Assuring Shielded Cables as EMI Mitigation in Automotive ADAS

Oskari Leppäaho
VALEO GEEDS, 2 rue André Boulle, Créteil, France. E-mail: oskari.leppaaho@valeo.com

Mark Nicholson
Dept. of Computer Science, University of York, Deramore Lane, York, UK.

Frédéric Lafon
VALEO GEEDS, 2 rue André Boulle, Créteil, France.

Mohammed Ramdani
ESEO - IETR, 10 Boulevard Jeanneteau, Angers, France.

Shielded cables are an important mitigation for electromagnetic interference (EMI) in high-speed data systems. In the automotive domain, one use for them is to transmit image data from a front camera to an advanced driver assistance system (ADAS) controller. Some ADAS functions have implication for human safety and thus place extra requirements for the design of the transmission path including its resilience to EMI.
This paper presents a case study of an automated lane centering (ALC) system with the above-mentioned shielded cable use case. The study starts from a National Highway Traffic Safety Administration (NHTSA) concept level assessment. Subsystem components are then separated and a physical realization derived. Goal Structuring Notation (GSN) is used to present EMI assurance scenarios over the safety requirements. First, the ability of a shielded cable reliability argument to cover the derived safety requirements during different operating scenarios is studied. It is found that relying on reliability alone, it is challenging to fulfil all the safety requirements. To overcome this challenge, an alternative systems safety based method is studied.

Keywords: EMI, Shielded Cable, Functional Safety, Automotive, Lane Centering System, ADAS.

1. Introduction

The aim of safety assurance is not only to ensure the safety of the system, but to assure that to other people. To assure safety of complex systems, information from different fields of expertise is combined to provide a credible safety justification. There is a practical challenge to even speak the same language in terms of used terminology, depth of information exchange and the scope of work. This is especially true, when incorporating electromagnetic compatibility (EMC) topics into a safety case as demonstrated by Armstrong and Duffy (2020). In this paper, the authors discuss how to overcome these challenges and propose a new way to integrate EM risk management as part of an automotive system safety case. The method relies on a combination of three areas of expertise: state-of-the-art safety assurance, safety related systems engineering, and EMC engineering.

The proposed safety assurance process relies on systems theoretic process analysis (STPA) (Leveson, 2011). The process is used to form a safety control structure and to identify causal EMI scenarios that could cause unsafe control actions, which are discussed in section 2. Then, an assurance case demonstrating that the designed safety control structure can mitigate the effects of the EMI scenarios is formed and presented using GSN in section 3. GSN based assurance case documentation was chosen as Kelly (2004) and Pissoort et al. (2019) have shown it to be a powerful tool in safety and EMC domains, respectively.

EMC engineering topics revolve around the shielded cable and extend slightly to the ADAS and front camera. Shielded cables have typically two purposes: to provide a defined impedance transmission line for a high frequency signal and to provide electromagnetic protection to the conductors inside the shield (Palmgren, 1981). In this paper, only the protection from external electromagnetic fields is addressed. If this protection is not adequate, the signals in the cable can be disturbed impeding data transmission. A poorly shielded cable can also pick-up and conduct interference from its environment to the system components that it connects to. These disturbance cases need to be managed.

The management of electromagnetic distur-

Proceedings of the 31st European Safety and Reliability Conference
Edited by Bruno Castanier, Marko Cepin, David Bigaud, and Christophe Berenguer
Published by Research Publishing, Singapore.
ISBN: 978-981-18-2016-8; doi:10.3850/978-981-18-2016-8_263-cd

bances that can cause functional safety risks, also called as EM resilience, is covered by two main international standards: IEC (2016) 61000-1-2 and IEEE (2020) 1848. The IEC standard provides a generic high-level approach whereas the new IEEE 1848 provides, especially in its Appendix A, more concrete guidance on the actions needed to reduce the risks originating from electromagnetic disturbances to a level that is As Low As Reasonably Practicable (ALARP). However, the guidance is still at a very generic level.

This paper studies an EM resilience case study, namely a very specific automotive safety related electronics subsystem: shielded cable connection between the ADAS computer and a front camera in an ALC system. This study provides an example of a practical workflow to demonstrate the EM resilience of the subsystem. With some added effort, the authors see that the presented workflow can be generalized to other automotive safety related EM resilience cases. Moreover, the workflow could be developed to be applied in other industries and use cases outside the functional safety domain, where assurance over EM resilience is needed.

2. ALC System Level Analysis

ALC involves many sensors, actuators and a computing system to relate sensor data into correct actuation. Shielded cable connection between the ADAS module and a front camera is the scope of this study. Part of the NHTSA concept level system diagram in Fig. 1 was modified for clearer scope illustration.

Following STPA workflow the system is analyzed in four steps: identifying hazards, modeling the control structure, identifying unsafe control actions, and causal scenarios leading to unsafe control actions. The NHTSA assessment by Becker et al. (2018) recognized five vehicle level hazards. Simplified versions are:

(i) Insufficient lateral adjustment
(ii) Excessive lateral adjustment
(iii) Unexpected loss of the ALC system
(iv) Improper transition of control between driver and the ALC system
(v) ALC system impedes the actions of other vehicle systems

The first three hazards are relevant for the current case, where EMI could cause corrupted or missing sensor data from the front camera. ADAS controller coordinating the ALC function is the critical system component to avoid these vehicle level hazards. The control structure in Fig. 2 is derived from Ziegler et al. (2014). It divides sensors into two different groups: vehicle and environment. The front camera belongs to the environment sensors group. Based on its data combined with other available sensor data, a model of the environment

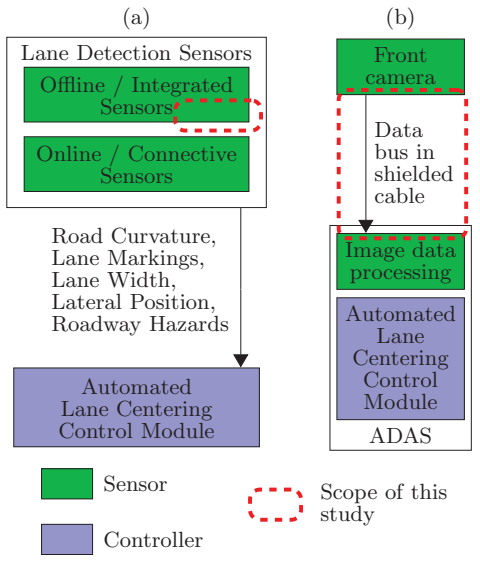

Fig. 1. Scope of the study shown equivalent to (a) the NHTSA concept level block diagram and (b) a derived realization for this study.

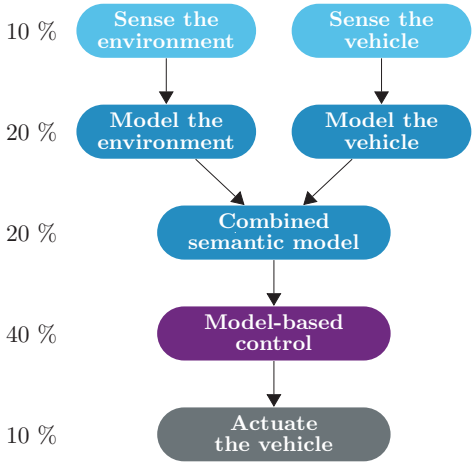

Fig. 2. ALC control structure with a safety importance rating given for each component

is formed. Similarly a model of the vehicle state is formed based on the vehicle sensors. These models are merged into a combined semantic model as introduced by Zhang et al. (2017) that contains all the information of the vehicle and its surroundings. Based on this model, the controller actuates the vehicle to fulfill the system functional targets

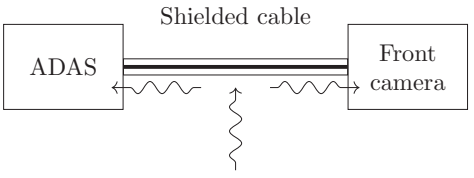

Fig. 3. EMI coupling paths within the system scope

while avoiding the previously mentioned hazards. The unsafe control actions are therefore any control actions that result in any of the hazards.

A relative safety importance score is given to each section of the control system. It provides guidance on where the majority of the effort needs to be concentrated to achieve the best end-result: ALARP EMI risk under this scenario. The relative safety risk of a single failure in the communication lines is of smaller importance than failure of the control system. The control system can be thought to consist of two major parts: model and the controller. As the controller operates based on the data from the model, both are considered equally important. A perfectly functioning controller results in adverse control action if it bases its decisions on invalid input data. The semantic model is built in two stages with checks at both stages to ensure decisions are not made on invalid data.

The causal scenarios in this context mean EMI events capable of disturbing the normal execution of the ADAS controller. Here, only radiated EMI is taken into account. It is recognized to have three paths to cause disturbances in the system as illustrated in Fig. 3: disturbing the signal in the shielded cable, being picked up by the shielded cable and disturbing the operation of either or both the front camera and the ADAS module.

3. Assurance Case

A system safety assurance case provides reasoned argument that is supported by a body of evidence that the system is safe to operate (Kelly, 2004). As absolute safety cannot be achieved, the assurance case aims to show that a sufficiently low safety risk exists in the operation of the system. To provide a clear scope for the assurance case, limitations on its applicability are set. These include limitations to e.g. operator capability, operating environment and usage patterns. In this section two assurance cases are built: one that relies on a shielded cable connection reliability argument and another that relies on systems safety approach. These assurance cases form part of a larger safety assurance case for the ALC system or even the whole vehicle, and as such their top-goal will be a child of some higher level goal.

The assurance cases are presented using Goal Structuring Notation (GSN) standardized by The Assurance Case Working Group (2018). GSN provides a clear way to separate larger goals into smaller, more achievable goals. It might not always be clear for the reader how the lower level goals are intended to support the higher level ones. Strategies are used to clarify the argumentation flow between the goals. To provide sufficient context for the argumentation, different assumptions and context elements describing and limiting the scope of work are added. The lowest level goals should have been reduced so that a simple test report or a design document is enough to show their fulfillment. This enables easy comparison between the cases and helps the assurance case reader to compare their quality.

As the two assurance cases have the same target for the shielded cable function, they share a common top-level goal (G1) and its context items shown in Fig. 4 and 6. A stronger case could be made by instantiating both approaches, but this is unlikely to be necessary nor cost effective. The main assumption: the ALC system is safe when EMI is not present (A1), and context C1 on ALC system documentation ensure that the system design has been documented correctly and serve to limit the scope of this study. Context item (C2) provides documentation of the vehicle as the system of interest.

The Electromagnetic Disturbance (EMD) envelope definition in C3 is one of the center pieces of this argument. In our approach, it is divided into two sections: regular and intentional disturbance. Regular disturbance is equal to the level of the immunity requirements in applicable standards (regulatory & OEM). For example, up to 100 V/m for radiated fields. Here, intentional disturbance is categorized to start from where the regular limits stop (Sabath, 2021). While the higher disturbance can also be unintentional, the same mitigation methods apply and thus only the intentional term is used. An important step in defining this context is choosing the maximum applicable level.

Communication interface design in C4 provides relevant design detail including the type of cable and number of conductors, but also the signal level, frequency and driver/receiver configurations. Shielded cable assembly data sheet C5 provides the detailed characteristics of the cable and its connectors. C4 and C5 combined provide the basic interface properties whose EM immunity can then be assessed.

3.1. *Reliability argument (Fig. 4)*

The cable reliability argument builds on one child-goal of sufficient EMD attenuation (G2). There the significance of EMD envelope context (C3) is reduced as the cable performance needs to be demonstrated inside and outside of the envelope. However, the EMD envelope definition over the vehicle lifetime (A2) is still critical as the suf-

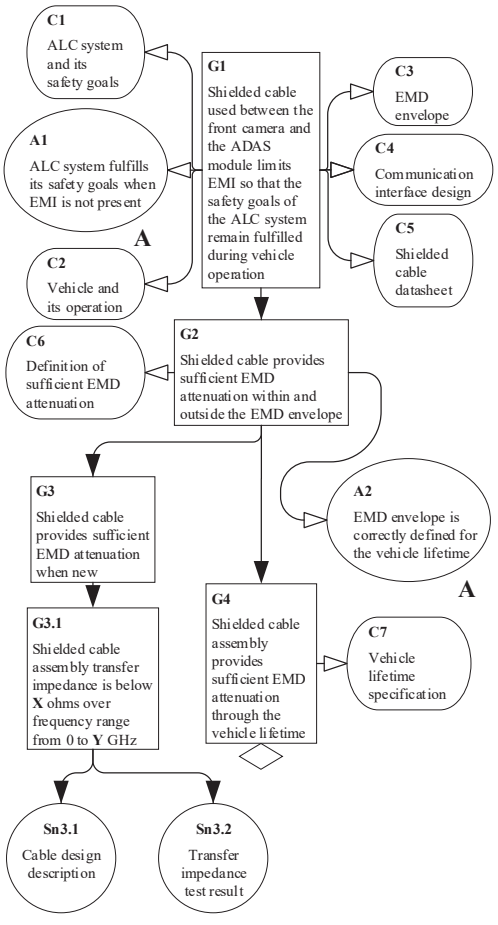

Fig. 4. Top-level goals of the reliability assurance case

ficient EMD attenuation argument is based on the correctness of the EM environment definition. Otherwise it is not possible to rely on the reliability of the cable alone. Defining sufficient EMD attenuation context (C6) for G2 is of utmost importance. It is also one of the most difficult design tasks. At higher Automotive Safety Integrity Levels (ASIL), the failure of the system can be allowed to occur only in the vicinity of once per million samples per year. Decomposition of this budget leads to a requirement of less than once per 100 million samples per year. Assuming a 33 % market share of the yearly vehicle production reported by OICA (2019), this means that a cable EMI failure should happen only in three samples per production year over the average vehicle lifetime of 12 years. This level of reliability can only be achieved by using high-specification EMD mitigation approaches and thus a very high value of attenuation will need to be defined.

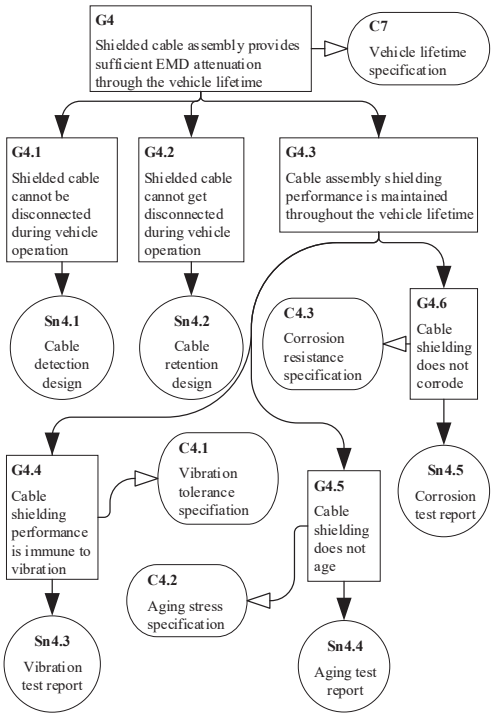

Fig. 5. Reliability goals through the vehicle lifetime

To address cable assembly reliability over the vehicle lifetime, two different arguments are needed: G3 argues that the cable attenuation design is sufficient as designed and tested during development, and G4 argues that the designed cable performance is maintained over the specified vehicle lifetime (C7). The design and production time goal (G3.1) is a simple transfer impedance requirement over a frequency range after sufficient EMD attenuation (C6) is defined. It is instantiated by two solutions: cable assembly design description (Sn3.1) and the transfer impedance test result (Sn3.2). Proving sufficient EMD attenuation of the cable assembly during the lifetime of a vehicle is a more complex task as shown in Fig. 5. The first task is to assure that the cable cannot be (G4.1) or get (G4.2) disconnected during vehicle operation. The claims are supported by cable detection (Sn4.1) and retention (Sn4.2) designs. Second, the cable lifetime performance is assured (G4.3) by three supporting performance goals: vibration (G4.4), aging (G4.5) and corrosion (G4.6) robustness. Best compromise to demonstrate robustness is with accelerated lifetime testing on each area (Sn4.3-4.5) against the specifications C4.1-C4.3. Again, harsh specifications are needed to guarantee extremely low failure rate during operational life.

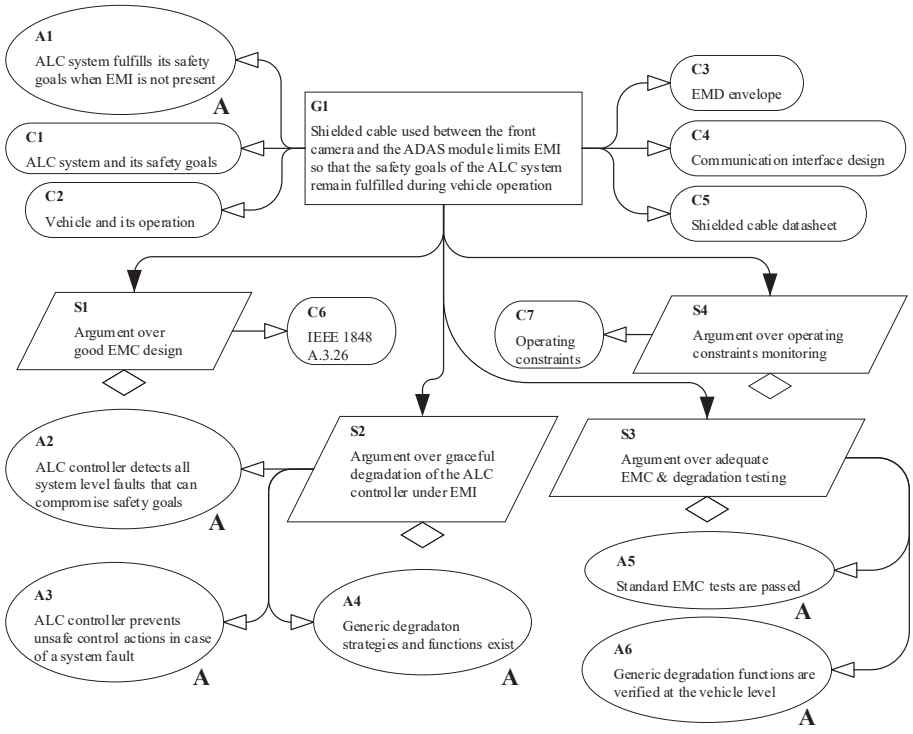

Fig. 6. Top-level goal and systems argumentation strategies to show its validity

3.2. *System safety argument (Fig. 6)*

Top-level strategies are a key element in arguing safety from a systems point of view. A sound argument is built by taking into account all the key areas of the design and showing how they ensure safety. The process starts with argument over good EMC design (S1) according to best practice, such as IEEE 1848 A.3.26, (C5) and continues with graceful degradation functions (S2) as a back-up if the EMC design fails to prevent an impact on data transmission. Testing (S3) is applied to ensure that the design elements work as expected. Constraints monitoring (S4) builds additional margin between the EMC design failure and the activation of degradation functions if the selected EMD envelope is exceeded.

For graceful degradation strategy S2 it is assumed that: ALC controller detects all system level faults compromising safety goals (A2) and prevents unsafe control actions (A3). They require that the general degradation mechanism has been successfully designed and implemented at system level (A4). Thus, it is possible to concentrate only on the needs arising from the EMI to the shielded cable interface. Similarly under verification strategy S3 assumptions A5 and A6 require the design to pass standard tests. The assurance case concentrates on the tests related to the safety functions.

Good EMC design argument (S1, Fig. 7) relies on two main goals: shielded cable interface performance (G1.1) and reduction of common-cause failures (G1.2). The former is ensured by providing good enough cable design and implementation (G1.3), and foreseeing high enough signal-to-noise ratios (G1.4). Common-cause failures are minimized by providing sufficient noise attenuation at the ADAS terminals (G1.5), and providing a compartmentalized ADAS module with sufficient functional redundancy and diversity (G1.6).

Graceful degradation argument (S2, Fig. 8) applies for low automation levels, where the system can quickly fall back to driver operation (G2.1). This choice was made to provide a simplified argument example. With higher automation levels this strategy would increase in importance as driver supervision and takeover capability could not be assumed. Care would need to be taken in reaching an appropriate level of detail to describe the relevant degradation means against EMI induced faults. This argument is complemented by ensuring that the ADAS module can function during the transition phase from an EMI event to driver operation (G1.6), and resume operation after a transient EMI event has passed (G2.2).

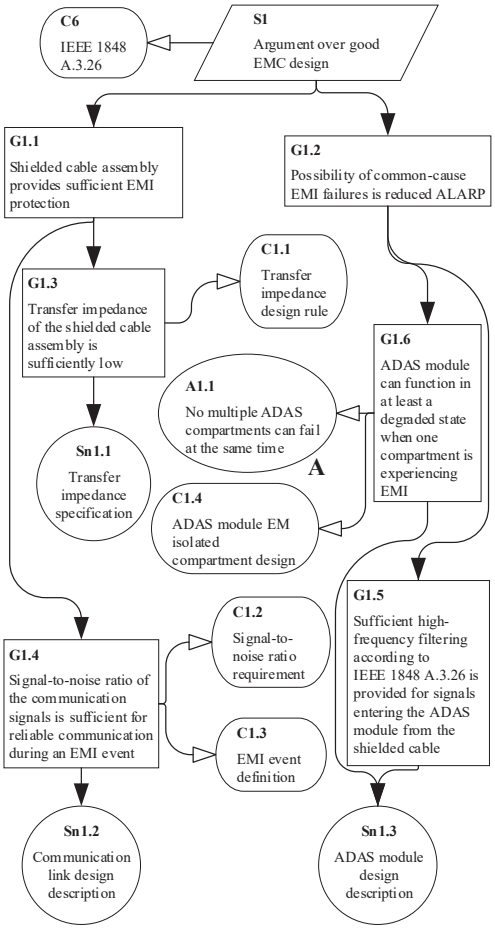

Fig. 7. Strategy 1 - Argument over good EMC design

The goal fulfillment is shown as incomplete as further detail would need to be added once the exact degradation functions have been designed.

Adequate testing argument (S3, Fig. 9) relies on testing the specific EMI mitigation functions (G3.1-2), most challenging scenarios (S3.1) and new tests recognized during the design phase (G3.3). EMI mitigation scenarios are incomplete as more details on their tests would need to be added after the exact function design is known. The most challenging scenarios strategy is divided into two goals complementing each other. One fault & EMD tests (G3.4) simulate a situation, where a system component has failed causing the system to be more susceptible to EMI. Here, it is a common responsibility for EMC and system designers to recognize the most challenging scenarios. EMI tests during the most challenging driving scenarios (G3.5) on the other hand test

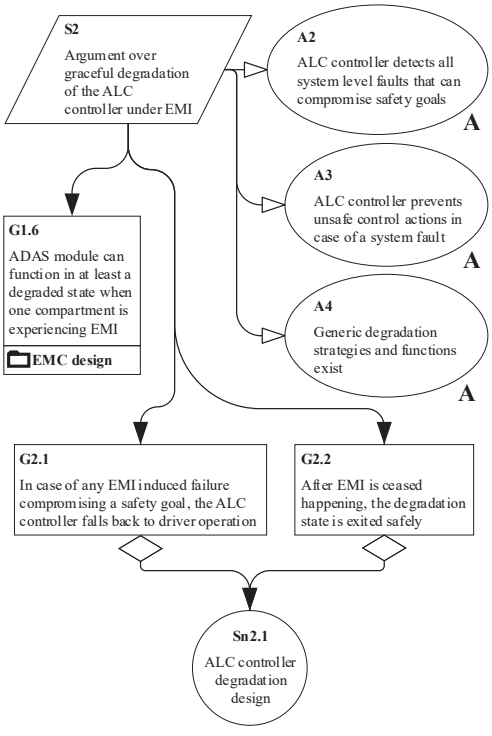

Fig. 8. Strategy 2 - Argument over graceful degradation

the versatility of the control system to manage situations, where safety margins might be limited and sensor data corrupted due to EMI. The most challenging driving scenarios are assumed to have been recognized before the start of this work (A3.1) and simulated during testing.

Constraints monitoring argument (S4, Fig. 10) relies on three goals. The EM environment needs to be constantly monitored (G4.1), and if the preselected operating envelope (C3, Fig. 6) is exceeded, an effective degradation routine started (G4.2). Once the normal EMD envelope is reentered, the degradation states are exited in a safe manner (G4.3). Practical monitoring is done with EMI sensor(s) (Sn4.1), and the EMI sensor data is then processed in the envelope monitoring function (Sn4.2). If the envelope is exceeded, the degradation rules (Sn4.3) dictate a set of actions.

4. Integrating Shielded Cable Assurance Case

Integration of the assurance case is done by collecting the assumptions and presenting them as assertion requirements for the upper-level design following a design by contract theorem (Meyer, 1992). A check-list approach is proposed, where

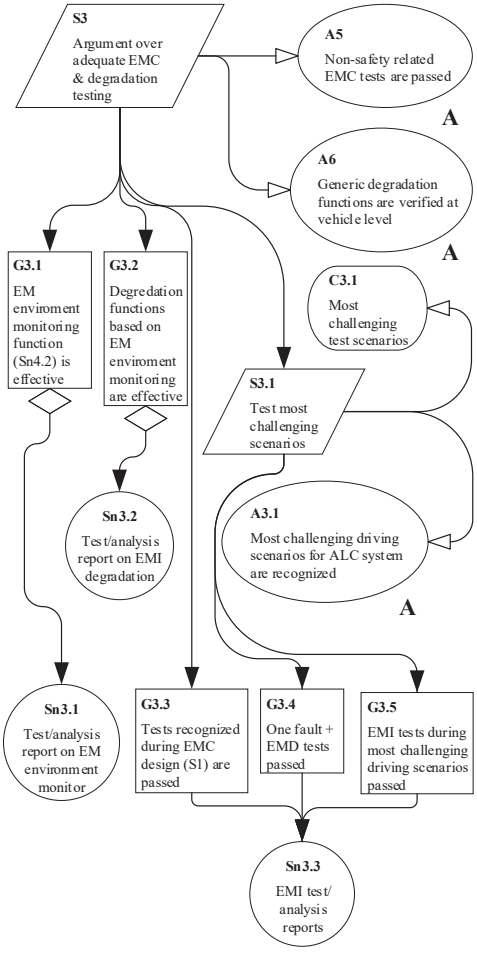

Fig. 9. Strategy 3 - Argument over adequate testing

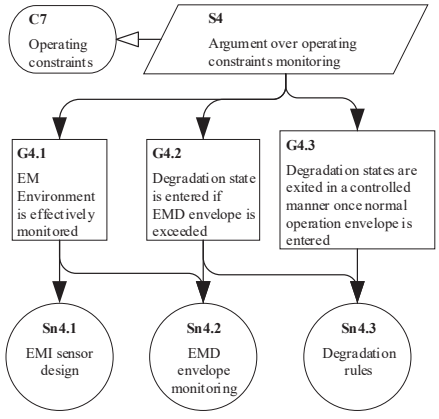

Fig. 10. Strategy 4 - Argument over constraints monitoring

Table 1. Assertion requirements for the upper-level system

ID	Requirement
1	ALC system fulfills its safety goals when EMI is not present
2	EMI envelope is correctly defined for the vehicle lifetime
3	ALC controller detects all system level faults that can compromise safety goals
4	ALC controller prevents unsafe control actions in case of a system fault
5	Generic degradation strategies and functions exist (at the system level)
6	Generic degradation functions are verified at the vehicle level
7	Non-safety related EMC tests are passed
8	No multiple ADAS compartments can fail at the same time
9	Most challenging driving scenarios for the ALC system are recognized

assertions are gathered in Table 1 that can then be communicated to the stakeholders responsible for the overall system safety design. The reliability approach poses only the first two requirements to the upper system whereas the systems approach poses eight of the nine requirements (req. 2 excluded).

5. Conclusion

One way to construct an assurance case for EM resilience of a shielded cable connection between ADAS controller module and a front camera in an ALC system was presented. Two clear assurance cases were formed with the help of GSN. The first case used a reliability based approach, where the case could be decoupled from the other parts of the vehicle level safety case, but few challenges were recognized: an EMD envelope definition did not help to decrease the reliability requirements as there was no way to guarantee or detect if the system was staying within the envelope. Additionally, severe requirements for environmental testing were imposed to guarantee the operation over the vehicle lifetime. This approach would result in mitigation methods, whose bill-of-material cost would be high due to the need to use high-specification components to achieve the reliability targets. The second case using systems safety approach proved to provide similar levels

of assurance without high material costs. It relied on system level graceful degradation and EMD envelope monitoring reinforced with good EMC design, especially on ADAS module, and standard testing together with carefully selected worst-case tests to ensure that the corner-cases are also covered. In the end, a list of assumptions made during the safety case development was gathered, which acts as a list of required assertions expected to be fulfilled in the system-level safety case to which the presented case could be joined as a module.

The assurance case patterns presented here give arguments for why the shielded cable would be acceptably safe to use in the ALC system. They indicate the set of information required to back up this argument. They also indicate the thresholds that determine whether accompanying goals can be declared to be met. The solutions (circles in the diagram) should call out to the relevant information results and reports when they are instantiated. However, they do not indicate how much confidence we can have in the contexts holding true and the evidence being correct. This is provided by an accompanying confidence case which acts as a tool for (independent) assessors to consider the validity of an instantiated assurance case pattern.

The results of this study suggest that alternatives to rugged EMD mitigation in functional safety systems exist. In this case, they come at cost of added system level coordination requirements. When done correctly and on-time with the rest of the development project, this type of coordination may save development cost by introducing a first-time-right principle. Further, it ensures that the safety requirements are developed at the same time as the other system requirements thus avoiding costly redesigns. Finally, it makes fitting EMI challenges into safety assurance arguments more straightforward and compelling as ADAS autonomy level increase. This case study was one example, but it could be used as the basis of a generic pattern to be used to address EM resilience in the functional safety domain.

Acknowledgement

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 812.790 (MSCA-ETN PETER). This publication reflects only the authors' view, exempting the European Union from any liability. Project website: http://etn-peter.eu/.

References

Armstrong, K. and A. Duffy (2020). Reducing the Functional Safety Risks (and Other Risks) That Can Be Caused by EMI —New IEEE Standard 1848. *IEEE Lett. on Electromagn. Compat. Pract. and Appl. 2*(3), 9.

Becker, C., L. Yount, S. Rozen-Levy, and J. Brewer (2018, August). Functional Safety Assessment of an Automated Lane Centering System.

IEC (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*.

IEEE (2020). *P1848/D7, Mar 2020 - IEEE Approved Draft Techniques & Measures to Manage Functional Safety and Other Risks With Regard to Electromagnetic Disturbances*. New York, USA: IEEE.

Kelly, T. (2004, March). A Systematic Approach to Safety Case Management. In *SAE 2004 World Congr. & Exhib.*.

Leveson, N. (2011). *Engineering a Safer World: Systems Thinking Applied to Safety*. Engineering Systems. Cambridge, Mass: MIT Press.

Meyer, B. (1992). Design by Contract. In D. Mandrioli (Ed.), *Advances in Object-Oriented Software Engineering*, Prentice Hall Object-Oriented Series, pp. 1–50. New York: Prentice Hall.

OICA (2019). World Motor Vehicle Production by Country and Type.

Palmgren, C. M. (1981, August). Shielded Flat Cables for EMI and ESD Reduction. In *1981 IEEE Int. Symp. on Electromagn. Compat.*, Boulder, Colorado, USA, pp. 1–8. IEEE.

Pissoort, D., T. Bultinck, J. Boydens, and J. Catrysse (2019, September). Use of the Goal Structuring Notation (GSN) as Generic Notation for an "EMC Assurance Case". In *2019 Int. Symp. on Electromagn. Compat. - EMC EUROPE*, Barcelona, Spain, pp. 465–469. IEEE.

Sabath, F. (2021, January) Lecture Script: "EMI Risk Management". Hannover : Institutionelles Repositorium der Leibniz Universität Hannover.

The Assurance Case Working Group (2018). GSN Community Standard.

Zhang, S., I.-L. Yen, F. Bastani, H. Moeini, and D. Moore (2017). A Semantic Model for Information Sharing in Autonomous Vehicle Systems. In *2017 IEEE 11th Int. Conf. on Semantic Computing (ICSC)*, San Diego, CA, USA, pp. 32–39. IEEE.

Ziegler, J., P. Bender, M. Schreiber, H. Lategahn, T. Strauss, C. Stiller, et al. (2014). Making Bertha Drive—An Autonomous Journey on a Historic Route. *IEEE Intell. Transport. Syst. Mag. 6*(2), 8–20.