An Industrial Experience in Cross Domain Assurance Projects

Alejandra Ruiz[1(✉)], Xabier Larrucea[1], Huascar Espinoza[1], Franck Aime[2], and Cyril Marchand[2]

[1] ICT – European Software Institute Division, Tecnalia, Derio, Spain
{alejandra.ruiz,xabier.larrucea,huascar.espinoza}@tecnalia.com
[2] Airworthiness & Certification Directorate, Thales Avionics, Toulouse, France
{franck.aime,cyril.marchand}@fr.thalesgroup.com

Abstract. Companies related to safety critical systems developments invest efforts and resources to assure that their systems are safe enough. Traditionally reuse strategies have been proposed to reduce these efforts in several domains which criticality is not a key aspect. However reusing software artefacts across different domains establishes new challenges especially between safety critical systems. In fact we need to take into account different domain specific standards requirements at the same time. In this paper we present our experience on cross domain assurance involving a reuse of a software component developed for the railway domain, and to be used for the avionics domain.

Keywords: Compliance · Cross domain · Reuse · DO-178 · EN 50128

1 Introduction

Some challenges for safety assurance and (re)certification approaches are identified in [1]. Authors mention that one of the difficulties for a cross domain reuse is the need to comply with multiple standards and to provide a seamless certification process. This process needs to take into account different domains when developing a new product in a safety critical context. The main purpose when reusing one artefact from one domain into another is basically to reduce efforts and resources, and to increase the return on investment of this kind of products.

Cross-domain requires a common understanding of both domains, and to consider different processes and requirements from different sources at the same time. This understanding should include all stakeholders from these domains, and to define consistently a set of structured arguments to be used during the assessment process. In order to be able to reuse assessment data of already approved components we need to define some reuse criteria. It is important to gather this information in order to build a predictive performance model and to manage assessments in order to meet the certification objectives.

This paper is structured as follows. First a background is provided. Second our use case is described and our approach is described in detail. Third some results are presented. And a final section ends this paper.

R.V. O'Connor et al. (Eds.): EuroSPI 2015, CCIS 543, pp. 29–38, 2015.
DOI: 10.1007/978-3-319-24647-5_3

2 Background

Safety standard guidelines on how to manage safety design so as to mitigate the possible risk as a direct impact on cost. [3] Machrouh also mentioned that "Defining the commonalities between safety standards in various domains allows one to reduce the development cost of the critical embedded systems by mutualising the developments by reuse of components".

Reusing a project is difficult and even more when the context changes for example reusing across domain. Very few attempts have been made in order to harmonized the different domain approached in order to proposed a cross-domain reuse [3], [4], [5] have analysed the similarities and divergences of the different standards. Blanquart makes an analysis from the critical categories and highlight that all standard share the same fundamental concepts where critical categories are linked to the risk and effects of potential failures. The main divergence comes from acceptance frontier.

Papadopoulos and McDermid [6] defined a reference structure for the comparative review of standards. The structure is based on five principal dimensions of the certification problem: (1) Requirements for system development and safety processes, (2) Method for establishing the system Safety Requirements, (3) Definition, treatment and allocation of development assurance levels, (4) Requirements on techniques for component specification, development and verification and (5) Requirements on the content and structure of the safety case.

Zeller [7] proposed cross-domain assurance process in conjunction with any development methodology for safety-relevant software. The objective was to reduce the effort for safety assessment by reusing safety analysis techniques and tools for the product development in different domains.

As a result of these previous analyses the following similarities between the examined standards have be identified:

- Common notion of safety and certification
- Linear progressing safety process with dedicated phases
- Combined hazard assessment and risk analysis to derive safety requirements
- Criticality levels as means to allocation safety (integrity) requirements to system elements
- Verification activities are driven by the safety requirements
- Safety case provides evidence that safety requirements are fulfilled which is needed for certification

SAFECER project [8] proposed some cross domain case studies, the focus of the reuse across domain on these studies were on the tool qualification. On tool qualification there is a large overlap between standard. The main targets on these case studies were the DO -178 [9], IEC 61508 [10] and ISO 26262 [11]

3 Use case

3.1 Business Case

General context of the Avionics Use Case is a situation of product reuse from one domain (Railways) to another domain (Avionic). The goal is to build the Qualification Dossier, based on elements provided with the reused parts. The Qualification Dossier is then presented for certification. The reused product is the Execution Platform (Computing Unit and Operating System) which was developed for a given domain (Railways) and it will be installed in another domain (Avionic). The execution platform is considered as an independent item for which a qualification dossier will be built. This qualification dossier consists of plans, technical documents, and certification documents. Technical documents are specifications, validation and verification life cycle data. The certification documents are configuration index documents and accomplishment summaries. The initial execution platform and the associated documentation issued from the railway domain comply with railway standards (CENELEC EN50128 [12]). The final execution platform and the elaborated qualification documentation to be used in avionics domain must comply with avionics standards (ED-12c/DO-178).

One of the first challenges was to establish a mapping between standards from different application domains. When reusing from one domain to another the compliance evidence used for one standard need to find their equivalence of the new standard. Some standards are process oriented while others are product oriented. Therefore equivalences between standards require a detailed description of items. In addition we need not only to set up these equivalences, but also to define how assurance information is going to be reused on the new domain. We defined a cross domain reuse based on 3 criteria:

- Associated Process / Design Assurance: Process domain shall be reusable from source domain to target domain
- Technical Solution: Design details shall be available from source domain to target domain
- Intended function boundary: Intended function shall be reusable from source domain to target domain

3.2 Our Approach

Our approach is designed in four steps which are illustrated in the following Fig. 1.

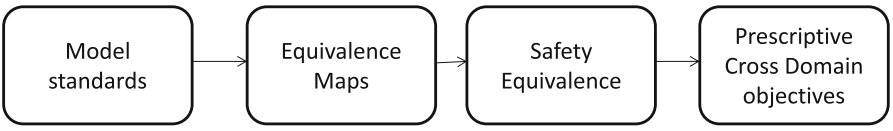

Fig. 1. The main steps in our approach

The first step in our approach is to model railway and avionics standards and we used the same metamodel [2]. In our case we will be focused on DO-178C and the EN 50128. This metamodel [2] is domain agnostic, and we can specify some requirements from standards. We developed an Eclipse based tool according to this metamodel, and we model these standards. Fig. 2 provides an overview of the main sections of the DO178C and a snapshot of our tool.

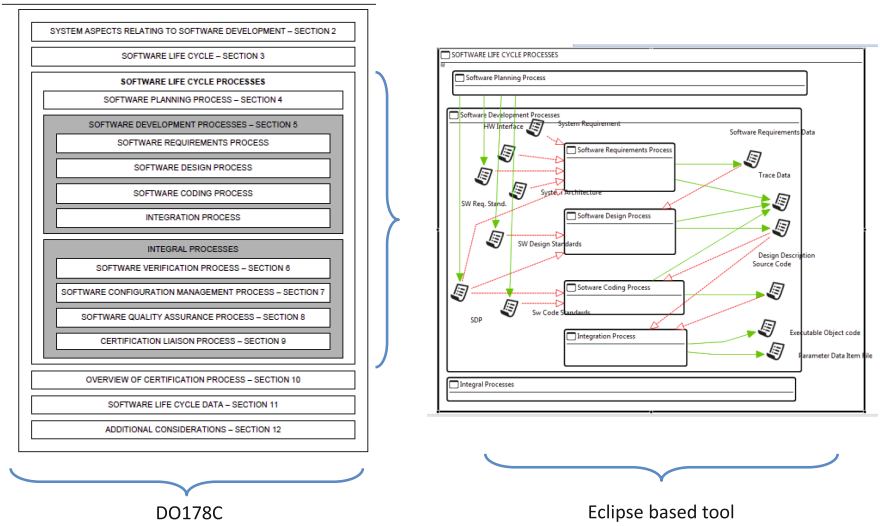

Fig. 2. DO178c standard and its representation in our Eclipse based tool

A second step is to compare each standard concept from railway domain to avionic domain. This mapping is called “equivalence map”. In fact this mapping is not just focused on activities but also on generated work products. For example on the one hand EN50128 is a product based standard, and it prescribes product based features to ensure safety. On the other hand DO-178 prescribes processes to ensure safety. This equivalence map is graphically represented in Fig. 3. Both standards contain traceable activities and work products between them which represent 27,75% of the items. However there are other situations where there is no such relationship (19,23%) or even we can identify a partial relationship between items (53%). There are some orphan sections where standards requirements do not apply in our case study. Therefore there is no possible equivalence map. Fig. 3 illustrates these relationships and our findings can be summarized as follows:

- Roles and responsibility (§5 of EN50128) in railway are no equivalent in avionic,
- Validation in avionic is an Aircraft/System dedicated process and a part of ED79A /ARP4754A,
- Generic Software Development (§7 of EN50128) in railway are no equivalent in avionic at DO-178 level. Therefore, at system level, the Technical Standard Order (TSO) may be viewed as a generic development regarding the targeted aircraft but with the intended function well specified,

- Software deployment and maintenance (§9 of EN50128) in railway are no equivalent in avionic at DO-178 level. Therefore, at system level, the means of compliance of Certification Specification 25.1529 “Continued Airworthiness” may be viewed as an equivalent objective.
- Safety function in railway is the equivalent of avionic safety-related * functions at A/C definition level.
- Validation in avionic is an Aircraft/System dedicated process and a part of ED79A /ARP4754A.
- Transition criteria are an important asset for avionic domain, based on process control demonstration.
- Derived Requirement is an important asset for avionic domain, based on intended function demonstration (Certification Specification 25.1301).

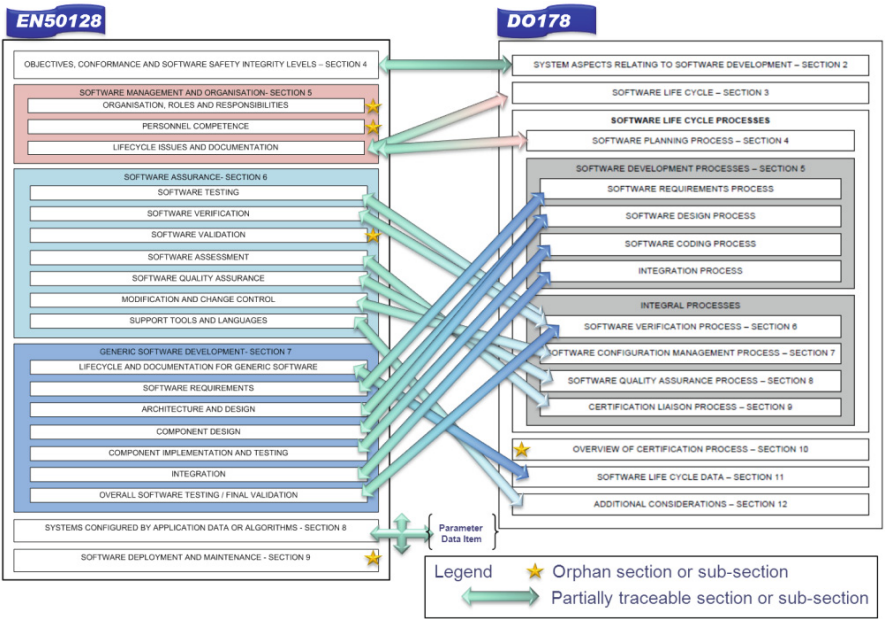

Fig. 3. Safety Standards Documents framework

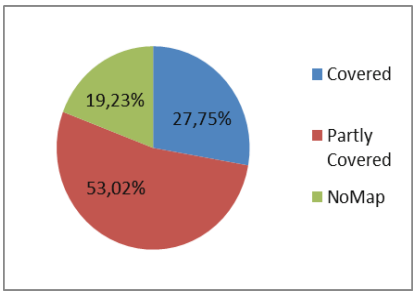

Fig. 4. Coverage between DO178C and EN50128

The third step for our analysis is focused on providing a mean to claim equivalence levels of safety from one domain to another. In this sense we need to identify Prescriptive Product Based objectives and Prescriptive Process Based objectives. All requirements are traced and evaluated. In addition we trace each objective from the railway process based standard to the objectives on the avionics base standard. These traces represent our prescriptive cross domain standard (PxB) including all requirements, and which represent safety equivalences.

The final step is the function analysis based on this Prescriptive Cross Domain Based standard. We need to identify additional or missing activities from source to target safety standard represented as post- conditions. These activities are carried out to meet objectives which are partially mapped or there is no map at all. All these elements are required to make the Execution platform ready to show compliance with certification requirements. Once equivalence mappings are created we apply them to our assurance project created for the railway domain. These equivalence mappings contain assurance information, and it generates the compliance artefacts from EN 50128 standard to Do178c standard.

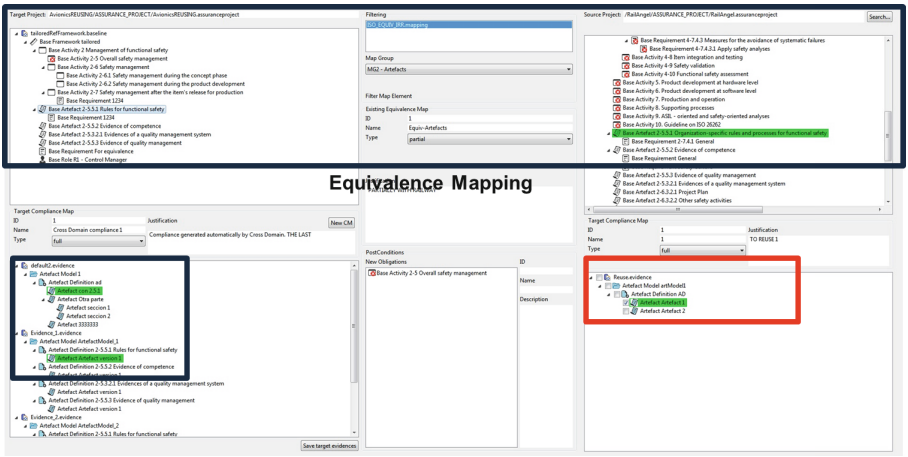

Fig. 5. Equivalence mapping application

Fig. 5 shows a wizard which supports our equivalence mapping between EN50128 and D0-178c. On the upper side equivalences between standards are identified. On the lower part the information about the specific standard is described. If we apply these equivalence maps we get the information complying with DO 178c standard.

4 Results

In order to measure the results of our cross domain experience we defined a set of metrics, and we gathered some values. Fig. 6 shows these metrics and values. We identified 4 aspects to be measured which can be seen on the question column on Fig. 6:

- Cost effectiveness of the assurance process across systems: This industrial experience focuses on the reuse of the execution platform from the railway domain to the avionics domain. The objective is to eliminate or limit additional activities to the original certification activity in the railway domain. Traditionally this activity leads to directly build qualification documents (configuration management and accomplishment summaries) according to avionics standards. Traditionally we manually perform an equivalence using existing documents from railway domain and then to build a qualification documents according to avionics standards.
    - Assurance asset reuse focusses on requirements defined in the standards. In this metric, we measure the total number of requirements which can be accomplished in the avionics domain as result of validating equivalent requirements in the railway domain.
    - Baseline elements that do not need a new compliance map, takes into consideration the expected detection of standards' elements in the avionics assurance project whose compliance with can be fully validated from the requirements already accomplished in the railway assurance project.
    - Assurable elements with applicable equivalence maps, metric refers to the equivalence maps between avionics and railway reference assurance frameworks, with focus on reference requirements. Making explicit the equivalence between standards from different application domains facilitate the assurance tasks.

Question	Metric	Value	Comments
Cost-Effectiveness of the Safety Assurance Process across Systems and Markets	**Assurance asset reuse**	0,74	Focused on Baseline Requirements
	Reused Assurance Assets	155	Reused Compliance Requirements
	Total Assurance Assets	210	Total Set of Avionics Baseline Requirements
	Baseline elements that do not need a new compliance map	0,19	Focused on Baseline Requirements
	Baseline elements that do not need a new compliance map	40	Number of assets reused whose compliance map is Full
	Total Baseline Elements	210	Total Set of Avionics Compliance Requirements
	Assurable elements with applicable equivalence maps	0,67	Focused on Reference Requirements
	Assurable elements with applicable equivalence maps	210	Number of Ref Requirements with Equivalence maps
	Total Assruable Elements	315	Total set of Ref Requirements
Automation of the Safety Assurance Process	**Automated compliance map creation**	0,74	Focused on automated compliance maps for base requirements
	Compliance maps automatically created	155	
	Total compliance maps	210	
	Automated impact analysis	0	None
	Automatically detected Impacted Elements	0	
	Total impacted elements	210	
Safety Assurance Reuse across Domains	**Assurable elements equivalence**	0,67	Focused on Reference Requirements
	MASE1 + MASE2	210	Number of Ref Requirements with Equivalence maps
	ASE1+ASE2	315	Total set of Ref Requirements
	Assurance asset reuse across application domains	0,74	Focused on Baseline Requirements
	Reused across domains Assurance Assets	155	Reused Compliance Requirements
	Total Assurance Assets	210	Total Set of Avionics Baseline Requirements
Awareness of Reuse Consequences	**Assurance assets whose reuse is possible**	0	None
	Estimated Reusable Argumentation Elemnts	0	
	Total predicted Argumentation Elements	100	
	Baseline elements whose compliance with has to be shown	0,81	Focused on Baseline Requirements
	Baseline elements that need a new compliance map on the new domain	170	Number of assets that need a compliance map, Full or Partial, in the new domain
	Total Baseline Elements	210	Total Set of Avionics Compliance Requirements

Fig. 6. Metric Measurement Results for Reduction of Recurring Costs

- Automation of the Safety Assurance Process: Our platform provides automated support for generating avionics artefacts.
    - Automated compliance map creation, this can occur in an avionics assurance project regarding cross-domain reuse if equivalence maps have been specified between railway and avionics reference assurance frameworks. Our tool suite creates compliance maps automatically, so that all the possible baseline requirements in the avionics project, with full and partial equivalence in the railway project, are created automatically with the Cross-Domain reuse tool.

- Assurance Reuse across Domains: The problem of cross-domain transfers is that certification objectives may be specific to a domain, or differently expressed. The objective of the metrics is not to measure the level of commonality between domains, but its ability to help translation of artefacts between domains when correspondence can be established.
    - Assurable elements equivalence. This metric refers to the cross-domain equivalence maps between avionics and railway reference assurance frameworks, with focus on reference requirements.Making explicit the equivalence between standards from different application domains facilitate the assurance tasks.
    - Assurance asset reuse across application domains. In this metric, we measure the total number of requirements which can be accomplished in the avionics domain as result of validating equivalent requirements in the railway domain.Rationale for improvement: Having available the equivalence between requirements to be accomplished in different domains help reduce re-assurance costs.

- Awareness of Reuse Consequences: Our approach provides models for safety certification; it should be possible to improve the determination of reuse consequences.
    - Baseline elements whose compliance with has to be shown. When reusing information from the railway assurance project, out tool platform is expected to detect the baseline elements in the avionics assurance project whose compliance must be revised.

Fig. 7 summarizes the main numbers for this cross domain experience. “Traditional approach” header represents the effort and cost of activities which are under our approach influence. For instance, Standard interpretation for cross-domain reuse sub-activities called “Specification of cross-domain equivalences”, “Compliance traceability”, and “Specification of compliance requirements in relation to reused projects” can be improved by using out tool suite. These sub-activities represent the 45% of effort of the whole evidence collection activities. We can see that the 41,5% of the effort in global assurance and certification activities are susceptible of

improvement by using our approach. The numbers showing on the figure were extracted from the reuse metrics described for the previous figure. The effort savings is approximately 26.95% based on our experience. However when we are using our approach, the effort savings is 54.4%.

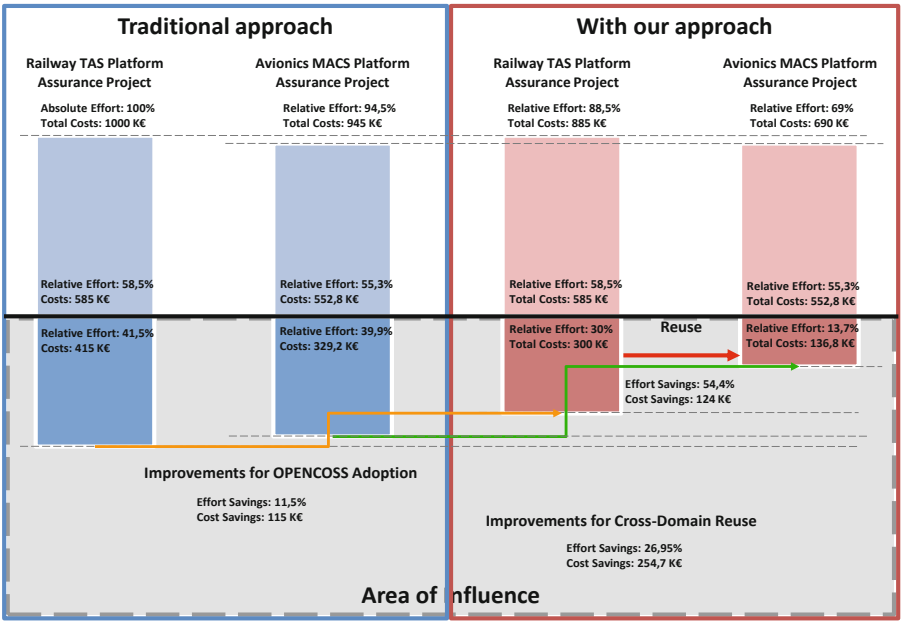

Fig. 7. Railway to Avionics Case Study

5 Conclusions and Future Work

From this industrial experience we can conclude that safety engineering activities in one domain have similarities to safety activities in other domain. Even safety related techniques have several commonalities. Our approach is based on a common meta-model for describing safety standards requirements in order to provide a common understanding between domains. In a near future this common understanding is going to be shared between stakeholders from different domains.

Criteria of cross domain reuse are identified in this paper. Innovative aspects based on cross-over effects between application domains are carried out in a real situation. We are able to reuse assessment data of already approved components from one domain into another. In addition our approach helps to identify gaps between standards. An improved version of this paper provides a deeper analysis of this case study, and it provides a better view on verification and validation data, and traceability.

The presented approach provides an agile assessment process for identifying and it increases understandability of standards requirements from different domains. In addition it enables a preliminary assessment of targeted certification objectives.

It also allows the development of a consistent set of structured arguments from different domains. We have proved a reduction of recurring costs for this case study mainly relate to costs for cross-domain assurance and certification.

From this experience Thales considers to implement a product family strategy to reduce costs, especially in recertification activities. These strategies may use cross domain reuse and model based engineering including certification language.

References

1. Espinoza, H., Ruiz, A., Sabetzadeh, M., Panaroni, P.: Challenges for an Open and Evolutionary Approach to Safety Assurance and Certification of Safety-Critical Systems 2011, pp. 1–6 (2011)
2. de la Vara, J.L., Panesar-Walawege, R.K.: SafetyMet: a metamodel for safety standards. In: Moreira, A., Schätz, B., Gray, J., Vallecillo, A., Clarke, P. (eds.) MODELS 2013. LNCS, vol. 8107, pp. 69–86. Springer, Heidelberg (2013)
3. Machrouh, J., Blanquart, J.P., Baufreton, P., Boulanger, J.L., Delseny, H., Gassino, J., Ladier, G., Ledinot, E., Leeman, M., Astruc, J.M.: Cross domain comparison of system assurance. In: ERTS 2012, Toulouse, pp. 1–3 (2012)
4. Blanquart, J.P., Astruc, J.M., Baufreton, P., Boulanger, J.L., Delseny, H., Gassino, J., Ladier, G., Ledinot, E., Leeman, M., Machrouh, J.: Criticality categories across safety standards in different domains. In: ERTS 2012, Toulouse, pp. 1–3 (2012)
5. Ledinot, E., Astruc, J.-M., Blanquart, J.-P., Baufreton, P., Boulanger, J.-L., Delseny, H., Gassino, J., Ladier, G., Leeman, M., Machrouh, J., et al.: A cross-domain comparison of software development assurance standards. In: Proc. of ERTS2 (2012)
6. Papadopoulos, Y., McDermid, J.A.: The potential for a generic approach to certification of safety critical systems in the transportation sector. Reliability Engineering & System Safety **63**(1), 47–66 (1999)
7. Zeller, M., Höfig, K., Rothfelder, M.: Towards a cross-domain software safety assurance process for embedded systems. In: Bondavalli, A., Ceccarelli, A., Ortmeier, F. (eds.) SAFECOMP 2014. LNCS, vol. 8696, pp. 396–400. Springer, Heidelberg (2014)
8. Safecer Project Safety Certification of Software-Intensive Systems with Reusable Components Web: http://www.safecer.eu
9. RTCA DO-178/EUROCAE ED-12, Software Considerations in Airborne Systems and Equipment Certification (2011)
10. IEC 61508 IEC61508, 61508 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. International Electrotechnical Commission (2011)
11. International Organization for Standardization (ISO), ISO26262 Road vehicles – Functional safety, ISO (November 2011)
12. CENELEC EN 50128 - Railway applications — Communication, signalling and processing systems — Software for railway control and protection systems (2011)