© 2022 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. 2022 International Symposium on Electromagnetic Compatibility - EMC EUROPE, 5-8 September, 2022

Providing Assurance that Risks Associated with Electromagnetic Disturbances are Sufficiently Managed

Mohammad Tishehzan
Department of Computer Science
University of York
York, United Kingdom
mohammad.tishehzan@york.ac.uk

Mark Nicholson
Department of Computer Science
University of York
York, United Kingdom
mark.nicholson@york.ac.uk

John F. Dawson
Department of Electronic Engineering
University of York
York, United Kingdom
john.dawson@york.ac.uk

Davy Pissoort
M-Group (Mechatronics Group)
KU Leuven
Bruges, Belgium
davy.pissoort@kuleuven.be

***Abstract*—Over the last decade, awareness has grown that compliance to EMC standards does not necessarily imply that all properties of a system, such as reliability, safety, and security, are adequately assured when the system is exposed to electromagnetic disturbances. While the application of a risk-based approach has been proposed to overcome this issue, a methodology to demonstrate that the employed risk-based activities provide compelling arguments and evidence to assure the properties of interest seems to be missing. In this paper, the application of assurance cases and associated activities in demonstrating properties like safety and security of systems in the presence of electromagnetic disturbances is explored by using Goal Structured Notation (GSN) to present the structure of the assurance argument.**

***Index Terms*—electromagnetic interference, risk-based EMC, assurance case, safety, Goal Structured Notation, 4+1 principles**

I. Introduction

The way we manage risks due to electromagnetic disturbances is undergoing significant change in both goals and approaches. In the past, EMC engineers were mostly focused on achieving compliance with the EMC Directive and, as such, were dealing with reducing the risk of having Electromagnetic Interference (EMI). The traditional way to approach this, was to show – through physical testing – that the system-at-hand passed all emission and immunity standards that had been identified as being relevant for the system and its application.

Especially in the last decade, awareness has grown that the above approach has serious limitations, not at least as standard development processes struggle to keep up with technological evolution [1]. Moreover, the rising cost of certification and achieving full compliance in some industries such as maritime, along with accessible Commercial Off The Shelf (COTS) equipment that may not comply with maritime EMC standards [2], signals the need for a new approach. Therefore, a risk-based approach for EMC has been put forward as an alternative. Such a risk-based approach considers the actual intended electromagnetic environment of the system-at-hand together with the actual intrinsic immunity of that system and correlates both to make a better estimate of the expected risk of occurrence of EMI. By following a good system engineering approach, these identified risks are transformed into an EMC management, EMC control, EMC Implementation and EMC Test plan [3].

However, with the rapid emergence of new technologies, we see that complex electronics are increasingly used in or for safety- or mission-critical applications. Think about self-driving cars, autonomous vessels, or even surgical robots. This has led to the realisation that electromagnetic disturbances can have a significant impact on other properties of the system, such as safety and security. So, we should not only be concerned about the risks of occurrence of EMI, but also the safety or security risks that electromagnetic disturbances might lead to [4]. To address this, the IEEE recently published a full standard on how to manage (functional) safety and other risks with regards to electromagnetic disturbances [5].

Despite these trends towards moving away from showing pass/fail compliance to prescribed standards to a more in-depth risk-based approach, guidance seems to be missing on how to properly assure - with clear claims, arguments and evidence - that the different types of risks due to electromagnetic disturbances are being adequately managed [5].

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No 812790 (MSCA-ETN PETER). This publication reflects only the authors' view, exempting the European Union from any liability. Project website: http://etn-peter.eu/.

978-1-7281-5579-1/20/$31.00 ©2022 IEEE

Therefore, in this paper, we propose the use of an assurance case to achieve this. Assurance is a "positive declaration intended to give confidence"; thus, an assurance case is defined as "a reasoned, audit-able artefact that supports the contention that its top-level claim (or set of claims), is satisfied, including systematic argumentation, its underlying evidence, and explicit assumptions that support the claim(s)" [6]. In this paper, the application of assurance cases in demonstrating achievement of system properties such as EMC, safety and/or security is investigated. The use of Goal Structuring Notation (GSN) as one of the main tools in assurance case presentation is explored.

The remainder of the paper is organised as follows. In Section II, the necessity of employing assurance cases in a risk-based approach is explained. Then, in Section III, further details on the assurance cases and the structure of GSN are given. Finally, in Section IV, as an example, the contribution of GSN in demonstrating safety principles is provided.

II. Necessity of Assurance case in Risk-Based EMC

There are multiple approaches for demonstrating the properties of a system and for providing certification for these properties. While the practices are different through domain and regulation bodies in different countries, they can be categorised into two types [7]: the Prescriptive approach and the Goal-based approach. In the prescriptive approach, standards and guidelines provide rules that must be followed for a product or a process to achieve certification. On the other hand, the Goal-based approach focuses on the achievement of the required outcome. Therefore, a set of criteria should be identified to achieve certification and the means and the validity of the means used to meet the criteria should be demonstrated by the applicant for certification.

Rule-based EMC originated from the prescriptive approach. It aims to achieve compliance with EMC standards which heavily rely on immunity and emission tests. In other words, the main argument for achieving acceptable EMC in the rule-based EMC approach is passing EMC tests in specific scenarios defined in the standards. Therefore, the need for an argumentation tool has not been extensively noticed; even though an assurance case for demonstrating the argument for compliance with EMC standards (***Compliance Case***) facilitates the certification process [8].

On the other hand, the risk-based approach aims to argue about achieving goals regarding various system properties by providing arguments related to scenarios which might not be anticipated in EMC standards. As a result, the associated arguments are not limited to conformance with test requirements in EMC standards and additional arguments and evidence are required. Furthermore, from the certificating parties perspective, validation of compliance with relevant requirements once the risk-based EMC approach is applied, has been observed to be more difficult [3]. Hence, demonstrating achievement of EMC goals are not straightforward like in the case of the rule-based approach, and a systematic argumentation tool is required to justify the realisation of goals and to assist certification.

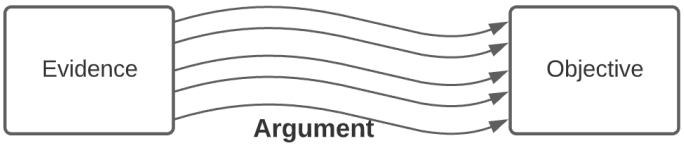

Fig. 1. Argument answers the question 'How does the provided evidence lead to the achievement of the Objective?'

III. Assurance Case

A. Assurance Case Structure

The Assurance case idea is rooted in the goal-based approach toward achieving defined goals. Every assurance case comprises three elements: Objective, Argument and Evidence. The argument provides the reasoning behind the achievement of the Objective by considering the appropriate evidence (Fig. 1).

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. Supporting evidence includes analysis results, test results and other clues that back up the argument that the case is based on. All three elements are required in an assurance 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. This is because the applied tools for providing the evidence, the rationale of the argument and Objective validity will inevitably include uncertainty and may include errors. The confidence a reader should have in the assurance case's elements need to be evaluated. Therefore, a '***Confidence Case***' is required to demonstrate how confident we are in the elements of the assurance case [9].

An Assurance case, such as 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 can be supported by evidence directly (Fig. 2).

There are several ways of illustrating the argumentation in an assurance 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 engaged parties. Besides, traceability between assurance case elements can also be problematic. Thus, graphical methods are preferred for argumentation. One such method is Goal Structuring Notation (GSN) which is a graphical argumentation tool that explicitly connects the assurance case elements and provides a comprehensible structure for argumentation [10].

B. Goal Structuring Notation (GSN)

GSN facilitates demonstrating the interaction between objectives, arguments, and evidence through a set of graphical el-

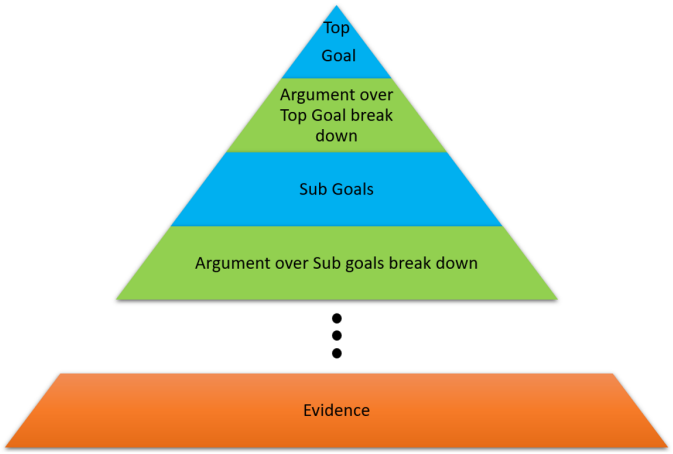

Fig. 2. The hierarchical structure of the Assurance Case

ements and consequently a better projection of argumentation is achieved. 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. For instance, a goal could be a claim that the radiated emission of a system is lower than a specific level.
- **Strategy**: The reasoning behind how goals break down into sub-goals. It is the nature of the argument which connects different levels of goals. For example, one strategy could be a defined approach for demonstrating that the radiated emission is lower than a specific level.
- **Solution**: The items of evidence provided to support claims. A solution could be the results of tests, simulations, 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, tests, environment, or requirements.
- **Assumption, Justification**: In some cases, defining goals, reasoning about an argument, or using a piece of evidence requires some assumptions or justifications. In GSN, this information could be presented via Assumption or justification elements. For instance, reasoning about radiation limit lines could be considered as an Justification.

The relationship between 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. An illustration of the elements and relationships is provided in Fig. 3.

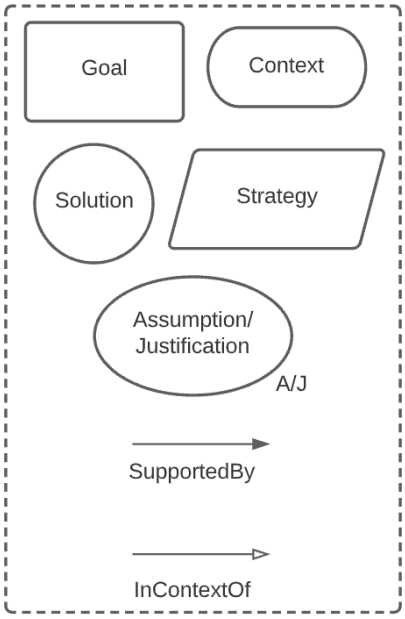

Fig. 3. Illustration of GSN elements and relationships

IV. Application of Assurance Case in EMC

Employing assurance cases for argumentation about achieving EMC goals has not been a common practice so far. In [11], the application of GSN in demonstrating compliance with EMC directive standards has been investigated for the first time. This study comprises two use cases: an EMC Compliance Case for equipment tested in the EMC lab and for in-situ EMC testing of large machines. However, the application of GSN in argumentation about safety goals regarding Electromagnetic Disturbance (EMD) has not been examined.

In this section, the assurance case for implementing the first and third principles of EM risk management is addressed and presented in GSN in order to demonstrate the application of GSN in achieving EMC safety goals. The 4+1 principle of EM risk management has been introduced in [12] and are derived from the principles of software safety assurance [13].

A. Principle 1

The first principle of EM risk management states that "EM [Safety] risk requirements shall be defined to address the contribution of EMDs to a specific system's property [hazard]". This principle requires that all risks (relating to the property of interest) arising from all possible EMDs be identified and appropriate requirements for managing those risks be defined. For safety, for example, it argues that the contribution of each EMD to any known hazard is identified.

In Fig. 4, the GSN for this first principle is depicted. The main target is to show that the contribution of EMDs to hazards has been considered acceptably through the generation of EM safety requirements (G1). Arguing about this goal requires some contexts such as information about the system of interest and its behaviour in the considered EM environment (C1).

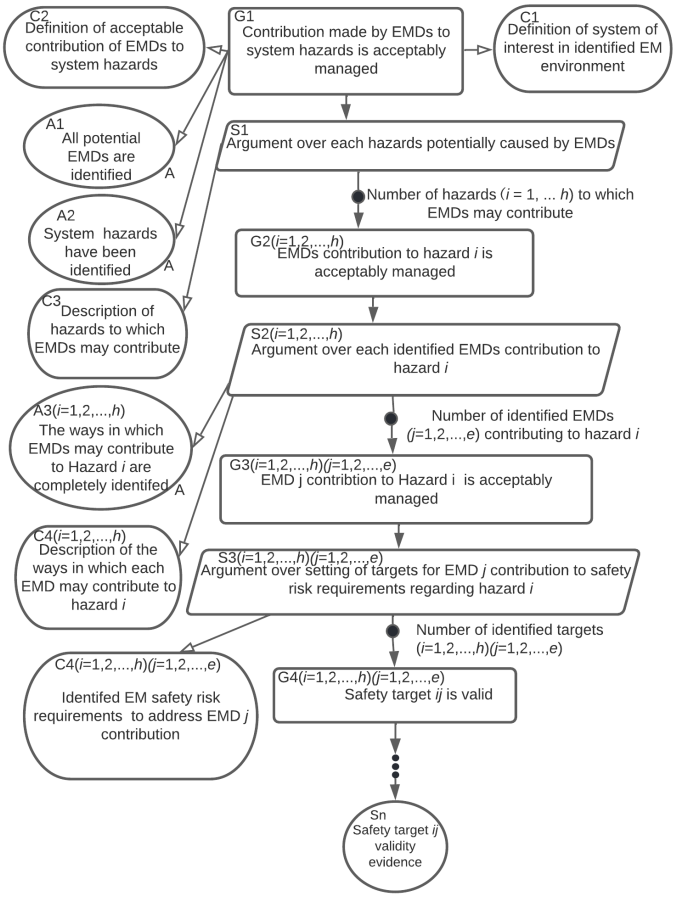

Fig. 4. Principle 1 of EM risk management illustration by GSN

Moreover, the definition of acceptable management should be provided (C2).

Furthermore, to argue about G1, assumptions about identification of all potential EMDs (A1) and all potential hazards (A2) should be stated. The strategy (S1) is to breakdown this goal by arguing separately about each identified hazard (***i***=1,2,...,***h***) and to make sure that the contribution of EMDs to each hazard is acceptably managed. The respective goals for these claims are described as (G2(***i***=1,2,...,***h***)). At this stage, the contextual information of the description of hazards associated with EMDs (C3) is provided.

In the next step, argument must be provided to the contribution of each EMD to each hazard (S2(***i***=1,2,...,***h***)). This strategy breaks down the G2 goals into (G3(***i***=1,2,...,***h***)(***j***=1,2,...,***e***)) which claim that these contributions are acceptably managed. Besides, this strategy requires assumptions (A3(***i***=1,2,...,***h***)) that the way in which each EMD leads to the hazard is identified and provided as contextual information (C4(***i***=1,2,...,***h***)).

Furthermore, to argue about addressing the contribution of each EMD to each hazard through EM risk requirements and setting corresponded safety targets (S3(***i***=1,2,...,***h***)(***j***=1,2,...,***e***)), the final goals (G4(***i***=1,2,...,***h***)(***j***=1,2,...,***e***)) for identification of valid requirements are defined and requirements are provided as contextual information (C3(***i***=1,2,...,***h***)(***j***=1,2,...,***e***)). At this stage, the goals may still need to be broken down further before they can be addressed by evidence directly. The evidence for demonstrating that appropriate EM risk requirements have been defined can be instantiated as solutions (Sn) to support G4. Once the evidence is provided, the goals which have been broken down during argumentation, are supported and finally it can be concluded that the top level goal (G1) is achieved.

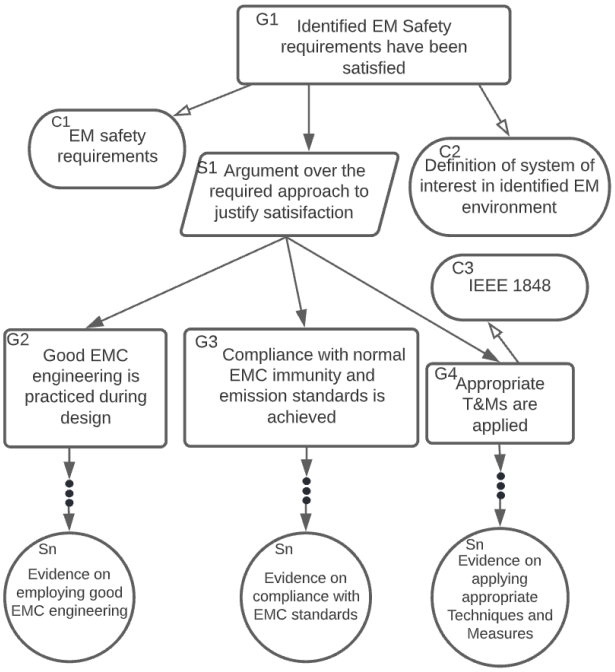

Fig. 5. Principle 3 of EM risk management illustration by GSN

B. Principle 3

The third principle of EM risk management focuses on the verification of the satisfaction of EM requirements. While there is no unique approach to verify this claim, for illustration of the third principle, the recommended approach in [5] is considered.

In Fig. 5 the main goal (G1) claims that all identified EM requirements are satisfied. The Contextual information for this goal includes the description of EM safety requirements (C1) and the definition of the interested system (C2). The strategy (S1) breaks down the main goal into three subgoals including practising good EMC engineering (G2), complying with relevant EMC standards (G3) and applying appropriate Techniques and Measures (T&Ms) defined in [5] (C3). The satisfaction of these subgoals is argued by further strategies until a point at which claims can be supported directly by evidence (Sn).

Clearly, developing and supporting such [safety] assurance cases requires activities to be undertaken during the system development lifecycle and maintenance of required activities during operation. These activities should be the subject of regulation/certification guidance and embedded efficiently in organisation processes. Also, support will be required against the remaining two principles in a proportionate manner.

V. Conclusion

In this paper, we consider the necessity of using assurance cases where the risk-based EMC approach is being employed. The risk-based approach argumentation is not as straightforward as the rule-based approach and consequently the EMC certification process for a product becomes more difficult. Therefore, using assurance cases as an argumentation tool facilitates certification and communication with engaged parties. Furthermore, to demonstrate the application of the graphical assurance case for argumentation on safety goals, the GSN of the first and third principles of EM risk management, which assures that appropriate EM risk requirements have been defined and all hazards associated with EMDs are covered by the requirements along with assurance of satisfaction of the requirements, are provided and discussed. Finally, the next steps around developing the assurance case structure and activities required to support it are presented.

References

[1] A. R. Ruddle and A. J. Martin, "The Need for a Risk-Based Systems Engineering Approach in Automotive EMC Engineering," in *2018 International Symposium on Electromagnetic Compatibility (EMC EUROPE)*, Aug. 2018, pp. 293–298, iSSN: 2325-0364.

[2] F. Leferink, J. van der Ven, H. Bergsma, and B. van Leersum, "Risk based EMC for complex systems," in *2017 XXXIInd General Assembly and Scientific Symposium of the International Union of Radio Science (URSI GASS)*, Aug. 2017, pp. 1–4.

[3] J. van der Ven and F. Leferink, "An interference risk–based approach for naval vessels," *Ciencia y tecnología de buques*, vol. 11, no. 21, pp. 65–73, Sep. 2017, number: 21. [Online]. Available: https://shipjournal.co/index.php/sst/article/view/154

[4] D. Pissoort, A. Degraeve, and K. Armstrong, "EMI Risk Management: A necessity for safe and reliable electronic systems," in *2015 IEEE 5th International Conference on Consumer Electronics - Berlin (ICCE-Berlin)*. IEEE, Sep. 2015, pp. 208–210.

[5] "IEEE 1848 - IEEE Standard for Techniques and Measurement to Manage Functional Safety and Other Risks with Regards to Electromagnetic Disturbances," 2021.

[6] "IOS/IEC 15026-1: 2019 ;Systems and Software Engineering - Systems and Software Assurance Part 1: Concepts and vocabulary," 2019.

[7] N. G. Leveson, "The Use of Safety Cases in Certification and Regulation," Massachusetts Institute of Technology. Engineering Systems Division, Working Paper, Nov. 2011, accepted: 2016-06-02T14:53:36Z. [Online]. Available: https://dspace.mit.edu/handle/1721.1/102833

[8] P. Graydon, I. Habli, R. Hawkins, T. Kelly, and J. Knight, "Arguing Conformance," *IEEE Software*, vol. 29, no. 3, pp. 50–57, May 2012, conference Name: IEEE Software.

[9] R. Hawkins, T. Kelly, J. Knight, and P. Graydon, "A New Approach to creating Clear Safety Arguments," in *Advances in Systems Safety*, C. Dale and T. Anderson, Eds. London: Springer, 2011, pp. 3–23.

[10] "SCSC - Goal Structuring Notation Community Standard (Version 3)." [Online]. Available: https://scsc.uk/SCSC-141C

[11] 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.

[12] D. Pissoort and M. Nicholson, "The 4+1 Principles for EM Risk Management," in *2021 IEEE International Joint EMC/SI/PI and EMC Europe Symposium*, Jul. 2021, pp. 1030–1030.

[13] R. Hawkins, I. Habli, and T. Kelly, "The Principles of Software Safety Assurance," in *31 international system safety conference*, Boston, Massachusetts USA, 2013.