phase. Moreover, this stage includes satisfying the EM installation requirements such as wiring, earthing, etc.

4.1.6. Verification

EM verification is not limited to the right-hand side of the V diagram of development. As mentioned before, early verification during environment assessment and also system architecture is crucial. There are three methodologies for EM verification (see Figure 20). The applicability of each methodology depends on the phase under verification, the development level and the required confidence for the verification. The verification plan provided by the ODM determines the testing methods, levels and procedures. It also provides the required information for modelling and simulation in the analysis approach as another verification methodology. The similarity approach comprises reusing arguments that are verified before and can be instantiated into the current context. The verification processes provide most of the required evidence and confidence case materials.

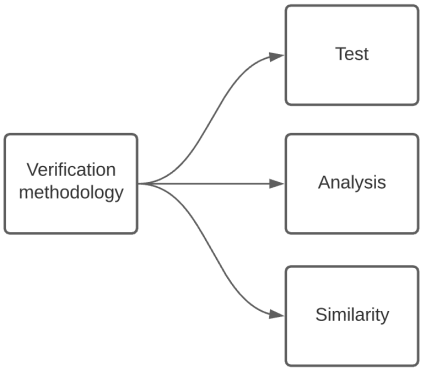

Figure 20- Different verification methodologies

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/

4.1.7. Through Life maintenance of EMI contribution

During the development steps, the operational requirements and instructions for maintaining safety against EMI in the operation mode of the system are defined. They include the instructions on modifying the system and its impact on the EMI-aware safety case modules, managing the impact of physical stresses, obsolescence, and ageing on the system's EMI-related behaviour. Moreover, the instructions on monitoring the environment and detecting EMI along with the system's behaviour during exposure to EMI are considered in the operational EMI-aware safety case.

5. Application of Workflow in a Maritime Context

The introduced EMI-aware safety case development workflow is considered to be applicable in a variety of different contexts. Nonetheless, it will be applied to a complex system in a maritime context to investigate the workflow in practice. The candidate case study system is the Integrated Bridge System (IBS) of the ships. IBS can be described as 'a combination of systems which are interconnected in order to allow centralised access to sensor information or command/control from workstations, with the aim of increasing safe and efficient ship's management by suitably qualified personnel' [27]. This system can be considered as a safety-critical system that is vulnerable to EMI in the harsh electromagnetic environment of the ships and, consequently, an appropriate case study for the workflow. This case study is the subject of a secondment at RH Marine. The results of the investigation will be reported in the following versions of this deliverable.

6. Conclusion and Further Works

In this deliverable, an overview of the workflow for developing an EMI-aware safety case is presented. The evolution of argumentation about safety regarding EMI is explored, and the 4+1 safety principles as a possible trustable argument are introduced. Furthermore, the steps for developing the safety case and its relationship with the lifecycle are stated. At last, the EM activities during the development phases are briefly described.

In the next steps, the applicability of different EM activities in developing the safety case will be investigated in order to extend the details of the workflow. Moreover, the workflow will be applied to the IBS as a case study to be evaluated.

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/

7. References

[1] 'IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems', IEC, 61508, 2010.

[2] 'ARP4754A: Guidelines for Development of Civil Aircraft and Systems - SAE International'. Accessed: Dec. 08, 2020. [Online]. Available: https://www.sae.org/standards/content/arp4754a/.

[3] 'ARP4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment - SAE International'. https://www.sae.org/standards/content/arp4761/.

[4] 'IEC 61000-1-2:2016, Electromagnetic compatibility (EMC) - Part 1-2: General - Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena'. https://webstore.iec.ch/publication/24517.

[5] 'IEEE 1848-2020 - IEEE Approved Draft Techniques & Measures to Manage Functional Safety and Other Risks With Regard to Electromagnetic Disturbances'. https://standards.ieee.org/standard/1848-2020.html.

[6] N. U. I. Hossain, R. M. Jaradat, M. A. Hamilton, C. B. Keating, and S. R. Goerger, 'A Historical Perspective on Development of Systems Engineering Discipline: A Review and Analysis', *J. Syst. Sci. Syst. Eng.*, vol. 29, no. 1, pp. 1–35, Feb. 2020, doi: 10.1007/s11518-019-5440-x.

[7] J. Birch *et al.*, 'A Layered Model for Structuring Automotive Safety Arguments (Short Paper)', in *2014 Tenth European Dependable Computing Conference*, May 2014, pp. 178–181, doi: 10.1109/EDCC.2014.24.

[8] R. Hawkins, 'The Principles of Software Safety Assurance', presented at the 31 international system safety conference, Aug. 2013.

[9] R. Hawkins, I. Habli, and T. Kelly, 'Principled Construction of Software Safety Cases', Sep. 2013, p. NA, [Online]. Available: https://hal.archives-ouvertes.fr/hal-00848485.

[10] T. P. Kelly, 'Arguing safety: a systematic approach to managing safety cases', PhD Thesis, University of York York, UK, 1999.

[11] R. Hawkins, T. Kelly, J. Knight, and P. Graydon, 'A New Approach to creating Clear Safety Arguments', in *Advances in Systems Safety*, 2011, pp. 3–23.

[12] O. Jaradat, I. Sljivo, R. D. Hawkins, and I. Habli, 'Modular Safety Cases for the Assurance of Industry 4.0', Feb. 2020.

[13] 'SCSC - Goal Structuring Notation Community Standard (Version 3)'. https://scsc.uk/SCSC-141C.

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/

[14] T. P. Kelly and J. A. McDermid, 'Safety Case Construction and Reuse Using Patterns', in *Safe Comp 97*, London, 1997, pp. 55–69, doi: 10.1007/978-1-4471-0997-6_5.

[15] D. Pissoort, T. Bultinck, J. Boydens, and J. Catrysse, 'Use of the Goal Structuring Notation (GSN) as Generic Notation for an "EMC Assurance Case"', in *2019 International Symposium on Electromagnetic Compatibility - EMC EUROPE*, Sep. 2019, pp. 465–469.

[16] 'Electromagnetic Compatibility (EMC) Directive', *Internal Market, Industry, Entrepreneurship and SMEs - European Commission*, Jul. 05, 2016. https://ec.europa.eu/growth/sectors/electrical-engineering/emc-directive_en.

[17] K. Armstrong, 'New guidance on EMC-related functional safety', in *2001 IEEE EMC International Symposium. Symposium Record. International Symposium on Electromagnetic Compatibility (Cat. No.01CH37161)*, Aug. 2001, vol. 2, pp. 774–779 vol.2.

[18] E. K. Armstrong, 'introduction to EMC for functional safety', Newbury, UK, 2004.

[19] 'IET Guide on EMC for Functional Safety'. 2008.

[20] 'Overview of Techniques & Measures for EMC for Functional Safety'. IET, 2013.

[21] 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)*, May 2018, pp. 199–204.

[22] K. Armstrong, 'EMC for the functional safety of automobiles why EMC testing is insufficient, and what is necessary', in *2008 IEEE International Symposium on Electromagnetic Compatibility*, Aug. 2008, pp. 1–6.

[23] 'Its EMC Jim but not as we know it, InCompliance magazine July 2015 - EMC Standards'. https://www.emcstandards.co.uk/its-emc-jim-but-not-as-we-know-it-incompliance.

[24] D. Pissoort and M. Nicholson, 'The 4+1 Principles for EM Risk Management', presented at the International Symposium on Electromagnetic Compatibility - EMC EUROPE, 2021.

[25] A. R. Ruddle and A. J. M. Martin, 'Adapting automotive EMC to meet the needs of the 21st century', *IEEE Electromagnetic Compatibility Magazine*, vol. 8, no. 3, pp. 75–85, 2019.

[26] C. Mao and F. Canavero, 'System-Level Vulnerability Assessment for EME: From Fault Tree Analysis to Bayesian Networks—Part I: Methodology Framework', *IEEE Transactions on Electromagnetic Compatibility*, vol. 58, no. 1, pp. 180–187, Feb. 2016, doi: 10.1109/TEMC.2015.2484067.

[27] 'Integrated bridge system (IBS)'. https://www.imo.org/en/OurWork/Safety/Pages/IntegratedBridgeSystems.aspx.

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/