The SEMA referential framework : avoiding equivocations on security and safety issues

SEMA : un référentiel pour éviter équivoques et ambigüités entre sûreté et sécurité

Ludovic Piètre-Cambacédès
Claude Chaudet

2010D005

février 2010

Département Informatique et Réseaux
Groupe RMS : Réseaux, Mobilité et Sécurité

SEMA : un référentiel pour éviter équivoques et ambigüités entre sûreté et sécurité

The SEMA referential framework: Avoiding equivocations on security and safety issues

Ludovic Piètre-Cambacédès[a,b], Claude Chaudet[b]

Département Informatique et Réseaux

Institut Télécom, Télécom ParisTech

February 5, 2010

[a]Electricité de France (EDF) R&D, 1, avenue du Général de Gaulle, 92141 Clamart, France
[b]Institut Télécom, Télécom ParisTech, CNRS LTCI UMR 5141, 37-39, rue Dareau, 75014 Paris, France

Résumé

The meaning of the terms security and safety varies considerably from one context to another, leading to potential equivocations. The Critical Infrastructure Protection domain, involving multiple actors and engineering disciplines, is particularly concerned by such a situation. Avoiding equivocations and misunderstandings can save time and resources, especially in the earliest stages of system design or assessment projects; it may also help to ensure a more consistent and complete risk coverage. Based on a review of the existing definitions of security and safety, we propose a conceptual tool, called the SEMA referential framework, which makes the differences hidden behind the use of the terms security and safety explicit. It can also underline inconsistencies and overlaps in existing definitions. The power grid, nuclear power generation and the telecommunications & data networks sectors are examined as use-cases.

La signification des termes « sécurité »et « sûreté »varie considérablement d'un contexte à l'autre, ouvrant la voie à diverses équivoques et incompréhensions. Le domaine de la protection des infrastructures critiques, impliquant un grand nombre d'acteurs et de disciplines techniques diverses, est particulièrement concerné par cet état de fait. Eviter en amont les pièges d'une telle confusion terminologique permet gains de temps et de ressources, mais également une meilleure couverture de risques dans les phases de conception de d'évaluation. Sur la base d'une analyse des définitions existantes, nous proposons un outil conceptuel, dénommé SEMA, offrant un cadre de référence permettant de rendre explicite les différences de significations cachées derrière l'utilisation des termes sûreté et sécurité. Il permet également de souligner les éventuelles incohérences ou recouvrements dans les définitions existantes. Les secteurs du système électrique, de la production électronucléaire ainsi que celui des télécommunications et réseaux de données sont analysés à travers ce prisme.

1 Introduction

Security and safety are part of these words which seem clear and precise at first sight, but which can in fact be understood very differently depending on the context and the backgrounds involved. This often leads to serious misunderstandings. The Critical Infrastructure Protection (CIP) domain is particularly prone to such difficulties. Safety and security are core and omnipresent issues of the area, both at the policy and the technical levels. They are in fact inseparable from CIP, encompassing the protection of hazardous industries and vital assets for the nations. The complexity of the systems at stake involves the coordination of multiple actors, and on a technical side, of multiple engineering disciplines. Each of them carries its own understandings of the safety and security domains. The meaning of security for the electrical engineer is for instance not the same as for the computer scientist; it can also differ for the nuclear expert and for other specialists. The same applies for safety. Nevertheless, when it comes to CIP, different communities have to work together. This paper intends to help to establish, at the earliest stages, a common understanding in such situations. Avoiding equivocations will save time and resources; on a holistic point of view, it may also help to ensure a more consistent and complete risk coverage.

The paper is organized as follows: after having stressed the diversity of the associated definitions, Section 2 shows how it is in fact much more constructive to focus on the most recurrent distinctions made between safety and security, rather than to look for absolute definitions. Section 3 develops this track by presenting the main contribution of this paper, the SEMA referential framework. This conceptual tool aims at explicitly setting the limits of these moving concepts, in given contexts and situations. Section 4 provides concrete examples of application, in three different cases related to CIP. Section 5 concludes the paper.

2 Different uses and distinctions between security and safety

2.1 A confusing situation

The scientific and normative literature offers a surprising diversity regarding the use of the terms safety and security. In fact, dozens of explicit but distinct definitions can be found [41, 26], ranging from slightly

different to completely incompatible ones. See section 4 for examples.

Linguistics traps worsen the situation when translations are involved. As noticed by [26], some languages have a single word for both safety and security. If we look only at the European scale, this is for instance the case of Spanish (*seguridad*) or Portuguese (*segurança*), but also of Swedish (*säkerhet*) or Danish (*sikkerhed*). Similarly to English, other languages distinguish two words, like in French (*sûreté* and *sécurité*). Unfortunately, the association to their English equivalents can switch from one domain to another. Sticking to French, safety is for example directly translated by *sûreté* in the nuclear area [17], whereas the International Organization of Standardization (ISO) translates it by *sécurité* in many others domains [20]. The same applies for security, which can be translated either by *sécurité* or *sûreté*, depending on the context.

This very confusing situation establishes an ideal ground for misunderstandings, and calls for an effort for rationalization.

2.2 Reasoning on distinctions

Examining the corpus dealing with security and safety, there are of course several common points [13]. In particular, the notion of risk has a pivotal place and is defined by the macro-equation risk = likelihood x impact, summarizing very analogous definitions across different sectors and communities [17, 22, 14]. Such similarities may explain the difficulties to differentiate properly the concepts; they have been largely identified and discussed [26, 24] and have fostered cross-fertilization efforts in terms of methods still vivid today (see for instance [36, 4] or more recently [33]). But one can also spot some recurrent distinctions between the two concepts.

In fact, whereas it seems not possible to infer universal definitions for safety and security, taking a look with this new perspective, namely at what distinguishes the two concepts, has turned out to be more constructive. Reviewing previous surveys on safety and security (e.g. [41, 26, 13, 2, 34, 35]), enlarged by the main normative and scientific references related to CIP, it is in fact possible to identify two recurrent distinctions. Both of them discriminate the risks addressed by each concept, based on their origin and their nature:

- The first approach, called S-E later on, is based on a System vs. Environment distinction: security is concerned with risks originating from the environment and potentially impacting the system, whereas safety deals with risks coming from the system and potentially impacting the environment.
- The second approach, more widely adopted and called M-A later on, is based on a Malicious vs. Accidental distinction: security typically addresses malicious risks whereas safety addresses purely accidental risks (e.g. [17, 38]).

Note that these two distinctions are abstracted from existing definitions: few of them follow exactly these lines of differentiation, but a large majority can be associated with one of the two approaches. Moreover, the methods and tools involved are also highly dependent on these distinctions: for instance, stochastic modeling is a well-established practice to assess accidental risks in the industry whereas it is still marginal to capture malicious behaviors with such approach, because of their very different nature [30]. In fact, stochastic modeling is adopted for safety or security analysis depending on which side of the M-A axis the scope of the study is situated.

Once the S-E and M-A distinctions identified, it is possible to analyze the consequences of their cohabitation, very likely when dealing with the notions of security and safety in a multi-domain, cross-cultural environment. Fig. 1 graphically represents the combination of both distinctions. They are fortunately not completely orthogonal: it is possible to define sub-domains unambiguously related to security or safety with respect to both S-E and M-A. They correspond to the quadrants numbered 1 and 3 in Fig. 1. Nevertheless, the two other sub-domains represented by quadrants 2 and 4 cannot be unambiguously associated to either security or safety.

Fig. 1 illustrates the clear potential of misunderstanding when S-E and M-A distinctions are used at the same time implicitly. Quadrants 2 and 4 will be seen as safety or security issues depending on the reference adopted. But it also suggests that it is possible to decompose the safety and security generic notions into sub-notions, allowing consistent discussions with respect to both S-E and M-A.

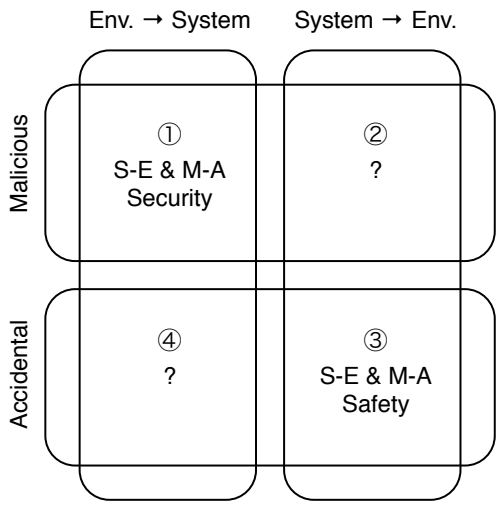

Figure 1: Crossing the S-E and M-A distinctions

3 The SEMA referential framework

3.1 Description

Based on the statements of Section 2.1, we have devised a referential framework called SEMA, taking into account S-E and M-A. It aims at providing a neutral tool to support common understanding when dealing with safety and security. SEMA gives explicit names to the sub-notions captured by the quadrants of Fig. 1, augmented for the sake of completeness by a System-to-System dimension. This framework is represented in Fig. 2. It splits the security and safety space into six distinct sub-notions: Defense, Safeguards, Self-Protection, Robustness, Containment Ability and Reliability.

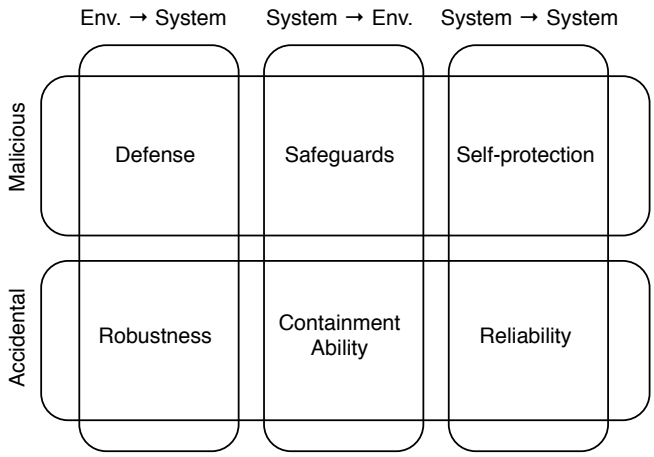

Figure 2: The SEMA referential framework

We argue that those sub-notions are semantically less ambiguous than the generic terms security and safety, and that they consistently pave their conceptual domains. Table 1 summarizes and complements the framework description.

SEMA sub-notion	Risk Covered			Remarks
	M-A	S-E		
	Intent	Origin	Target	
Defense	Malicious	Env.	System	General and military terminology
Safeguards	Malicious	System	Env.	Adapted from the nuclear industry
Self-Protection	Malicious	System	System	Internal threat protection
Robustness	Accidental	Env.	System	Used differently in recent works [13] but still considered as explicit
Containment Ability	Accidental	System	Env.	General terminology
Reliability	Accidental	System	System	Definition consistent with international standards and practices

Table 1: The six SEMA sub-notions dividing the safety and security conceptual space

3.2 SEMA scope, relevance and limits

The objective of SEMA and its associated sub-notions is of course not to replace the terms safety and security. It is mainly intended to help to establish a common understanding when different communities exchange using those words, and to provide a handy reference to "draw" the respective limits of these concepts. It is particularly appropriate for early-stages in system design or assessment, for instance when selecting the most relevant collaborations or task assignment on CIP-related projects, or when defining the scope of risk analysis. Besides, by helping to situate a given problematic in a wider scope, SEMA also provides a mnemonic tool to keep in mind the diversity of the possible risk dimensions on a holistic point of view. This said, the relative limits of the sub-notions defined by SEMA are themselves closely related to the considered context. In particular, the limit between system and environment is crucial to select a SEMA sub-notion but can largely vary depending on the analyst perspective: system boundaries need to be clearly identified and explicitly stated. Finally, the sub-notions are not exclusive one to another, in the sense that a given undesirable event or technical measure can in some cases span across several sub-notions.

4 Examples and use-cases

This section provides concrete illustrations of the changing meanings of the terms safety and security in CIP-related areas, and shows how SEMA can help to capture these differences. Three specific sectors of critical infrastructures are examined: the power grid and nuclear power generation sectors, which provide good examples of multiple definitions for which SEMA is directly usable to make their differences explicit, and the case of the telecoms and data networks infrastructure, in which SEMA rather reveals the limits, inconsistencies and overlaps of the most common definitions.

4.1 The power grid

Electrical transmission and distribution networks are highly technical systems, under fast mutations, and associated to diverse security and safety issues and challenges [9, 27]. In such context, the involved actors have different backgrounds, making the power grid a good example of thematic area full of traps and potential equivocations when it comes to safety and security. In fact, regarding the first aspect, the term safety is rather consensually used to denote the prevention of accidental harm from the power system and its components on human lives and the environment [28]. The term security is much more ambiguous.

Indeed, from a strict electrical engineering perspective, security is usually understood in this context as the ability to survive disturbances, such as electric short circuits or unanticipated loss of system elements, without interruption to customer service [1, 16]. The nature of the causes is usually not considered, and the meaning generally suggested is represented in Fig. 3: the malicious dimension is not explicitly excluded neither but is marginally considered; system impacts on the environment are out of the scope, rather treated as a safety aspect. Nevertheless, the growing concerns for CIP reinforced in the aftermath of the 9/11, have led to considerable efforts to address malicious risks, in particular regarding terrorist and external threats, driven by strong political impulses (cf. [5] in the United States or [10] in Europe). The term security is in this perspective associated to a different meaning, much more often delimited by the M-A distinction as illustrated by Fig. 3.

Besides, the increased penetration and dependence on Information and Communication Technologies (ICT) of the power system, embodied by the world-wide infatuation for Smart Grid and Advanced Metering Infrastructure initiatives, give birth to new kinds of malicious risks [9]. Cyber security concerns have for instance led the United States to define a restrictive regulatory framework to protect the electrical infrastructure against computer attacks [31]. This context involves another way to apprehend the word security also represented in Fig. 3. (Note that the representation takes into account the fact that the "internal threat" is in some cases treated as a separate issue).

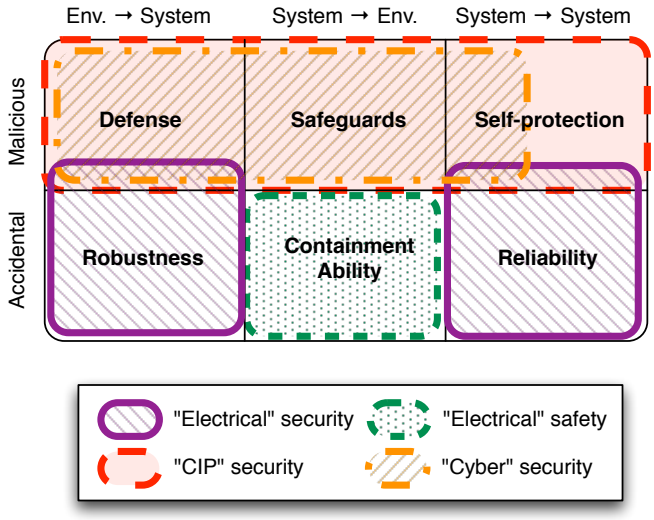

Figure 3: Security and safety in the power grid

4.2 Nuclear power generation

The nuclear industry is intimately associated to safety and security issues. Internationally, these notions are generally used in the sense given by the International Atomic Energy Agency (IAEA) [17]:

- (Nuclear) safety: "The achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation hazards."
- (Nuclear) security: "The prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities."

It is straightforward to map the corresponding definitions on the SEMA referential framework, as illustrated in Fig. 4: security, in the sense of the IAEA, spans Defense, Safeguards and Self-Protection while

safety focuses in this context on Containment Ability (if we assume that workers are considered as external to the technical system).

Nevertheless, misunderstanding is still possible as other uses of these terms in the nuclear domain are sometimes encountered. This is for example the case in France with the most recent legal framework regulating the nuclear industry [23, 15], in which the notion of nuclear security is clearly larger than the IAEA classical sense. It includes the latter but also prevention and protection against malicious and sabotage acts, as well as emergency response. This scope is represented with a dotted perimeter in Fig. 4. Once projected on the six sub-notions, the differences between these different usages are made explicit.

Finally, like in the power grid (§4.1) and more generally in all critical infrastructures, risks related to cyber attacks on digital systems are also the object of a growing attention in the nuclear power generation area. At the international level, the IAEA and more recently the IEC (International Electrotechnical Commission) are working on guidance to tackle this issue [18, 19]; focusing on the United-States, multiple texts are already issued and structure the area, e.g. [32, 29], while several others should follow shortly. Some of these references address digital system security with slightly different scopes: SEMA could here also be used to make these differences explicit.

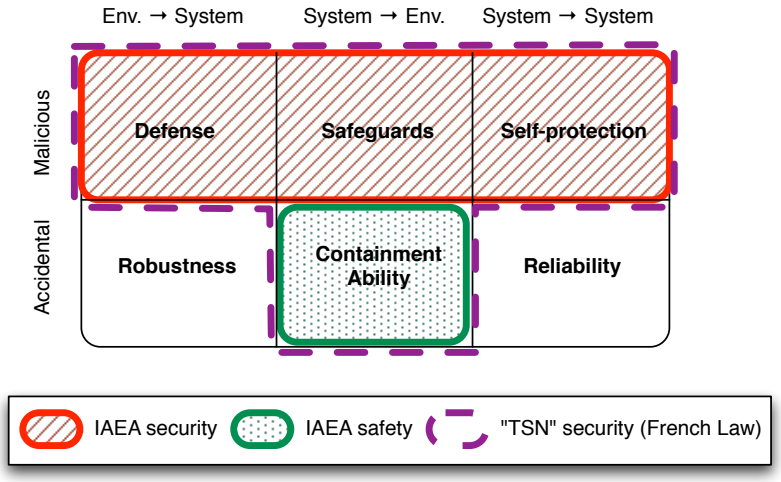

Figure 4: Using SEMA for nuclear power generation

4.3 Telecommunications and data networks

Telecommunications and data networks have, like the power grid, a specific place among the critical infrastructure sectors: they are at the same time a critical infrastructure per se but also a constitutive part of all the other critical infrastructures. Indeed, they are all highly dependent on networked digital systems and communications capabilities. The protection of such capacities is sometimes referred as CIIP (Critical Information Infrastructure Protection) [11]. The usage of the terms security and safety in this context reflects the pervasiveness of telecoms and data networks in our societies vital infrastructures, and varies accordingly.

Regarding the Internet, the Internet Engineering Task Force (IETF), recognized as one of the main technical bodies of reference, has published an Internet security glossary [37] where:

- Security is: "A system condition in which system resources are free from unauthorized access and from unauthorized or accidental change, destruction, or loss."
- Safety is: "The property of a system being free from risk of causing harm (especially physical harm) to its system entities."

In both definitions, the M-A axis has no relevance. Safety is seen as a system-to-system issue whereas security is potentially much wider. Another differentiation, not captured by SEMA, lies on the nature of the

consequences; unfortunately, it is expressed in an ambiguous way, harm being closely linked to destruction or loss. Analyzing this set of definitions through SEMA can only stress overlaps and ambiguities in the original definitions, as clear limits are difficult to draw (cf. Fig. 5).

The definitions about security found in the ISO/IEC series on "Information technology - Security techniques" cover also malicious and accidental aspects: reference [21] specifies about information security risk that "threats may be of natural or human origin, and could be accidental or deliberate". In fact the domain covered is even wider as it also states that "a threat may arise from within or from outside the organization." No position with regards to safety is mentioned in the series, which may explain the conceptual width given to the security domain.

Unfortunately, both the IETF and ISO/IEC large security definitions are not in line with those in use in specific CIIP sectors, closely linked with malicious aspects. This is the case in the power grid and the nuclear power generation sectors, as discussed in Sections 4.1 and 4.2, but also in many others like water, chemicals or oil and gas sectors (see [8, 7, 6] for associated US references). The pre-existence and importance of safety-related issues and standards, and the use of this term, in those domains may explain this different position. Nevertheless, this pre-existence may have also contributed to a rather confusing situation in which safety is also defined in CIIP as a very wide concept: one of the most cited reference in the scientific literature on dependable and secure computing for critical systems [3] defines safety as "absence of catastrophic consequences on the user(s) and the environment", whereas the ISO/IEC standards are harmonized throughout several industrial fields around the definition of safety as "freedom from unacceptable risk" [20]. In such situations, like for Internet, SEMA cannot draw clear limits between concepts whose definitions are inherently overlapping. It is rather an efficient tool for revealing such issues, illustrated by the lack of readability of Fig. 5, and may prove useful to reorganize and propose more consistent definitions.

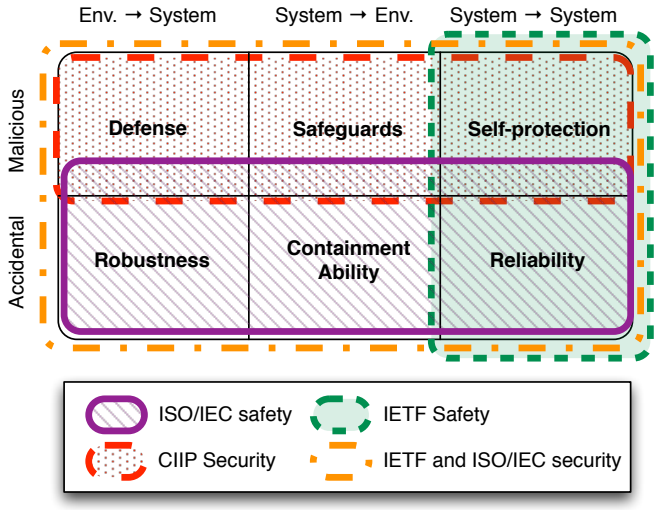

Figure 5: Security and safety in the telecoms and data networks sector.

5 Concluding remarks and perspectives

As illustrated in this paper, security and safety have different meanings depending on the context in which they are used. The CIP domain is particularly prone to such difficulties, involving multiple actors, backgrounds and engineering disciplines. The SEMA framework can help distinguish and make the differences hidden behind the use of these terms explicit. Power grid or nuclear power generation provide good sectorial cases for comparison as developed in Section 4, but CIP can offer much more complicated situations. For

instance, the recent coordination between the US Federal Energy Regulatory Commission and the US Nuclear Regulatory Commission regarding the cyber security of nuclear power plants [12] is an interesting example where safety and security terms may have been seen under a triple perspective: power grid, nuclear industry and control systems/telecoms.

Avoiding equivocations is always beneficial and should start from the earliest stages, being for system design or system assessment projects, policy making or collaborative research processes. Moreover, if making differences explicit can save time and resources, SEMA can be useful in other ways. It can underline inconsistencies and overlaps in existing definitions, as shown in Section 4.3 for the telecommunications sector. It can also serve as a mnemonic tool to keep in mind the diversity of the possible risk dimensions, and to ensure a consistent risk coverage on a holistic point of view.

To prepare this work, we have presented preliminary versions of the SEMA framework and the associated terminology to different audiences and integrated their feedback. By enlarging scrutiny to the CIP community, we hope to further enhance the proposed decomposition as we believe that such referential framework has a particular relevance in this domain.

On-going work and identified perspectives include augmenting the framework by explicitly differentiating the physical and cyber dimensions involved by safety and security digital systems. This would allow a finer conceptual decomposition. Such work would of course have to integrate state of the art developments in the Cyber-Physical Systems (CPS) area [25]. Finally, advanced decompositions of the safety and security concepts as initiated by this work may enable a finer analysis of their interdependencies, a recurrent but still open question [39, 40], equally at the core of CIP design and implementation choices.

References

[1] S. Abraham. National transmission grid study. US DoE, May 2002.

[2] M. Al-Kuwaiti, N. Kyriakopoulos, and S. Hussein. A comparative analysis of network dependability, fault-tolerance, reliability, security, and survivability. *IEEE Communications Surveys and Tutorials*, 11(2):106–124, 2009.

[3] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, 1(1):11–33, 2004.

[4] S. Brostoff and M. Sasse. Safe and Sound: a safety-critical approach to security design. In *Proceedings of the Workshop on New Security Paradigms (WNSP'01)*, pages 41–50, New Mexico, USA, 2001.

[5] G. W. Bush. HSPD-7 homeland security presidential directive for critical infrastructure identification, prioritization, and protection. Presidential Directive, Dec. 2003.

[6] LOGIIC - Linking the Oil and Gas Industry to Improve Cybersecurity. U.S. Department of Homeland Security, Sept. 2006.

[7] Roadmap to secure control systems in the water sector. U.S. Department of Homeland Security, Water Sector Coordinating Council Cyber Security WG, Mar. 2008.

[8] Roadmap to secure control systems in the chemical sector. U.S. Department of Homeland Security, Chemical Sector Roadmap WG, Sept. 2009.

[9] G. N. Ericsson. Information security for Electric Power Utilities (EPUs) - CIGRÉ developments on frameworks, risk assessment, and technology. *IEEE Transactions on Power Delivery*, 24(3):1174–1181, 2009.

[10] Critical infrastructure protection in the fight against terrorism. European Commission, COM(2004)702 final, Oct. 2004.

[11] Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience. European Commission, Communications SEC(2009)399 and SEC(2009)400, Mar. 2009.

[12] Nuclear plant implementation plan for CIP standards. Cyber Security Order 706B, Federal Energy Regulatory Commission (FERC), 2009.

[13] D. G. Firesmith. Common concepts underlying safety, security, and survivability engineering. Technical Note CMU/SEI-2003-TN-033, Carnegie Mellon University, Software Engineering Institute, Dec. 2003.

[14] IEEE, editor. *The Authoritative Dictionary of IEEE Standards Terms (IEEE-100)*. Institute of Electrical and Electronic Engineers, seventh edition, 2000.

[15] Institut de Radioprotection et de Sûreté Nucléaire. Approche comparative entre sûreté et sécurité nucléaires. Report (in French) 2009/117, IRSN, Apr. 2009.

[16] Definition and classification of power system stability. CIGRÉ-IEEE Joint Task Force, Technical Brochure No. 231, June 2003.

[17] IAEA safety glossary: terminology used in nuclear safety and radiation protection, 2007 edition. International Atomic Energy Agency, ref. STI/PUB/1290, 2007.

[18] International Atomic Energy Agency. Computer security at nuclear facilities (draft). Reference manual, International Atomic Energy Agency, unpublished, 2009.

[19] Nuclear power plants - instrumentation and control important to safety - requirements for computer security programmes (NWIP). Ref. 45A/742/NP, IEC New Work Item Proposal (NWIP IEC62645), 2009.

[20] Safety aspects - guidelines for their inclusion in standards. ISO/IEC Guide 51, 1999.

[21] Information technology - Security techniques - Information security risk management. ISO/IEC International Standard ISO/IEC 27005:2008(E), 1st edition, June 2008.

[22] Information technology - security techniques - information security management systems - overview and vocabulary. ISO/IEC International Standard 27000:2009(E), 1st edition, May 2009.

[23] Loi 2006-686 du 13 juin 2006 relative à la transparence et à la sécurité en matière nucléaire. Journal Officiel de la République Française du 14 juin 2006 (in French), June 2006.

[24] S. Lautieri, D. Cooper, and D. Jackson. SafSec: Commonalities between safety and security assurance. In *Proceedings of the 13th Safety Critical Systems Symposium*, pages 65–75, Southampton, UK, Feb. 2005. Springer London.

[25] E. A. Lee. Cyber physical systems: Design challenges. Technical Report UCB/EECS-2008-8, Univ. of Berkeley, EECS, Jan. 2008.

[26] M. B. Line, O. Nordland, L. Røstad, and I. A. Tøndel. Safety vs. Security? In *Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management (PSAM 2006)*, New Orleans, Louisiana, USA, May 2006.

[27] V. Madani and R. King. Strategies to meet grid challenges for safety and reliability. *International Journal of Reliability and Safety*, 2(1-2):146–165, 2008.

[28] Electric safety. National Grid website (last checked 30th Dec 2009) - http://www.nationalgridus.com/masselectric/safety_electric.asp.

[29] Protection of digital computer and communication systems and networks. Regulation 10 CFR73 part 54, U.S. National Regulatory Commission (NRC), Mar. 2009.

[30] D. M. Nicol, H. Sanders, William, and K. S. Trivedi. Model-based evaluation: From dependability to security. *IEEE Transactions on Dependable and Secure Computing*, 1(1):48–65, 2004.

[31] Cyber Security Standards. CIP-002-1 through CIP-009-1, North American Electric Reliability Council (NERC), 2006.

[32] Cyber security program for power reactors. Nuclear Energy Institute Std., NEI04-04, Feb. 2005.

[33] L. Piètre-Cambacédès and M. Bouissou. Beyond attack trees: dynamic security modeling with Boolean logic Driven Markov Processes (BDMP). In *Proceedings of the 8th European Dependable Computing Conference (EDCC)*, Valencia, Spain, Apr 2010.

[34] D. Prasad, J. McDermid, and I. Wand. Dependability terminology: similarities and differences. In *Proceedings of the 10th annual Conference on Computer Assurance (COMPASS '95)*, pages 213–221, Gaithersburg, Maryland, USA, June 1995.

[35] J. Rushby. Critical system properties: Survey and taxonomy. *Reliability Engineering and System Safety*, 43(2):189–219, 1994.

[36] B. Schneier. Attack trees: Modeling security threats. *Dr. Dobb's Journal*, 12(24):21–29, 1999.

[37] R. Shirey. Internet security glossary, version 2. IETF, RFC4949, Aug. 2007.

[38] J. Smith, S. Russell, and M. Looi. Security as a safety issue in rail communications. In *Proceedings of the 8th Australian Workshop on Safety Critical Systems and Software (SPS'03)*, volume 33, pages 79–88, Canberra, Australia, Oct. 2003.

[39] V. Stavridou and B. Dutertre. From security to safety and back. In *Proceedings of the Computer Security, Dependability, and Assurance: From Needs to Solutions (CSDA'98)*, pages 182–195, York, UK, July 1998. IEEE Computer Society.

[40] M. Sun, S. Mohan, L. Sha, and C. Gunter. Addressing safety and security contradictions in Cyber-Physical Systems. In *Proceedings of the 1st Workshop on Future Directions in Cyber-Physical Systems Security (CPSSW'09)*, Newark, NJ, USA, July 2009.

[41] M. Van Der Meulen. *Definitions for Hardware and Software Safety Engineers*. Springer, first edition, Apr. 2000.

Dépôt légal : 2010 – 1er trimestre
Imprimé à Télécom ParisTech – Paris
ISSN 0751-1345 ENST D (Paris) (France 1983-9999)

Télécom ParisTech

Institut TELECOM - membre de ParisTech

46, rue Barrault - 75634 Paris Cedex 13 - Tél. + 33 (0)1 45 81 77 77 - www.telecom-paristech.frfr

Département INFRES