Convergence of the Latest Standards Addressing Safety and Security for Information Technology

Adrien Derock [1,2,3], Patrick Hebrard[1], Frédérique Vallee[4]

1: DCNS – SIS – BP403 – F – 83055 Toulon cedex
2: Laboratoire IMATH, Université du Sud – 83000 Toulon
3: ESIEA – 9, rue Vésale – 75005 Paris
4 : MATHIX - ALL4TEC - Immeuble Odyssée - 2 -12 rue du Chemin des Femmes - 91300 Massy (France)

Abstract: Safety and Security have always been considered separately in most industrial process. Actually, there is a growing consensus that for many applications, Safety as well as Security demands have to be observed in a coherent manner. Risk analysis to counter malicious attacks can be also reused with appropriate modification for unplanned system failure.

Keywords: safety, security, convergence.

1. Introduction

For numerous years the “Software Safety” and “Information Systems Security” communities have been following their own ways with a few interactions.

This independence emerges when reviewing the standards issued by both communities until 2000-2005. Among them two major standards are well representative of each community:

- “Common Criteria” for Information Technology Security Evaluation [1],
- “ISO 61508” for Functional safety of electrical / electronic / programmable electronic safety-related systems [2].

To roughly summarize the differences between the two approaches described in these two standards, we can say that Information Security Community recommends a combination between “system specification audit” (inheriting from the historical MARION method developed by the CLUSIF in 1983) and “implementation requirement” for security, while functional safety approach is based on an adaptation of usual product risk management techniques associated to process requirements.
From their side “usual” product risk management techniques for programmable systems are well defined into the ISO/CEI 15026 standard [4].

This differentiation between security and safety is nowadays becoming unbearable because both aspects are more and more merged in modern complex systems such as Naval System for the particular case of DCNS or in other embedded communication systems (in Nuclear Power Plants for example). This is particularly true for complex system based mostly on software.

Recently, in 2008, a new international standard ISO/IEC 2700X [3] has been issued. This standard describes an information security risk management process and associated actions to help organizations of all types that are concerned by threats that could compromise their information security. And for the first time the security approach required by the standard ISO/IEC 27005 has many communalities with the risk management approaches required by the ISO/IEC 61508 family standards and that are the main topic of the ISO/IEC 15026 standard [4].

This convergence is worth to be mentioned and is the subject of this paper. Actually the harmonization of security and safety studies can be a source of productivity improvement for many companies.

The next sections will successively:

- briefly describe the security and safety standards that are examined in this paper,
- enlighten the communalities that can be found in both security and safety new standards,
- propose a generalised process approach that is consistent with most of the safety and security standards requirements,
- conclude by showing which benefits many companies could gain in harmonising their safety and security organisations (through DCNS perspective).

2. Short description of the selected security and safety standards

2.1 ISO 27005 standard

The ISO 27005 is the prime 27000 series standard covering information security risk management. It has been published in June 2008.

This standard provides guidelines for information security risk management (ISRM) in an organization, specifically supporting the general concepts of

information security management system specified by ISO 27001.

The ISO 27005 standard does not provide neither recommend a specific methodology. It is up to the organization to define its approach that will depend upon a number of factors, such as the actual scope of the Information Security Management System (ISMS), or the industry/commercial sector. The EBIOS 27005 methodology could be used for this purpose. [X]

The ISO 27005 standard is based on a risk management approach, i.e. it specifies a structured, systematic and rigorous risk management process from analyzing risks to creating the risk treatment plan.

The information security risk management process consists of:

- Context Establishment: intends to define the risk management's boundary
- Risk Assessment:
    - Risk Analysis (Risk Identification & Estimation phases): intends to define the assets, the threats and vulnerabilities and concludes by evaluating the risk level.
    - Risk Evaluation: takes into account the objectives of the organization and prioritizes the risks.
- Risk Treatment: to reduce, retain, avoid or transfer the risks.
- Risk Acceptance: to formally record the decision to accept the residual risks.

In parallel support processes are described, such as:

- Risk Communication: for exchanging and/or sharing information about risk between the decision makers and other stakeholders.
- Risk Monitoring and Review: to maintain an overview of the complete risk snapshot.

2.2 ISO/IEC 61508 family standards

The Created in European version by CENELEC in 2002 as EN 61508, the IEC 61508 standard has its origins in the process control industry sector. It is intended to be a basic functional safety standard applicable to all kinds of industry. This standard sets out a generic approach for all safety lifecycle activities for systems comprised of electrical and/or electronic and/or programmable electronic components (electrical/electronic/ programmable electronic systems (E/E/PESs)) that are used to perform safety functions.

Functional safety is defined in the IEC 61508 standard as: "part of the overall safety relating to the EUC (Equipment Under Control) and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities."

The safety lifecycle described in the standard covers all activities needed for an E/E/PES system development and use, going from initial design until decommissioning through development, installation, and operation phases.

The safety approach is based on risk prevention and the system SIL (Safety Integrity Level) determination classified on a 4 degrees scale going from SL1 (the less critical) to SIL4 (the most critical).

For the 2 more critical levels (SIL 3 and SIL4), the standard is very stringent regarding the number and variety of techniques that must be applied. Moreover these techniques are not always consistent and often very costly to operate in usual industrial contexts. When the system is not a pure safety system (i.e. implementing a "safety" dedicated function such as "nuclear emergency stop" for example) but only a safety-related system (as in numerous embedded automotive systems for example), the notion of safety function described in the ISO/CEI 61508 standard is not very easy to handle.

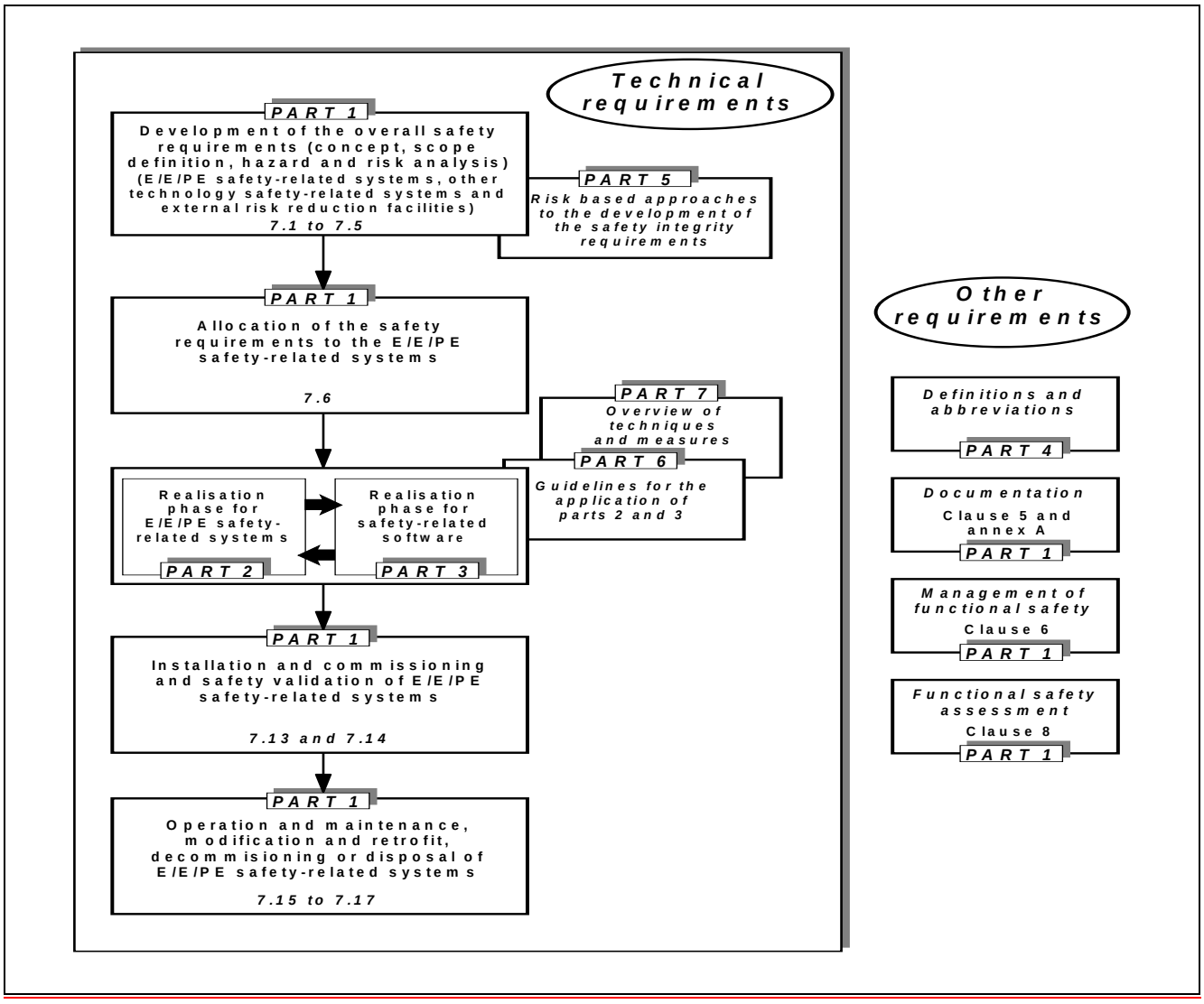

Figure 1 :Safety requirements

As it was designed to be a generic standard, the IEC 61508 standard has quickly led to several derivatives more adapted to specific areas.

This has resulted in what we call the “ISO/IEC 61508 family” that is regularly enriched and consists today among others in:

- the CEI 61511 standard for industrial processes,
- the CEI 61513 standard for the nuclear sector,
- the CEI 62061 standard for the safety of machines,
- the CEI 62304 [5] standard for medical device software,
- the future ISO 26262 [6] standard for the automotive sector …

2.3 ISO/IEC 15026 standard

The ISO/IEC 15026 standard introduces the concepts of software integrity levels and software integrity requirements. It defines the concepts associated with integrity levels, defines the processes for determining integrity levels and software integrity requirements, and places requirements on each process.

It does not prescribe a specific set of integrity levels or software integrity requirements that can be established either on a project by project basis or for a specific sector.

The risk management process required by the ISO/IEC 15026 consists of:

- Risk Analysis: covering threat identification, frequency analysis, consequence analysis and leading to risk calculation.

- Risk Evaluation: concluding with tolerability decisions.
- Risk Control: consisting in System Integrity Level determination, software integrity level determination and concluding with software integrity requirements determination.

2.4 Advantages of ISO/IEC 15026 versus ISO/IEC 61508

Using the ISO/IEC 15026 standard instead of the ISO/IEC 61508 standard brings the advantage to avoid the burden of the second standard as described in paragraph 2.2.

In the ISO/IEC 15026 standard, an integrity assurance authority is indeed in charge of assessing the compliance of the system with its integrity requirements.

Once the safety integrity level determination has been correctly done and assessed by the integrity assurance authority, each industrial may define the techniques that are the most appropriate to its context. The only requirements to fulfil is again to get the assessment of the integrity assurance authority on the set of techniques proposed to achieve the degree of confidence necessary for each integrity level.

3. Comparison between ISO 27005 and ISO 15028

The first important communality to highlight is that both standards are fundamentally based on a “risk management oriented” approach.

This ISO 27005 summarizes its approach in the following figure:

.

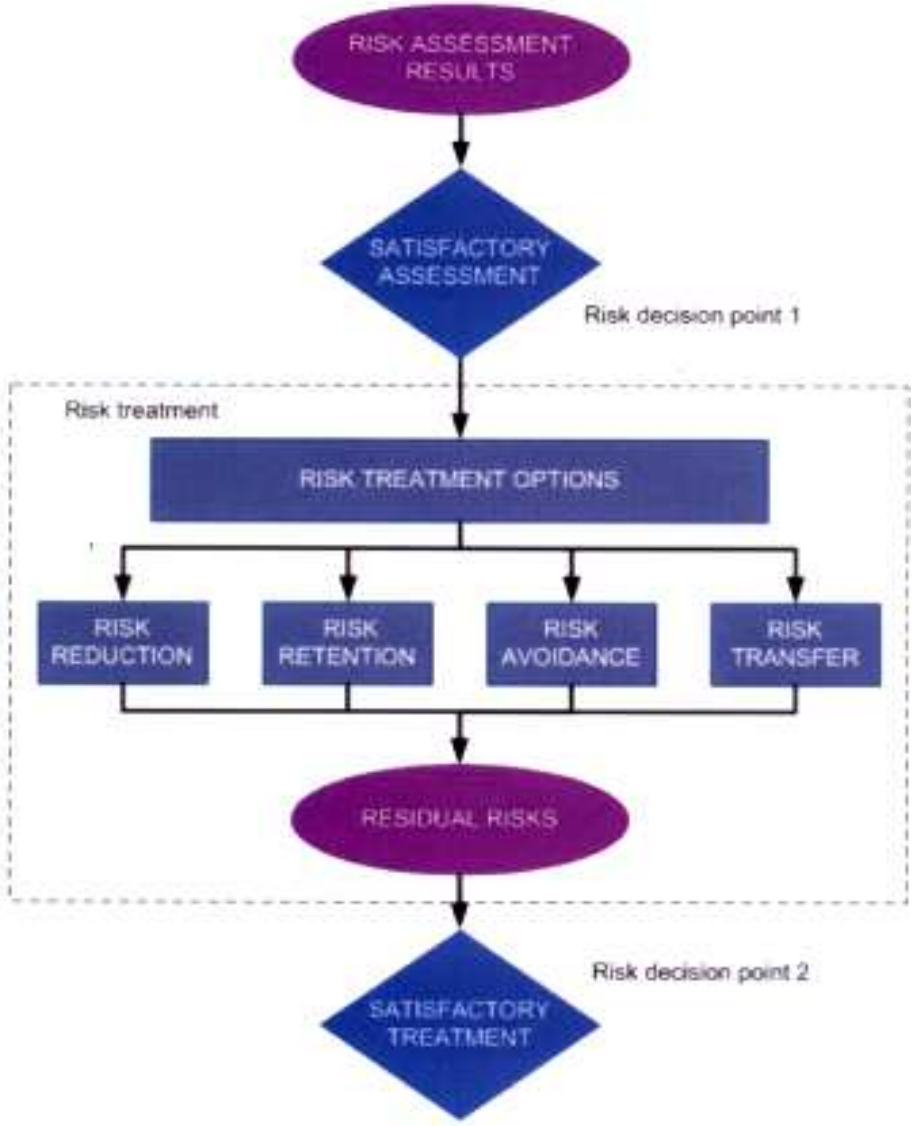

Figure 2 : ISO 27 005 process

And besides, the ISO/CEI 15026 standard describes its approach through the following figure:

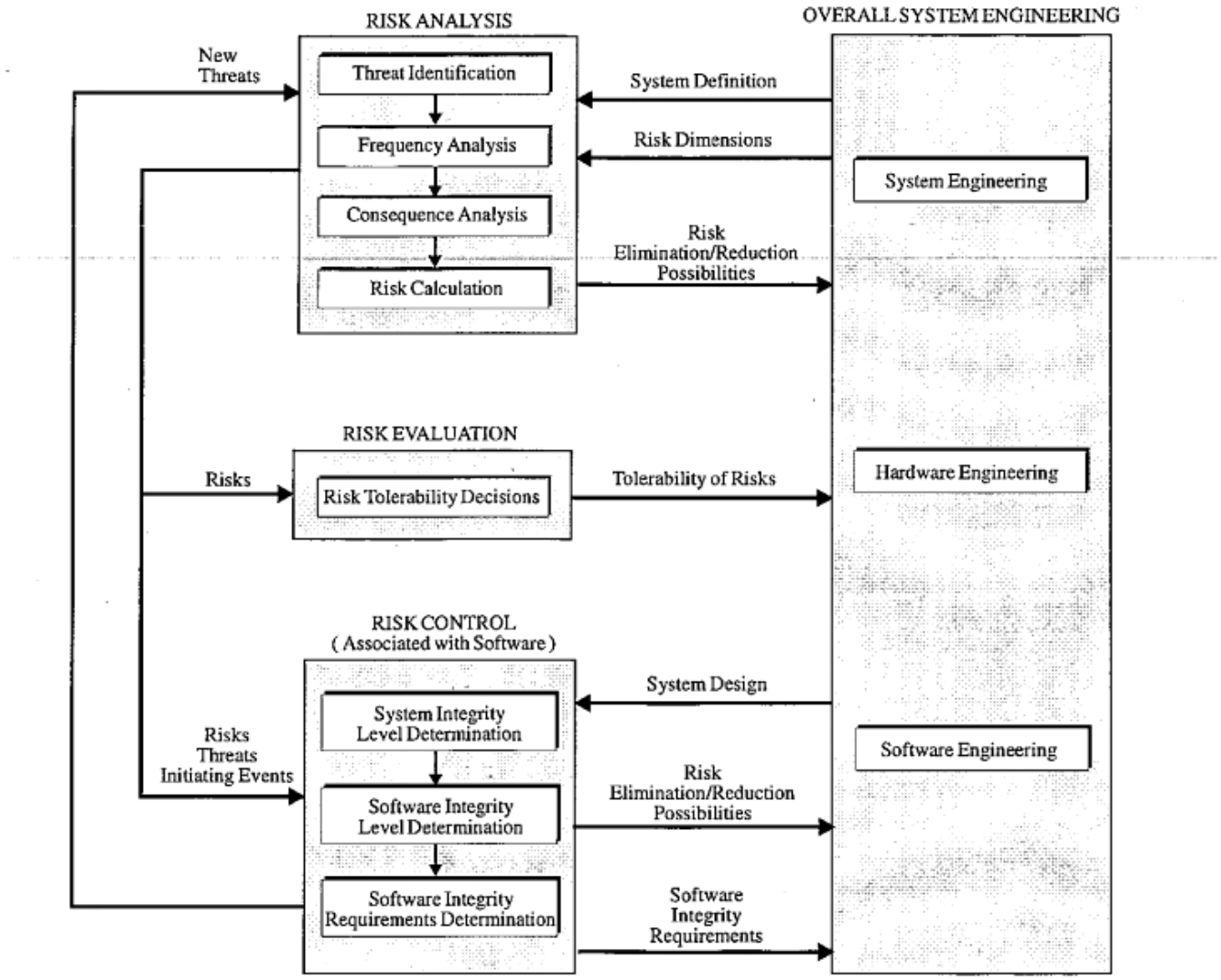

Figure 3 : ISO 15026 Standard

Another important communality is that the processes required by both standards are very similar and can be easily merged into a unique “generalized safety process” as it is explained in the following section.

1. Generalised safety process

In order to harmonize the safety and security processes at DCNS, a “generalized safety process” has been designed. The main phases of this process are:

- Definition and scheduling of safety activities
- Preliminary hazard analysis
- Risk analysis during the specification phase
- Risk analysis during the design phase
- Transfer of safety requirements
- Verification of safety requirements fulfilment on components
- Verification of the test phases
- Closure of the safety process

All activities required by both ISO/IEC 15026 and ISO 27005 are covered by the “generalized safety process”. The traceability is given in the following comparative figure:

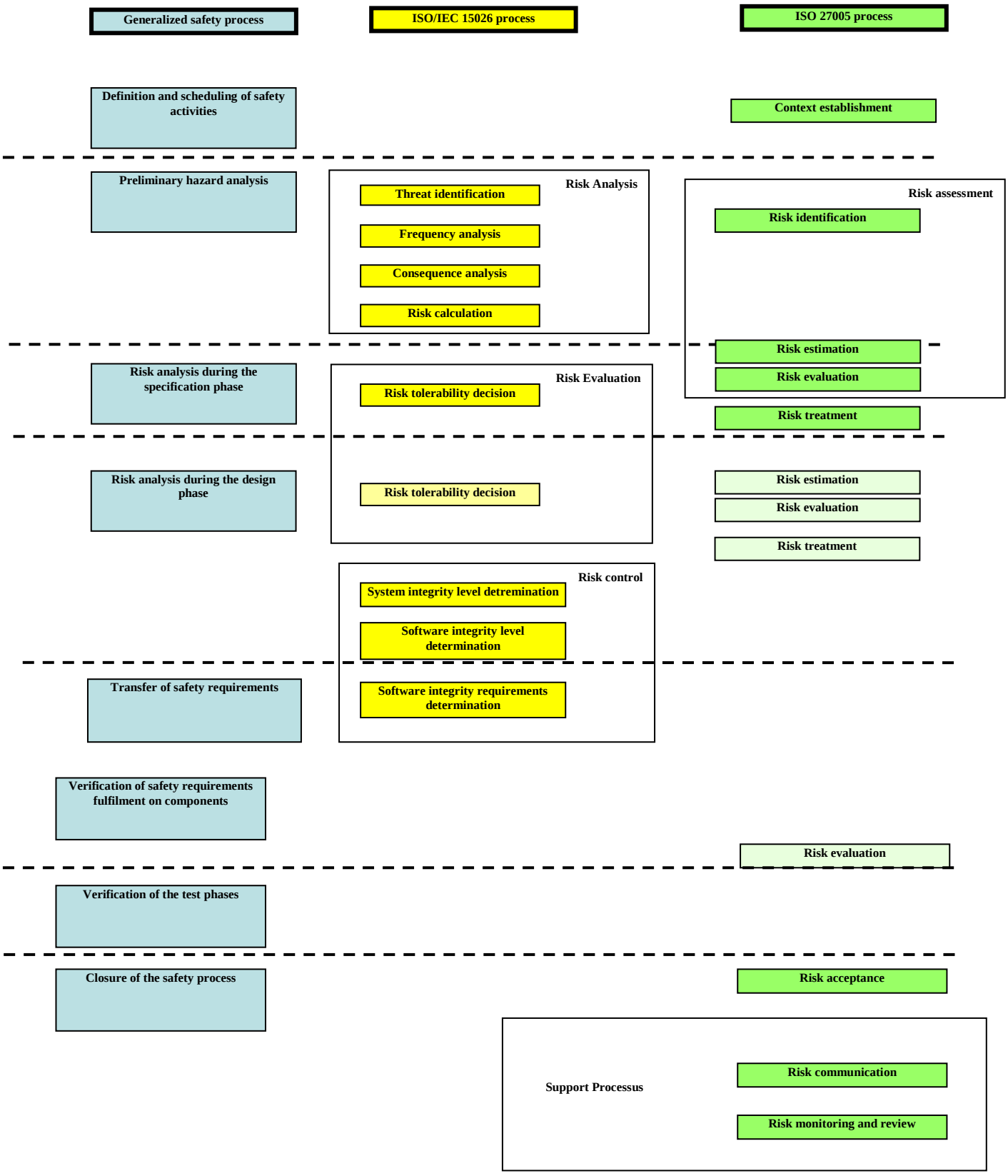

Figure 4 : Convergence between ISO27005 and ISO15026

The previous diagram show clearly the convergence announced between ISO 27005 and IEC 15026. That convergence enables the risk manager to operate as well in the security point of view during the analysis to prevent malicious attacks as in the safety point of view to prevent from unplanned system failure.

It is however important to notice that this parallelism between security and safety standards has been made feasible only provided that a common vocabulary is set up between the two areas. For example:

- « high level assessment » described in § 8.1 of ISO 27005 is comparable to « risk analysis during the specification phase »,
- « next iteration further in depth » also described in § 8.1 of ISO 27005 is associated to « risk analysis during the design phase »,
- the concepts of “primary assets” and “supporting assets “ used by ISO 27005 are equivalent to the concepts of “functions” and “organs” used in system engineering,
- etc.

From a process point of view; the ISO/IEC 15026 does not require support processes such as « communication » or « monitoring and review » in the ISO 27005 standard. However these processes are taken into account by the ISO/IEC 61508 family standards.
Inversely some other useful support process such as “change management” should be taken into account into the ISO 27005 standard.

4. Benefits of the convergence

As new technologies become increasingly complex, the need to merge security and safety processes in a common analysis process is crucial.
The convergence is mainly useful to reduce analysis time and cost for security and safety. To be efficient, only one engineer should work on both. He should have both expertises to achieve his task. Indeed, the analysis tasks for a system require being aware of all specification and conception data. This requirement takes a long time, especially in a complex system. This task done for safety is so not required for security.

An other benefit is the simplification of the project organization. The process is unique between safety and security. The interlocutor is also unique.

The third advantage is the proposition of recommendation coherent between the safety needed and the security needed. For example, in naval ship, a local must be always closed if there are some sensitive cryptographic algorithms processing inside. This is a main security requirement often proposed as recommendation. In the safety point of view, in certain condition, the door of the local will be demanded to be kept opened to permit the evacuation in case of fire. These two recommendations are antinomic but expected. Only the risk analysis even though in security and safety point of view will find the recommendation so needed.

5. Conclusion

This paper has provided guidelines to manage to create a unique process for safety and security. This process give immediate and long term benefits for companies. DCNS uses this approach without trouble for all project demanding safety and security analysis. In the future, we expected a more pronounced convergence by the emergence of a unique and global standard addressing security and safety.

5. Acknowledgement

We would like to thanks MATHIX Company for helping DCNS to build the adapted safety/security process.

7. References

[1] ISO/IEC 15408 - Common Criteria for Information Technology Security Evaluation

[2] ISO/IEC 61508 - Functional safety of electrical/electronic/programmable electronic safety-related systems (March 2002)

[3] ISO/IEC 27005 – Information Technology – Security techniques - Information security risk management (first edition – 2008-06-15)

[4] ISO/IEC 15026 – Information technology - System and software integrity levels (1998)

[5] ISO/IEC 62304 – Medical device software - Software life cycle processes

[6] ISO 26262 – Road vehicles - Functional safety

8. Glossary

Acronyms	*Significations*
CEI / IEC	*Commission Electronique Internationale / International Electronical Commission*
CLUSIF	*CLUb des Systèmes d’Information Français*
CMS	*Combat Management Systems*
DCNS	*Direction de Constructions Navales*

Acronyms	*Significations*
E/E/PE	*Electrical/Electronic/ Programmable electronic*
ISO	*International Standard Organisation*
SIL	*Safety Integrity Level*