Illustration of Cybersecurity and Safety co-engineering using EBIOS RM and IEC 61508

Pierre-Marie Bajan, Martin Boyer, Anouk Dubois, Jérôme Letailleur, Kevin Mantissa, Yohann Petiot, Jeremy Sobieraj, Mohamed Tlig

Illustration of Cybersecurity and Safety co-engineering using EBIOS RM and IEC 61508

Pierre-Marie Bajan, Martin Boyer, Anouk Dubois, Jérôme Letailleur, Kevin Mantissa, Yohann Petiot, Jeremy Sobieraj and Mohamed Tlig

IRT SystemX, 2 boulevard Thomas Gobert, 91120 Palaiseau, France.
E-mail: firstname.lastname@irt-systemx.fr

Risk analyses of complex Cyber-Physical Systems represent a persistent challenge both in Functional Safety and in Cybersecurity. Those two domains traditionally conduct their risk analyses independently. However, that independence is now questioned. The emergence of Cybersecurity risks with Safety impacts, such as killwares, acts as a serious incentive to evolve conventional methods and risk cultures. The objective of this article is to define the potential links between Functional Safety and Cybersecurity risk analyses. To that end, we made our Safety and Cybersecurity teams work on two use cases and exchange their opinions on their respective methods: HARA in Safety and EBIOS RM in Cybersecurity. In the first use case, the Cybersecurity team studies with the EBIOS RM a safety-related function : the Safe Remote Control (SRC). In the second use case, the Safety team presents a SIL assessment for SRC to the Cybersecurity team which identifies parameters to influence. Through those activities, both teams identify several points of divergence and challenges to deal with in order to enrich Cybersecurity/Safety approaches.

Keywords: Safety, Cybersecurity, Cyber-Physical Systems, Co-engineering, Risk Analysis, EBIOS RM, IEC 61508.

1. Introduction

Cyber-Physical Systems (CPS) are used in strategic areas in society, the economy and the environment. To improve the robustness and resilience of such key systems, we turn to the engineering activities of Safety (meant to prevent harm from failures) and Cybersecurity (meant to prevent harm from cyberattacks), which are independent.

However, the increasing emergence of Cybersecurity threats in CPS, and their potential impacts on customers, call into question the independence between Cybersecurity and Safety activities. Cybersecurity should take a bigger place in the context of highly connected industries. Combining Cybersecurity with Safety is a new trend that could evolve the conventional methods and risk cultures of Cybersecurity and Safety engineering towards a co-engineering method.

The objective of this article is to determine, thanks to two use cases, the potential interactions to enable Cybersecurity/Safety co-engineering. We also aim to highlight the potential divergences between these two domains.

We first introduce the current state of the art regarding Cybersecurity/Safety co-engineering in section 2.

Then, in section 3 we present the two reference methods of our use cases: the EBIOS RM methodology used in Cybersecurity, and the IEC 61508 used in Functional Safety.

The first use case presented in section 4 is the Safe Remote Control. Using EBIOS RM methodology, the Cybersecurity team identifies potential attacker profiles along with cybersecurity assets and associated vulnerabilities.

The second use case in section 5 is based on a completed Safety Hazard Analysis and Risk Assessment (HARA) analysis of an autonomous system, using IEC 61508. In an a posteriori review, the Cybersecurity team identifies new cybersecurity-related scenarios that could challenge the assessment of Safety feared events.

Then, in section 6, we give a brief overview of divergences identified during our activities.

We end with a conclusion synthesizing all the contributions of this article in section 7.

Proceedings of the 32nd European Safety and Reliability Conference.
Edited by Maria Chiara Leva, Edoardo Patelli, Luca Podofillini and Simon Wilson C

2. State Of The Art

The topic of Cybersecurity/Safety co-engineering is a pressing topic, but is not yet properly addressed in the industrial culture. Paul et al. (2016) define how standards approach this notion of co-engineering. While most of Safety and Cybersecurity standards were developed independently, more and more Safety standards suggest considering scenarios with malicious intent during risk analysis. This is the case of the transverse Functional Safety standard IEC 61508 (2010) as well as its derived automotive standard ISO 26262 (2018).

Carreras Guzman et al. (2021) highlight the evolution of Cybersecurity/Safety co-engineering approaches. They consider that conventional Safety domain should evolve to include "Security for Safety" considerations in its scope. "Security for Safety" consists in identifying Cybersecurity threats with safety issues in the Safety development process.

Boyer et al. (2021) present a classification of co-engineering methods in the automotive world. They introduce ways to include Cybersecurity in different Safety methods:

- By applying a "Security for Safety" approach to Safety risk analysis methods. For example, Schmittner et al. (2015) extends the FMEA method (Failure Mode and Effect Analysis) in Safety, by adding the notions of attacker and vulnerability: it becomes the FMVEA (Failure Mode, Vulnerabilities and Effect Analysis) method.
- By combining Safety and Cybersecurity results at specific different stages. For example, Macher et al. (2015) propose the SAHARA method which uses as inputs the Safety HARA method from ISO 26262 and the Cybersecurity STRIDE method.
- By proposing a Cybersecurity assessment score based on Safety assessment scores from ISO 26262, like in the Cybersecurity automotive standard ISO/SAE 21434:2021 (2021). Another example is Sabaliauskaite et al. (2018) who propose an automotive risk assessment classification based on vehicle autonomy level.

The drawback of the current methods is that they do not emphasize enough the interactions between the Safety and Cybersecurity teams. Thus, we study two use cases in a "Security for Safety" approach to identify and solve practical issues of Cybersecurity/Safety co-engineering:

- In the first use case, we use the Cybersecurity risk analysis EBIOS RM, applied to a safety-related system, to identify potential contributions of the Safety team.
- In the second use case, the Cybersecurity team provides feedbacks a posteriori on a Safety risk assessment based on IEC 61508.

3. Presentation of the methods: EBIOS RM & IEC 61508

In sections 4 and 5 of this article, we present two use cases relying on different reference methods that serve as a starting point for our considerations on co-engineering.

The first use case is an inspiration from the EBIOS RM (2018) methodology, while the second use case is inspired from the IEC 61508 standard. In this section, we introduce briefly the outlines of those two methods.

3.1. *Presentation of the Cybersecurity method*

EBIOS Risk Manager (EBIOS RM) is a risk analysis method created by the French cybersecurity national agency, ANSSI, in 1995. This methodology, first known as EBIOS, was updated in 2004 and 2010 before finally changing to EBIOS RM in 2018.

This method is actively pushed by ANSSI to French companies in order to raise awareness of the cybersecurity threats and is developed with two goals in mind: to be a toolbox adaptable to every context and to rapidly identify key issues.

We select EBIOS RM for the cybersecurity risk analysis method for two reasons. First, it is a

familiar method used by the Cybersecurity team in our projects, providing us with an in-depth practical experience of the method. Secondly, this method is acknowledged as a potential method for cybersecurity risks management in the PD CLC/TS 50701 (2021) standard.

Currently, EBIOS RM is decomposed in five workshops, with their respective activities:

(1) Workshop 1 consists in the identification of the security scope of the system and the stakeholders involved in its nominal functioning (its ecosystem). The functions and/or items judged as a priority target are called *business assets*.
(2) Workshop 2 consists in the identification of the main attackers profiles along their motivations. The combination of those two elements is called a *Risk Origin / Target Objective (RO/TO)* pair.
(3) Workshop 3 consists in the identification of high-level *strategic scenarios* and the evaluation of their severity.
(4) Workshop 4 consists in the identification of detailed attack paths called *operational scenarios* that are associated to *strategic scenarios*. We also evaluate the likelihood of *operational scenarios*.
(5) Workshop 5 consists in the elaboration of a risk score, that combine likelihood and severity scores. From that score, we propose a list of cybersecurity measures, and put in place a steering committee to ensure the application of the measures and the resilience of the system over time.

3.2. *Presentation of the Functional Safety reference*

IEC 61508 is a transverse standard used internationally for the Functional Safety of Electric/Electronic/Programmable Electronic Systems. It gave birth to several standards specific to industrial domains (automotive, railways, nuclear, etc.). In the absence of an existing standard on certain specific domains, this standard is often used as a reference.

The second edition of IEC 61508 (2010) is open to security topics in the Safety analysis. Indeed, the standard indicates in section 7.4.2.3 that *"if the hazard analysis identifies that malevolent or unauthorised action, constituting a security threat, as being reasonably foreseeable, then a security threats analysis should be carried out"*. However, it does not detail how (Cyber)Security can be incorporated in Safety processes.

The IEC 61508 defines how to identify and select critical scenarios using Safety Integrity Levels (SIL). The SIL is the expected level of efforts and measures to comply with in order to satisfy Safety at a system, equipment, or component level. The score range goes from SIL 1 to SIL 4, with SIL 4 being the most stringent level. Multiple methods exist to attribute a SIL. For the use case studied in section 5, we use the Risk Graph method.

4. First use case: Cybersecurity activities at the service of Functional Safety

The main objective of this study is to identify in which way the Safety team contributes to the Cybersecurity EBIOS RM analysis. For this purpose, we study a system called Safe Remote Control (SRC) used in railways for safety-related functions such as management of temporary speed restrictions. We select a system for which Safety is already integrated in the design process, known as "Safety-by-design". However, a Cybersecurity study has yet to be performed. Therefore, the Safety team collaborates with the Cybersecurity team to make sure the safety-related system is also resilient to cyberattacks. The use case benefits from a previous EBIOS RM evaluation of a more global system. As such, we focus on the workshops that bring added value to the previous evaluation, namely Workshops 2, 3 and 5.

4.1. *Principle of Safe Remote Control*

The SRC is a system that allows safe inputs and that processes commands applied by an operator to a target equipment. It relies on a double-command principle: the human operator inputs the same command in two different manners, which are consecutively received and verified by the target equipment. This equipment then confirms to the operator if the global command is validated

or rejected (in case of error or contradicting commands). This double-command reduces the risk of input error from the operator. We illustrate the SRC principle in Figure 1.

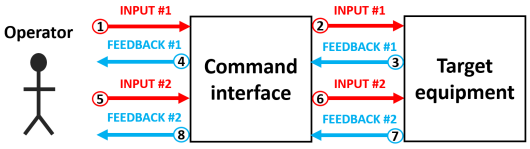

Fig. 1.: General principle of Safe Remote Control

The main Safety feared event for SRC is to put the target equipment in an unsafe situation following an unwanted command validation.

4.2. *Identification of Cybersecurity feared events and risk sources:*

Based on the initial Safety feared event of SRC, the Cybersecurity team first identifies four important functions (*business assets*) in the SRC: the reception of the command, the periodic delivery of the command, the status checking of the target equipment and the speed restrictions scheduling.

Afterwards, from the security criteria of the global EBIOS RM analysis, the Safety team identifies four Security criteria relevant for Safety: authenticity, authentication, availability, and integrity.

From our analysis of each couple of assets and criteria, we propose a list of twenty Cybersecurity feared events for SRC which are safety-relevant. Some examples of feared events are the reception of a command whose origin is not certified, the delivery of a command from an unauthorized computer, or the corruption of the speed restriction scheduling.

Then, we select from the list of attackers' profiles (*RO*/*TO* pairs) those likely to target the SRC and that are unfazed by potential safety impacts. An example of *RO*/*TO* pairs for SRC would be the Organized crime, aiming for Extortion. Visualizing those *RO/TO* pairs is helpful for Safety to consider other sources of harms not related to failures or misuses, and involving active human actors. Those can be integrated in new safety scenarios to be referenced in the Safety risk analysis.

4.3. *Defining safety-related strategic scenarios and cybersecurity measures:*

Strategic scenarios can be built by coupling *business assets* with *RO*/*TO* pairs. For each triplet, we define one or several *strategic scenarios* for SRC. We identify twenty-six *strategic scenarios* likely to occur such as the Organized crime, which installs a ransomware on the command interface, in a goal of extortion. Another example is, with the same goal, the Organized crime can block the command signals sent to the target equipment. These *strategic scenarios* differ from usual safety scenarios which may not be as detailed and are specified at a functional level.

Normally, *strategic scenarios* are only used to evaluate the severity or risk scenarios. In our use case, the technical perimeter of our study is limited and we do not require detailed attack paths to identify security measures. Thus we do not go beyond strategic scenarios to identify security measures.Those measures aim to reach an acceptable *threat level* for the stakeholders. In the study of SRC, we propose a list of twenty-two security measures sufficient for all identified *strategic scenarios*, such as: the deployment of antiviruses and security patches, a strong update policy, the deactivation of USB ports on command interface, the application of secured boots, etc. Those measures are not part of initial Safety requirements applied on SRC, and thus their application improves the resilience of the system.

Those aforementioned Cybersecurity measures are reviewed by the Safety team, to identify their compatibility with Safety measures. For example, in the case of SRC, rapid deployment of security patches is a conventional control measure in Cybersecurity. However, in Safety, this measure can impact safety mechanisms already in place and introduce new considerations. Thus, it is imperative to first ensure that those corrective patches comply with safety mechanisms before proceeding to deployment.

Thanks to this activity, we manage to design a safety device more resilient. Cyberattacks can impact the proper working of the SRC, thus inhibit-

ing its safety properties. With the application of a Cybersecurity analysis, we reinforce the resilience of the SRC against cyberattacks, which warrants its safety properties against threats.

However, this activity also raises the following topic for Safety: does the Safety team need to integrate all defined Cybersecurity measures and requirements into their analysis, and what would be the rationale to dismiss some of them? This topic needs to be discussed further.

The process for this use case is synthesized in Figure 2.

5. Second Use Case: Cybersecurity inputs in SRC SIL assessment

In a second use case, we study possible interactions between both teams for the assessment of risk scenarios, in a two-step approach: one theoretical and one example, to determine how Cybersecurity could influence a Safety assessment.

5.1. *Cybersecurity/Safety co-engineering using IEC 61508 Risk Graph method*

During conventional Safety HARA, we identify safety risk scenarios and assess their criticity. The process to assess the risk scenarios may differ depending on the considered standard: ASIL from ISO 26262 in the automotive field, SIL from NF EN 50126 (2017) in the railway field, etc. To be as general as possible, we use the transverse IEC 61508 standard as reference for this use case.

In the IEC 61508, one of the proposed methods for SIL assessment is the Risk Graph method, presented in Figure 3. In our use case, we limit our application of the IEC 61508 approach to the Risk Graph method. It allows to define a SIL for a system via a qualitative analysis of four parameters:

(1) C, the consequence of the feared event.
(2) F, the frequency or duration of exposure in the hazardous situation.
(3) P, the probability of occurrence of the unwanted event.
(4) W, the possibility of avoiding the feared event.

Depending on the value of each parameter, a given SIL is attributed to the risk scenario and associated feature, using the Figure 3.

Using the Risk Graph method, we divide the work in two steps:

(1) The first step is to define, on a generic level, what are the impacts of cybersecurity threats on each parameter defining the SIL.
(2) The second step is to validate our hypothesis: can the Cybersecurity team provide legitimate cybersecurity scenarios contesting the assessment?

5.2. *First step: Generic Methodology*

For the first step, the Cybersecurity and Safety teams determine which parameter is impacted by Cybersecurity.

(1) C : we identify that the Cybersecurity team only has a minor impact on this parameter. Indeed, since the Safety team already applies a “worst case” approach, a cybersecurity-related scenario with maximal consequence can simply be considered as a variant of an existing scenario. However, when relevant, the Cybersecurity team can propose new scenarios instead of modifying existing ones.
(2) F : the Cybersecurity team can propose new ways or approaches that lead to a similar failure. Those approaches can be triggered in a larger area than expected or with an increased frequency compared to the safety scenario. Reports such as Embroker (2022) consider that there is one ransomware cyberattack in 11 seconds in 2021. Besides, it could be relevant to study the association of the qualitative metric of F parameter with other qualitative metrics like the Likelihood/Feasibility in Cybersecurity studies such as EBIOS RM or ISO/SAE 21434.
(3) P : Since safety mechanisms are implemented to protect the system in case of failure, we consider it plausible for an attacker to deactivate those mechanisms before a failure happens. A lack of awareness regarding Cybersecurity risks, as well as human negligence can impede the capacity to avoid hazards. Thus, Cybersecurity can impact the parameter P.
(4) W : with a cyberattack, an attacker can easily

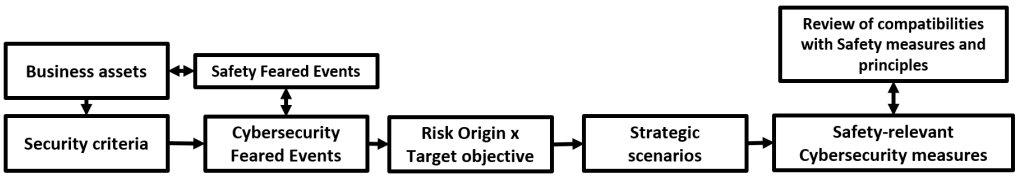

Fig. 2.: Process applied for the first use case

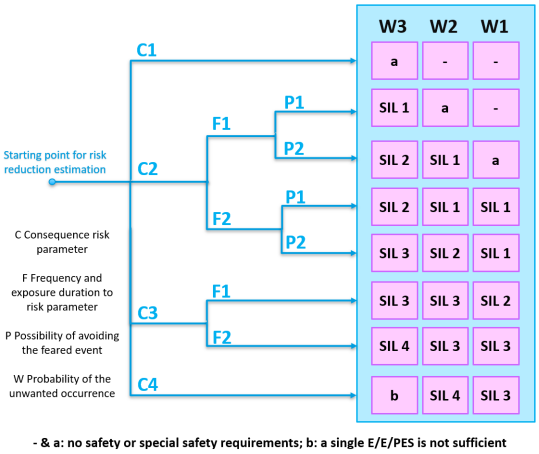

Fig. 3.: Risk Graph from IEC 61508

reproduce a hazardous scenario. Thus, similarly to the parameter F, Cybersecurity can increase the parameter W.

To summarize the first step of our approach, we envision that Cybersecurity can impact the F, P and W parameters of existing safety scenarios for SIL assessment. Besides, if there is a preliminary Cybersecurity study prior to the Safety assessment, attack scenarios could be used to justify impacts on F and W parameters. However, these impacts should not be one-sided proposals from Cybersecurity. They should serve as a basis of discussion with the Safety team, to develop a more robust Safety argumentation taking into account the cybersecurity threats.

5.3. *Second step: Application*

In the second step, we consider the following use case: a driving autonomous system with safety-related properties using SRC for several features.

Using SRC, we can command the autonomous system to bypass an obstacle: this feature is called *Obstacle Avoidance*. We consider that this feature has been assessed beforehand by a Safety assessor as SIL 1, with the following parameters: [C2, F1, P2, W2]. This score is based on Figure 3.

For the parameter C, based on the first step of this approach, we do not change the parameter C. However, we can create another scenario which is cybersecurity-related.

For the parameter F, this parameter is increased, from F1 to F2, since it is possible to trigger this function erroneously with a cyberattack.

For the parameter P, a cyberattack targeting other components could decrease our trustworthiness in the perception system. However, since the parameter P is already at the highest level P2, it cannot be further increased, and remains unchanged.

Finally, the probability of occurrence of the feared event W is increased due to the added effect of a cyberattack. This means that we go from W2 to reach the highest level of this parameter, W3.

The resulting [C2, F2, P2, W3] rating from the cybersecurity threats on this feature increases the initial SIL from SIL 1 to SIL 3, mainly by impacting the parameters F and W. We summarize the results for other features of SRC in the table 1.

This use case shows that taking Cybersecurity inputs in the activity of Safety assessment can influence the discussions and conclusions on the HARA, by identifying new Cybersecurity-related safety scenarios, which can impact the SIL assessment. A mix of additional Cybersecurity and Safety measures can be used to justify the SIL of a system in a co-engineering context. While the doubt of an overqualified safety risk can dispute the influence of Cybersecurity inputs on the SIL score, it remains undeniable to integrate the cybersecurity concerns to the SIL process in order to treat them. This integration is key to build a system robust to failures and resilient to cyberattacks.

Feature	Initial C F P W	Initial SIL	Cybersecurity impact	New SIL
Minimum Risk Maneuver	C4 - - W1	SIL 3	W	SIL 4
Speed Limitation	C3 F1 - W1	SIL 2	F	SIL 3
Obstacle Avoidance	C2 F1 P2 W2	SIL 1	F and W	SIL 3

Table 1.: Cybersecurity impacts on SIL assessments using IEC 61508

6. Discussion

Thanks to the previous use cases, we identify several topics of divergence between the Safety and Cybersecurity teams. Those divergences are diverse and can present a challenge for Cybersecurity/Safety co-engineering.

6.1. *Role of individuals in hazardous scenarios as risk sources*

The impact of human intent on safety scenarios in our two use cases illustrates an inherent divergence between Cybersecurity and Safety. In Cybersecurity, the sources of risk come from an intentional action of cyberattackers. In Functional Safety, the sources of risks are generally unintentional, with some cases of misuse resulting from human error.

The integration of cyberattackers in safety scenarios impacts the type of risks, as well as the design of the system to ensure that safety-critical functions are properly protected. It also reveals a lack of compatibility between Safety and Cybersecurity metrics, which is a challenge identified in co-engineering. This means that a change of mindset in the Safety culture is needed to ensure proper Cybersecurity/Safety co-engineering. This evolution can be captured in some standards (IEC 61508, etc.), which make it possible to integrate cybersecurity-related scenarios in Safety risk analyses.

6.2. *Compatibility between Safety and Cybersecurity measures*

The first use case illustrates that some conflicts can emerge from the compatibility between Safety and Cybersecurity mitigation measures.

As seen in subsection 4.3, contradicting principles on implemented Safety and Cybersecurity measures can appear during the design or modification of systems. In Safety, the modification of a safety-related system can be done only after we perform non-regression testing, to ensure that the modification does not introduce new risks or change the behaviour of the safety measures. In Cybersecurity, the detection of new vulnerabilities or cybersecurity threats must be quickly corrected by patches to mitigate the risk. These two approaches are valid in their respective domains, but can be in contradiction in the context of co-engineering on CPS.

6.3. *Treatment of Cybersecurity requirements compared to Safety*

In section 4.3, we raise the question of incorporating every cybersecurity measure identified along the current safety measures. Indeed, in a cybersecurity analysis, the resulting cybersecurity measures are often considered as recommendations and not mandatory. Thus, a system owner may assume the risks of deploying its system without complying with every identified cybersecurity measure.

In Functional Safety, the proper implementation of Safety requirements and measures constitutes the Safety demonstration. A safety-related system cannot be commercialized for a certified SIL indicated if its safety requirements are not satisfied. Their satisfaction is often implemented and justified in a Safety assurance case. The Safety assurance case is a traditional work product expected by Safety standards, at the end of a development. However, in Cybersecurity, this approach is not as widespread.

This can be detrimental to Cybersecurity in a co-engineering context: in situations of conflict between Cybersecurity and Safety, a priority might be erroneously given to the implementation of Safety measures, whereas Cybersecurity mea-

sures may be just as essential. However, emerging standards in Safety assurance for automotive autonomous driving, such as UL 4600 (2020), insist on the importance of integrating Cybersecurity risks in the Safety demonstration. Recent standards in Cybersecurity, such as the TS 50701 standard in railway Cybersecurity, relies on existing Safety standard (in this case the EN 50126) to propose Cybersecurity assurance case that can potentially synchronize with Safety activities.

7. Conclusion

Through two use cases, we realize the potential of Cybersecurity/Safety co-engineering to reach a mutual understanding on respective best practices, methodologies and potential synergies.

With the first use case, thanks to the EBIOS RM method, we identify several cybersecurity artefacts likely to impact the Safety of a system. The review of those artefacts by the Safety team enables to identify new causes of hazards for their safety scenarios, as well as potential conflicts between the safety and cybersecurity mitigation measures.

In the second use case, based on a IEC 61508 methodology, we identify potential impacts of the Cybersecurity on the risk identification and SIL assessment of the system. It is an incentive to take into account Cybersecurity expertise in the Safety analysis of a CPS from the beginning. This still needs to be materialized in industrial contexts.

Finally, we identify various divergences between Cybersecurity and Safety domains, such as how to combine safety and cybersecurity mitigation measures without conflicts. They need to be addressed in future works for the sake of co-engineering.

Acknowledgement

This research work has been carried out in the framework of IRT SystemX, Paris-Saclay, France, and therefore granted with public funds within the scope of the French Program "Investissements d'Avenir". Authors are listed alphabetically by last name.

References

Boyer, M., T. Chelim, and J. Sobieraj (2021). Hybridization of safety and security for the design and validation of autonomous vehicles: where are we? In *ESREL 2021 - 31st European Safety and Reliability Conference*.

Carreras Guzman, N. H., I. Kozine, and M. A. Lundteigen (2021). An integrated safety and security analysis for cyber-physical harm scenarios. *Safety Science vol. 144*, p. 105458.

EBIOS RM (2018). Ebios risk manager – the method.

Embroker (2022). 2022 must-know cyber attack statistics and trends. Report, San Francisco 24 Shotwell St San Francisco, CA 94103.

IEC 61508 (2010). Iec61508:2010 functional safety of electrical/electronic/programmable electronic safety-related systems. Iec, International Electrotechnical Commission.

ISO 26262 (2018). Iso 26262-1:2018 road vehicles — functional safety. Standard, International Organization for Standardization, Geneva, CH.

ISO/SAE 21434:2021 (2021). Road vehicles — cybersecurity engineering. Standard, International Organization for Standardization, Geneva, CH.

Macher, G., A. Höller, H. Sporer, E. Armengaud, and C. Kreiner (2015). A combined safety-hazards and security-threat analysis method for automotive systems. In *Computer Safety, Reliability, and Security*, pp. 237–250. Springer International Publishing.

NF EN 50126 (2017). Nf en 50126-1: Railway applications – the specification and demonstration of reliability, availability, maintainability and safety (rams) – part 1: Generic rams process. En, Comité européen de normalisation en électronique et en électrotechnique.

Paul, S., J. Brunel, L. Rioux, F. Vallée, J. Oliveira, G. Gailliard, J.-L. Gilbert, T. Wiander, M. E. Bakkali, A. Faucogney, and D. Chemouil (2016). Recommendations for security and safety co-engineering (release n°3) - part a. Technical report.

PD CLC/TS 50701 (2021). Pd clc/ts 50701: Railway applications - cybersecurity. En, BSI.

Sabaliauskaite, G., J. Cui, L. S. Liew, and F. Zhou (2018). Integrated safety and cybersecurity risk analysis of cooperative intelligent transport systems. In *Proceedings - 2018 Joint 10th International Conference on Soft Computing and Intelligent Systems and 19th International Symposium on Advanced Intelligent Systems, SCIS-ISIS 2018*.

Schmittner, C., Z. Ma, E. Schoitsch, and T. Gruber (2015). A case study of fmvea and chassis as safety and security co-analysis method for automotive cyber-physical systems. In *CPSS 2015 - Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, Part of ASIACCS 2015*.

UL 4600 (2020). Ul 4600:standard for evaluation of autonomous products. Standard, Underwriters Laboratories Inc.