Bridging the European and North American Rail Safety Assurance Gaps
Examples of Typical Cases of Cross Acceptance in Both Directions

Laurent BOILEAU
ALSTOM Signaling Inc. 1025 John Street, West Henrietta, NY 14586, USA

ABSTRACT
In the past few years evolution in the cross-acceptance process between rail equipment developed to North America and Europe standards provides lessons learned to help bridge the certification gap. Recently, efforts to align technical requirements (e.g. EMC-EMI) between FRA / AREMA and CENELEC have made significant progress.

Two examples illustrating successful cross acceptance processes can be used to address the key elements needed to achieve safety approvals.

The intent of this paper is to illustrate the steps taken to gain FRA safety certification under 49 CFR Part 236 Subpart H, of a track circuit product for train detection, developed in Italy according to CENELEC standards and conversely, a U.S. based interlocking system developed according to FRA regulation and AREMA recommended practices and its acceptance according to CENELEC standards for use in The Netherlands.

In illustrating the actions to achieve certification, the principal questions that were necessary to address are highlighted in three levels of potential difficulties:

- How do you present the safety report according to the applicable regulations, standards and best practices?

- How do you demonstrate and present the safety concepts and dependent factors of the vital product (safety architecture, Vital Software and Hardware development)?

- How do you address the technical gaps related to the environmental conditions (Temperature, Vibration, EMC-EMI, Electrical including Vital spacing...)?

Word Count = 6,503
INTRODUCTION

The aim of this paper is to present how the structure of the safety documentation for Vital Products for Railway Signaling, has been structured in order to address both European i.e. CENELEC, and, North American Standards and Regulations i.e. AREMA, IEEE and Federal Railroad Administration (FRA).

The proposed method is designed to cover existing vital products already accepted by the safety authorities (e.g. FRA, Transit Authorities…) of one area (either in Europe or in USA), in order to evaluate the gaps for cross acceptance in the other area and then build a safety documentation structure with a reasonable effort by re-using the existing safety evidences as much as possible.

This communication is a natural continuation of the previous communication "Bridging the European and U.S. Rail Safety Assurance Gap: The Feasibility of Cross Acceptance James B. Balliet, Battelle Memorial Institute, Rail Safety and Security, AREMA, 2011.

WHAT ARE THE RISKS?

First of all, it is important to clarify what the Risks are, before starting a cross acceptance process. In fact the risks are not so different by nature than the ones faced during an acceptance process in North America of a Vital Product designed according to the American Standards in the U.S., meaning:

- Risk 1 [R1]: The design of the Vital Product or its safety exported constraints to an Application Project does not comply with the mandatory requirements of the new standards. The acceptance is rejected and product design change is requested for example: modification of the product architecture, vital software modification and/or modification of Class I or Class II hardware.

- Risk 2 [R2]: The existing safety demonstration does not comply with the mandatory requirements of the new standards. The safety demonstration is not accepted as it is presented and additional evidences are requested. Additional effort could be related to new safety analyses, additional Verification and Validation (V&V) including new testing etc.

The consequences in term of delay impacting the signaling project using a Vital Product not accepted by the Safety Authority, in terms of cost degradation due to additional activity not scheduled or the negative impact on the company reputation are not evaluated in this paper. However, the implicit judgment behind the proposed method is that Risk [R1] is Unacceptable. That means after detailed evaluation, if a Vital Product candidate for cross acceptance, may require a fundamental design modification in order to get acceptance according to the new standards, then the cross acceptance strategy is not recommended and an alternative solution is requested.

Risk [R2] may be Acceptable, depending on the level of additional effort on the safety demonstration to be done. It is a case by case study according to a defined strategy.

The following two sections briefly describe the fundamental gaps between CENELEC standards applicable in Europe for Transportation and the Standards / Recommended Practices applicable in North America i.e., the U.S. The objective is not to present in detail each single Standard from CENELEC (reference from (15) to (24)) and the ones applicable in North America (reference from (1) to (14)), then analyze the different gaps, one by one; this job has been already done with a more or less completeness, refer for example to (26) and (27).

The objective of the following sections is to provide an overview of the safety approach in Europe and in the U.S. in order to identify the blocking points and the accepted points for cross acceptance in order to build a unique structure for safety documentation.
This comprehensive overview of the two safety approaches is coming from the analysis of the standards and from the author’s return of experience gained during the last fifteen years of Vital Product development and Projects Application in Europe, in China and now in the U.S.

**THE SAFETY ASSURANCE APPROACH IN EUROPE: CENELEC**

The CENELEC approach is vertically integrated in a top-down system approach (including the scope of responsibilities from the Operator to the Supplier), modular and hierarchically organized in Generic Product / Generic Application / Specific Project. The structure of the CENELEC standards is almost coherently structured and now supported by guidance of application.

The safety report is defined as Safety Case per CENELEC. The Safety Case format is defined and constrained in great detail by CENELEC including up to four levels of sub-sections, refer to (16).

The CENELEC approach also restricts in detail the organization to be implemented to support an acceptable development process for Vital Products, defining the mandatory independence between Design, Verification and Validation including the Safety Assurance organization, in order to mitigate the human error during the entire development cycle of the Vital Product / Subsystem / System. The Independent Safety Assessor, whom is a formally certified organization, is mandatory for each project application.

According to CENELEC, the way of working is almost as important as the technical safety target to be reached.

The potential drawback of this approach is the tremendous effort required in order to demonstrate process compliancy, could be at the expense of the technical safety assessment of the vital product itself.

The following figure presents the overview of the CENELEC standards from References (15) to (24).

**Figure 1. The set of CENELEC Standards**
The following figure presents the Safety Case format compliant to CENELEC EN50129 (16) supported by ISO 9000 (25).

Figure 2. The Safety Case Format according to CENELEC 50129 (16)

THE SAFETY ASSURANCE APPROACH IN NORTH AMERICA

In the early 1990's, the U.S. government began a move towards “consensus based Standards and Regulations” whereby all parties affected by the Standards and Regulations were involved in the process of their creation.

In 1995, the FRA created the Rail Safety Advisory Committee (RSAC) to assist in the creation of a number of regulations in many areas including those for Safety Critical Processors 49 CFR 236 Subpart H (1) and ultimately Positive Train Control 49 CFR 236 Subpart I (2) used in the railroad industry. The railroads and railroad labor desiring more flexibility pushed for “performance based rather than prescriptive based regulations”.

Under this approach, each railroad would develop various Safety Plans within certain guidelines (i.e. Railroad Safety Program Plans and Product Safety Plans under Subpart H, PTC Implementation Plans and PTC Safety Plans under Subpart I).

This approach allowed each railroad the flexibility to define what was necessary and tailored for their individual requirements. Once approved, the FRA would regulate each railroad to their individually approved plans.

The approach in North America from ALSTOM return of experience as Product Supplier in the United States, could be more complex than in Europe due to the different bodies involved in the definition of the way of working.

The set of documentation defining the safety approach to be respected, is a mix of Recommended Practices from AREMA, mandatory Federal Regulation from FRA or recommended Federal Regulation from FTA and Standards such as IEEE or MIL STD.

All of these different initiatives are at the same time independent and interconnected representing a certain level of difficulty for ease of understanding and correct application. The Request For
Proposal (RFP) from the Customer and then the contract should clarify the preferred standards and guidelines to be respected for safety demonstration.

The following figure presents the typical overview of the main standards applicable in the U.S. for signaling in transportation: Federal Regulations (1) and (2), AREMA Recommended Practices (4), IEEE Standards from (5) to (13) and MIL STD (14) all coming from the U.S. in fact.

<table>
<thead>
<tr>
<th>Customer Request for Proposal – Mandatory Requirement per Contract</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal Railroad Administration (FRA)</td>
</tr>
<tr>
<td>Title 49 Part 238 Subpart A to F, Subpart H (1) and I (2) with Appendix A to F (for PTC)</td>
</tr>
<tr>
<td>Federal Transit Administration (FTA) Guidance (3)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AREMA, 2013 (4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communications and Signals Manual of Recommended Practices</td>
</tr>
</tbody>
</table>

| Volume 1: RAILROAD SIGNAL... CROSSING... |
| Volume 2: RELAY... SIGNAL... TRACK CIRCUIT... |
| Volume 3: POWER SUPPLY... 11.5.1 Environmental Requirements for Electrical Electronic Railled Signal System Equipment... |
| Volume 4: ELECTRICAL... VITAL CIRCUIT AND SOFTWARE DESIGN... |
| SECTION 17 – QUALITY PRINCIPLES |
| Part 17.1.1 Recommended Safety Assurance Program |
| Part 17.1.3 Recommended Practice for Hardware Analysis for Vital Electronic/Software-Based Equipment Used in Safety-Critical (Vital) Applications: Class I (Vital), Class II (Class III (partly for Vital)) |
| Part 17.3.8 Recommended Procedure for Hazard Identification and Management |
| Part 17.4.1 Recommended Reliability and Maintainability Assurance Program |

| Volume 5: ELECTRICAL PROTECTION... /INDUCTIVE INTERFERENCE.../DATA TRANSMISSION... RADIO... COMMUNICATION-BASED SIGNALING... POSITIVE TRAIN CONTROL (PTC)... |

<table>
<thead>
<tr>
<th>IEEE 1483TM-2000 (5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard for Verification of Vital Functions in Processor-Based Systems Used in Rail Transit Control</td>
</tr>
<tr>
<td>A.1.2.1 Safety concept: Intrinsical fail-safe design</td>
</tr>
<tr>
<td>A.1.2.2 Safety concept: Checked Redundancy</td>
</tr>
<tr>
<td>A.1.2.3 Safety concept: N-Version Programming</td>
</tr>
<tr>
<td>A.1.2.4 Safety concept: Diversity and Self-Checking</td>
</tr>
<tr>
<td>A.1.2.5 Safety concept: Numerical Assurance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IEEE 1550TM-2004 (6)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard for Software Documentation for Rail Equipment and Systems</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IEEE 790TM-2002 (7)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard for Software Quality Assurance Plans</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IEEE 800TM-1998 (8), (9), (10)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommended Practice for Software Configuration, Test and Requirement Specification</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IEEE 1012TM-1998 (11)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard for Software Verification and Validation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IEEE 1020TM-1998 (12), (13)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard and Recommended Practice for Software Design and Project Management</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MIL STD 882C, 1993 (14)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task 103/104/107 Management of Contractors / Review / Audit / Safety Working Group / Safety Progress</td>
</tr>
<tr>
<td>Task 401/402: Safety Verification / Safety Compliance (Task 403/404: Explorative)</td>
</tr>
</tbody>
</table>

**Figure 3. Standards applicable in North America for Signaling in Transportation**

Note: the revisions D and E of the MIL STD 882 are not typically recognized for Signaling and are rarely referenced in the Request For Proposal (RFP) even if they are the most recent update in comparison with the dated revision C from 1993.

Regarding the development cycle for Vital Products for Signaling in the U.S., AREMA compliance is either mandatory or highly recommended. The format of the safety report (also called Safety Case per CENELEC, Proof of Safety or Product Safety Plan according to FRA) presenting the overview of the safety evidences is not constrained by AREMA. In fact, the Certification or the Homologation of the Generic Product does not exist independent of the Project Application in the North American approach.

Specific to projects, the safety evidences of the generic product are rarely mandatory standalone deliverables. The safety evidences of the generic product are subject to safety audit and safety assessment after non-disclosure agreement according to the contract. By consequence, the safety evidences from the Generic Product Safety Case are then presented through the Project Safety Report according to the contract requirements in the operational context in a case by case for AMTRAK, Freight Operators or Transit Operators.

The approach followed in the U.S. does not strictly constrain the Safety and Verification & Validation organization that the supplier has to respect in order to develop Vital Product. The development process is also less constrained in comparison with the one defined in CENELEC.

The Independent Safety Assessor (ISA) or Third Party assessment is not systematically requested in the U.S. in comparison with Europe. It is important to note that the consultancy company or individuals, candidates for safety assessment activity are not accredited according some standard rules in North America compared to Europe. That is, the experience, the background and
competences of the assessment team members i.e., their resume, is the recognition for the job capacity.

The following figure presents an example of the format of the Safety Report / Safety Case for Vital Product called « Product Safety Plan (PSP) » according to Federal Railroad Administration (FRA).

<table>
<thead>
<tr>
<th>§ 236.907 Product Safety Plan (PSP)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Section 1:</strong> Product Description</td>
</tr>
<tr>
<td><strong>Section 2:</strong> General Railroad Operation</td>
</tr>
<tr>
<td>train movement density, gross tonnage, hazardous materials volume, operating rules, speeds</td>
</tr>
<tr>
<td><strong>Section 3:</strong> Concept of Operation</td>
</tr>
<tr>
<td>(including a complete description of the product functionality and information flows)</td>
</tr>
<tr>
<td><strong>Section 4:</strong> safety requirements</td>
</tr>
<tr>
<td><strong>Section 5:</strong> safety Architecture</td>
</tr>
<tr>
<td><strong>Section 6:</strong> Hazard Log</td>
</tr>
<tr>
<td><strong>Section 7:</strong> Risk Assessment §236.909 and Part 236 Appendix B</td>
</tr>
<tr>
<td><strong>Section 8:</strong> Hazard Mitigation Analysis</td>
</tr>
<tr>
<td><strong>Section 9:</strong> Safety Assessment and Verification and Validation processes Part 236 Appendix C</td>
</tr>
<tr>
<td><strong>Section 10:</strong> Safety Assurance Concept</td>
</tr>
<tr>
<td><strong>Section 11:</strong> Human Factor Analysis Part 236 Appendix E</td>
</tr>
<tr>
<td><strong>Section 12:</strong> Safety Training to ensure the safe installation, implementation, operation...repair...</td>
</tr>
<tr>
<td><strong>Section 13:</strong> Safety Procedure to ensure the safe installation, implementation, operation...</td>
</tr>
<tr>
<td><strong>Section 14:</strong> Title 49 Part 236 Subpart A-G Compliance</td>
</tr>
<tr>
<td><strong>Section 15:</strong> Security measures for the product over its life-cycle</td>
</tr>
<tr>
<td><strong>Section 16:</strong> Warning in Operations and Maintenance Manual and Warning Labels on Product</td>
</tr>
<tr>
<td><strong>Section 17:</strong> Safety Validation Testing Procedures and Test Results</td>
</tr>
<tr>
<td><strong>Section 18:</strong> Post Implementation Testing and Monitoring</td>
</tr>
<tr>
<td><strong>Section 19:</strong> Safety-Critical Assumptions and Fallback Operations Safety Exported Constraints</td>
</tr>
<tr>
<td><strong>Section 20:</strong> Incremental &amp; Predefined Changes</td>
</tr>
</tbody>
</table>

**Figure 4.** Format the Product Safety Plan according to FRA

For Europe, it could be confusing that a Safety Report is called “Plan” usually meaning Program. In fact, this product “Safety Report” / “Safety Case” becomes a “Plan” from the end user’s viewpoint, to be used by System and Operation & Maintenance, e.g. the safety exported constraints from the Product to be respected by Project Application, the mandatory Training for the staff in charge of Installation, Testing, Operation and Maintenance of the Product etc.

**WHICH METHOD?**

After the overview between CENELEC and FRA / AREMA / IEEE / MIL STD, in order to evaluate the fundamental gaps between the two approaches from Europe and from the U.S., the first phase of the proposed method is the **Technical Gaps Analysis** broken down into three different levels, and, for each of them, the likelihood of Risk [R1] or [R2] is evaluated:

1) The format of the product safety report itself (Safety Case, Product Safety Plan etc.)

2) The safety concepts supporting the product safety architecture based on Vital Hardware Class I and Class II with Vital Software, the Safety Verification Reports of Dependent Factor, Validation Reports etc.

3) The environmental constraints (Temperature, Electrical, Mechanical, EMC-EMI, etc.).

At the end of the three step analysis, the method also highlights the strengths and weaknesses of the Product regarding its chance of success for cross acceptance.
In the second phase of the method and according to the results from the previous phase of the technical gaps analysis, a **Safety Documentation Structure** centered around the Safety Case itself, suitable for both Europe and the U.S., has been built, the simplest possible, reusing the existing safety evidences as much as possible each time it makes sense.

As a final phase of the method, the author applied and evaluated the proposed document structure for the safety documentation with two **Real Cases** presented at the end of the document:

- **Case #1**, Vital Track Circuit for Signaling « Made per CENELEC » accepted by Federal Railroad Administration (FRA) in the U.S., in 2012.
- **Case #2**, Vital Computer Based Interlocking « Made in the U.S.» accepted by Independent Safety Assessor in The Netherlands in 2013 as SIL 4 equivalent according to CENELEC.

This paper is not presenting the exhaustive list of all the technical gaps, gap by gap, for each of the three levels of analysis, as it would require another type of communication (e.g. Report or Book), rather this paper is presenting the main conclusions of the author regarding the Risk [R1] or [R2], illustrated by one or two typical examples supporting the argumentation.

**The Technical Gaps Analysis**

1. **The Format of the Safety Report / Safety Case**

The safety report / Safety Case is the key document and the most important but at the same time it is also the final document used to support the safety acceptance process. It is the key document supporting the review cycle involving Partner, Customer, Operator and then the Safety Authority, with the following three potential statuses:

- “Reviewed with correction” meaning “Rejected” leading to Risk [R1] or Risk [R2],
- “Reviewed with comments” meaning “Not Accepted as it is presented” leading to Risk [R2]
- “Reviewed without comment” equivalent to “Accepted”

The Safety Case or safety report also presents the overview of the complete safety assurance process followed for the safety demonstration including the test reports with final results, and at the end, it presents the Safety Related Application Conditions. By consequence the Safety Case is the final and the last document in the development cycle.

In order to avoid any difficulties regarding the format, the presentation and at the end, the acceptance itself, the Safety Case format shall be compliant to the national regulations and customer practices. Even if the format of the Safety Case according to CENELEC could be accepted in the U.S., in theory, it is still too early to present the CENELEC Safety Case in U.S without the supplementary effort of Presentation.

At this stage of the process, no blocking points have been identified that could require design modification on the product due to Safety Case format and presentation. In fact, all the different standards defining the Risk Assessment and Hazard Control (Hazard identification, Risk assessment, Safety Analysis, FMEA or FTA, Hazard Log etc.) are all inherited from the original MILITARY STANDARD (14) defined 30 years ago. There is no fundamental difference here between Europe and the United States.

In addition, qualitative safety requirements and some quantitative safety requirements are now very close between CENELEC and AREMA e.g. for both standards the requirement: “no single point failure”, is mandatory and for combination of failures, the “Tolerable Hazard Rate (THR)” from CENELEC (16) Annex A, and, “Probability of Failure per Operating Hour” from AREMA (4) section 17.3.5., are now very close.

The « Mean Time To Hazardous Events (MTTTE), or, « Mean Time Between Hazardous Events (MTBHE) » according to MILITARY STANDARD (14) expressed in Hours (or in Years depending on the contract), could be simply calculated by the inverse of the THR.
Since 2013, AREMA EMI/EMC has been updated to be very close to the CENELEC / IEC (17) requirements.

The Risk regarding the Safety Case Format is evaluated as Risk 2: “Risk of documentation”.

2. The demonstration of the safety concepts and safety architecture

After the review of the Safety Case format, it is necessary to enter into the detail of the safety architecture and its associated safety concepts.

This is the most important point of the cross acceptance process. It is from the safety architecture and its verified and validated safety concepts, that the main safety characteristics of the product are defined and guaranteed e.g. the safety threshold in Voltage / in Current, the safety reaction time etc.

The Risk [R2] and possibly [R1], could be realized if the safety concepts are not correctly presented, demonstrated in order to be understood by the reviewers and then accepted by the Operator and at the end by the Safety Authority.

The following table traces the « safety principles» according to CENELEC EN50129 (16) and the « safety concepts » according to IEEE 1483 (5) and AREMA (4):

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>B.3.1 3) Inherent fail-safety</td>
<td>A.1.2.1 Intrinsic fail</td>
<td>17.3.3 F Class I</td>
</tr>
<tr>
<td>B.3.1 2) Reactive fail-safety</td>
<td>A.1.2.5 Numerical Assurance</td>
<td>17.3.3 G Class II, 2c Numerical Assurance</td>
</tr>
<tr>
<td></td>
<td>A.1.2.4 Self-Checking part</td>
<td>17.3.3 G Class II, 2a Self-Checking</td>
</tr>
<tr>
<td>B.3.1 1) Composite fail-safety</td>
<td>A.1.2.2 Checked Redundancy</td>
<td>17.3.3 G Class II, 2b Checked Redundant Comparison</td>
</tr>
<tr>
<td></td>
<td>A.1.2.3 N-Version Programming</td>
<td>Not Referenced</td>
</tr>
<tr>
<td></td>
<td>A.1.2.4 Diversity part</td>
<td>17.3.3 G Class II, 2b Checked Redundant Comparison (partial)</td>
</tr>
</tbody>
</table>

Table 1 Example of traceability table for the Safety Concepts

Also here, there is no fundamental difference between CENELEC and Standards applicable in the U.S., but, there is an important divergence regarding the presentation.

CENELEC is presenting its safety principles in a pure functional and theoretical manner without the idea of the technical solution able to support the principles. IEEE 1483 (5) not only presents its safety concept from the pure functional definition, the IEEE standard presents every concept detailed with its suitable technical solution and the required method of Verification and Validation of its dependent factors. In that manner, IEEE is more guiding than CENELEC regarding the expected way to demonstrate the Technical Safety.

When there is only one technical solution suitable for the Safety Principle from CENELEC, then, the Safety Concept from IEEE is identical i.e. “Inherent fail-safety” and “Intrinsic fail” presented in the first line of the Table 1, are identical. AREMA is then detailing how to demonstrate the safety of Class I Hardware, defining the mandatory Failure Modes of electronic.

These activities of “analyze”, “comparison”, “traceability” and “presentation of synthesis” between CENELEC and American Standards and Regulations, are called Traceability, Translation and Presentation in this document.

Compliance with IEEE 1483 (5) is a highly recommended practice in North America and especially in the U.S. The Safety Concept document is requested by IEEE in the early phase of the development. In comparison, the Safety principles are usually presented in the Safety Case
according to CENELEC meaning in the latest phase of the development. A special effort regarding the Presentation, the Traceability and the Translation shall be done as soon as possible when the project has been launched, in both directions from CENELEC to IEEE, and vice versa.

IEEE 1483 (5) also requests breaking down the fault tree in two trees hierarchically organized: the first one purely functional, the Functional Fault Tree (FFT) from the top, and then, the second one detailing the vital hardware and vital software contributing to the safety demonstration according to the safety architecture, the Fault Tree Analysis (FTA).

The hardware and software solution implemented and modelled in the FTA, shall define the safety requirements based on the expected behavior of the Product in nominal and degraded modes, in case of internal and external failures.

Regarding the vital protocol of data communication, CENELEC EN 50159 (23) does not have (yet) an equivalent standard in the U.S. As a result, the author of this paper highly recommends respecting the EN 50159 requirements wherever the product is designed, in Europe or in the U.S. (refer to the case #2 presented at the end of this document).

The following step covers the Software and Hardware development of Vital Products with respect to the safety concepts implemented in the safety architecture.

2a. The Development of Vital Software

The main point regarding the development of Vital Software is the exhaustive Verification and Validation of the functional and safety requirements defined in the previous stage during the design of the safety concepts.

CENELEC EN50128 (24) for Software, constrains the organization to be put in place, the software languages to be used, the methods of Verification and Validation to be selected, and, to a lesser extent, also constrains the method of software design to be followed.

IEEE 1483 (5) provides a stronger link between the vital functions and the mandatory requirements to beVerified and Validated according to the Dependent Factors for each of the safety concepts. IEEE 1483 (5) applicable for Vital functionality is then completed by a series of IEEE standards grouped under IEEE 1558 (6) defining the recommended structure of documentation for the complete software development, not only for Vital software.

As the standards and regulation in the U.S. do not require a strict independence between the Design and the Safety Verification & Validation teams, the cross acceptance in Europe according to CENELEC may be very difficult if the supplier does not respect this best practice also recommended by AREMA (4) 17.3.1.

At the end, the safety level of the vital software developed with either set of standards i.e. CENELEC 50218 (24) or IEEE 1483 (5) completed by IEEE 1558 (6), is expected to be equivalent.

By the way, a significant effort of Translation and Traceability with additional information if necessary, should be expected and scheduled in order to support the cross acceptance process without having to question everything and restart from scratch.

This effort could be managed in order to directly present in the safety report or Safety Case, the summary of the results from low level safety evidences of software Verification & Validation and how these evidences meet both sets of standards. This activity would require a significant level of safety expertise in the area of Vital Software development.

2b. The Development of Vital Hardware

The hardware safety analyses are based on FMEAs at the component level for single point failures, supported by tests of failures and then completed by the combinations of failures modelled throughout the FTA for Class I and Class II Hardware according to AREMA (4) section 17.3.3. These activities are equivalent to the hardware safety analyses requested by CENELEC EN50129 (16) Annex C. There are no fundamental differences between Europe and the U.S. for hardware safety analyses.
However the mandatory Component Failure Modes are not exactly one to one identical between CENELEC and AREMA. It requires a component by component study in order to evaluate if it is Risk [R2], or, potentially Risk [R1]. Globally, it cannot be claimed that AREMA is more constraining in comparison with CENELEC, and vice versa. Once again, it is case by case depending on the component.

In conclusion for this second level of the technical gap analysis of the method, the Risk regarding the Safety Architecture with Safety Concepts based on Vital Software and Hardware development, should be a Risk R2: risk of documentation. However, beware of the Hardware Safety studies (including vital spacing differences, dielectric isolation differences, and intrinsically failsafe component assumptions) for Hardware Class I based on special components which may be not recognized by one of the two standards (either AREMA or CENELEC) leading to Risk [R1].

The equivalence between AREMA and CENELEC regarding the Component Failure Modes shall be demonstrated according to the need from the safety architecture. If the equivalence is not demonstrated when needed, then Risk [R1] is Possible.

3. The gap analysis of the environmental constraints

The gaps between environmental constraints defined by AREMA and by CENELEC represent the most important contributor for Risk [R1]. By consequence, it is highly recommended to start with the detailed analysis of the environmental constraints and requirements in order to identify the potential blocking points as soon as possible before going too far in the cross acceptance process.

The environmental constraints are broken-down as following:

- Temperature,
- Electrical (including dielectric),
- Mechanical shock and Vibration,
- Electromagnetic Compatibility (EMC-EMI),
- and, the constraints related to the Altitude and Pressure.

There is no particular difficulty to define the worst case for example for Temperature or Vibration, and then to test the product to meet requirements defined by CENELEC Reference (17) to (22) and by AREMA (4) sections 11 and 17. But it is not so easy to do the same analysis regarding Electrical constraints including vital spacing or regarding Electromagnetic compatibility. Expert judgments are then necessary.

In addition, the Operator may add more severe environmental conditions e.g. NYCT had taken AREMA environmental recommendations and modified them for their own use making them more stringent. In France SNCF the Railway Operator also requires more severe environmental conditions than the common CENELEC requirements.

It is a case by case study regarding the environmental conditions in the context of the use of the product.

Alstom defined working groups with European Experts in CENELEC and American Experts in AREMA in order to address the following technical gaps between the standards, especially for: Vital Spacing, component failure modes, combination of failure modes etc.

The Risk regarding the **Environmental Constraints** is evaluated as Risk 1: Risk of Design modification.

A detailed analysis would be required with the appropriate level of expertise. Additional Qualification Testing would also be expected on a case by case basis, (refer to the case # 1 presented at the end of the document). This is a task of Verification and Validation to be managed (be careful regarding the duration of additional tests which is usually not negligible) unless the Vital Product takes into account both CENELEC and AREMA. Using both standards for environmental test requirements has historically not been common until now for new products for Transportation.
The Safety Documentation Structure

At the end of the three levels of technical gap analysis presented in the previous sections, the decision was made to create no new safety document at the architecture level and re-using the existing safety evidences for Vital Hardware and Vital Software as it is.

Then the first action was concentrated on the Safety Case format compliant with CENELEC at the product level. The decision to go with the format recommended by CENELEC comes from the fact that it is the most structured and constrained format for a generic product and the most recognized worldwide. Then, the second action was to create a Product Safety Plan (PSP) in order to complete the safety documentation structure for FRA submittal in the U.S.

The activities of Presentation, Traceability, Translation supported by the supplemental information when necessary (mainly additional qualification tests reports), have been done directly in the safety case and in the PSP. In other words, all of the existing safety evidences have neither been challenged nor modified for the two cases presented at the end of this document illustrating the implementation of the method is valid.

However, it is important to note that in the two cases used to test the method, the two Vital Products have a strong background of field in-service unit-years in addition to the well-organized and up-to-date safety evidences (List of Hazards, FMEAs, Fault Trees, Safety Exported constraints etc.).

The Safety Case format compliant to CENELEC has been implemented also for new generic products designed in the U.S. for the North American market, even if it is not mandatory, as CENELEC is recognized beyond its original boundaries such as China and India, which is less true for American standards (AREMA could be required from ALSTOM’s return on experience in China and Taipei but it is not a Standard).

For European products having their Safety Case compliant to CENELEC, then it is a reasonable job of Presentation, Traceability, and Translation with a limited complement of information required to be done to create the Product Safety Plan (PSP) according to FRA.

Knowing that the information provided to the U.S. authorities are subject to publication in the public domain, available on Internet without limitation, the PSP created also allows filtering of information (redacting) which is sometimes too detailed in the CENELEC Safety Case. See illustration in the case #1.

For the U.S. products intended for the European market, a Safety Case format compliant to CENELEC must be created for eventual acceptance in Europe; this is a "must", there is no other choice today. See illustration in case # 2.

The global approach for unique safety documentation by Alstom is summarized as followed (see next Figure):

I. Establish the modular structure of the Safety Case in conformity with CENELEC compatible with IEEE and AREMA

II. Integrate the results of safety evidences (Hazard Analysis, FMEA, Fault Tree etc.) into the modular structure of the Safety Case:
   a. in natural way for products designed according to CENELEC,
   b. with an effort of Translation and Traceability for products compliant with American Standards.

III. Once completed, the generic product Safety Case CENELEC format is ready to support either the project Safety Case naturally for projects formatted for CENELEC, or, supporting the project safety report, for example: the Product Safety Plan according to FRA in the following figure. Finally, complete the PSP according to operational context where the Product is used.

Note: Product Safety Plan (PSP) may be easily replaced by any other format of safety report, for example: the one recommended by the Federal Transit Administration (FTA).
Figure 5. The structure of the safety documentation based on CENELEC Product Safety Case and Product Safety Plan (FRA)
CASE #1: VITAL PRODUCT FROM EUROPE ACCEPTED IN THE UNITED STATES

Case #1: Vital track circuit for signaling « Made in CENELEC » accepted by Federal Railroad Administration (FRA) in the U.S., in 2012.

Context: the existing Generic Product Safety Case of the vital track circuit designed and manufactured in Bologna, Italy, is fully CENELEC compliant.

Activity for cross acceptance: The main effort was focused on compliance with environmental constraints to American standards, leading to additional activities of Verification and Validation i.e. Product Validation and System integration testing of the product according to the project requirements for Port Authority Trans-Hudson (PATH) between New York and New Jersey under FRA regulations.

No major design change, some limited configuration adjustments and filtering have been done.

In parallel, the effort was focused on the completion of the Product Safety Plan (PSP) directly since the product already had its Generic Product Safety Case according to CENELEC, presenting the results of existing safety evidences according to CENELEC (activities of Traceability, Presentation and Translation) into the U.S. format.

Then the PSP was completed by integrating the results of Verification and Validation with respect to environmental constraints by AREMA & FRA, and, by adding information required by the FRA as the Chapter 20 of the PSP for future developments of the product (i.e. Section 20 : Incremental Changes).

No new safety study was necessary!

Result: Refer to (28) FRA Approval letter for Smartway Digital Track Circuit, 2012-0075.

CASE #2: VITAL PRODUCT FROM U.S. ACCEPTED IN EUROPE

Case #2: Vital Computer Based Interlocking "Designed and Manufactured in the U.S." approved by an Independent Safety Assessor in accordance with CENELEC, in The Netherlands, in 2013.

Context: the Vital Computer Based Interlocking VPI™ / iVPI™ designed and manufactured in the U.S. has proven safety evidences in compliance with American Standards but had no Safety Case format compliant to CENELEC.

However, the original VPI™ was evaluated by Independent Security Assessor in The Netherlands (Railcert in the 2000s) as SIL4 equivalent. The product VPI™ is in revenue service in The Netherlands and worldwide with excellent service record for over two decades.

Case # 2 is in fact limited to demonstration of the safety of the new product iVPI™ as a natural evolution replacing VPI™.

Activity for cross acceptance: The main effort was concentrated on the creation of a Safety Case format according to CENELEC. Indeed the development of new iVPI™ was not changing the proven safety architecture, re-using the safety concepts of the VPI™.

The first activity was therefore to populate the Safety Case format according to CENELEC, explaining the nature of the new iVPI™ developments in comparison with VPI™.

Then the major job was translating into the CENELEC language, the results of existing safety evidences according to American standards (activities of Presentation, Translation and Traceability). These activities were also supporting the safety reviews and safety audits conducted by the Independent Safety Assessor, Railcert.

For the new Vital communication protocol via Ethernet which does not exist for VPI™, the safety requirements of CENELEC 50159 (23) were followed and respected for the development of iVPI™.
With regard to environmental requirements, the feedback from nearly two decades specifically in the Netherlands environment, provides high confidence demonstrated by use in accordance with CENELEC 50129 (16) Table E9, in addition to the test reports of iVPI™ demonstrating compliance to AREMA Class C. This has been subject of limitations with respect to CENELEC standards (17) to (19) and (21). Information presented in the chapter dedicated to the exported constraints in the product Safety Case presents no major open points at project level, since the new iVPI™ does not degrade the performances of VPI™ currently in service and even improves on VPI™. 

For example, electromagnetic compatibility is managed at the project enclosure with particular attention to the cables and power supplies used in The Netherlands without compromising the design of the generic product iVPI™ Computer Based Interlocking. This is the same approach adopted previously for the VPI™ which was renewed for iVPI™.

This work was conducted in open, pragmatic and close collaboration, among all partners including the Customer and Operator, ProRail, and the Independent Safety Assessor, Railcert.

No new safety study was required at the product level!

Results: Reference to (29) Statement letter for iVPI by Railcert, RC100703-PvdV-131004-01, 10 October 2013.

AN ALSTOM ORGANIZATION TO SERVE THE METHOD

This method has been greatly facilitated and made possible thanks to the international organization and the Safety Assurance process implemented by Alstom Transport through a global network of safety experts and internal safety assessor for more than fifteen years.

CONCLUSION

The effort that has been made in order to obtain the cross-acceptance of a Vital track circuit "Made in CENELEC" by the Federal Railroad Administration (FRA) in the United States, in 2012 (case # 1), then a Vital Computer Based Interlocking "made in the U.S. "approved by a European Independent Safety Assessor in accordance with CENELEC, in The Netherlands, in 2013 (case # 2), was quite reasonable thanks to the method presented in this paper.

Like any method supported by a limited number of applications, it does not represent a benchmark but it opens up the possibility of making cross-acceptance between Europe and North America quite simple in some conditions. Indeed, in both cases illustrating the method applied, a very limited number of new documents and no new safety analyzes was produced at product level in order to obtain acceptance by the safety authorities.

Finally, it is obvious that this method implies collaborative and open-minded approach to safety demonstration such that the intent of the safety demonstration is not lost.

The cross-acceptance process is best served if the safety community is open to embracing new and novel ways of working with our mutual global standards.

If these two conditions were not met the author simply recommends not engaging in cross-acceptance process between Europe and the United States.

ACKNOWLEDGEMENTS

The author thanks all those who participated in any way in the drafting of this paper, they will recognize…
REFERENCES

(1) Federal Railroad Administration, Title 49 Transportation CFR Part 236 - RULES, STANDARDS, AND INSTRUCTIONS GOVERNING THE INSTALLATION, INSPECTION, MAINTENANCE, AND REPAIR OF SIGNAL AND TRAIN CONTROL SYSTEMS, DEVICES, AND APPLIANCES - Subpart H - Standards for Processor-Based Signal and Train Control Systems, 2010

(2) Federal Railroad Administration, Title 49 Transportation CFR Part 236 - RULES, STANDARDS, AND INSTRUCTIONS GOVERNING THE INSTALLATION, INSPECTION, MAINTENANCE, AND REPAIR OF SIGNAL AND TRAIN CONTROL SYSTEMS, DEVICES, AND APPLIANCES - Subpart I - Positive Train Control Systems, 2010

(3) Federal Transit Administration, 49 CFR Part 659 - Rail Fixed Guideway Systems; State Safety Oversight, 2005

(4) AREMA, Communications and Signals Manual of Recommended Practices, 2013


(12) IEEE 1016™ -1998, IEEE Recommended Practice for Software Design Description


(15) EN 50126, Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS), 1999

(16) EN 50129, Railway applications - Communications, signalling and processing systems - Safety related electronic systems for signalling, 2003

(17) EN 50121 Series, Railway applications – Electromagnetic compatibility, 2006
(18) EN 50124-1, Railway applications – Insulation coordination – Part 1: Basic requirements - Clearances and creepage distances for all electrical and electronic equipment, 2001


(20) EN 50125-1, Railway applications – Environmental conditions for equipment – Part 1: Equipment on board rolling stock, 1999


(22) EN 50155, Railway applications – Electronic equipment used on rolling stock, 2007

(23) EN 50159, Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems, 2010

(24) EN 50128, Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems, 2011


(28) FRA Approval letter for Smartway Digital Track Circuit, 2012-0075

(29) Statement letter for iVPI by Railcert, RC100703-PvdV-131004-01, 10 October 2013
Bridging the European and North American Rail Safety Assurance Gaps

Examples ofTypical Cases of Cross Acceptance in Both Directions

Laurent Boileau
Safety Assurance Manager
Alstom Transport, Rochester NY
Table of Content
Definition of the Risk of Cross Acceptance
Overview of the European Approach
Overview of the North American Approach
Analysis of Technical Gaps
The Structure of Documentation
Two Cases illustrating the method

Definition of the Risk of Cross Acceptance

Risk 1 [R1] “Risk of redesign”
The design of the Vital Product or its safety exported constraints
to an Application Project does not comply with the mandatory
requirements of the new standards. The acceptance is rejected
and product design change is requested.

Risk 2 [R2] “Risk of documentation / additional evidences”
The existing safety demonstration does not comply with
the mandatory requirements of the new standards. The safety
demonstration is not accepted as it is presented and additional
evidences are requested.

Overview of the European Approach

The CENELEC approach is vertically integrated in a top-down system
approach: Generic Product / Generic Application / Specific Project

The CENELEC approach restricts in detail the organization, the
development process, up to the content of the Product / Project Safety
Case

According to CENELEC, the way of working is almost as important as the
technical safety target to be reached

The Independent Safety Assessor (ISA), whom is from formally certified
organization, is mandatory for each project application

Overview of the European Approach: The Safety Case

Overview of the North American Approach

Recommended Practices (AREMA)
Regulations mandatory (FRA) / recommended (FTA)
Standards such as IEEE or MIL STD

The railroads and railroad labor desiring more flexibility
organization, development process, etc.) pushed for
performance based rather than prescriptive based regulations”

The Independent Safety Assessor or Third Party assessment is not
systematically requested in the U.S. in comparison with Europe
Analysis of Technical Gaps

1. The Format of the Safety Report / Safety Case

2. The Demonstration of the Safety Concepts and Safety Architecture
   2a. The Development of Vital Software
   2b. The Development of Vital Hardware

3. The Gap Analysis of the Environmental Constraints

2. The Safety Concepts and Safety Architecture

The most important point of the cross acceptance process! No Fundamental Technical Divergences e.g. “Safety Principles”<>“Safety Concept”

<table>
<thead>
<tr>
<th>CENELEC EN50126 (16) Safety Principle</th>
<th>IEEE 1483 (1) Safety Concept</th>
<th>AREMA (1) Class I and II</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1 1) Inherent Fail-Safety</td>
<td>3.1.1) Safety Function</td>
<td>3.1.1) Safety Function</td>
</tr>
<tr>
<td>3.1 2) Reactive Fail-Safety</td>
<td>3.1.2) Hazard Analysis</td>
<td>3.1.2) Hazard Analysis</td>
</tr>
<tr>
<td>3.1 3) Composite Fail-Safety</td>
<td>3.1.3) Composite Hazard</td>
<td>3.1.3) Composite Hazard</td>
</tr>
</tbody>
</table>

Effort of Translation / Traceability / Presentation


2a. The Development of Vital Software (Sw)

The safety level of the vital software from CENELEC 50128 or form IEEE 1483 completed by IEEE 1558, is expected to be equivalent

- Effort of Translation and Traceability with additional information if necessary, without having to question everything and restart from scratch
- Directly present the summary of the results in the Safety Report or Safety Case
- This activity would require a significant level of safety expertise in the Vital Software development

Vital Software is Risk [R2] “Risk of documentation” / possibly [R1] “Redesign”
2b. The Development of Vital Hardware (Hw)

No Fundamental Technical Divergences

- Hw safety analyses are based on FMEAs at the component level for single point failures, combinations of failures and FTA for Class I and II. Therefore...
- Mandatory Component Failure Modes are not exactly one to one identical between CENELEC and AREMA => Expert judgments
- Vital Spacing, dielectric isolation => Expert judgments

Vital Hardware is Risk [R2] "Risk of documentation" / possibly [R1] "Redesign".

3. The Environmental Constraints (Temperature, Electrical, Vibration, EMC/EMI...)

The most critical point of the cross acceptance process! It cannot be claimed that AREMA is more constraining in comparison with CENELEC, and vice versa. Case by Case!

- Temperature: Not a Big Challenge!
- Vibration, Electrical constraints including Vital Spacing or Electromagnetic Compatibility (EMC/EMI) => Expert judgments
  - More Severe Environmental Conditions
    e.g. NYCT: Requirements more stringent than AREMA, in France SNCF: requirements more stringent than CENELEC

Environmental Constraints is Risk [R1] "Redesign" / Additional Test is a Cost
**Case #1 VITAL TRACK CIRCUIT FROM EUROPE ACCEPTED IN USA**

- The main effort for “environmental constraints”
  => additional activities of Product Verification and Validation (V&V) / AREMA
- No major design change, some limited configuration adjustments and filtering have been done
- Create the Product Safety Plan (PSP) reusing data from Generic Product Safety Case according to CENELEC
- Complete the new PSP by integrating the results of V&V
- No new safety study at Product level was necessary!
- FRA Approval letter for Smartway Digital Track Circuit, 2012-0075

**Case #2 VITAL CBinterlocking FROM U.S. ACCEPTED IN EUROPE**

- Create the iVPI™ Generic Product Safety Case according to CENELEC reusing data from Hw / Sw evidences compliant to AREMA / IEEE
- Safety Related Application Conditions for “environmental constraints” e.g. EMC/EMI managed at Application Project level
- No design change
- No new safety study at Product level was necessary!
- Statement letter for iVPI as SIL4 by Railcert ISA, RC100703-PvdV-131004-01, 10 October 2013, in Revenue Service since 29 June 2014

**Conclusion**

ALSTOM Organization is adapted to serve the Method and Cases

Not a benchmark but it opens up the possibility of making cross-acceptance between Europe and North America quite simple in some conditions

No Product Design Change, No new safety study at Product level was necessary!

This method implies collaborative and open-minded approach to safety demonstration such that the intent of the safety demonstration is not lost

**Bridging the European and North American Rail Safety Assurance Gaps**

Thank You!

Laurent Boileau
Safety Assurance Manager
Alstom Transport, Rochester NY

© AREMA 2014