Cross domain comparison of System Assurance

Joseph Machrouh [1], Jean-Paul Blanquart[2], Philippe Baufreton[3], Jean-Louis Boulanger[4], Hervé Delseny[5], Jean Gassino[6], Gérard Ladier[7], Emmanuel Ledinot[8], Michel Leeman[9], Jean-Marc Astruc[10], Philippe Quéré[11], Bertrand Ricque[3], Gilles Deleuze[12]

(1): Thales R&T; (2): Astrium Satellites; (3): Sagem Défense Sécurité; (4): CERTIFER; (5): Airbus; (6): IRSN; (7): Aerospace Valley; (8): Dassault Aviation; (9): Valeo; (10): Continental; (11): Renault , (12) : EDF R&D

Topics: ☑ Dependability, fault tolerance, safety, certification
☑ Standards and norms

Keywords: Safety standards, DAL, SIL, cross-domain comparison

Contact Author Details: Joseph Machrouh (joseph.machrouh@thalesgroup.com)
Thales R&T, Campus Polytechnique, 1 avenue Augustin Fresnel, 91767 Palaiseau Cedex, France.
Tel: +33 1 69 41 57 21; fax: +33 1 69 41 60 01

Abstract:

This paper presents an analysis of the impact of the Development Assurance Level (DAL) or Safety Integrity Level (SIL) on the system activities in various application domains represented in the CG2E "Club des Grandes Entreprises en Embarqué") and specially on the dependability, safety norms and standards working group. The main goals of this paper are to:

- Analyse the impact in each application domain,
- Identify and discuss the similarities and the dissimilarities in order to find the cross domain synergies

The covered application domains and norms are:

Civil aviation (ARP 4754, ARP 4761),

Automotive (ISO 26262),

Space (ECSS-Q-ST-30C, ECSS-Q-ST-40C),

Nuclear plants (IEC 60880, IEC 61513),

Railway (CENELEC 50126, 50129),

Automation, industrial control (IEC 61508, 61511, 62061).

Keywords: Safety, criticality categories, DAL, SIL, ASIL, SSIL, standards

1. Introduction, Objectives

CG2E ("Club des Grandes Entreprises de l'Embarqué") is an initiative launched (mid 2007) by major industrial companies involved in the development of critical embedded systems in a very wide spectrum of application domains. Its objectives are to improve its members' capabilities to meet the major challenges of the development of embedded systems, in particular software intensive safety critical embedded systems. It elaborates propositions, recommendations, roadmaps etc. based on collaborative work and discussions in dedicated thematic Working Groups.

This paper presents an overview of the activities of one of these working groups dedicated to safety. This working group discuss on the impact of safety activities on critical systems. For such systems, the conception is highly constrained by standards. These standards provide general guidance in evaluating the safety aspects of a design. For this purpose, it recommends guidelines and methods to be used to achieve different level of safety. These levels of safety define the rigour to be applied in the conception on the critical systems. In the avionics domain, this safety level named Development Assurance Levels varies from A to E where A is the highest. In the Railway domain this level named Software Safety Integrity Levels (SSIL) varies from 1 to 4 where 4 is the highest. High levels mean high impact of a failure on safety. This classification has a direct impact on architectures, with physical segregation between the subsystems contributing to each *level*. However, for efficiency or to increase capabilities, a number of defence and aerospace applications tend to require more and more communication between subsystems (hence, between pieces of software) attached to different levels of safety.

Whatever standards and regulations, high level expectations on safety have a direct impact on product cost. 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.

We will describe the standards used in the various application domains represented in the CG2E: avionics, space, railway, automotive and nuclear. This paper focus on the activities performed in the system level while [Blanquart et al., 2012] focus on the comparative analysis across several industrial domains, of the fundamental notion of safety categories or levels and [Ledinot et al., 2012] focuses on the analysis of impact of safety level at the software level.

This paper is organized as follows: Following the introduction, each section describes the standards used for a particular application domain. The last section provides a synthesis of the overall study.

2. Avionics

The ED79A/ARP4754A addresses the total life cycle for Systems that implement aircraft level functions. It excludes specific coverage of detailed Systems, software and hardware design processes beyond those of significance in establishing the safety of the implemented system. More detailed coverage of the software aspects of design are dealt with in EUROCAE/RTCA document ED-12B/DO-178B. Coverage of complex hardware aspects of design are dealt with in ED80/DO254. Methodologies for safety assessment processes are outlined in SAE document ARP4761.

In ED79A/ARP4754A, the process includes validating requirements, and verifying that requirements are met, together with the necessary configuration management and process assurance activities. As development assurance level assignments are dependent on classification of Failure Conditions, the safety analysis process is used in conjunction with the development assurance process to identify Failure Conditions and severity classifications which are used to derive the level of rigor required for development.

The level of validation and verification rigor is determined by the function development assurance level(s) for the aircraft or system (FDAL) and item development assurance level(s) for the item (IDAL).

The application of independence is also dependent upon the development assurance level and is commensurate with the development assurance level.

Two tables identify the validation and verification methods and data as a function of the allocated development assurance level A-E. According to the Assurance Level, methods and data could be either Recommended for certification, As negotiated for certification, or simply Not required for certification for level E.

The ARP 4761 describes guidelines and methods of performing the safety assessment for certification of civil aircraft. It is primarily associated with showing compliance with FAR/JAR 25.1309. The methods outlined in the document identify a systematic means, but not the only means, to show compliance. The document introduces the concept of Aircraft Level Safety Assessment and the tools to accomplish this task are outlined. The overall aircraft operating environment is considered.

ED135/ARP4761 presents guidelines for conducting an industry accepted safety assessment consisting of Functional Hazard Assessment (FHA), Preliminary System Safety Assessment (PSSA), and System Safety Assessment (SSA). It also presents information on the safety analysis methods needed to conduct the safety assessment.

These methods include qualitative analyses for failure conditions such as the Fault Tree Analysis (FTA), Dependence Diagram (DD), Failure Modes and Effects Summary (FMES) and quantitative analyses such as the Fault Tree Analysis (FTA), Dependence Diagram (DD), Markov Analysis (MA), Failure Modes and Effects Summary (FMES) etc

Common Cause Analysis (CCA) addresses common cause faults and generic errors. [CCA is composed of Zonal Safety Analysis (ZSA), Particular Risks Analysis (PRA), and Common Mode Analysis (CMA)]. It is required for DAL A and DAL B systems.

The guidelines and methods provided in ED135/ARP4761 are intended to be used in conjunction with other applicable guidance materials, including ARP4754, ED12B/DO178B, ED80/DO254, and with the advisory material associated with CFR/JAR Parts 25.1309 and 23.1309.

A process is needed, which establishes levels of confidence that development errors that can cause or contribute to identify Failure Conditions have been minimized with an appropriate level of rigor. This henceforth is referred to as the Development Assurance process.

The determination of the classification of the Failure Condition Effects is accomplished by analyzing accident/incident data, reviewing regulatory guidance material, using previous design experience, and consulting with flight crews, if applicable. The depth of analysis undertaken depends on the Development Assurance Level (DAL) associated with a particular system. The DAL is allocated depending on the potential criticality and risk associated with a system failure. The classifications are: Catastrophic (DAL A), Severe-Major/Hazardous (DAL B), Major (DAL C), Minor (DAL D) and No safety effect (DAL E).

Safety Assessment Overview

The safety assessment process includes requirements generation and verification which supports the aircraft development activities. This process provides a methodology to evaluate aircraft functions and the design of systems performing these functions to determine that the associated hazards have been properly addressed. The safety assessment process is qualitative for Major Failure Conditions and qualitative and quantitative for Catastrophic and Severe-Major/Hazardous Failure Conditions.

Qualitative and quantitative analysis are required for system FHA catastrophic and hazardous failure conditions. Major failure conditions may be satisfactorily analysed with methods that are less rigorous and complete that those of catastrophic or hazardous (e.g. FMEA containing failure rates)

In terms of methodology, the safety assessment process begins with the concept design and derives the safety requirements for it. The safety assessment process ends with the verification that the design meets the safety requirements.

A Functional Hazard Assessment (FHA) is conducted at the beginning of the aircraft/system development cycle. It identifies and classifies the failure condition(s) associated with the aircraft functions and combinations of aircraft functions. These failure condition classifications establish the safety objectives.

Functional Hazard Assessment (FHA):

A Functional Hazard Assessment is defined as a systematic, comprehensive examination of functions to identify and classify failure conditions of those functions according to their severity.

An FHA is usually performed at two levels. These two analyses are known as an aircraft level FHA and a system level FHA.

The aircraft level FHA is a high level, qualitative assessment of the basic functions of the aircraft as defined at the beginning of aircraft development. An aircraft level FHA should identify and classify the failure conditions associated with the aircraft level functions. However, if separate systems use similar architectures or identical complex components and introduce additional aircraft level failure conditions involving multiple functions, then the FHA should be modified to identify and classify these new failure conditions. The classification of these failure conditions establishes the safety requirements that an aircraft must meet.

3. Railway

For railway domain, the reference standards in Europe are the CENELEC reference system: (in particular EN50126 and EN50129 at system level, and the IEC 61508. The latter (a generic standard applicable after appropriate instantiation to any type of electrical/electronic/programmable electronic safety-related system) is furthermore a founding standard from which many aspects of the CENELEC series are derived as railway applications of IEC 61508 prescriptions.

As a particularly important example, systems known as safety critical are systems which can in case of failure cause important damage to people and by extension to the private or public property or the environment. For this class of systems, it is necessary to perform analyses in order to demonstrate the absence of failures scenarios, whatever are the causes of elementary faults involved in these scenarios (physical, environment, development, interaction…), which could lead to this kind of consequences.

All systems sharing not the same criticality level, there are scales which make it possible to define levels which are associated to safety targets. In the field of the complex electronic and/or programmed systems, IEC standard 61508 defines the concept of SIL (Safety Integrity Level).

The SIL makes it possible to quantify the safety level of a system and consequently to evaluate criticality. It can take the following values 1 (system which can cause light wounds), 2 (system which can cause serious wounds), 3 (system which can cause the death of a person: individual accident) and 4 (system which can cause the death of a whole of people: collective accident). A system without system without impact on the safety of people is called Not-SIL,

The CENELEC standards indicate that the depth of analysis undertaken depends on the SIL associated with a particular system/sub-system/equipment.

The CENELEC EN 50126 is dedicated to the railway system analysis; The CENELEC EN 50129 is dedicated to the safety demonstration of equipment and more oriented on the hardware part.

The CENELEC EN 50129 defines the content of the SAFETY-CASE.

The CENELEC standard defines four mandatory documents:

Safety Assurance Plan (SAP): this plan defines the methodology for obtain the safety taking into account the THR and the SIL;

Preliminary Hazard Analysis (PHA): A preliminary Hazard analysis is defined as a systematic, comprehensive examination of undesirable event to identify and classify the risk;

Hazard-Log (HL): This document contains all the undesirable event, risk and anomalies.

Safety-Case (SC): a documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment.

The CENELEC standard introduced some table that give a link between the activities (and their depth) and the SIL.

The CENELEC standards, which are discussed in this paper, do not concern the technology, but provide good methods to avoid systematic or random faults in railway applications.

Concerning the safety aspect, the normative reference frame proposes a scale making it possible to quantify the criticality level of a system, making then it possible to define the development and demonstration effort needed. The control of the safety of a critical system thus passes by the definition of processes mainly based on test activities.

4. Space

The ECSS safety (Q-ST-40C) and dependability (Q-ST-30C) standards introduce a 4-level scale for categorizing systems, functions and hardware and software components implementing them, based on a ranking of severity of consequences of their potential failures.

At system level, the allocated criticality category impact is twofold:

Generic product safety requirements with direct impact on the design;

Process safety requirements with direct impact on the activities to perform

System level product safety requirements

The ECSS standards do not set requirements in terms of maximum probability of occurrence for the events in the various categories. However they impose a minimum number of independent faults for any combination that could lead to a failure in the most two severe categories: no combination of two independent faults (resp. no single (or common mode) fault) can induce catastrophic (resp. critical) consequences. This has a direct impact on the level of redundancy and diversification to implement in the architecture of the system.

System level process safety requirements

The ECSS standards state rules applicable to the safety and the dependability programs, roles and responsibilities, safety and dependability engineering, analysis and verification, and their articulation in the system life cycle along the various phases of a space program from phase 0 (mission analysis) to phase E (disposal).

They also require that the way and rigor to implement these rules must be adapted to the category, but without provided guidance on these adaptations, left to be negotiated and agreed for each project.

Indeed, the safety standard (ECSS-Q-QST-40C) states also specific rules applicable to “safety critical systems”, corresponding to the most two demanding categories. However, these two categories are the only ones corresponding to significant safety effects of potential failures, whereas the other two categories are indeed a subdivision, from mission perspective and dependability, of a single safety category corresponding to “minor or no safety effect”.

5. Automotive

The ISO26262 standard introduces a 4-level ASIL scale for categorizing systems, hardware and software components based on a ranking of criticality of the consequences of their potential failure.

System level process safety requirements

Most of the requirements of Part 4 of the ISO26262 standard (system development), with the addition of requirements of part 8 (supporting processes) and part 2 (management) define a system development process. As for the other parts of this standard, many requirements of part 4 are ASIL dependent or at least the recommended methods to comply with the requirement are ASIL dependent. The higher the ASIL, the most demanding are the requirements. The ASIL to be taken as a reference is the highest allocated ASIL.

The methods to be used for requirements capture depends on the ASIL. For ASIL A (lowest assurance level), the use of natural language is sufficient. For ASIL D (highest assurance level), semi formal language such as SYSML is also required as a complement to natural language. Validation of system requirements is not ASIL dependent.

The amount and depth of safety analyses are ASIL dependent. For the lowest ASIL, only a qualitative FMEA is required. For higher ASIL FTA and quantification are required in addition. Quantification, dealing only with random hardware failures, is not only about quantified FTA but also about calculation of architectural metrics that necessitates quantified FMEA. Common Cause Analysis is required when there are independence requirements to fulfill on the system, whatever the ASIL.

Concerning verification of the implementation for ASIL A, it is only required to cover each requirement with at least one test case. For ASIL D, additional test cases based on analysis of the interfaces, environmental conditions, field experience… are also mandatory. For the lowest ASIL, neither fault injection nor vehicle tests are required.

Configuration management is ASIL independent

Requirements on the management of the safety activities such as planning and the existence of a safety manager are ASIL independent.

The safety assessment is constituted by reviews on the key safety documents (such as Hazard & Risk Analysis, safety analyses…) and an audit of the safety process performed by independent safety assessors. The number of reviews and the level of independence of the safety assessors is function of the ASIL. It is to be mentioned that this is the only independence requirement concerning people involved in the process. There is no requirement for independence between the development team and the verification and validation team.

System level product safety requirements

Some requirements of part 4 of the ISO26262 have a direct impact on the system definition itself. These are the quantitative requirements and concern random hardware failures. They are key requirements to define the level of redundancies such as multi channelling. They are of course ASIL dependent. For an ASIL A system there are no quantitative requirements.

6. Nuclear

In nuclear domain the term “safety” is used for prevention of accidents, when other domains use instead the term “security”. This latest term is in the nuclear domain, used for malevolent actions that are not in the scope of this paper. Note also, that for the domain, we have to make a distinction between the “nuclear facility” as a system and the “I&C systems”, that can be based on “conventional” technologies (relays, hardwired logic) or programmed technologies (computer based).

Allocation to components

An initial safety analysis of the reactor has to be completed before to classify the functions supported by I&C systems. It is summarized in [Blanquart et al., 2012-a]. The IEC 61226 standard explains how to classify the functions of a nuclear facility according to categories (A,B,C and Non Classified). A functional analysis, based on the severity of the potential consequences, taking into account the frequencies of Initiating Events, permits the classification of mitigation and supporting functions. The main inputs of the classification scheme are the nature of the NPP and the reactor type (for example : pressurized water reactor, boiling water reactor…), the associated Initiating Events, the operational states and accident conditions and the defined radiological limits, the design basis events, the major mitigation functions of Initiating events. The classification is independent of the technological nature of the systems supporting the functions (they can be for example programmed I&C, conventional I&C, electrical, mechanical, hydraulic systems …).

As it is impractical to design a large set of functions and systems in a continuum of functional assurance, and quality requirements, classes of I&C systems are defined, whom assurance level is determined by the category (importance for safety) of function they support.

In all countries, the reference standard is the IEC 61513 standard. The IEC 61513 provides equivalencies between a safety function category (A, B, C) and the class of a programmed I&C system (1, 2, 3). A programmed system has to comply to design, manufacturing and qualification relevant for its class. The equivalencies between class and category are the following:

Function Category	Programmed I&C system class
A	1
B	1 or 2
C	1 or 2 or 3
Non Classified	1 or 2 or 3 or NC

In France the time required for the protection function actuation and the reactor states determine the categorisation for I&C. The NS-G-1.3 safety guide introduces temporal factors relevant to the case of programmed I&C systems like for example:

- the operating time required to the I&C system once started;

- the duration while alternative actions can be achieved

- the duration of detection and correction of hidden failures.

Design provisions at system level

Before any design provision is taken at equipment level, there are minimum requirements related to the architecture of the system. In term of basic functionality, there are four family of programmed I&C systems. They are usually structurally distinct and contribute to the global architecture of a nuclear facility (see the table B.1. from appendix B (informative) of IEC 61513). Major deterministic systems design principles (redundancy, diversity, separation) result from this classification.

	Class 1	Class 2	Class 3	Not Classified
Plant Automation and Control Systems		X	X	X
HMI Systems		X	X	X
Protection systems and safety actuation systems	X			
Emergency Power actuation systems	X			

Additional independence requirements may be imposed to ensure:

- that no function of a lower category can impair a function of higher category,
- that no failure of I&C equipment can impair successive lines of defence,
- that there is no common cause source of multiple failures that can impair a function added

specifically to address these multiple failures.

System Assurance at equipment level

For programmed I&C equipments, two standards present the requirements associated with the various classes. The IEC 60880 standard considers programmed I&C systems supporting functions of category A (with a Pfd target better than 10-3, and possibly better than 10-4). The IEC 62138 standard considers programmed I&C systems supporting functions of category B or C (with a Pfd target better than 10-2). The content of these standards correspond approximately to the Part 3 of IEC 61508.

The assumption is that quality assurance influences reliability, just as required reliability clearly influences the quality assurance procedures applied in the design, operation, and maintenance of the function.

The CEI 62138 standard describes requirements on comparable issues, with the significant differences that common cause software failures are not considered and that the requirements are less important and less accurately described (near 55 pages). Categories of requirement are: general requirements for software development project, requirements for software (specification, self testing, periodic testing, documentation), principles, languages and tools for design and implementation, qualification of pre-developed software …Again, the document describes principles to be applied but does not specify accurately methods, tools…

In addition to international standards, there are various national declinations, as in France, the RCC-E that provides complementary requirements [RCC]. These requirement are in complement to independence requirements at system architecture level (already seen above) with the constraint that undue complexity should not be introduced in systems of class 1 or 2.

Main features for nuclear domain.

We can summarize the system assurance features for I&C including software as follows:

- A safety assessment at nuclear facility level. The « system » level correspond to the level of a whole nuclear facility, function classification influences mostly the design and architecture of programmed I&C systems, through deterministic principles (redundancy, diversity, separation). There is no other particular impact on the « system engineering » activity.
- A functional analysis, based on severity of the potential consequences, taking account of the frequency of Initiating Events, is used to classify the functions relevant for safety on four categories (A,B,C and Non Classified).
- Use of the IEC 61513 standard to have an equivalency between the safety category of a function (A, B,C) and a quality calls of an I&C programmed system (1,2,3)
- No international agreement about probabilistic approach for I&C in the nuclear domain. Acommon approach is to consider programmed I&C systems supporting functions of category A with a Pfd target better than 10-3, and possibly better than 10-4; and programmed I&C systems with a Pfd target better than 10-2.
- The nuclear domain does not use so explicitly than other domains the concept of « Safety Level » with quantitative reliability goals. In particular, the terms SIL and ASIL are not used. Thus, although 61513 is a domain declination of IEC 61508, equivalencies of classes between these standards is uneasy.
- Use of the IEC 60880 and IEC 62138 standards to handle respectively I&C systems supporting functions of category A or I&C systems supporting functions of category B ou C.
- The guidelines require "principle compliance", the choice of relevant methods and tools is quite open. It reflects variations between national practices.
- In addition to international standards, there are various national declinations.

7. Automation

By automation, we understand the industries that are not already described in the previous chapters of this paper. This includes the continuous process industries such as nuclear facilities (beside energy production), non nuclear energy, metals, cement, oil and gas and chemicals, the manufacturing industries with the exception of automotive and the batch production industries such as pharmaceuticals and food and beverage. These industries are relevant of IEC61511 for the continuous and batch processes and of IEC62061 for manufacturing industries. Both standards are derivates of IEC61508 and, as they are not self supporting, refer to IEC61508.

These three standards address only the electric, electronic, programmable electronic systems under the concept of functional safety, that is systems distinct from the controlled equipment (plants, machines, and processing lines) contributing to risk reduction. The standards are performance oriented. This means that, as for the other industries, the functions contributing to risk reduction are classified in 4 levels (SIL) according to the impact of a failure on safety. The requirements are thus increasingly stringent with the SIL number.

The central concept of these standards is to achieve the targeted safety integrity and performance by putting requirements in 5 different fields. The standards assume that there are two types of failures. The failures that are introduced before the commissioning of the systems that are only systematic failures and the failures occurring after system commissioning and that can be either systematic or random. The standard thus addresses:

- incorrect specifications of the system, hardware or software;
- omissions in the safety requirements specification;
- random hardware failure mechanisms;
- systematic hardware failure mechanisms;
- software errors;
- common cause failures;
- human error;
- environmental influences;

The five domains of action of the standards are as following:

- Requirements aiming to avoid and eliminate the introduction of systematic faults during the specification, development and test phases;
- Requirements to guarantee a robust design through methods and techniques allowing systematic fault tolerance;
- Constraints on hardware architectures in order to improve the dangerous failure detection by means of increased hardware fault tolerance;
- Requirements on the probability of failure on demand or on the average failure rate;

- If software is involved, requirements on its robustness and its integrity concerning systematic failures.

The IEC61508 lifecycle encompasses the safety related system life from concept design to dismantling, including planning, design, installation, validation, operation and maintenance. The prerequisite to the use of these standards is the availability of a PHA stating objectives of tolerable risk and defining the need for automated safety related functions. The IEC61508 framework includes then provisions to transform these specifications in safety functional specifications and in safety integrity specifications. For each phase of the lifecycle, the standards include sets of requirements as well as mandatory or recommended methods, techniques and practices to achieve the requirements objectives.

The standards include provisions to guarantee that the safety integrity levels are maintained during the system life-time by the means of periodic audits and evaluations.

The main benefit of the IEC61508 framework is its ability to be transposed to any context where the expected performances can be sorted and graded according to a decimal logarithmic scale. It allows guaranteeing that a system realised according to SIL_n requirements is 10 times more performing than another realised according to SIL_{n-1}.

8. Synthesis

Safety is in all cases defined in relation to the concept of risk. The common notion of safety as freedom from unacceptable risk is the basis of significant commonalities between all standards. The most decisive influence is on the processes which are recommended to establish the system safety requirements.

Standards generally agree on a common framework for the derivation of safety requirements which combines hazard assessment and risk analysis techniques. The aim of the analysis is to determine the critical system functions, i.e. functions the loss or malfunction of which is catastrophic or hazardous; safety requirements for these functions, i.e. the maximum tolerable failure probabilities; demands, if any, for additional safety functions in order to achieve acceptable levels of risk for the system.

The certification of safety-critical systems is typically demonstrated by compliance with safety standards. Some safety standards are domain-specific, for example ARP4754/ARP4761 (civil aerospace), CENELEC 50159 (rail), ISO26262 (automotive) and IEC61513 (nuclear). Others, such as the functional safety standard IEC61508, are more generic. All the studied standards such as IEC61508, ISO26262 and DO178B are process-based standards. Engineers typically demonstrate that the system is acceptably safe by applying a set of techniques and methods that the standards associate with a specific Safety Integrity Level (SIL), Development Assurance Level (DAL) or risk classification.

Within process-based certification, there are variations in the way in which SILs, DALs or risk classifications are defined. For example, in IEC61508, the allocation of safety integrity levels to functions is based on the required risk reduction associated with some probabilistic criteria. IEC61513 (a derivative of IEC61508 for the nuclear domain), in contrast, adopts a safety classification scheme, defined in accordance with the IAEA principles, in which safety categories are allocated to functions based on deterministic criteria and engineering judgment in relation to the safety consequences of potential malfunction. Specifically, IEC 61226 assigns safety categories, A, B or C, to functions based on the importance of these functions to safety. Importance to safety is determined against three criteria: the role of the function in the achievement or maintenance of the safety of the nuclear power plant, the potential consequences of failure of the function and the probability of the potential consequences of the failure of the function.

In civil aerospace, ARP 4761 presents information on the safety analysis methods needed to conduct the safety assessment. These methods include the Fault Tree Analysis (FTA), Dependence Diagram (DD), Markov Analysis (MA), Failure Modes and Effect Analysis (FMEA), Failure Modes and Effects Summary (FMES) and Common Cause Analysis (CCA). [CCA is composed of Zonal Safety Analysis (ZSA), Particular Risks Analysis (PRA), and Common Mode Analysis (CMA)].

In railway, the CENELEC (EN 50126 and EN 50129) standard presents information on the safety analysis methods needed to conduct the safety assessment. The safety assessment is done by a person independent from the project. The safety analyses for railway are: PHA, IHA (Interface hazard Analysis), SHA (System Hazard Analysis), FMEA, CCA, FTA and SEEA (Software Error Effect Analysis).

This clear identification of the differences and common principles complements the analysis undertaken by the CG2E working group on standards, on the one hand on the principles underlying the identification and allocation of safety categories in the various domains, and on the other hand on the impact of the category on the engineering and validation activities at lower levels, namely software and hardware. This provides the necessary bases towards better and more cost effective processes, tools and products for critical embedded systems across application domains.

9. Acknowledgement

The authors wish to thank Eliane Fourgeau (Dassault Systèmes), Sébastien Bardoz (Dassault Systèmes), Jean-Claude Derrien (Sagem), Jean-Louis Camus (Esterel Technologies) and Cyril Comar (AdaCore) for their valuable contributions to the working group.

10. References

[Blanquart et al., 2010] P. Baufreton, JP. Blanquart, JL. Boulanger, H. Delseny, JC. Derrien, J. Gassino, G. Ladier, E. Ledinot, M. Leeman, J. Machrouh, P. Quéré, B. Ricque, "Multi-domain comparison of safety standards", ERTS-2010, Toulouse, 19-21 May 2010, Toulouse, France.

[Blanquart et al., 2012] JP. Blanquart, JM. Astruc, P. Baufreton, JL. Boulanger, H. Delseny, J. Gassino, G. Ladier, E. Ledinot, M. Leeman, J. Machrouh, P. Quéré, B. Ricque, "Criticality categories across safety standards in different domains", ERTS-2012, Toulouse, 1-3 February 2012, Toulouse, France.

[Ledinot et al., 2012] E. Ledinot, J. Gassino, JP. Blanquart(, JL. Boulanger, P. Quéré, B. Ricque "A cross-domain comparison of software development assurance", ERTS-2012, Toulouse, 1-3 February 2012, Toulouse, France.

[Machrouh et al., 2012] J. Machrouh, JP. Blanquart, P. Baufreton, JL. Boulanger, H. Delseny, J. Gassino, G. Ladier, E. Ledinot, M. Leeman, JM. Astruc, P. Quéré, B. Ricque, "Cross domain comparison of System Assurance", ERTS-2012, Toulouse, 1-3 February 2012, Toulouse, France.

[ECSS-Q30] "Space product assurance – Dependability", European Cooperation for Space Standardisation, ECSS-Q-ST-30C, 6/3/2009.

[ECSS-Q40] "Space product assurance – Safety", European Cooperation for Space Standardisation, ECSS-Q-ST-40C, 6/3/2009.

[ECSS-Q80] "Space product assurance – Software product assurance", European Cooperation for Space Standardisation, ECSS-Q-ST-80C, 6/32009.

[ED12B/DO178B]"Software considerations in airborne systems and equipment certification", EUROCAE ED-12 and RTCA DO-178, issue B, 1/12/1992.

[ED79A/ARP4754A] "Guidelines for Development of Civil Aircraft and Systems", EUROCAE ED-79A and SAE Aerospace Recommended Practice ARP 4754A, 21/12/2010.

[ED80/DO254] "Design Assurance Guidance for Airborne Electronic Hardware", EUROCAE ED-80 and RTCA DO-254, 4/2000.

[ED135/ARP4761] "Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment", EUROCAE ED135 and SAE Aerospace Recommended Practice ARP 4761, 12/1996.

[EN 50126] "Railway applications – The specification and demonstration of reliability, availability, maintainability and safety (RAMS)", CENELEC, EN 50126, 1999 AMD 16956, 28/2/2007

[EN 50128] "Railway applications – Communications, signalling and processing systems – Software for railway control and protection systems", CENELEC, EN 50128:2001, 15/5/2001

[EN 50129] "Railway applications – Communications, signalling and processing systems – Safety related electronic systems for signalling", CENELEC, EN 50129:2003, 7/5/2003

[EN 50159] "Railway applications – Communications, signalling and processing systems.
Part 1: Safety related communication in closed transmission systems",
Part 2: Safety related communication in open transmission systems
CENELEC, EN 50159-1:2001 (11/2001) and EN 50159-2:2001 (12/2001).

[IEC 60880] "Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions", IEC 60880, edition 2.0, 2006-05.

[IEC 61226] "Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions", edition 3.0, 2009-07.

[IEC 61508] "Functional safety of electrical/electronic/ programmable electronic safety-related systems
Part 1: General requirements
Part 2: Requirements for electrical/electronic/ programmable electronic safety-related systems
Part 3: Software requirements
Part 4: Definitions and abbreviations
Part 5: Examples of methods for the determination of safety integrity levels
Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
Part 7: Overview of techniques and measures."
IEC 61508 Parts 1-7, Edition 2.0, 4/2010.

[IEC 61511] "Functional safety – Safety instrumented systems for the process industry sector.
Part 1: Framework, definitions, system, hardware and software requirements"
Part 2: Guidelines in the application of IEC61511–1
Part 3: Guidance for the determination of the required safety integrity levels".
IEC 61511 Parts 1-3, edition 1.0, 3/2003

[IEC 61513] "Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems", edition 1.0, 22/3/2001.

[ISO/FDIS 26262 "Road vehicles – Functional safety"
Part 1: Vocabulary
Part 2: Management of functional safety,
Part 3: Concept phase
Part 4: Product development: system level
Part 5: Product development: hardware level
Part 6: Product development: software level
Part 7: Production and operation
Part 8: Supporting processes
Part 9: ASIL-oriented and safety-oriented analyses
Part 10: Guideline
ISO/FDIS 26262 Parts 1-10, Final Draft International Standard, 2010:

[SCDM] "Safety Case Development Manual", Eurocontrol, 13/10/2006.

11. Glossary

AFNOR	Agence Française de Normalisation
ARP	Aerospace Recommended Practice
ASIL	Automotive Safety Integrity Level
ASN	Autorité de Sûreté Nucléaire
CENELEC	European Committee for Electrotechnical Standardisation
CG2E	Club des Grandes Entreprises de l'Embarqué
CNES	Centre National d'Etudes Spatiales (French National Space Agency)
COTS	Commercial Off-The-Shelf (component)
COPUOS	Committee on Peaceful Uses of Outer Space
FDIS	Final Draft International Standard
E/E (/PE)	Electrical/Electronic (/Programmable Electronic)
EASA	European Aviation Safety Agency
ECSS	European Cooperation for Space Standardisation
EPSF	Etablissement Public de Sécurité Ferroviaire
ERA	European Railways Agency
ERTMS	European Rail Traffic Management System
ESA	European Space Agency
EUC	Equipment Under Control
EUROCAE	European Organisation for Civil Aviation Equipment
FAA	Federal Aviation Authority
I&C	Instrumentation and Control
IAEA	International Atomic Energy Agency
ICAO	International Civil Aviation Organization
IEC	International Electrotechnical Commission
IRSN	Institut de Radioprotection et de Sûreté Nucléaire
ISO	International Organisation for Standardisation
NWI	New Work Item
PES	Programmable Electronic Systems
PSS	(ESA) Procedures, Specifications and Standards
RTCA	Radio Technical Committee for Aeronautics
SAE	Society of Automotive Engineers
SIL	Safety Integrity Level
STRM-TG	Service technique des Remontées Mécaniques – Transports Guidés