Multi-domain comparison of safety standards

Philippe Baufreton, Jean-Paul Blanquart, J. Boulanger, H Delseny, J. Derrien, J. Gassino, G Ladier, E Ledinot, M Leeman, P Quéré, et al.

Multi-domain comparison of safety standards

P. Baufreton[1], JP. Blanquart[2], JL. Boulanger[3], H. Delseny[4], JC. Derrien[1], J. Gassino[5], G. Ladier[4], E. Ledinot[6], M. Leeman[7], P. Quéré[8], B. Ricque[1]

1: Sagem Défense Sécurité, 180 Avenue de Paris, 91300 Massy, France

2: Astrium Satellites, 31 rue des cosmonautes, 31402 Toulouse Cedex 04, France

3: CERTIFER, 1 place de Boussu, 59416 Anzin, France

4: Airbus, 316 route de Bayonne, 31060 Toulouse Cedex 09, France

5: Institut de Radioprotection et de Sûreté Nucléaire (IRSN), BP 17, 92262 Fontenay-Aux-Roses, France

6: Dassault Aviation, 78 quai Marcel Dassault, 92552 Saint-Cloud Cedex, France

7: Valeo, 2 Avenue Fernand Pouillon, 94042 Créteil, France

8: Renault, 1 avenue du Golf, 78288 Guyancourt, France

Abstract: This paper presents an analysis of safety standards and their implementation in certification strategies from different domains such as aeronautics, automation, automotive, nuclear, railway and space. This work, performed in the context of the CG2E ("Club des Grandes Entreprises de l'Embarqué"), aims at identifying the main similarities and dissimilarities, for potential cross-domain harmonization. We strive to find the most comprehensive 'trans-sectorial' approach, within a large number of industrial domains. Exhibiting the 'true goals' of their numerous applicable standards, related to the safety of system and software, is a first important step towards harmonization, sharing common approaches, methods and tools whenever possible.

Keywords: standards, safety, cross-domain comparison, software, certification

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 wide spectrum of application domains. Today this organization comprises more than twenty large, medium and small innovative companies, covering six important industrial fields that will be referred to in this paper.

Several technical working groups have been launched in 2008, one of them addressing "standards & norms", mainly related to the safety of critical embedded systems and software. After a wide state of the art survey performed in 2009, comparing the various standards and practices in many different industrial fields, several areas were identified including "dependability and certification", the object of this paper.

The CG2E objectives are the leverage of the domain-specific best practices in the development of software intensive safety critical embedded systems. It elaborates proposals, recommendations, roadmaps etc. based on collaborative work and discussions in dedicated thematic working groups.

A team of about 20 experts and contributors to this activity has been working for one year. They have the opportunity to share their expertise within a transversal approach between the companies involved in this working group.

Our meeting discussions led us to initiate the elaboration of a common terminology to address all these topics.

Dedicated seminars helped us perform deep analyses of the main system and software standards, used in 6 industrial domains (civil aviation, automotive, space, automation and industrial control, nuclear plants, railway).

This constitutes the basis for a comparative analysis and synthesis of the relevant standards for these major industrial domains, taking care of both technological and economical factors, without losing the main focus on safety.

This paper presents a summary of the main topics that are addressed in more details in a deliverable of our working group, currently under preparation.

2. History and positioning of standards

This section presents a brief overview of the history and positioning of the analysed standards. We first present the generic multi-domain IEC 61508 standard and the more specific standards derived from it, applicable mainly in automation, railway and automotive domains. Then we present the situation in three other domains which for various reasons use standards not directly related to the IEC 61508: nuclear, aeronautics and space.

2.1. IEC 61508, automation, rail, automotive

In September 1985, the International Electrotechnical Commission (IEC) set up a Task Group to assess the viability of developing a generic standard for Programmable Electronic Systems

(PESs). The outcome of which was the setting up of a working group to develop a system-based approach. A working group has previously been set up to deal with safety-related software. Both working groups collaborated on the development on an international standard that was to become IEC 61508.

The original scope of PESs was extended to include all types of electro-technical based technologies (electrical, electronic and programmable electronic systems (E/E/PE). Parts 1-7 of IEC 61508 were published during the period 1998-2000. In 2005 IEC Technical Report 61508-0 was published. A review process initiated in 2002 to update and improve the standard will be completed with the publication of IEC 61508 Edition 2 targeted by March / April 2010.

The standard came up to meet the demand for moving from a prescriptive approach to a performance-based approach. The intention of the workgroup was to produce a base standard, i.e. according to IEC rules a standard to be used only to write other standards. However, the reality today is that IEC 61508 is directly used by industries. Sector specific standards have been derived from IEC 61508, the closest one being IEC 61511 for process industries as most of the IEC61508 workgroup were coming from this sector. This resulted also in standard application conflicts between industry sectors having already operational standards with a holistic approach to systems. This is mainly the case with aeronautics. The paternity of IEC61508 over some standards is subject to controversy as some "sector-specific" standards (e.g. IEC61513 nuclear sector) were issued earlier and developed a very different safety approach.

Concerning the automotive domain, in the 90's, because of the increasing number and complexity of the safety critical systems embedded in a car, it has been felt that a common reference to define the state of the art was needed in order to avoid liability issues. Some carmakers and suppliers started to use the IEC 61508. Although the IEC 61508 framework is considered very useful, many difficulties were experienced using this standard coming from process automation industry. Therefore, it was quickly felt in the community that a strongly adapted variant of IEC61508 was needed.

Approved NWI (New Work Item) was registered in July 2007 starting the 4-year ISO 26262 project. Ten nations (Japan, USA, Germany, France, Italy, UK, Canada, Sweden, Austria and Belgium) are represented in the working group in charge of development of this standard and most industry key players participate. Nations no yet involved (India, China, Korea, Russia) will also apply this standard since they are willing to sell cars in European, USA or Japanese markets. We are confident that this standard will be applied on a worldwide scale.

The project is currently in Draft International Standard (DIS) status.

Standards derived IEC61508 include standards for process industries, machinery (IEC 61511:2003, 62061:2005), power drive systems, programmable controllers (IEC 61800:1997, 61131-6(CDV)), communication networks (61784-3:2007), explosive atmospheres, detection, measurement, apparatus (EN 60079, 50271, 5042), medical devices (IEC 60601:2005), railway (EN 50126, 50128, 50129) and automotive (ISO/DIS 26262).

2.2. Nuclear domain

The IAEA (International Atomic Energy Agency) was created in 1957 within the United Nations to promote and support the safe use of nuclear technology for peaceful applications, and has currently 151 Member States.

In particular, its Safety Guide [IAEA NS-G-1.3] provides general guidance on "Instrumentation and Control (I&C) Systems Important to Safety in Nuclear Power Plants". This guide addresses the classification, safety requirements, and design of these systems.

[IAEA NS-G-1.3] was published in 2002; it combines and revises earlier guides published in 1980 (50-SG-D3: Protection System and related features) and 1984 (50-SG-D8: Safety-Related Instrumentation and Control Systems).

This chronology shows that the Protection System was regarded as the most important one and was addressed first in 1980, followed by the other systems important to safety in 1984. The revision and combination of these guides into NS-G-1.3 was motivated in particular by the need to take into account the evolution in computer-based systems and to include guidance on the classification of systems.

According to an agreement with IAEA, the Technical Committee 45 of IEC (International Electrotechnical Commission) developed standards to implement IAEA safety principles in technical details.

The approach of the following IEC-TC45 standards to design and verify computer-based systems has been tailored since the 1980's to meet the needs of the nuclear plants:

IEC 61226 establishes a method of classification of the I&C (instrumentation and control) functions for nuclear power plants.

IEC 61513 provides general guidance for I&C systems used to perform functions important to safety, taking into account their classification.

IEC 60880 provides requirements for the software of the highest class I&C systems of nuclear power plants, to achieve highly reliable software.

IEC 60880 is the earliest of the IEC-TC45 standards addressing software-based systems: it was edited in 1986 (and revised in 2006) as a formalization of the experience gained during the development of the first computer-based Protection systems. In France, such digital protection systems were developed in the early 1980s'.

Again, this shows that the most critical problem, i.e. how to develop class 1 software has been addressed first, and the need to cover the overall architecture progressively emerged when more and more functions moved from hard-wired logic to interconnected computer-based systems.

2.3. Aeronautics domain

In 1980, the Radio Technical Commission for Aeronautics, now RTCA Inc., established a committee for the development and documentation of software practices that would support the development of software-based airborne systems and equipment. The European Organisation for Civil Aviation Electronics, now the European Organisation for Civil Aviation Equipment (EUROCAE), had previously established a working group to produce a similar document and, in October 1980, was ready to publish document ED-35, "Recommendations on Software Practice and Documentation for Airborne Systems.". EUROCAE decided to stop editing its own document and instead to join RTCA to develop a common set of guidelines. The joint document named ED-12/DO-178 *"Software Considerations in Airborne Systems and Equipment Certification"* was published in 1982, followed by a revision A in 1985 and a revision B in 1992.

During the development of revision B, it became apparent that system-level information would be required as input to the software development process. Since many system-level decisions are fundamental to the safety and functional aspects of aircraft systems, regulatory involvement in the processes and results relating to such decisions is both necessary and appropriate.

ED-79/ARP-4754 *"Certification Considerations for Highly-Integrated or Complex Aircraft Systems"* was then published in 1995 by SAE (Society of Automotive Engineers) and EUROCAE for that purpose. It addresses the total life cycle of systems that implement aircraft level functions. It excludes specific coverage of the different systems, software and hardware design processes, beyond the issues of significance in establishing the safety of the implemented system.

Specific coverage of complex hardware design aspects are dealt with in EUROCAE/RTCA document ED-80/DO-254 *"Design Assurance Guidance for Airborne Electronic hardware"* published in April 2000.

Methodologies for safety assessment processes are detailed and illustrated in SAE document ARP4761.

A revision A to ED-79/ARP-4754 is scheduled to be issued in 2010 and a revision C to ED-12/DO-178 will be published in 2011 including technology-specific or method-specific guidance and guidelines.

2.4. Space domain

The history of regulation in the space domain dates back to the very early days of the domain itself with the creation in 1958 by the United Nations of the COPUOS, Committee on Peaceful Uses of Outer Space. This committee has elaborated a series of treaties and principles, establishing in particular the responsibility of countries for the potential damages caused by launches from their territory. As a result most countries willing to proceed to space launches have established a set of rules and a legal authorisation scheme applicable to space launch activities.

In addition to this legal regulation regime, the space industry has recognised the value of and need for standards to establish and implement space products and programmes. For instance in Europe, after the progressive elaboration of the ESA standardisation system PSS (Procedures, Specifications and Standards), ESA with the European space agencies and industries established in the early nineties the ECSS, European Cooperation for Space Standardisation, a cooperative effort for the purpose of developing and maintaining a single, coherent, recognised and accepted system of common standards. Important updates have been performed from mid 00's with the so-called "-C issues".

The application of the ECSS standards is not enforced by law. The standards are proposed to be adopted, possibly with adaptations, by contract on a case by case basis. This scheme is facilitated by the fact that they are elaborated through cooperative work involving all stakeholders.

ECSS series is organised as three major branches (M: Space project management; Q: Space product assurance; E: Space engineering) under a global heading (ST: System description, glossary).

Each branch consists in a first level of standards, possibly complemented by additional documents (more detailed standards or guidance to apply the first level standard, or handbooks providing additional not-normative information).

3. Regulation regimes and certification

3.1. Certification

To compare the various industrial domains with respect to the notion of certification, we first propose a domain independent definition, and then consider

how the various domain specific safety demonstration processes fit the generic definition.

Certification aims at verifying that the industrial actors that deliver safety-sensitive products or services in a domain (e.g. energy or transport), actually deliver safe products or services. Certification involves an applicant, a regulation, an Authority, and an assessment body that has to be independent, or partially independent, of the applicant.

In many cases the regulations were established by international organizations grouping member states that agreed on establishing shared rules to prevent shared risks e.g. ICAO in civil aviation, AEIA in nuclear industry, United Nations in space industry.

In some cases, regulation came into force at national level, and then at international level to solve cross-border interoperability issues. This is especially the case in the railway industry where the European member states are presently carrying out a regulation harmonization process, in particular through reciprocal acceptance of their national certificates.

There are cases where the Authority and the assessment body are identical (e.g., FAA and EASA in civil aviation), and cases where an Authority granting certificates exists but there is no assessment body distinct from the applicant (e.g., automation and space industries).

Preventing conflict of interest between applicant and assessment body is a key aspect of nuclear (IRSN), railway (ERA, EPSF, STRM-TG), and aeronautics (EASA-FAA) certification.

In no industrial domain does certification lead to responsibility transfer from applicant to Authority. In case of severe accident, the involved manufacturer or service provider is the only entity liable for prosecution.

The international or national regulations are high-level texts stating very high level safety objectives. They are not to be confused with the safety standards discussed in this paper that are conformance means negotiated between industry and Authority to substantiate that the engineering process of the applicant meets these high level regulatory objectives.

A noticeable exception is automotive industry which has no Authority, nor international functional safety regulation to conform to. However, it has to conform to regulation on specific technical domains (e.g., braking, steering …) to receive the required clearances to market a car.

Typical certification of a product (e.g., in aeronautics) involves:

(a) the process of assessing the design of a product to ensure that it complies with a set of standards applicable to that type of product so as to demonstrate an acceptable level of safety;

(b) the process of assessing an individual product to ensure that it conforms with the certified type design;

(c) the issuance of a certificate required by national laws to declare that a) or b) compliance with the standards is met.

3.2. Qualification

A qualification is defined for a specific task in a specific project. It is a set of activities to grant a confidence level to an entity, be it an organisation, a person or a tool. For instance, qualification is used to assure that a software life cycle process automated by use of a tool will result in the same or higher quality output as if the process had been performed manually.

3.3. Approval credit

3.3.1. Aeronautics

In civil and military aviation, independent authorities like Federal Aviation Administration or European Aviation Safety Agency are in charge of certification of aircraft and their embedded systems regarding safety.

Certification typically applies to aircraft or engine types. The certification authority considers the software as part of the airborne system or equipment installed in the certified aircraft or engine; that is, the certification authority does not approve the software as a unique, stand-alone product. Currently, computer hardware and software must be approved as a "system" for every installation.

3.3.2. Space

The standards applicable to the space sector in Europe correspond to the series of standards elaborated by the ECSS, European Cooperation for Space Standardisation, a cooperative effort of the European Space Agency, national space agencies and European industry associations for the purpose of developing and maintaining common standards.

In terms of regulation, it is worth noting that the application of the ECSS standards is not enforced by law, but proposed to be, and generally is, adopted, possibly with adaptations, by contract on a case by case basis.

This does not mean that the space sector is not subject to certification in a stricter meaning. In particular most countries, as they are responsible for all launches on their territory, have set up legal rules associated to launchers, spacecraft, launch installations and procedures, and the corresponding licensing scheme. For instance launches from the “Centre Spatial Guyanais” in Kourou are submitted by delegation to the authority of the French National Space Agency CNES.

3.3.3. Automotive

In the automotive domain, the ISO/DIS 26262 provides a set of requirements, so called confirmation measures, to ensure that an assessment of safety is properly done on EE aspects.

The actors performing the confirmation measures shall have a minimum level of independence from the people in charge of development and release for production. The higher the ASIL the higher the independence required. It is to be noted that the highest level of independence required may be reached within the same company.

The confirmation measures consist in:

- safety reviews to verify key deliverables,
- a safety audit to verify the appropriateness of the process,
- a safety assessment to evaluate the whole safety case.

3.3.4. Railway

The major standards are the European Railway Standards required by law:

- CENELEC EN 50126 establishes a method for the specification and demonstration of reliability, availability, maintainability and safety (RAMS), for railway domain.
- CENELEC EN 50129 provides general guidance to demonstrate the safety of electronic systems and to construct the safety case for signalling railway application.
- CENELEC EN 50128 provides requirements for the software used in signalling railway application.
- For safety related communication, CENELEC EN 50159-1 is dedicated to closed transmission systems and CENELEC EN 50159-2 is dedicated to open transmission systems.

In general, the safety related series of CENELEC 5012x standards was derived from IEC 61508.

The benefits from using this standard were mentioned as they are the “code of practice” for railroad industries in the European Union and a prerequisite for the approval of safety relevant applications in the railroad context. Furthermore, CENELEC standards are international standards that facilitate market access.

Certification and qualification are given by conformity to the specific standard and/or meeting the regulatory requirements. Some may require third party certification while others allow self assessment.

In general, national regulation and law have a strong impact on the system and its required safety. Up to now, they differ much in different European countries. This makes certification and approval on a cross-country basis very difficult and expensive. But with the new European view for opening the market, new practices are put in place: standards that define what is a railway system, what is a subway system, what is an interoperable system, etc.

For the railway domain, all European countries (see the directive 2004/49/CE) must have a Safety Authority to control its use and protect the people and the environment from the harmful effects of railway accident. In case of ERTMS[1] (European Rail Traffic Management System) components the certification is mandatory. For ERTMS certification, each nation recognizes a “notified body”. In France the notified body is “CERTIFER[2]” for interoperability of the Trans-European rail system directives: 96/48/CE for high speed transportation, 2001/16/CE for conventional speed.

ERA is the European Railways Authority, and in France the Railway Safety Authority is “Etablissement Public de Sécurité Ferroviaire” (EPSF[3]).

According to the new European commercial plans and laws, railway systems are designed to be operated in more than one country. Since 2007, cross-acceptance has been coming out, which should ease such certification activities. Basically it means that for instance, a train certified or approved in one country, will get approval in other countries as well. In contradiction to the cross-acceptance, the different national regulations can impose additional requirements.

3.3.5. Automation

The standard IEC 61508 does not provide provisions for any type of certification.

The European Machinery Directive requests a type certification associated with the CE label. This is achieved by the manufacturer through an auto-certification process.

3.3.6. Nuclear

All countries using nuclear energy have set up a Safety Authority to control its use and protect the people and the environment from the harmful effects of radiations. In France the Safety Authority is “Autorité de Sûreté Nucléaire” (ASN). Its technical support is “Institut de Radioprotection et de Sûreté Nucléaire” (IRSN).

The nuclear power plants are not submitted to “certification”, but to authorization for creation and operation. This authorization is formally delivered by a decree of the government following a proposal of ASN.

[1] http://www.ertms.com/
[2] http://www.certifer.fr
[3] http://www.securite-ferroviaire.fr

The only documents having full regulatory status are the “arrêtés” (orders) issued by the government. They provide high level requirements and do not enter into technical details. In practice, regarding the computer-based safety systems, the documents issued by IAEA for the general approach and by TC45 of IEC for the development are proposed by the utility and considered as acceptable means by IRSN and ASN.

4. Technical comparison highlights

The review of similarities and dissimilarities on the technical content, interpretation and utilisation of the standards is highlighted in this section through a selection of important topics: the orientation of standards towards integrated or external safety, towards the prescription of objectives vs. means, their notions of severity, criticality and assurance levels, their focus on fault tolerance or fault prevention, on probabilistic vs. deterministic safety assessment methods, and the notion of safety case.

4.1. Integrated safety or external safety systems

Depending on applications and sectors, safety is ensured by means of different architectures. Plant (classical or nuclear), machine automation and railway promote specialised safety systems: the safety is monitored and guaranteed by a specific system, distinct from the system implemented the required function. Automotive and aeronautics promote safe systems: the safety is “integrated” in the functional system. These possibilities are determined in practice by the structure of the risks versus the protective systems. For instance when no specific safe state exist, a separated protection system will be useless as there will be no possibility of driving the controlled equipment to a safe state upon failure of the protection system. It becomes then necessary to focus on a safe control system, rather than on a dedicated independent protection system. The intrinsic characteristics of the industrial sectors are then the design drivers to choose how to integrate or segregate the safety management part.

In the automotive industry, the key design driver is hardware cost. Therefore, a dedicated independent protection system is never considered. In most applications the control system provides built-in mechanisms to detect failures and put the system in a safe state. However, in some cases, external safety is considered when it is possible to use an existing feature of another system as a protection mechanism.

4.2. Objectives vs. Means prescription

The authors of safety standards have to choose between being prescriptive on the means to satisfy high-level safety objectives, or prescriptive on the objectives, considering that the means are completely under the applicant's responsibility.

A means-prescriptive standard is easy to use when applied strictly in the conditions envisioned by its authors. However it does not address easily the emergence of new technology, methods and tools.

An objectives-prescriptive standard can apply to a large variety of technologies, life cycles, tools, etc. but needs to be interpreted before being used; and the interpretation may be questionable and could seriously differ from the intent of the standard’s authors.

The different standards reflect a large variety of positions, between these two extremes (means- or objectives-prescriptive), for example:

- IEC 61508 is definitely means-prescriptive as it “recommends”, “highly recommends” or even “mandate” specific means to achieve safety objectives.
- ED-12/DO-178 is widely recognized as an objectives-prescriptive standard

4.3. Categorising severity and assurance levels

In all investigated domains, the standards introduce a categorisation into “levels” which may be called safety integrity levels, criticality categories etc., The idea is to associate to a system (or function, component etc.) an attribute characterising the worst case consequences (severity) of its potential failures, possibly combined, for some domains (e.g., automotive), with the notion of exposure frequency. In a classical risk assessment based approach this sets a limit on the likelihood of failure occurrence so that the risk remains acceptable.

Criticality categories are in general allocated to functions. This defines (a part of) the requirements applicable to the development (and validation) of the elements implementing them (systems, hardware, software items) so as to address the possible sources of failures appropriately with respect to the categories,:

- Random hardware faults: standards define the target maximum probability of failure and/or a maximum number of independent faults leading to a failure, for each category.
- Development faults, affecting system, hardware or software design: standards define the requirements applicable to all the development and validation processes needed to elaborate these items, especially development and validation processes. Requirements vary according to the “criticality” (or equivalent) levels, defining different DAL (Development Assurance levels). The idea is that, as discussed in §4.5, there is no attempt to evaluate numerically the probability of failure due to such faults, but to consider that fulfilling these requirements

provides a level of confidence compatible with the severity of the risk.

There are significant variations between standards on how the severity of consequences is defined and ranked and how criticality categories are allocated (e.g., on whether and how it is possible to realise a function at some level with elements at some other (lower) level, using such or such redundancy scheme). However all standards agree on the basic principles and on the necessity to enforce a strong isolation against fault propagation between elements at different categories.

There are also differences in the requirements associated to each category and even on their nature. For example ED12B/DO178B states process objectives whereas IEC 61508 or EN 50128 list explicitly some recommended techniques. ISO/DIS 26262 and ECSS are somewhat hybrid with some requirements on objectives supplemented by some suggested means.

In the current situation, it is very difficult and expensive for software or tool providers to address several domains because of the necessity to comply with the union of the requirements of each domain. Conversely there is little evidence that the specificities of each domain are sufficient to justify all the observed differences.

4.4. Fault tolerance or fault prevention

Basically, in the domains covered by the paper, the fault tolerance is required at the system level, not at the software level: the software standards addressed in this paper basically target the achievement of fault-free software, either explicitly stated (EC 60880 or CENELEC EN 50128) or not (DO178, etc.)

This is achieved through requirements on both the processes (e.g. clear and extensive documentation, adherence to specification, design, code standards) and the product (e.g. verification, restriction to unambiguous constructs, mastering of parallelism, behaviour completely determined by the functional inputs).

Self-supervision usually required by software standards such as IEC 60880 is mainly oriented to the detection of random hardware failures such as corruption of memory content or transmission errors. In case of detected failure, the standards do not require the continuation of the normal processing but require that a predefined action be taken (e.g. outputs set to a safe position when applicable).

The tolerance of software to its own errors is not required, because this could need detection and reconfiguration algorithms more complex than the functional software itself, and could therefore significantly increase the potential for errors. To avoid this, standards such as IEC 60880 require that self-supervision does not adversely affect the intended functions. In the railway sector, the CENELEC EN 50128 (table A.3) states that the backward and forward recovery, the dynamic reconfiguration and/or fault correction of software are not recommended.

The tolerance to hypothetical software errors is implemented at system level or at top-level architecture by means based on functional diversity. For example a secondary computer within the system may monitor the main one and check the plausibility of its outputs with a different algorithm, or two different systems may independently trigger a given safety action, based on different algorithms involving different physical measurements. The choice between such architectural solutions mainly depends on the characteristics of the underlying controlled process.

4.5. Probabilistic versus deterministic

It is remarkable that the approach to quantification of system failure risks is identical in the aeronautic, automation, automotive, nuclear, railway and space dependability standards. In particular, none of them gives credit to probabilistic assessment of software failure.

The standards in the 6 domains considered in this paper uniformly regard software as a deterministic artefact whose functional failures, contrary to hardware, can only be caused by residual specification, design or implementation faults. Therefore, software safety building, assessment and measure is uniformly handled through design assurance, a design assurance policy being enforced through a standard- dependent mix of process-based and product-based development activities.

The stringency of the development fault avoidance policy is graded into a few discrete levels, 3 to 5 depending on the standards that determine different sets of quality and development activities objectives. But there is no quantified likelihood of residual fault or functional failure associated to these levels.

The effects of the residual software faults that may lead to systematic software-induced system failures are handled through fault tolerance mechanisms, which still lie in the deterministic arena, be they implemented in software or hardware.

Probabilistic assessment comes into play to quantify the likelihood of component-level hardware failures on the one hand, and the likelihood of system-level user-oriented dreaded events on the other hand. All the standards set probability-based rareness objectives to the system level feared events, depending on their respective severity.

Almost no standard recommends probabilistic safety assessment methods to propagate the probabilities from hardware level up to system level.

Following a simple divide and conquer approach, which by the way is the only tractable one in practice, the probabilistic assessment methods of the density of the system level dreaded behaviours that are explicitly or implicitly recommended by the standards do not rely on system level behavioural analysis. They rely on architectural modelling, possibly including time-dependent fault-tolerance reconfiguration logics, by means of reliability diagrams, fault trees or state machines that capture the event-to-functions and the function-to-resources dependencies.

In particular, the Boolean models (possibly sequential) that support the probabilistic computation get rid of any analysis of the complex behavioural propagation of the quantified failures from hardware level up to user level through the networked software and hardware machinery. Depending on the dependability engineer's expertise in modelling, this behavioural abstraction is done in a conservative way regarding probabilistic estimation.

So in all standards, a state of the art pragmatic and hopefully sound separation of concerns is admitted: deterministic analysis of local behaviours (hardware or software) ruled by design assurance policies on one side, probabilistic analysis of events through global function-organ dependency graphs, ruled by severity-based rareness objectives on the other side.

As stated by the IAEA, “it is not possible to derive a failure rate for a software based system on an objective and fully defendable basis. The reliability assigned to the system is ultimately a matter of judgement” [IAEA 1135].

Thus the software standards concentrate on deterministic verification, for example through tests selected to cover all functionalities and further verification of the adequate structural coverage achieved by these tests. For safety critical software (e.g. in the nuclear or aeronautic sector), these tests are built by people independent from the development team.

In order to provide inputs to the probabilistic requirements assigned to systems embedding software, it is agreed within most sectors that the development of software in compliance with the sector’s specific standards makes it possible to meet the safety requirements, assigned as probabilistic targets to the system (such as 10^{-4} failure per demand or 10^{-9} failure per hour), while considering software as deterministic.

4.6. Safety case

We define a safety case as: 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. Its purpose is to participate to the demonstration that a product is safe. It is a keystone in certification. It is generally produced incrementally during the life cycle, and can be delivered at milestones such as before progressing to detailed development and before installation and commissioning.

A safety case is a reasoned and supported argument, a way of documenting and providing assurance to the stakeholders that a system is acceptably safe thanks to compliance with a particular safety standard. It must be updated during all the life of the product and must be available even after stop of production (number of years will depend on the domain).

A safety case is a requirement in some safety standards for example that of the railway domain (CENELEC EN 50129) and the automotive domain (ISO/DIS 26262). CENELEC EN 50129 even defines the content of the safety case.

Depending on the industrial domain or country, its constitution may differ. It can be as simple as a collection of information produced during the development or a thorough and coherent stand alone argumentation substantiated by evidence collected during the complete safety lifecycle. In aeronautics, nuclear or space we can consider that even if not mentioned as such, the safety case results from the documents and assurance provided as the result of the conformance to the safety standards of the sector.

The safety case is one subject of further analysis within the CG2E working group.

5. Conclusion, perspectives

5.1. Conclusion

This paper presented major relevant topics regarding the comparison of the safety standards of six industrial domains, and identified some important principles that may now be considered for harmonization purposes. We also observed that some topics remain domain-specific.

We identified the possibility to group the domains into a small number of categories. However this grouping may vary according to the considered topic. For instance, all the covered domains agree upon the articulation of a deterministic view of software and the system safety goals, including the probabilistic ones. Conversely, the regulation regime and certification scheme is similar for aviation, nuclear and, to some extent, railway and space, but significantly different for automation and automotive.

Aviation, space and nuclear are very close domains, sharing many concerns, needs and solutions in terms of processes, methods and techniques. These fields have developed since the 80’s software standards reflecting their safety approach, i.e. requiring a strong, deterministic demonstration of design correctness. These standards do not promote

or require the use of specific tools, methods or languages because this would require taking into account all possible applications, company practices, people skills and future technology evolutions, which is not realistic. For these reasons, using the generic standard IEC 61508 in its current approach is not possible in these fields.

Automation and railway are difficult to compare on a global perspective because automation is a very large domain covering different systems and practices. The standards applicable to automation, automotive and rail are different but are indeed principally derived from the generic standard IEC 61508. Note however that another difference comes from the fact that most products for rail applications are at the highest criticality level (SIL 4), while it is much more variable for automation products.

The clear identification of these similarities, dissimilarities and trends could provide important sources of improvement (especially for safety analysis, process efficiency and cost) mainly for tool and COTS providers. Tracks for possible harmonization have been exhibited for each of the industrial domains, in full compatibility with its own standards.

In addition to some terminology discrepancies, the main identified limits to harmonization, are:

- the way to allocate the development assurance levels to system, software and hardware with respect to the safety requirements (we have shown some common approaches can be envisioned),
- the regulation regime and certification scheme for critical embedded systems software,
- the standards elaboration bodies, which are specific for each domain, with little or no interest for cross-domains standardizations.

5.2. Perspectives

The existence of common high-level goals in the different sectors shows the need and the possibility for harmonization and alignment of the standards analyzed in this paper. A preferred way would be to refer to a generic safety standard which would establish these high level goals, and then would be implemented in detail in sector-specific ones.

No existing standard could be a candidate for such a generic role. Therefore we intend in a future work to define the set of common high level safety objectives and rationale underlying the justification scheme.

Even if some standardization bodies are willing to operate such a convergence, as we see for example in the nuclear field the endorsement of IEC/45A standards by CENELEC and the development of "dual-logo" standards by IEC/45A and IEEE, it is still not a generalized attitude. Our working group, composed of some of the major contributors to the various standards, and the work we want to complete could influence this, showing that it is possible and worthwhile.

We aim at complementing the studies that we have initiated, by sharing as many common sub-processes as possible between various domains, which in fact have similar issues when developing complex embedded systems.

For example, we are working on consolidation and harmonization of C-coding rules, with also important consequences on the possible rationalisation of associated support tools. This work, which will be presented at "Assises Franco-Allemandes de l'Embarqué", in October 2010 is a first concrete example of benefits expected from such an initiative.

A probable extension of our work will be pushed forward in 2011 at a European level, for instance within the ARTEMIS Joint Undertaking or the 7th Framework Programme of the European Commission (e.g., ProSE).

6. Acknowledgement

The authors wish to thank Jean-Louis Camus (Esterel Technologies), Eliane Fourgeau (Geensoft), Jean Gauthier (Dassault Aviation), Olivier Guetta (Renault), Dominique Paquot (Sagem) and Virginie Wiels (ONERA) for their contribution.

7. References

[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.

[ED79/ARP4754] "Certification Considerations for highly integrated or complex aircraft systems", EUROCAE ED79 and SAE Aerospace Recommended Practice ARP 4754, 11/1996.

[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.
CENELEC, EN 50159-1:2001 (11/2001) and EN 50159-2:2001 (12/2001)
Part 1: Safety related communication in closed transmission systems",
Part 2: Safety related communication in open transmission systems.

[IAEA NS-G-1.3] "Instrumentation and Control (I&C) Systems Important to Safety in Nuclear Power Plants", IAEA Safety Standards Series n°NS-G-1.3, 25/4/2002

[IAEA 1135] "Regulatory review of probabilistic safety assessment (PSA). Level 1", IAEA, IAEA-TECDOC-1135, February 2000

[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" IEC 61508 Parts 1-7, First edition 12/1998.
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 61511] "Functional safety – Safety instrumented systems for the process industry sector.
IEC 61511 Parts 1-3, edition 1.0, 3/2003
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 61513] "Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems", edition 1.0, 22/3/2001

[ISO/DIS 26262 "Road vehicles – Functional safety" Draft International Standard ISO/DIS 26262: 2009
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:

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

8. Glossary

AFNOR	Agence Française de Normalisation
ARP	Aerospace Recommended Practice
ARTEMIS	Advanced Research and Technology for Embedded Intelligence and Systems
ASIL	Automotive Safety Integrity Level
ASN	Autorité de Sûreté Nucléaire
CDV	Committee Draft for Vote
CE	Conformité Européenne
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
DIS	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
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
ISO	International Organisation for Standardisation
NWI	New Work Item
PES	Programmable Electronic Systems
ProSE	Promoting Standardisation for Embedded systems
PSS	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