Disentangling the relations between safety and security

PIETRE-CAMBACEDES LUDOVIC[1,2], CHAUDET CLAUDE[2]
[1]Electricité de France R&D
1, avenue Général de Gaulle, 92141 Clamart
[2]Institut Telecom, Telecom ParisTech, LTCI CNRS
39, rue Dareau, 75014 Paris
FRANCE
{pietreca, chaudet}@telecom-paristech.fr

Abstract: This article aims at a finer apprehension of the relations between safety and security, which are intrinsically and increasingly intricate. We introduce a new conceptual framework to better capture their moving perimeters. Then, we present our on-going work to characterize safety and security interactions, varying from reinforcement to strong antagonism. A property decomposition analysis and its limits are discussed; research tracks are finally identified.

Key-Words: Security, safety, dependability, computer security, safety systems, SIS, industrial control systems

1 Introduction

Safety and security are both key issues in most industries today, as reflected by the sheer quantity of related standards and investments. They have long been considered as separate issues and dealt by different communities. If their intimate relation is now admitted [1,2], fostering all-hazards approach and shared efforts, it has still not been clearly characterized. For instance, whereas security and safety objectives may seem convergent, their concretization can turn out to be antagonistic in some cases [3]. This finds a simple physical illustration in the "exit doors dilemma": the number of emergency exit doors left opened in a building should be kept at its maximum in one perspective, and to its minimum in the other.

The rising convergence of safety and security issues makes us believe that it is worth characterizing more thoroughly their relations. It is particularly the case for computerized systems used in risk-prone industries, where safety systems are being exposed to new security risks associated to digital technologies and their growing interconnectivity [4]. These systems, formerly isolated and dedicated, will have to be protected with specific security measures. In this context, the identification of potential side-effects involved by such cohabitation, and more generally, a good understanding of the safety and security interdependencies have become a critical issue. This paper is an attempt to organize the concepts needed for such project, pointing out the deficiencies of the common formalisms and suggesting new basis and related research tracks to tackle this challenge.

A first step consists in identifying the limits between safety and security. Section 2 discusses their usual definitions and suggests a new conceptual framework to overcome the identified ambiguities. The second step involves a good understanding of their macroscopic similarities and differences, then a first grasp and classification of their potential interactions, which are presented in Section 3. At this stage, different approaches are possible. Section 4 suggests analyzing safety and security relations through their classical constitutive properties. The limits of this initial approach and other tracks are identified to conclude in Section 5.

2 An ambiguous conceptual framework

2.1 Sorting the definitions confusion

A first level of ambiguity appears in the definitions themselves. Security and safety can have different meanings depending on the context. Their signification can even swap from one industry to the other or merge in certain languages [5]. A literature and standards survey leads to tenths of different definitions. However, two distinctive paradigms emerge and allow a first classification. The first one, called S-E later on, is based on a System vs. Environment distinction, where the system can be arbitrarily large, and the following definitions, adapted from [1,5]:

- *Safety* characterizes the inability of the system to have an undesired effect on its environment;
- *Security* denotes the inability of the environment to have an undesired effect on the system.

The second paradigm, called M-A later on, distinguishes malicious and accidental events [6]:

- *Safety* designates the degree to which accidental harm is prevented, detected and reacted to;
- *Security* designates the degree to which malicious harm is prevented, detected and reacted to.

Most of the literature dealing with security and safety is based on definitions, sometimes implicit, that can be brought back to one of these two paradigms.

2.2 The two dominant paradigms inconsistency

Figure 1 represents the crossing of the S-E and M-A paradigms. Unfortunately, it is easy to see that they are only partially consistent. Quadrants 1 and 3 belong respectively to security and safety without any ambiguity; quadrants 2 and 4 are much more equivocal and can be considered either as safety or as security relevant, depending on the paradigm considered.

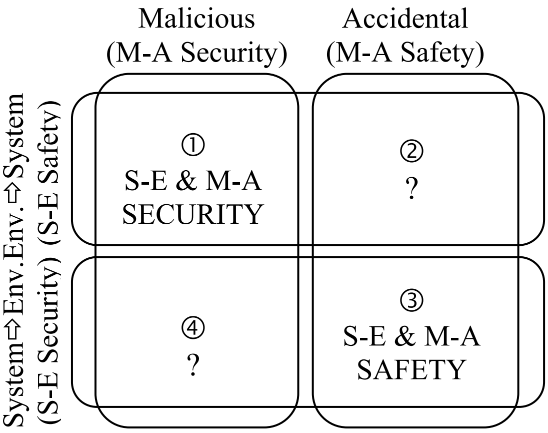

Figure 1: Crossing the S-E and M-A definitions.

2.3 Towards a new and sound framework

To overcome these inconsistencies, we suggest naming explicitly the notions captured by each quadrant of Figure 1, and creating, from this basis, a new hybrid paradigm. This paradigm, which integrates both the S-E and M-A dominant approaches, distinguishes:

- *Defense*, dealing with external (*i.e.* coming from the environment) malevolent actions on the system;
- *External Accident Protection*, concerned by protecting the system against external accidents consequences;
- *Accidental Safety*, aiming at limiting the incidence of non-malicious system faults on the environment.
- *Safeguards*, dealing with the limitation of malicious actions impact from the system on the environment.

Moreover, in order to complete the framework, System to System, *i.e.* strictly internal events, should also be considered by introducing:

- *Internal Sabotage*, designating issues related to internal malicious actions on the system;
- *Robustness,* covering non-intentional internal faults with no harm to the environment.

Note that a given situation may be relevant to different domains depending on the focused system and its boundaries definition. This new paradigm, composed of the six disjoint notions previously defined is represented on Figure 2and will be denoted by the acronym SEMA.

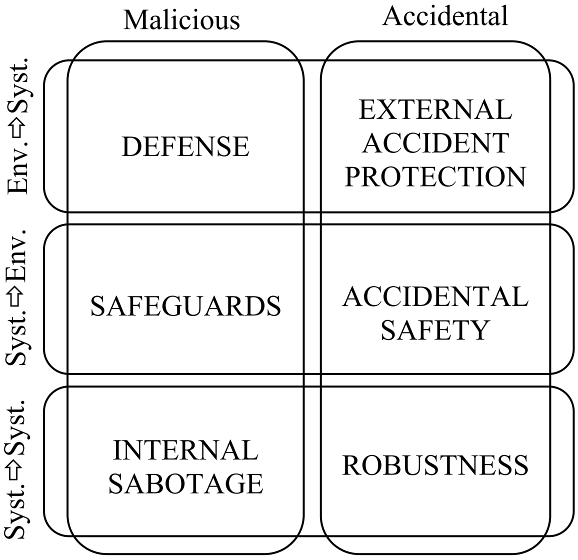

Figure 2: The SEMA paradigm.

The SEMA paradigm is neither aimed at replacing the common and historical definitions of safety and security, nor at competing with attempts to redefine them consistently (e.g. [7,8]). We rather expect it to provide a fast analysis framework allowing a better understanding of these moving notions' perimeters. The plasticity of the terms security and safety calls for systematic preliminary definitions, for which SEMA is intended to provide a useful reference. This paper provides a relevant basis for a first illustrative application of this principle. In the following sections, when not specifically refined by SEMA notions, the generic term security will encompass defense and internal sabotage issues; whereas safety will cover accidental safety and safeguards, especially when human life, loss of equipment or environmental damage is at stake.

2.4 Introducing the cyber-dimension

The notions of safety and security have been so far considered in a generic context. The situation is somehow different for digital networked systems. If their security, often called cybersecurity, is subject to the same equivoques as in the physical world, safety is not a commonly used word (except in distributed systems formal specifications [9]). Nevertheless, the underlying SEMA notions are also relevant in this case, and despite some reserves, the overall SEMA paradigm and its conceptual slicing are applicable to the digital world.

Distinguishing cyber and physical dimensions allows the identification of dependencies between physical and cyber security, but also between cyber security and physical safety, being accidental safety or safeguards in SEMA. Moreover, this distinction is especially relevant to analyze safety and security relations in the context of the growing cyber security concerns for digital safety systems in risk-prone industrial installations.

In complement to the conventions proposed for the generic terms safety and security in section 2.3 and their matching with SEMA, security will refer by default in this paper to both physical and cyber aspects, whereas safety will refer to its physical dimension.

3 A macroscopic analysis

3.1 General similarities and differences

3.1.1 Some fundamental similarities

A first common point between security and safety, regardless of the considered paradigm, is that they are both articulated around the notion of risk. In both cases, risk is defined by the macro-formula: *risk = f (likelihood, consequences)*. However, the nature of risk and its origin differ, mainly along the paradigms previously discussed; different risk assessment and management methodologies have been developed to address this diversity (cf. §3.1.2).

Another significant similarity is that neither security nor safety are directly composable or cumulative [10]: two safe or secure components do not necessarily constitute a safe or secure system, two barriers or counter-measures do not necessarily add their effects. For security, this may even reduce the overall level of security in some cases [11].

3.1.2 Some major differences

The natures of the considered threat agents are very different. Malicious actions imply intelligent attackers, with adaptive behaviors and potentially unknown (and in some cases changing) skills, resources and motivations. On the other side, protection against accidents deals with blind and random failures. System parameters or laws are often known and considered constant.

Accidental safety is generally considered as a mature discipline, with an established mathematical toolbox where Probabilistic Risk Assessment (PRA) plays a key role. Security is still very much comprehended with qualitative tools, the pertinence of quantitative methods to model intelligent attacks being a controversial debate [12]. In particular, the use of probabilities to define likelihood or chance of success is not straightforward to model attacker behaviors and dynamical parameters.

A related difference concerns the granularity used to qualify gravity, which tend to be coarser in security than in safety. The attacker potential is much more difficult to evaluate once the first sign of breach has been detected. This is especially manifest in cryptography, where a purely theoretical weakness is enough to consider an algorithm as “broken”. In safety, clear multi-levels scales are commonly adopted: e.g. the DO-178B [13] used in civil aviation has 5 levels of gravity, whereas the International Nuclear Event Scale has 7 levels [14].

3.1.3 A cross-fertilization already started

The proximity of the two domains has incited exchanges between both communities and already led to concrete developments. The attack trees popularized at the end of the 90’s [15], and still at the basis of numerous studies in security, have been directly adapted from fault-trees, widely used in safety since the 70’s. More recently, safety cases typically required by regulations have inspired, through a goal-based approach, assurance cases for security [16]. Reciprocally, the notion of security kernel for computer systems has been adapted successfully in safety-applications [17]. The concept of defense-in-depth illustrates the permeability between these domains: applied to sites defense in the military world for centuries, nuclear safety has integrated it more recently, before inspiring back computer security architects. We believe there is still a huge potential to explore in these cross-fertilizations (see [18] for a recent contribution on this area), which may help to integrate safety and security issues in common models.

3.2 A first generic relations classification

Characterizing the relations between safety and security requires going beyond their similarities and differences. Illustrated by different examples, their interactions, when they exist, can globally and empirically be classified into three kinds.

3.2.1 Conditional dependencies

The safety of risk-prone industries relies increasingly on digital systems. Malicious modifications or denial of access to their commands or to the data supporting their decisions can be critical in accidental sequences. Cyber-security is here a necessary condition for safety. Strong interconnection and mutualization tendencies reinforce this dependency: for instance, in-flight entertainment data and airflight data will most presumably share the same media in next generation carriers [19].

3.2.2 Antagonism

Safety and security measures can have antagonistic effects. The emergency exits dilemma presented previously illustrates such a situation, which can be translated in network architecture area: remote maintenance access can enhance the reliability and efficiency of safety-related systems, they introduce at the same time new vulnerabilities, directly exploitable by potential attackers. As another general example, redundancy introduced for safety purposes may in some cases increase the attack surface to protect [20]. The same applies for diversity [21]. In the physical world, following the 9/11 terrorist attacks, reinforced security measures, including anti-aircraft missiles and heavy weapons for guards, have been proposed for nuclear power plants [11], entering in conflict with sites safety.

3.2.3 Mutual reinforcement

Some measures can also be beneficial both in terms of safety and security. For instance, a fine-grain event and activity logging is a common basis for attack and accident anticipation, as well as post-event analysis. An enhanced maintainability may also be interesting on both plans, allowing for example up-to-date cybersecurity patching and a better reliability of safety-functions.

Static-code analysis is another good example of a technical measure being able to enhance both safety and cybersecurity by identifying errors that may lead to security vulnerability or hazardous behaviors.

4 Going deeper: the property approach

Unfortunately, if the generic classification proposed in the previous section may help to realize the scope of the different possibilities, it is not possible to systematically match a given measure to a given category. For instance, diversity has been cited as having potentially antagonistic effects, being in favor of safety but augmenting the attack surface, thus degrading security.

This is not always the case being in fact conditioned by the architecture considered: diversity can even be beneficial when used in consecutive lines of defense. Using two different firewall providers when designing cybersecurity architectures has become a common good practice. As stated in subsection 3.2.3, static code analysis can enhance safety and cybersecurity but contrary side-effects are possible. The critical vulnerability found in the cryptographic key generator of the OpenSSL library in 2008 had been introduced following such an analysis [22].

Finally, some measures seem to involve simultaneously several kinds of interactions, for specific aspects of safety or security. In fact, the global approaches so far adopted may be overcome by decomposing safety and security into their constitutive properties and examining their relations.

4.1 Safety and cybersecurity classical properties

Indeed, safety and cybersecurity can be decomposed into narrower notions. In particular, a widely accepted definition of security in the field of information technology is given by the ISO [23] as preservation of confidentiality, integrity and availability, with:

- *Confidentiality*: the property that information is not made available or disclosed to unauthorized individuals, entities, or processes;
- *Integrity*: the property of safeguarding the accuracy and completeness of assets;
- *Availability*: the property of being accessible and usable upon demand by an authorized entity.

Safety may also be considered as a global resultant of several properties. For risk-prone industries, it is directly linked to the dependability of the components in charge of preventing or limiting the consequences of mishaps. More precisely, such components have to be ready to ensure correctly their safety-functions when needed. Their integrity and availability are necessary conditions, which correspond also to cybersecurity properties. The IEC defines reliability and maintainability as two availability influencing factors [24], with:

- *Reliability*: the ability to perform a required function under given conditions for a given time interval;
- *Maintainability*: the ability of an item to be retained in, or restored to, a state in which it can perform a required function, under given use and maintenance condition

With safety and cybersecurity globally in mind, a group of five "classical" properties, namely *Confidentiality, Integrity, Availability, Reliability* and *Maintainability*, should be finally considered. Three kinds of possible interactions have globally been identified between safety and security, with the limits already stated. The following logical step is to check if such relations can be more easily identified at the property scale.

4.2 Potential intrinsic properties relations

In a first approach, we may wonder if the identified properties have intrinsic relations that could be systematized. Such intrinsic relation characterizes for instance the False Match Rate and the False Non-Match Rate of a given biometric technology, leading to choose an operational trade-off between security and usability [25]. By reviewing the different examples and situations discussed in Section 3 through the prism of properties, we can empirically infer some inter-properties relations stated in Table 1, in which // represents an independence, >/< an antagonism, ↔ a mutual reinforcement, ← means "depends on" and → stands for "contributes to".

Table 1: Relations between "classical" properties

	Confid.	Integrity	Availab.	Reliab.	Maint.
Conf.		//	>/<	>/<	>/<
Integrity	//		↔ >/<	↔	↔ >/<
Availab.	>/<	↔ >/<		↔	←
Reliab.	>/<	↔	↔		←
Maint.	>/<	↔ >/<	→	→	

Regrettably, some cases have several possible relations. Moreover, the indicated ones only reflect the considered examples, under subjective judgment, and can be opposed counter-examples in almost every case. In fact, classical properties do not seem to be articulated along intrinsic and systematic interactions.

4.3 Extrinsic properties relations

If no intrinsic relations seem to exist, the inter-properties relations may be extrinsic and have external causes, namely the security or safety measure considered. In this perspective, security and safety measures should be first grouped and classified in order to structure the analysis of their impact on safety and security properties. Of course, this is a challenging task for which several works have already paved the way (e.g. [2,26,27]), but more challenging is the decision about where the decomposition should stop. If we consider only fault-tolerance for safety systems, redundancy and diversity appears to be two major kinds of techniques, and their impact on security properties could be studied at this level [28]. Looking at redundancy, one may distinguish in a first approach hardware, software, temporal and informational redundancy. Each of these can in fact be further decomposed: hardware redundancy is either static (e.g. with voters) or dynamic; software redundancy can be based among others on N-version approaches or on replication, which itself can be decomposed in active, semi-active or passive [29]. Diversity can also be declined in numerous variants [28]. Regarding security, a coarse categorization of measures would include segmentation, filtering, authentication, authorization, monitoring or encryption, but finer and numerous kinds of functional measures and security controls could be considered [26], as well as technical solutions such as firewalls, anti-viruses, intrusion detection systems etc. Once a complete catalog of measures established, their effects on the properties have to be jointly evaluated, allowing the identification of potential antagonisms, reinforcements and dependences. Several approaches are then possible and discussed in the last section.

5 Conclusion and perspectives

Safety and security are intimately associated, but characterizing their relations with rigor is still to be done. The tremendous evolution of digital systems and their use in risk-prone industries make this better characterization crucial, as safety-related systems are getting exposed to new cybersecurity risks. This article has presented preliminary work in this direction.

Based on the most common definitions of safety and security, grouped into the System vs. Environment (S-E) and Malicious vs. Accidental (M-A) paradigms, we have devised a new referential framework, SEMA, allowing a consistent and integrated view of these notions, and supporting less ambiguous definitions. Fundamental similarities and differences between safety and security have also been discussed and a global classification of the possible interactions established. We have then adopted a finer grain approach, based on their constitutive properties as a new prism to analyze their interactions. The work done is only preliminary, though, and several problems are still to be solved.

The first problem deals with the properties joint evaluation: appropriate metrics should be defined, allowing objective identification of antagonisms, reinforcements and dependencies. Nevertheless, such definition, especially for security, is still a controversial issue and an active field of research [30].

The second one is about the properties themselves. The relevance of the five classical properties initially identified is questionable, and more rigorously defined properties could lead to better results. But if commonly agreed probabilistic forms exist in safety [31], security still lacks such formal and globally accepted properties and policy models. Among the numerous alternatives [32,33], *non-interference* has already been considered as pivotal notion between safety and security [20,34] and may support exploring their interactions.

Alternatively to formal properties, a more pragmatic approach might be to reason in terms of global system missions, in a goal-oriented approach, with assurance cases [16] encompassing security and safety objectives, and conditioned by quantitative thresholds or qualitative statements. For instance, such pragmatic properties would correspond, in the case of a communication network supporting safety functions, to maximum transmission delay, integrity assurance, or bandwidth reservation, needed to satisfy the safety cases. Computer network simulators (cf. for instance [35]) may then be used to evaluate the impacts of different measures on these needed properties.

Addressing both formal and pragmatic preoccupations, a perhaps more promising perspective to explore would be to extend a modeling language used in safety studies, like Figaro [36] or AltaRica [37], in order to integrate security considerations. These languages enable the definition of rigorous system models, which can then be used to simulate different behaviors and quantify safety-related properties. Extending them to integrate security properties would constitute a powerful step towards a better understanding of safety and security relations. In a similar way to safety-patterns [27], security patterns [38] could in addition be defined in these formalisms and used in the analysis. Such modeling languages appear as a solid basis to conciliate rigorous formalization and pragmatic quantifications and simulations.

Finally, any decomposition in properties, whatever their nature, is a subjective choice which goes with inherent limits of coverage. Moreover, it is most likely that the chosen properties to observe overlap several SEMA dimensions, stressing the importance to keep a global and systemic approach.

References:

[1] O. Nordland, Safety and security - two sides of the same medal, *European CIIP Newsletter*, Vol.3, No.2, 2007, pp.20-22

[2] A. Avizienis, J. Laprie, B. Randell, et C. Landwehr, Basic concepts and taxonomy of dependable and secure computing, *IEEE Trans. on Dependable and Secure Computing,* Vol.1, No.1, 2004, pp. 11-33

[3] G. Deleuze et al., Are safety and security in industrial systems antagonistic or complementary issues?, in *Proc. ESREL 2008*, Valencia, Espagna.

[4] T. Stauffer et C. Fialkowsi, Safety & Security: Can you have the best of both worlds?, *Proc. of the ISA 64th Annual Instrumentation Symposium for the Process Industries*, Texas, USA, 2009.

[5] M.B. Line, O. Nordland, L. Røstad et I.A. Tøndel, Safety vs. Security, *in Proc. of PSAM'06*, USA.

[6] D.G. Firesmith, Common Concepts Underlying Safety, Security, and Survivability Engineering, *CMU/SEI Technical Note No. 033*, 2003.

[7] G. Stoneburner, Toward a Unified Security-Safety Model, *IEEE Computer*, Vol. 39, 2006, pp. 96-97.

[8] E. Jonsson, Towards an integrated conceptual model of security and dependability, *Proc. ARES'06*, *IEEE,* pp. 646-653.

[9] E. Kindler, Safety and Liveness Properties: A Survey, *EATCS-Bulletin*, Vol. 53, pp.268-272, 1994

[10] N. Pham et M. Riguidel, Security Assurance Aggregation for IT Infrastructures, *Proc. 2nd Int. Conf. on Syst. and Networks Comm.*, USA, 2007.

[11] S.D. Sagan, The problem of redundancy problem: Why more nuclear security forces may produce less nuclear security, *Risk Analysis*, Vol. 24, No. 4, 2004, pp. 935-946.

[12] D.B. Parker, Risks of risk-based security, *Comm. of the ACM*, Vol. 50, No. 3, 2007, p. 120.

[13] RTCA and EuroCAE, DO-178B/ED-12B - Software Considerations in Airborne Systems and Equipment Certification, 1992.

[14] IAEA and OECD, the International Nuclear Event Scale User's Manual, 2001.

[15] B. Schneier, Attack trees: Modeling security threats, *Dr. Dobb's Journal*, Dec. 1999, pp. 21-29.

[16] R.E. Bloomfield et al., International Working Group on Assurance Cases (for Security), *IEEE Security &Privacy*, Vol. 4, No.3, 2006, pp. 66-68.

[17] J. Rushby, Kernels for Safety?, *Safe and Secure Computing Systems*, 1989, pp. 210-220.

[18] L. Piètre-Cambacédès et M. Bouissou, The promising potential of the BDMP formalism for security modeling, *Proc. DSN 2009 - FA*, Portugal.

[19] K. Zetter, FAA: Boeing's New 787 May Be Vulnerable to Hacker Attack, *WIRED*, Jan. 2008.

[20] V. Stavridou et B. Dutertre, From security to safety and back, *Proc. CSDA 1996*, pp. 182-195.

[21] K. Birman et F. Schneider, The Monoculture Risk Put into Context, *IEEE Security &Privacy,* Vol. 7, No. 1, 2009, pp. 14-17.

[22] SSLkeys, *Debian Wiki (consulted June 2009),* http://wiki.debian.org/SSLkeys

[23] ISO JTC1/SC27, ISO/IEC 27001:2005, Information technology - Security techniques - Information security management systems - Requirements.

[24] IEC/ITU, IEC60050(191):1990, International Electrotechnical Vocabulary Chapter 191: Dependability and Qualitity of Service.

[25] A. Jain, A. Ross et S. Prabhakar, An introduction to biometric recognition, *IEEE Trans. on Circuits and Sys. for Video Tech.*, Vol.14, No.1, 2004, pp. 4-20.

[26] ISO JTC1/SC27, ISO/IEC 27002:2005, Information technology - Security techniques - Code of practice for information security management, June 2005.

[27] C. Kehren et al., Architecture patterns for safe design, *Proc. of CS2E 2004*, Arcachon, France.

[28] B. Littlewood et L. Strigini, Redundancy and Diversity in Security, *ESORICS'04*, pp. 423-438

[29] M. Wiesmann et al., Understanding replication in databases and distributed systems, *Proc. Int. Conf. on Distributed Computing Sys.*, 2000, pp. 464-474.

[30] A. Hecker, On System Security Metrics and the Definition Approaches, in *Proc. Securware'08*, France, pp.412-419.

[31] M. Rausand et A. Høyland, *System Reliability Theory: Models, Statistical Methods, and Applications, 2nd Ed.*, Wiley-Interscience, 2003.

[32] R. Anderson et al., Security policies, *Advances in Computers*, Vol. 55, 2001, pp. 186-237.

[33] P.Y.A. Ryan, Mathematical models of computer security, *LNCS*, Vol. 2171, 2001, pp. 1-62.

[34] A. Simpson, J. Woodcock, et J. Davies, Safety through security, *Proc. 9th int. Proc. workshop on Soft. Spec. and Design*, Washington D.C., 1998.

[35] X. Chang, Network simulations with OPNET, *Proc. Winter Simulation Conf.*, 1999, pp. 307-314.

[36] M. Bouissou et al., Knowledge modeling and reliability processing: Presentation of the FIGARO language and associated tools, *Proc. Safecomp*, Trondheim, 1991, pp. 69-75.

[37] A. Arnold et al., The AltaRica formalism for describing concurrent systems, *Fundamenta Informaticae*, Vol. 40, 1999, pp. 109-124.

[38] Open Group Security Forum, *Security Design Patterns: Open Group Technical Guide*, 2004.

Acknowledgments:

The authors would like to thank Gilles Deleuze from EDF for having fostered the research presented in this paper by his work and discussions.