Criticality categories across safety standards in different domains

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

(1) Contact author, Astrium Satellites, jean-paul.blanquart@astrium.eads.net ;
(2): Continental; (3): Sagem Défense Sécurité; (4): CERTIFER; (5): Airbus; (6): IRSN; (7): Aerospace Valley; (8): Dassault Aviation; (9): Valeo; (10): Thales; (11): Renault

Abstract:

This paper presents a comparative analysis across several industrial domains, of the fundamental notion of safety categories or levels (Safety Integrity Levels, Development Assurance Levels, etc.) underlying the safety framework enforced by safety standards. This work is one of the facets of an in-depth comparison of safety standards across application domains [1], performed by a working group gathering experts from 6 industrial domains (automotive, aviation, industrial automation, nuclear, railway and space), which aims at establishing the bases for more efficient processes and tools to support the development, validation and support to certification of critical embedded systems.

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.

The paper presents the results of an analysis, performed by one Working Group of CG2E, of the dependability and safety standards, as well as their applicability within the engineering processes of industrial companies. The objectives are to identify their main similarities and dissimilarities with an aim to a potential cross-domains harmonization, when possible and relevant, in terms of processes, approaches, methods and tools.

The paper focuses on an important part of this work concerning the notion of categories or levels which, under various names (safety integrity levels, criticality categories, development assurance levels, etc.) constitutes a fundamental basis of safety standards in all addressed domains.

The paper is structured as follows. We first describe the notion of category and associated allocation process in each addressed application domain, following a same organisation: description of the source of the categories, of the initial element of the system which is categorised, of the process to allocate categories to lowest grain entities in the system decomposition, and of the impact of the dependability architecture and mechanisms on the allocated categories. Then we propose a cross-domain comparison and synthesis following this same organisation.

2. Aeronautics

2.1. Source of categories

The ARP 4754 / ED 79 classifies "failure conditions" i.e., hazardous situations resulting from potential failures of the aircraft functions.

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 defined herein to identify Failure Conditions and severity classifications which are used to derive the level of rigor required for development.

The Development Assurance Level is assigned depending on the severity classification of Failure Conditions considering the possible independence between development processes that can limit the consequences of development errors. The more severe the Failure Condition Classification, the greater the level of Development Assurance necessary to mitigate the Failure Condition.

The classification of each failure condition is based on its identified effects. Five categories are defined and ordered, labelled Catastrophic, Hazardous, Major, Minor and "no safety effect", corresponding to predefined descriptions of possible effects (multiple fatalities, reduction of the capabilities to cope with adverse situations, etc.). For each category there is a one-to-one mapping to a scale of "Development Assurance Levels" (DAL) labelled from A (most demanding, corresponding to catastrophic failure conditions) to E (least demanding, corresponding to "no safety effect").

2.2. Initial allocation

The Development Assurance Level assignment (allocation) process begins with FDAL assignment to

the Functions involved in the aircraft's and/or systems' FHA Failure Conditions.

An FDAL is assigned to the top-level Function, based on its most severe Top-Level Failure Condition Classification. This is performed for each Function in the aircraft and system FHAs in accordance with Table 2.1. This assignment establishes the rigor for the applicable Development Assurance processes described in the standard.

The standards provide a table which associates each of the five classes of failure conditions with:

- a functional safety requirement expressed in quantitative terms (maximum rate of failure per flight hour).
- a development assurance level for the system which implements the function.

Table 2.1 shows this relationship between the severity of a functional failure condition, the quantitative safety requirement for the function and the development level for the system.

Failure Condition Class	Quantitative Safety Requirement (failures/h)	Development Assurance level
Catastrophic	$P < 10^{-9}$	A
Hazardous	$P < 10^{-7}$	B
Major	$P < 10^{-5}$	C
Minor	None	D
No safety effect	None	E

Table 2.1: Relationship between severity of failure condition, safety requirement and development level (source: ARP 4754)

2.3. Allocation to components

The DAL is then allocated to the development process of the system and its items (down to hardware and software items).

FDAL and IDAL assurance level assignment is a top down process starting with the Failure Condition severity classification from the FHA and assigning the Top-level FDAL in the PASA/PSSA. After decomposing the top-level function into sub-functions, the sub-functions' FDALs are assigned. Each sub-function is then decomposed and/or allocated further into items and then items' IDALs are assigned. The FDAL and IDAL assignment process should be applied when developing new Functions and new items.

2.4. Dependability architecture and safety level

Redundancy and fault propagation mechanisms may be exploited to reduce the DAL allocated to the items of a system provided these architectural means are validated themselves at the DAL allocated to the system. Accordingly it is possible to achieve system DAL A with redundant parts at DAL B, with proper justification, in particular that only multiple independent failures may cause the catastrophic failure condition. This DAL decomposition can only be done once, at system level ("system" understood as what implements the aircraft topmost functions).

During allocation of a top-level function into two or more independent sub-functions (i.e. one sub-function by itself cannot cause the top level hazard), it is possible to assign an FDAL of at least one of the sub-functions lower than the top-level function's FDAL. However, there may also be functional allocations where the FDAL assignment of at least one of the sub-functions may be as high as the level of the top hazard.

Independence between aircraft/system functions or items can protect against potential common mode Errors and is a fundamental attribute to consider when assigning Development Assurance Levels.

The intent of Independence attributes is to have sufficient confidence that the likelihood of a common mode Error is minimized between two or more members commensurate with the severity of the Failure Condition Classification.

For the purposes of assigning Function DAL (FDAL) and Item DAL (IDAL), two types of independence attributes, Functional Independence and item Development Independence are considered.

Once an FDAL is assigned to the top-level aircraft function based on the top-level Failure Condition severity classification, the architecture of the system functions involved in the top-level Failure Condition are examined to delineate the Development Assurance levels of those system functions.

If it can be shown that the aircraft or system architecture provides containment for the effects of development errors by two or more independent members, Development Assurance Levels may be assigned with consideration of the containment provided by the architecture. System safety assessment techniques are used to identify the members within the Functional Failure Sets (FFSs) that lead to the top-level Failure Conditions.

The level of rigor for substantiating the independence among the members of the FFS is the same FDAL assigned to the top-level Failure Condition per Table 2.1.

The IDAL assignment always follows the FDAL process. When the system architectures are refined down to the item level, the FDAL is assigned to a FFS member using guidance provided in the standard. The assignment becomes the IDAL of the related item. This IDAL will be used as an input for the application of DO-178B/ED-12B (software development assurance) or DO-254/ED-80 (electronic hardware design assurance).

For IDAL assignment the applicant may use several options related to the top-level Failure Condition classification, provided the FFS has item

development independence. The FDAL does not impose the IDAL. In some cases, the IDAL can be higher than FDAL function using the item. However, whichever option is chosen the final FDAL and IDAL combination should be in accordance with the general principles exposed in the standard.

3. Automotive

3.1. Source of categories

The starting point of an hazard analysis and Risk assessment (H&R) according to ISO 26262 is the identification of the **vehicle-level hazards**, in terms of physical injuries or damage to the health of people, that can be triggered by failures or unintended behaviours of system(s) that implement a vehicle function (e.g. vehicle lighting is affected by a loss of head lighting due to a body controller malfunction).

'People' designates the person(s) at risk such as the driver of the subject vehicle, its passengers and/or any other road users in the vicinity of the subject vehicle (e.g. pedestrians, occupants of other vehicles).

The hazards are identified with no consideration for any safety mechanisms internal to the system being analyzed; i.e. either those intended to be implemented or those already implemented in similar existing systems.

Following the identification of vehicle-level hazards, the elements being categorized by ISO 26262 are the **hazardous events**. A hazardous event is a relevant combination of a hazard and an operational situation of the vehicle with potential to lead to an accident if not controlled timely (e.g. the driver is expected to slowdown his/her vehicle and switch on the hazard warning signal in case of loss of head lighting in darkness or other conditions of reduced visibility).

Figure 3.1 gives an example of the relationships between a system failure, the corresponding hazard, hazardous event and accident.

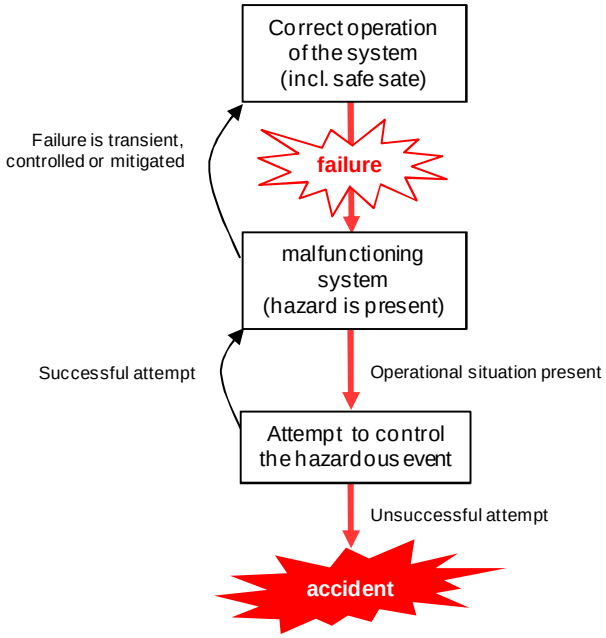


Figure 3.1 – Example of an accident scenario

3.2. Initial allocation

Each of the identified hazardous events is assigned an **ASIL** based on the ASIL classification method discussed hereafter. Per ISO 26262, ASIL stands for Automotive Safety Integrity Level and is based on determining three parameters associated with the hazardous events: the exposure 'E', the controllability 'C' and the severity 'S'.

There are four ASILs defined, with ASIL D representing the most demanding regarding a necessary risk reduction and ASIL A the less demanding. The events with no safety relevance are assigned 'QM', i.e. Quality Management.

ASILs are used in ISO 26262 for specifying the risk reduction measures for the development of the system and its electronic hardware and software components. Those measures address both residual probability of random hardware failures and avoidance of systematic failures.

Figure 3.2 gives an overview of the ASIL classification method.

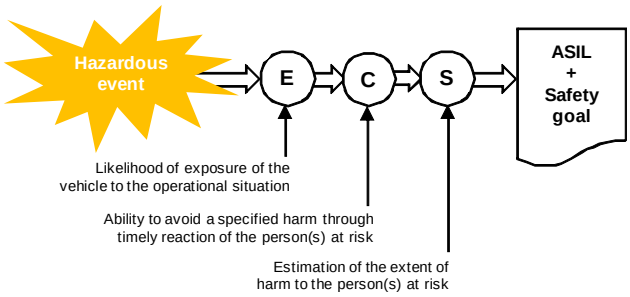


Figure 3.2: Overview of ASIL classification method

'E' defines the likelihood of exposure of the vehicle to an operational situation which may lead to a hazardous event in presence of the failure of the system. Depending on cases, the exposure rating is based on frequency of occurrence of the situation or on its duration (e.g. proportion of operating time in darkness or other conditions of reduced visibility compared to the total operating time of a vehicle).

'C' characterizes the ability of the person(s) at risk to react timely in order to avoid any harm when the hazardous event occurs (e.g. ability of the driver to slowdown his/her vehicle safely and switch on the hazard warning signal).

'S' is the estimation of the harm to person(s) at risk that may result from the occurrence of a hazardous event when not controlled timely (e.g. harm resulting from a front collision).

'S' represents the severity of the risk associated with a vehicle-level hazard. 'E' in combination with 'C' and with the residual failure rate of the system failure that potentially lead to the hazardous event under consideration corresponds to the probability of occurrence of this risk.

'E', 'C' and 'S' are rated using discrete scales. The ASIL assigned to the hazardous event is deduced from the combination of those three evaluated parameters by using a risk graph.

When more than one hazardous event is associated to the same system failure then the event with the highest ASIL is held.

Additionally to the ASIL, a **safety goal** is determined for each hazardous event. The safety goal represents a top-level safety requirement that is assigned to the system as a whole. Safety goals always inherit the ASIL of their corresponding hazardous event (e.g. the system shall only switch off the head lighting on driver's request).

When a safety goal is associated with more than one hazardous event, it inherits the highest ASIL.

Depending on cases, more than one safety goals with different ASILs may be assigned to a system.

3.3. Allocation to components

The H&R, which results usually in a set of safety goals with their ASIL, is executed early in the system development, typically during the concept phase.

The refinement of those safety goals in lower-level safety requirements and their allocation to the architectural components of the system is performed throughout the system design, the electronic hardware design and the software design.

Generally speaking, the ASILs of the safety goals are propagated throughout the system development. The following basic rules apply by default:

- Each safety requirement inherits the ASIL of the parent safety requirement it is derived from, starting from the ASIL of the safety goal,
- Any architectural component that implements a safety requirement has to be developed in compliance with the ASIL of this safety requirement.
- When safety requirements with different ASILs are implemented by the same architectural component, the complete component has to be developed in compliance to the highest ASIL, unless it can be shown that sufficient freedom from interference exists from the sub-components with the lower ASIL(s) to the sub-components with the highest ASIL.
- When a requirement with no safety relevance and a safety requirement are both implemented by the same architectural component, the complete component has to be developed in compliance with the ASIL of the safety requirement, unless it can be shown that sufficient freedom from interference exists from the sub-component with no safety relevance to the safety-related sub-component.

Here, 'freedom from interference' means the absence of cascading failures from the lowest ASIL(s) (or no-ASIL) sub-component(s) to the highest ASIL sub-component(s).

3.4. Dependability architecture and safety level

The ASIL inherited by a safety requirement can be downgraded provided the following design rule is applied:

> *An initial safety requirement is decomposed to redundant requirements implemented by sufficiently independent architectural components, where each decomposed requirement complies with the initial safety requirement by itself.*

Here, 'independence' means the absence of common cause failures and the absence of cascading failures between the architectural components that could lead to the violation of the initial safety requirement.

Reduction of ASIL does not apply to safety goals, i.e. the top-level safety requirements.

It may be applied to any lower safety requirements at system level, electronic hardware-level or software-level.

However, sufficient independence between the architectural elements has to be checked at the system level.

Reduction of ASIL may be applied more than once.

Table 3.1 gives the authorized ASIL reductions: the first column indicates the ASIL of the initial safety requirements and the second column the possible combinations of ASILs for the decomposed redundant requirements. The letters between brackets designate the ASIL of the safety goal from which the reduction of ASIL applies.

ASIL D	ASIL C(D) + ASIL A (D)
	ASIL B(D) + ASIL B(D)
	ASIL D(D) + QM(D)
ASIL C	ASIL B(C) + ASIL A(C)
	ASIL C(C) + QM(C)
ASIL B	ASIL A(B) + ASIL A(B)
	ASIL B(B) + QM(B)
ASIL A	ASIL A(A) + QM(A)

Table3.1: Authorized ASIL reduction schemes

4. Nuclear

This part is a summary of citations from reference documents, especially IEC 61226 and IEC 61838. We focus on the AIEA-IEC safety referential, representative of the European practices. Some simplifications have been done given the limited size of the paper.

4.1. Source of categories

An initial safety analysis of the reactor has to be completed before classifying the functions supported by Instrumentation and Control (I&C) systems.

The main inputs of the categorization or classification scheme are: the reactor type (for example: pressurized water reactor, boiling water reactor…), the Initiating Events, the plant states and accident conditions as well as the related acceptable radiological limits, the major functions needed to mitigate the consequences of Initiating Events, and their supporting functions.

A functional analysis, based on the severity of the potential consequences of Initiating Events and taking into account their frequencies, supports the classification of mitigation and supporting functions. The experience gained during the design and operation of previous facilities is preeminent, especially because there are few changes over time in the overall design of a given reactor type. The functional analysis relies on the safety design, and on the identification of Functions, Systems and their requirements.

Initiating Events root causes are identified by various risk assessment techniques (HAZOP, FMEA…) and experience, in some extent available in various technical reference documents.

The operating situations are classified into Plant Condition Categories (PCCs) based on frequency ranges and consequences. In each category, the occurrence of an event is assigned to a maximum allowed level of releases or radiation exposure. International standards determine the admissible damage for each PCC in terms of radiological effect. ANSI/ANS 51.1 provides such an example of frequency/damage curve. Consequences exceeding these levels are considered unacceptable, and prevention and/or mitigation functions must be added.

Safety of French nuclear facilities (NPPs, research reactors, facilities for enrichment, etc.) is based primarily on the internationally agreed concepts of deterministic design and Defense in Depth (INSAG-10). However, despite a large set of international standards, the practices are in detail dependent on the national regulations. For French NPPs, the Plant Conditions Categories are the following:

PCC	Frequency (order of magnitude/year)
PCC1:Operational Transient	Permanent or frequent
PCC2:Anticipated operational occurrences	10^{-2} to 1
PCC3:infrequent accidents	10^{-4} to 10^{-2}
PCC4: limiting accidents	Less than 10^{-4}

Both Deterministic and Probabilistic Safety Assessment (PSA) methods are used in plant design review, and each may result in the addition of new mitigating systems. In France, PSA are used to review the deterministic design. They are performed during the original plant design, and revised periodically during plant life. Sequences of probability greater than 10^{-7}/y are systematically taken into account

4.2. Initial allocation

The AIEA NS-R-1 safety standards series defines the classification of systems of nuclear facilities according to their importance and provides examples of classification of main systems for various types of nuclear reactors.

The IEC 61226 standard explains how to classify the functions of a nuclear facility into categories (A, B, C and Non Classified).

The classification is independent of the technological nature of the systems which implements the functions, they can be for example computer-based, conventional (relays, etc.), electrical, mechanical, hydraulic systems … The importance for safety of a function is assessed by the consequences of its failure (e.g. its failure on demand) or of its spurious activation.

4.3. Allocation to components

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, whose assurance level is determined by the category (importance for safety) of function they support.

In France the response time required for the actuation of the function and the reactor states in which it operates determine its categorization. The NS-G-1.3 safety guide introduces temporal factors relevant to the case of computer-based systems such as:

- -the operating time required to the system once started;
- -the period during which alternative actions can be achieved;

- -the detection and correction time of hidden failures.

In most 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 computer-based I&C system which implements it (1, 2, 3). A computer-based system has to comply with design, manufacturing and qualification requirements relevant for its class. The equivalencies between class and category are the following:

Function Category	Computer-based 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

The standard describes the framework of the system design activities and its implications on architecture and functions of computer-based systems. When such a system or sub-system supports different functions of different categories, its classification must be relevant to the highest function supported.

IEC 61513 is the interpretation of the IEC 61508 standard in the nuclear domain. It has to be noted that although formally comparable, it has very different conceptual basis, given the existing framework explained before. Thus, a comparison between 61508 and 61513 standards is difficult. For example, concepts such as SIL and ASIL are not used. Appendix D of IEC 61513 summarizes the main differences in scope and concepts between the two standards:

« … *there is not an equivalent scheme to the reliability/risk reduction SIL levels proposed in IEC 61508 […] The assignment to "integrity levels" of IEC 61508 corresponds almost entirely with the categorization of the nuclear industry. However, there is a significant difference in the assignment procedure:*

• *in IEC 61508, the assignment to safety integrity levels is based on a probabilistic hazard and risk analysis;*

• *in IEC 61226, the assignment to categories is based on deterministic criteria and engineering judgement about consequences in case of malfunction.* ».

Before any design provision is taken at equipment level, the architecture of the system must fulfill requirements to favour defence in depth (redundancy, diversity, independence, etc.). In terms of basic functionality, there are four families of computer-based systems. They are usually structurally distinct and contribute to the global architecture of a nuclear facility. Major deterministic system 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			

As in other domains, there is a debate on whether requirements determine the category or the category determines the requirements. This debate stems partly from the lack of clear distinction between "functional requirements" and "functional assurance requirements". This suggests the following interpretation, which is not yet fully accepted:

- Basic "functional requirements" (i.e. those applied in the safety analysis) determine the category;
- The category determines "functional assurance requirements".

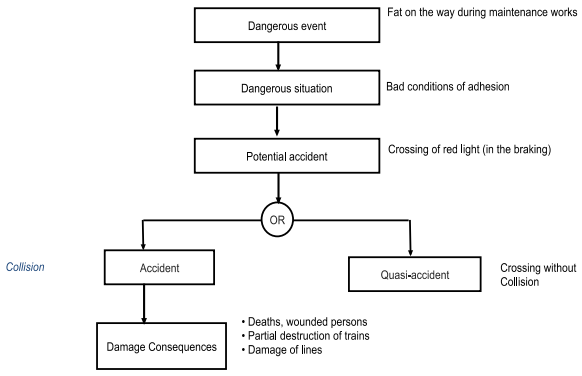
4.4. Dependability architecture and safety level

There is no way to reduce the level of an active function. Functions may only be upgraded in category or added. If an accident sequence appears to contribute to core-melting with a probability greater than 10^{-7}/y, then either an existing protection function is upgraded in category, or a new function is added to the plant.

5. Railway

5.1. Source of categories

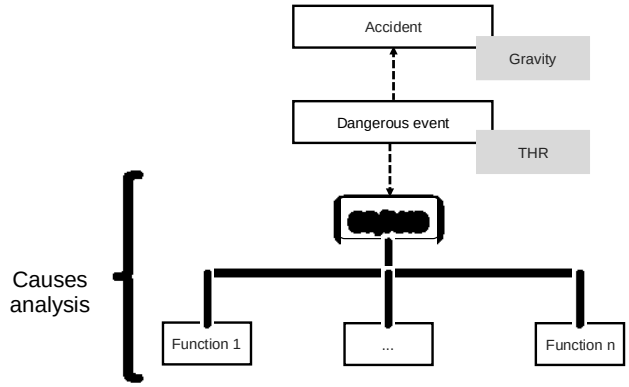
The first element considered in the railway is the dangerous event and the capabilities to go until the accident or the quasi-accident (see figure below).



For each hazard, the risk is estimated as the couple (severity frequency). The table below presents an example of risk matrix

* Frequency of occurrence of a hazardous event	Risk Levels			
Frequent	Undesirable	Intolerable	Intolerable	Intolerable
Probable	Tolerable	Undesirable	Intolerable	Intolerable
Occasional	Tolerable	Undesirable	Undesirable	Intolerable
Remote	Negligible	Tolerable	Undesirable	Undesirable
Improbable	Negligible	Negligible	Tolerable	Tolerable
Incredible	Negligible	Negligible	Negligible	Negligible
	Insignificant	Marginal	Critical	Catastrophic
	Severity Levels of Hazard Consequence			

For all intolerable and undesirable risks an action to reduce the risk is recommended. More concretely, for one accident, it is possible to identify the dangerous event and the function associated (see figure below)



5.2. Initial allocation

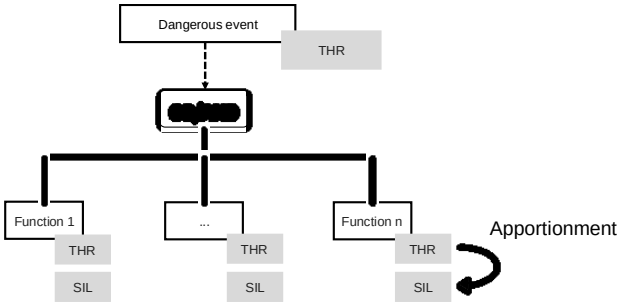
The standard EN 50129, derived from IEC 61508 through an instantiation to railway signalling systems, defines in a similar way the notion of levels, also called Safety Integrity Levels (SIL), linked to a probabilistic target called the Tolerable Hazard Risk (THR).

The THR is determined for each function (system, sub-system and equipment functions), which in turns determines the SIL of the corresponding system, sub-system or equipment and, based on analysis of the equipment architecture, the SIL is allocated to its hardware and software (it is then called a Software Safety Integrity Level (SSIL).

Same as in the IEC 61508, there are 4 levels of SIL, with 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). In general a system without SIL requirement is said “non-SIL”. Note that there are 5 Software Safety Integrity Levels (adding an explicit SSIL 0 for “no safety effect” to the IEC 61508 scale), ordered as in IEC 61508 from SSIL 4 (most dangerous) to SSIL 0 (no effect on safety).

5.3. Allocation to components

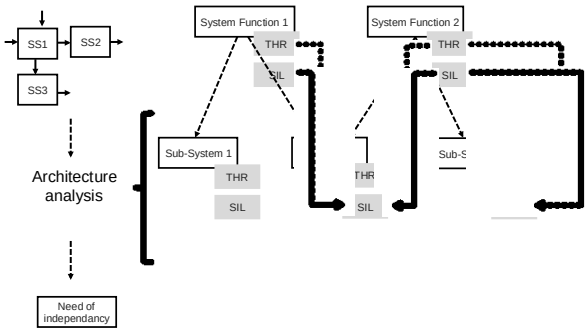
From the dangerous event, one can allocate some THR to the system function from the THR associated to the dangerous event.



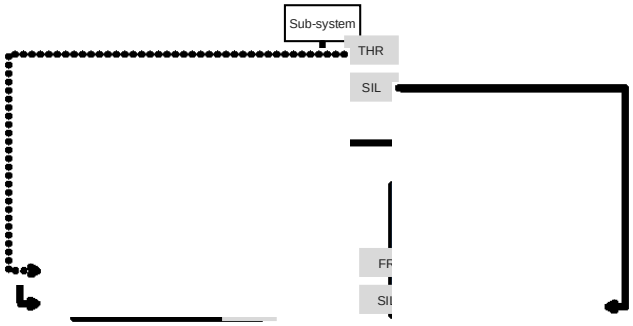
For the SIL apportionment, in the same way as IEC 61508, the close association between SIL and probabilistic targets (here THR) does not mean that a probabilistic assessment must be performed other than for random hardware failures (table below).

THR par heure et par fonction	SIL
$10^{-9} \leq$ THR $\leq 10^{-8}$	4
$10^{-8} \leq$ THR $< 10^{-7}$	3
$10^{-7} \leq$ THR $< 10^{-6}$	2
$10^{-6} \leq$ THR $< 10^{-5}$	1

The allocation from system to sub-system is presented in the figure below. We take into account the architecture and the sub-system independency and a sub-system can participate to many system functions and we affect the low THR and the high SIL to the sub-system.



The allocation from sub-system to equipment follows the same rule as for system to sub-system but we affect to the equipment a Failure Rate (FR) in place of THR and a SSIL for the software part.



5.4. Dependability architecture and safety level

There is no explicit indication in the standard on how to reduce the SIL in consideration of dependability architectural solutions, this being done following the basic principle i.e., through the analysis of the risks

associated to the potential failures of each considered element.

It's possible to allocate a low SIL to some equipment by taking into account the architecture and the independency of the equipment. But there is no explicit rule and a demonstration is needed.

6. Space

The relevant standards for space systems in Europe are the ECSS series (European Cooperation for Space Standardisation) coordinated by the European Space Agency. Of particular interest here are the ECSS-Q40 (Safety), Q30 (Dependability) and Q80 (Software Product Assurance).

6.1. Source of categories

The ECSS Q30 and Q40 define the source of categories as the end effects of the potential failures of the considered space system. These failures are categorised according to a ranking of the severity of their consequences, according to a four-level scale.

Interestingly the ECSS proposes indeed two three-level scales combined into a single consistent one:

- The first category (highest severity labelled 1, Catastrophic) corresponds to the most severe safety effects (loss of life etc.);
- The second category (2, Critical) combines critical safety effects (injuries etc.) and the most severe mission effects (mission loss);
- The third and fourth categories (3, Major and 4, Minor) correspond to effects only on the mission performance (no safety effect).

The categories are clearly defined taking into account only the severity and no probabilistic target is associated to these categories. However the standards require that such probabilistic targets be specified and met to comply to other applicable regulation schemes (this is the case for launch operations) or to the needs of each project.

6.2. Initial allocation

The allocation process starts at system level by the classification into categories of the system functions, based on the highest severity of the consequences that could result from their failures. These categories, for functions, are called "criticality categories".

It is worth noting that the same allocation process is applied also to the operations.

6.3. Allocation to components

Once the system functions (and operations) are categorised, this process being iterated along functional decomposition, the hardware and software products are themselves classified into categories, based on the simple general rule stating that a product is allocated the category corresponding to the highest criticality function among the possibly several functions associated to that product.

Here "product" is to be understood as a global consistent software or hardware entity, further refined into components. These components are themselves classified into criticality categories, following the same allocation approach i.e., by applying the same general and simple allocation rule based on the severity of the consequences of the potential failures of the considered component.

6.4. Dependability architecture and safety level

The ECSS standards do not describe explicitly how and to what extent it is possible to take into consideration the dependability architecture and adapt the allocation of safety categories to the elements of the system. This process is only supported by the general allocation rule. It is therefore necessary to analyse and justify on a case by case basis the propagation and impact of potential failures, taking into account the dependability architecture and mechanisms and the necessary independence arguments.

7. Synthesis

7.1. Source of categories

There are both differences and strong similarities across application domains in the source of categories and therefore on what they actually represent. All domains share the same fundamental basis where the categories represent the risks associated to the end effects of the potential failures of the considered system. Risks are classically measured by a combination of their severity and occurrence probability or likelihood. The fact that some domains focus more on the occurrence (e.g., railway, industrial automation) or on severity (e.g., space), or more explicitly on their combination, may be seen as a presentation choice. Indeed all domains rely on a similar scheme where there is one-to-one mapping between the severity and the maximum probability corresponding to the risk acceptability frontier for that severity. Therefore these notions can be considered as equivalent, provided the acceptability frontier is well defined.

However there remain differences, for instance in the acceptability frontier which may not be the same for all domains. This point is not easy to analyse in details, also because there are differences across domains in the definitions of the categories of severity (e.g., some domains consider different categories for a few and many deaths, or consider damage to environment or public or private property in same categories as injuries, etc.).

Another difficulty and difference comes from the fact that the characterisation of the risk occurrence does not only involve the causes internal to the considered system but also external causes which may be, according to the domain, taken or not into consideration for the evaluation of the category. This is the case for instance for the notion of “exposure” in automotive domain where two risks of same severity may be put in different categories whereas it is not the case in other domains such as aeronautics or space. Similarly the notion of “controllability” impacts the category in automotive, but here the aeronautics domain adopts partly a similar approach for instance by incorporating in the definition of a category the notion of “reduction of the capability of the crew to cope with adverse situations”, which may be interpreted more as a characterisation of occurrence than of severity of a risk.

7.2. Initial allocation and allocation to components

In aeronautics, nuclear, railway and space, the first categorised element of a system is a (top level) function, which inherits its category from the category of the risk induced by its potential failures. Then the categories are derived following the functional decomposition and finally allocated to the elements implementing the functions.

The situation is different for automotive where safety goals are defined for the identified risks, and further refined into safety requirements, and finally into architectural components. Categories are allocated first to the safety goals, and derived to safety requirements and finally components. This provides a different perspective and an interesting way of reasoning. However there is no evidence that it may result in practice in a different allocation as compared to other domains, because it relies on the same basic principles i.e., the consideration of the propagation and end effects of failures.

7.3. Dependability architecture and safety level

Concerning the way the standards address how and to which extent the dependability architecture and mechanisms may impact the allocation, one may distinguish three cases:

- Railway, space: the standards do not provide guidance, one must follow the generic allocation rule;
- Aeronautics, automotive: the standards provide detailed guidance and specific rules;
- Nuclear: not considered for allocation of categories.

However these three cases are not so different, considering that the detailed guidance and specific rules in aeronautics and automotive are intended to be compliant to the generic allocation rule. For nuclear the standards are specific to particular classes of systems with a general organisation such as the defence-in-depth principle. One may consider that the dependability architecture concepts as addressed e.g., at aircraft or spacecraft level, are also addressed in nuclear but at an upper level than the scope of the scope of a standard applicable e.g. to the protection system.

8. Conclusion, perspectives

The detailed analysis and comparison across application domains of the definition and allocation of safety categories show that the various schemes are not fundamentally different, and could be seen as various instances of a single consistent scheme. Of course there would remain difficulties e.g., in terminology or applicability of such or such specific rule, and there would remain also necessary differences. For instance one may understand that the loss or major degradation of mission performance are considered as more severe for an expensive long lifetime non repairable system (satellite) than in automotive.

A better understanding of the underlying rationale supports both the possible improvements and convergence of existing schemes, and the efficiency to develop systems, products or tools with easier adaptations to different schemes.

However this is an important part, but only a part of the complete picture because beyond the differences or similarities between the allocated categories, there may exist also differences or similarities in the rules applicable for the development and validation in various domains, for categories that seem to be similar as seen from their definition and allocation process. These aspects are also addressed by our CG2E working group as reported in [2], [3].

9. References

[1] 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.

[2] 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.

[3] 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.

[ANSI/ANS 51.1] Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants (1988).

[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., Parts 1 and 2
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 IEC 61508 Parts 1-7, Edition 2.0, 4/2010.

[IEC 61511] “Functional safety – Safety instrumented systems for the process industry sector.
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.

[IEC 62138] Nuclear power plants – Instrumentation and control important for safety –Software aspects for computer-based systems performing category B or C functions. Edition 1.0, 1/2004.

[IEC/TR61838] Nuclear power plants– Instrumentation and control important to safety– Use of probabilistic safety assessment for the classification of functions. Edition 2.0 2009-12.

[ISO 26262 “Road vehicles – Functional safety”
ISO 26262 Parts 1-9, first edition, 2011-11-15
ISO/FDIS 26262 Part 10, 2011-07-20

10. Glossary

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

FDIS Final Draft International Standard

E/E (/PE) Electrical/Electronic (/Programmable Electronic)

ECSS European Cooperation for Space Standardisation

ESA European Space Agency

EUROCAE European Organisation for Civil Aviation Equipment

FDAL Function Development Assurance Level

FDIS Final Draft International Standard

FHA Functional Hazard Assessment

FMEA Failure Modes and Effects Analysis

H&R Hazard analysis and Risk assessment

HAZOP HAZard and Operability studies

I&C Instrumentation and Control

IAEA International Atomic Energy Agency

IDAL Item Development Assurance Level

IE Initiating Event

IEC International Electrotechnical Commission

IRSN Institut de Radioprotection et de Sûreté Nucléaire

ISO International Organisation for Standardisation

NPP Nuclear Power Plant

PASA (Preliminary Aircraft Safety Assessment

PCC Plant Condition Category

PSA Probabilistic Safety Assessment

PSSA (Preliminary System Safety Assessment

QM Quality Management

RTCA Radio Technical Committee for Aeronautics

SAE Society of Automotive Engineers

SIL Safety Integrity Level

SSIL Software Safety Integrity Level

THR Tolerable Hazard Risk