available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/ijcip

The SEMA referential framework: Avoiding ambiguities in the terms "security" and "safety"

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

[a] *EDF R&D, 1, avenue du Général de Gaulle, 92141 Clamart, France*
[b] *Institut Telecom, Telecom ParisTech, CNRS LTCI UMR 5141, 46 rue Barrault, 75013 Paris, France*

ARTICLE INFO

Article history:
Received 15 January 2010
Accepted 10 June 2010

Keywords:
Security
Safety
Risk analysis
Ambiguities

ABSTRACT

The meaning of the terms "security" and "safety" varies considerably from one context to another, leading to potential ambiguities. These ambiguities are very problematic in the critical infrastructure protection domain, which involves multiple actors and engineering disciplines. Avoiding misunderstandings caused by the ambiguities during the early stages of system design and risk assessment can save time and resources; it also helps ensure a more consistent and complete risk coverage. Based on a review of the existing definitions of security and safety, this paper identifies the main distinctions between the two notions. It proposes a referential framework called SEMA, which makes the latent differences underlying the use of the terms security and safety explicit. Three sectors are examined as use cases: The power grid, nuclear power generation, and telecommunications and data networks. Mapping the different sector definitions of security and safety in the SEMA framework makes their respective meanings explicit and reveals inconsistencies and overlaps.

1. Introduction

"Security" and "safety" are words that seem clear and precise at first glance, but they may have very different meanings depending on the context. This situation leads to serious misunderstandings when individuals from different technical communities collaborate.

The critical infrastructure protection (CIP) domain is particularly prone to such difficulties. Safety and security are core, omnipresent concepts in the domain, both at the policy and technical levels. The complexity of critical infrastructure systems involves the coordination of multiple actors from multiple engineering disciplines. Each discipline has its own understanding of the terms safety and security. The meaning of security to an electrical engineer is different from the meaning to a computer scientist; and both meanings are different from the meaning of security to a nuclear expert. The same applies to safety.

This paper intends to help establish a common understanding of the terms security and safety. Section 2 presents an analysis of the definitions found in the literature and identifies two main distinctions based on the analysis. Section 3 presents the SEMA referential framework, which integrates the two distinctions and attempts to set the limits on security and safety in specific contexts. Section 4 presents examples involving the mapping of the definitions to the SEMA framework for three industrial sectors.

2. Distinguishing between security and safety

The scientific and normative literature offers a surprising diversity in the use of the terms security and safety. Dozens

* *Corresponding author at:* EDF R&D, 1, avenue du Général de Gaulle, 92141 Clamart, France.
E-mail addresses: Ludovic.Pietre-Cambacedes@edf.fr (L. Piètre-Cambacédès), Claude.Chaudet@enst.fr (C. Chaudet).

1874-5482/$ - see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.ijcip.2010.06.003

of explicit, but distinct, definitions can be found [1,2], ranging from slightly different to completely incompatible definitions. In this situation, searching for absolute, universal definitions is bound to fail. However, as suggested by Burns et al. [3], focusing on what distinguishes the two terms in the various definitions can provide considerable insight.

2.1. *Linguistic traps*

Linguistics and translation are responsible for some of the ambiguity regarding the terms safety and security. Some languages have a single word for both safety and security [2,3]. This is the case in Spanish (*seguridad*), Portuguese (*segurança*), Swedish (*säkerhet*) and Danish (*sikkerhed*). English distinguishes between the two words as does French (*sûreté* and *sécurité*). Unfortunately, the association of the English terms can vary or even be inverted from one domain to another. In French, the word safety is directly translated to *sûreté* in the nuclear power industry [4] while the International Organization for Standardization (ISO) translates safety to *sécurité* in other domains [5]. The same applies to security, which is translated to *sécurité* or *sûreté*, depending on the context. In this paper, we only consider English language documents to avoid such translation pitfalls. Nevertheless, these pitfalls should neither be ignored nor underestimated because they can contribute to significant misunderstanding in international contexts. The European Union provides an interesting example, in which the English words, safety and security, are translated into the 22 other official languages used in research and engineering programs related to European critical infrastructures [6].

2.2. *Literature survey*

Once the linguistic difficulties are set aside, the search for recurrent distinctions between security and safety needs to be based on relevant material.

First, we consider the academic literature. From among the vast material available, we have selected eight articles that explore the notions of security and safety [7,3,8–11,2,12]. These articles were selected because of their efforts to cover or discriminate both concepts. Second, we consider several standard documents that reflect how industry perceives the notions of security and safety.

Table 1 lists the non-academic documents considered in this study. They are classified by sector and separated into security-related documents and safety-related documents on a terminological basis, notwithstanding the meanings implied by the two terms.

Fig. 1 categorizes the analyzed documents based on the various industrial sectors. The documents come from a broad range of organizations. Several documents are published by international standardization organizations such as the International Electrotechnical Committee (IEC) and the International Organization for Standardization (ISO). Others are published by national standardization organizations such as the US National Institute of Standards and Technology (NIST) and the American National Standards Institute (ANSI). Yet others are from the United Nations, for example, from the

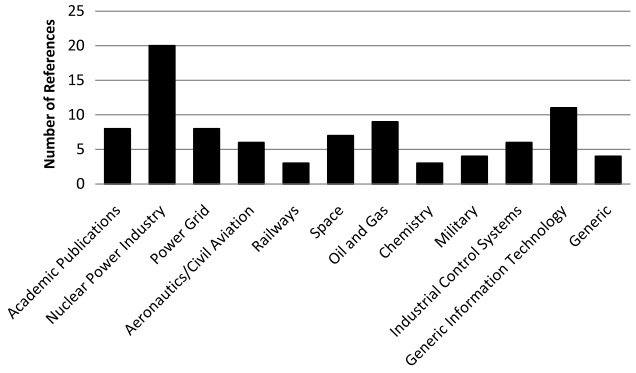

Fig. 1 – Categorization of the analyzed documents based on industrial sectors.

International Atomic Energy Agency (IAEA) and the International Civil Aviation Organization (ICAO). Many industrial consortia are active in creating reference documents that ultimately become *de facto* standards in their respective sectors. This is the case with the International Air Transport Association (IATA), the Radio Technical Commission for Aeronautics and the European Organization for Civil Aviation Equipment (EuroCAE) in the aviation and aeronautics sector; and with Oljeindustriens Landsforening (OLF) in Norway and the American Petroleum Institute (API) in the oil industry. Moreover, government agencies such as the US Department of Homeland Security (DHS), the US Department of Defense (DoD) and the US Nuclear Regulatory Commission (NRC) publish safety or security-related regulations, recommendations, standards and guidance. Finally, various legislative and executive directives are relevant; these include US Presidential directives, the US Code of Federal Regulations (CFR) and European Commission (EC) regulations. Our analysis considers representative documents from all these types of entities.

In total, 89 different documents were selected and analyzed. This corpus is by no means exhaustive. Some industrial sectors such as water supply and the automotive industry are omitted; others, like the military and railways, are glossed over. Also, some security-related documents (e.g., from the ICAO in the civil aviation sector) were unavailable for reasons of confidentiality. Nevertheless, the document corpus is large enough to be representative, and covers the security and safety of physical installations and computer systems.

2.3. *Distinctions in the literature*

Among the 89 documents in the corpus, only 14 documents provide explicit definitions of both security and safety (this takes into account contextualized forms such as “aviation security” and “nuclear safety”). Fig. 2 presents the categorization of the documents in the corpus by sector.

Only two of the 14 documents provide explicit and exclusive definitions of security and safety: the article published by Line et al. [2] and the report published by Firesmith [9]. One other document by Burns et al. [3] also provides clear and exclusive definitions, but in an indirect manner by defining “security-critical systems” and “safety-critical systems”. Table 2 presents these three sets of definitions.

Table 1 – Security- and safety-related documents (non-academic).

Sector	Security references	Safety references
Nuclear power Industry	**International:** IAEA reference manual (draft) [13] IEC 62645 (draft) [16] **National:** (US) Federal regulations 10 CFR 73 [19] (US) RG1.152 NRC guide [21] (US) 5.71 NRC guide [24] (US) IEEE 692-2010 standard [27] (KR) KINS/GT-N09-DR guide [28]	**International:** IAEA safety series (SF-1 [14], NS-G-1.1 [15], NS-G-1.3 [17], NS-R-1 [18]) IAEA glossary [4] 75-INSAG-3 IAEA report [20] IEC SC45A standards (61513 [22], 61226 [23], 60880 [25], 62138 [26]) **National:** (US) RG1.152 NRC guide [21] ANSI/IEEE 603-1998 [29] and 7-4.3.2 [30] standards
Power grid	**International:** IEC 62351 [31] **Regional:** (North America) NERC CIP standards [33] (Europe) UCTE Operation Handbook [34] **National:** (US) NIST IR 7628 (draft) [35] (US) IEEE 1402-2000 [36] (US) IEEE1686-2007 [37] (US) IEEE1711(draft) [38]	**Regional:** (North America) NERC Reliability Standards [32]
Aeronautics/Civil Aviation	**Regional:** (Europe) Regulation (EC) 2320/2002 [39] **National:** (US) NSPD 47/HSPD 16 [42]	**International:** ICAO Doc 9735 [40] RTCA DO-178B / EuroCAE ED12 B [41] **Regional:** (Europe) EuroControl ESARRs [43,44] (Europe) Regulation (EC) 216/2008 [45]
Railways	**National:** (US) 49 CFR Parts 1520 and1580 [46]	**International:** IEC 62278 [47] IEC 62279 [48]
Space	**National:** (US) 14 CFR Part 1203, 1203a, 1203b [49–51] (US) NASA EA-STD 0001.0 [53] (US) NASA NPR 1600.1 [54]	**Regional:** (Europe) ECSS-P-001B [52] **National:** (US) NASA-STD-8719.13B [55]
Oil and Gas	**National:** (Norway) OLF Guideline 104 [56] (US) API 1164 [58]	**International:** ISO 10418 [57] ISO 13702 [59] ISO 17776 [60] **National** (Norway) NORSOK S-001 [61] and I-002 [62] (Norway) OLF Guidelines 70 [63], 90 [64]
Chemistry	**National:** (US) 6 CFR Part 27 [65] (US) DHS CFATS (incl. RBPSG) [67]	**National:** (US) AIChE/CCPS combined glossary [66]
Military	**International:** NATO AAP-6(2009) glossary [68]	**International:** NATO AAP-6(2009) glossary [68] ARMP-7 ed.1 [69] **National:** (US) DoD MIL-STD-882D [70] (UK) MoD DEF Stan 00-56 [71,72]
Industrial control Systems (non sectoral)	**International:** IEC62443 series [73,74] **National:** (US) NIST SP 800-82 [76] (US) NIST SP 800-53 (annex I) [77] (US) ANSI/ISA99 00.01 [78] (UK) CPNI SCADA GPG [79]	**International:** IEC61508 [75]

(*continued on next page*)

Table 1 (*continued*)

Sector	Security references	Safety references
Generic Information Technology (non sectoral)	**International:** ISO/IEC 27000, 27001 [80,81] ISO/IEC 27002, 27005 [83,84] ISO/IEC 13335-1 [85] IETF RFC 4949 [86] IUT-T X.1051 [87] **National:** (US) NIST FIPS 199 [88] NIST IR 7298 [89] NSA NIAG glossary [90]	**International:** IEC 60950 [82]
Generic	**International:** ISO/IEC Guide 81 (draft) [91]	**International:** ISO/IEC Guide 51 [5] and Guide 2 [92] IEC 60050-191 [93]

Table 2 – Explicit and exclusive definitions of security and safety in the literature.

Reference	Safety	Security
Line et al. [2] (2006)	"The inability of the system to affect its environment in an undesirable way."	"The inability of the environment to affect the system in an undesirable way."
Firesmith [9] (2003)	"The degree to which accidental harm is prevented, reduced and properly reacted to."	"The degree to which malicious harm is prevented, reduced and properly reacted to."
Burns et al. [3] (1992)	"A system is judged to be safety-critical in a given context if its failure could be sufficient to cause absolute harm."	"A system is judged to be security-critical in a given context if its failure could be sufficient to cause relative harm, but never sufficient to cause absolute harm."

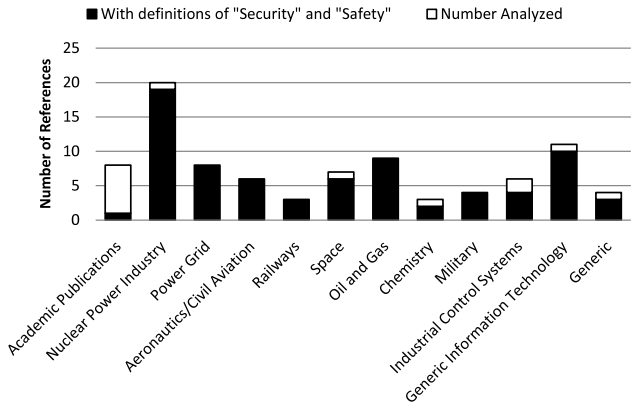

Fig. 2 – Sector-based characterization of documents that define both security and safety.

The remaining 11 documents define security and safety as overlapping notions. Some documents (e.g., from IAEA), explicitly mention the overlap, but most do not. The level of overlap varies from one document to another. For three of the 11 documents, the definition of safety includes security [66,73,78]. For example, two documents [73,78] define safety as the "freedom from unacceptable risk". Conversely, the definitions of security in three documents [12,73,78] include safety.

Twelve of the 89 documents in the corpus provide definitions of safety and/or security with broad implicit or explicit overlaps. Eight of them [5,47,66,61,70,73,78,92] propose definitions of safety that encompass most security definitions. On the other hand, four documents [94,78,84,85] propose generic or fuzzy definitions for security which may include safety.

Finally, 40 documents do not define security or safety. Nevertheless, most of them refer to a more general document (e.g., from IAEA) or define related notions (risk, threat, etc.) that shed light on the meaning of security or safety.

2.4. *Lexicographical analysis*

Few documents give clear and distinct definitions of security and safety. To go further, we examined the vocabulary used in the definitions found in the documents listed in Tables 1 and 2. The goal was to identify potential thematic clusters associated with each group of definitions and infer the implicit distinctions between the two concepts. Using an automated lexicographical analysis tool, we discovered that the definitions of security use a lexicon approximately half as large as that used to define safety (211 vs. 411 distinct, meaningful words). This fact indicates that the definition of safety benefits a larger audience as suggested in [2], or that the definition is more generic and does not require a domain-specific vocabulary.

Tables 3 and 4 present the most frequent words found in the definitions of security and safety, respectively. For reasons of space, we only list the words with at least four occurrences in the security definitions and three occurrences in the safety definitions. The safety vocabulary refers to accidental causes and to physical systems ("harm", "injury", "catastrophic" and "equipment"). The notion of the environment, as opposed to the system under consideration, is common in the safety definitions, but is generally absent in the security definitions. This last statement is consistent with

Table 3 – Most frequent words found in definitions of security.

Word	Occurrences
Information	25
System	25
Systems	24
Unauthorized	19
Access	15
Availability	13
Integrity	13
Confidentiality	12
Persons	11
Against	9
Measures	9
Protect	9
Data	8
Condition	7
Control	7
Reliability	7
Accountability	6
Authenticity	6
Critical	6
Disclosure	6
Loss	6
Protection	6
Sabotage	6
Achieving	5
Actions	5
Aspects	5
Cyber	5
Defining	5
Denied	5
Destruction	5
Harm	5
Maintaining	5
Modify	5
Provide	5
Repudiation	5
Software	5
Acts	4
Authorised	4
Cause	4
Ensure	4
Interference	4
Malicious	4
Safety	4
Unwanted	4

Table 4 – Most frequent words found in definitions of safety.

Word	Occurrences
System	17
Risk	15
Damage	14
Environment	13
Freedom	11
Harm	11
Unacceptable	9
Property	7
Injury	5
Acceptable	4
Level	4
Catastrophic	3
Cause	3
Conditions	3
Consequences	3
Equipment	3
Illness	3
Operating	3

the almost identical frequency of the words "system" and "systems" in the security definitions; safety definitions only use the singular form. On the other hand, security definitions often refer to malicious and voluntary actions ("unauthorized", "access", "against", "sabotage", "achieving", "actions" and "malicious"), with some specific terms related to information security (e.g., "confidentiality", "integrity" and "availability"). Thus, our lexicographical analysis confirms the relevance of the three approaches for differentiating the terms security and safety (summarized in Table 2) and does not favor one approach over the others.

2.5. *Distinctions between security and safety*

The analysis of the set of definitions indicates that certain limits exist between security and safety, although they are not defined uniquely and are seldom formalized explicitly. Nevertheless, based on a qualitative analysis of the documents in Table 1 and supported by the lexicographical analysis of the previous section, we argue that two relevant and representative distinctions can be identified. They are directly based on the definitions proposed by Line et al. [2] and Firesmith [9] (the definitions proposed by Burns et al. [3] are deemed to be more subjective). Both definitions differentiate security and safety based on the covered risk characteristics: the first in terms of the object of the risk and the second in terms of intentionality. Our work, therefore, is based on the following two distinctions:

- **System vs. Environment (S–E) distinction:** Security is concerned with the risks originating from the environment and potentially impacting the system, whereas safety deals with the risks arising from the system and potentially impacting the environment.
- **Malicious vs. Accidental (M–A) distinction:** Security typically addresses malicious risks while safety addresses purely accidental risks.

In the S–E definitions, the system represents the object of the study and can represent systems of any scale; the environment represents the set of other interacting systems whose behavior and characteristics are generally less known and beyond the control of the system owner. In the M–A definitions, the term accidental should be understood as "related to undesired events happening unexpectedly and unintentionally". Note that these two distinctions are only abstracted from existing definitions. Few of the definitions in the 14 documents that define both security and safety follow these lines of differentiation exactly, but the majority can be associated with one of the two approaches. Interestingly, the methods and tools involved are also highly dependent on the chosen distinctions. For example, stochastic modeling is a well-established method for assessing accidental risks in industry whereas it is unusual to model malicious behavior using this method because of its very different nature [10]. In fact, stochastic modeling is adopted for security or safety

Table 5 – Six SEMA sub-notions that divide the security and safety conceptual space.

SEMA Sub-Notion	Risk covered			Remarks
	M–A	S–E		
	Intent	Origin	Target	
Defense	Malicious	Env.	System	General and military terminology
Safeguards	Malicious	System	Environment	Adapted from the nuclear power industry
Self-Protection	Malicious	System	System	Internal threat protection
Robustness	Accidental	Env.	System	Used differently in recent works [9] but still considered as explicit
Containment Ability	Accidental	System	Environment	General terminology
Reliability	Accidental	System	System	Definition consistent with international standards and practices

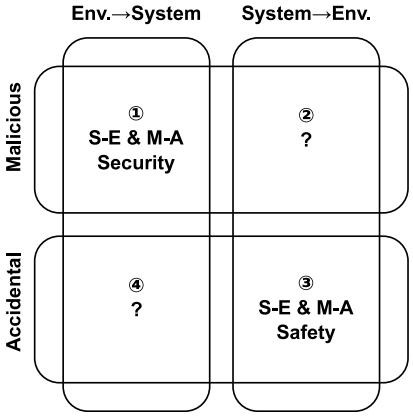

Fig. 3 – Crossing the S–E and M–A distinctions.

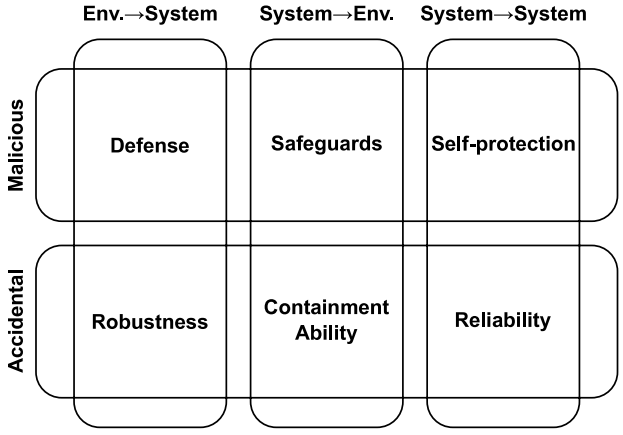

Fig. 4 – SEMA referential framework.

analyses depending on which side of the M–A axis the scope of the study is situated.

3. SEMA referential framework

Having identified the S–E and M–A distinctions, it is possible to analyze the consequences of their coexistence when dealing with the notions of security and safety in a multi-domain, cross-cultural environment. Fig. 3 provides a graphical representation of the combined S–E and M–A distinctions. Fortunately, they are not completely orthogonal: it is possible to define sub-domains related to security or safety with respect to both S–E and M–A in an unambiguous manner. These correspond to the quadrants numbered 1 and 3 in Fig. 3. The two other sub-domains, corresponding to quadrants 2 and 4, cannot be unambiguously associated with either security or safety.

Fig. 3 also illustrates the clear potential of misunderstanding when the S–E and M–A distinctions are used at the same time in an implicit manner. Quadrants 2 and 4 are seen to correspond to security or safety issues depending on the reference adopted. In fact, it may be possible to decompose the generic notions of security and safety into sub-notions, allowing consistent discussions with respect to both S–E and M–A.

3.1. *Description*

Based on the discussion in Section 2, we propose the SEMA referential framework, which takes into account S–E and M–A. It seeks to provide a neutral tool that supports a common understanding when dealing with the terms security and safety. SEMA gives explicit names to the sub-notions captured by the quadrants in Fig. 3, augmented by a system-to-system dimension for the sake of completeness. Note that, by definition, environment-to-environment issues are considered outside the direct scope of our analysis.

The SEMA framework is shown in Fig. 4. It divides the security and safety space into six distinct sub-notions: defense, safeguards, self-protection, robustness, containment ability and reliability. We argue that the six sub-notions are semantically less ambiguous than the generic terms security and safety, and that they consistently cover their conceptual domains. Table 5 summarizes and complements the description of the SEMA framework.

3.2. *SEMA scope, relevance and limits*

The objective of SEMA and its associated sub-notions is not to replace the terms security and safety. Rather, SEMA is intended to help establish a common understanding when different technical communities communicate with each other using these words, and to provide a convenient reference that conveys the limits of the concepts. SEMA is particularly useful during the early stages of system design and when defining the scope of a risk assessment. More generally, SEMA can be helpful when selecting the most relevant collaborations or task assignments on CIP-related projects that involve multiple communities. Also, by helping situate a given problem in a wider scope, SEMA also serves as a mnemonic tool that captures the diversity of the various risk dimensions from a holistic point of view.

Note, however, that the relative limits of the sub-notions defined by SEMA are themselves closely related to the context under consideration. In particular, the limit between the system and the environment is crucial to selecting a SEMA sub-notion, but it can vary depending on the perspective of the analysis — the system boundaries must be clearly identified and explicitly stated. Moreover, the sub-notions are not mutually exclusive in that an undesirable event or technical measure can span several sub-notions. Finally, SEMA cannot solve intrinsic problems arising from imprecise or inherently overlapping definitions of security and safety in certain sectors; however, SEMA can help identify the inconsistencies and overlaps as illustrated in the next section.

4. CIP sector examples

This section provides concrete examples of the different meanings of the terms security and safety in CIP-related areas, and shows how SEMA can help capture these differences. Three critical infrastructure sectors are examined. The first two are the power grid and nuclear power generation sectors, which provide good examples of multiple definitions that can be clarified by SEMA. The third is the telecommunications and data networks sector, for which SEMA reveals the limits, inconsistencies and overlaps of the most common definitions.

4.1. *Power grid*

Electrical transmission and distribution networks are highly technical systems that evolve rapidly and involve diverse security and safety issues and challenges [95,96]. In the power grid sector, the involved actors have different backgrounds, making it a good example of a thematic area that is full of traps and potential ambiguities with regard to the terms safety and security. The term safety is consistently used in the sector to denote the prevention of accidental harm from the power system and its components to humans and the environment [97,98].

The term security is much more ambiguous. From a strict electrical engineering perspective, security is usually understood as the ability to survive disturbances (e.g., short circuits and unanticipated loss of system elements) without interruptions in customer service [34,99,100]. The nature of the cause is usually not considered and the general meaning is represented in Fig. 5. Note that the malicious dimension is not explicitly excluded, but is considered marginally. Also, the impact of the system on the environment is not in scope because it is treated as a safety aspect. Nevertheless, the growing CIP concerns reinforced in the aftermath of the attacks of September 11, 2001 have led to numerous efforts to address malicious risks, especially regarding terrorist and external threats that are driven by strong political impulses in the United States [101] and Europe [102]. In this perspective, the term security is associated with a different meaning, one which is more often delimited by the M–A distinction as shown in Fig. 5.

Over the past decade, the increased dependence of the power grid on information and communication technologies coupled with the global interest in the smart grid and advanced metering infrastructures have introduced new types of malicious risks [95]. Cyber security concerns have led the United States to define a restrictive regulatory framework to protect the electrical infrastructure from computer attacks [33]. This context has caused the term security to be viewed in another manner, which is also represented in Fig. 5. Note that the representation takes into account the fact that the "internal threat" is, in some cases, treated as a separate issue.

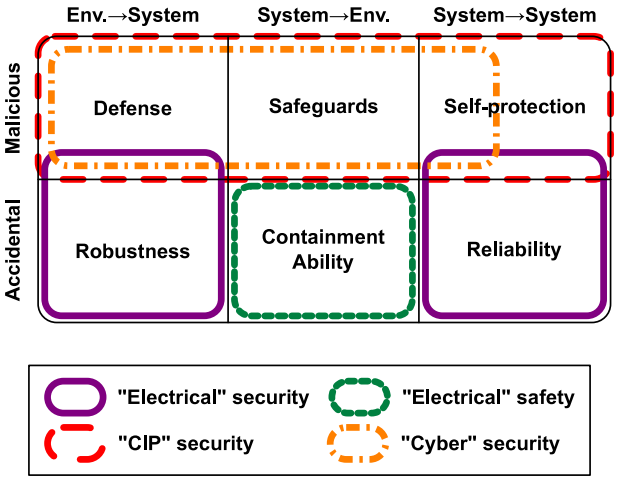

Fig. 5 – Security and safety in the power grid.

4.2. *Nuclear power generation*

In the nuclear power generation industry (international level), the terms security and safety are used in the sense specified by the IAEA [4]:

- (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.
- (Nuclear) Safety: The achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in the protection of workers, the public and the environment from undue radiation hazards.

It is straightforward to map these definitions within the SEMA referential framework as shown in Fig. 6. Security, in the sense of the IAEA, spans defense, safeguards and self-protection while safety focuses on containment ability (if we assume that workers are external to the technical system). Reliability issues that are not related to the potential impact on the environment fall under performance and availability, not safety. Likewise, robustness issues are considered separately.

Nevertheless, misunderstandings are still possible because other uses of the terms security and safety are sometimes encountered in the nuclear power generation industry. This is true in France, where the notion of security is clearly broader than the classical IAEA notion in the latest nuclear power regulations [103,104]. The notion covers the

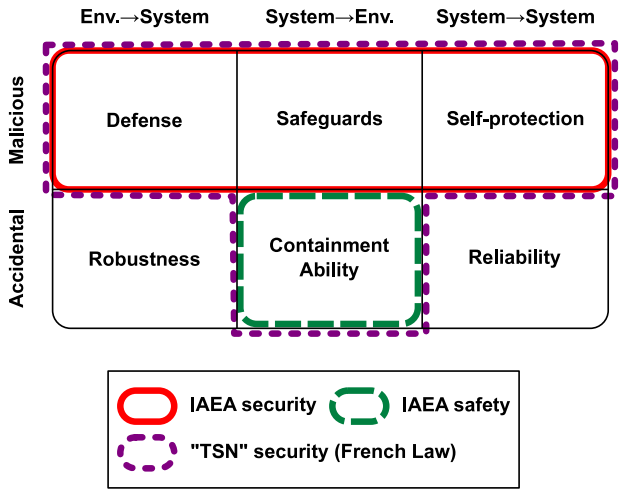

Fig. 6 – Using SEMA in the nuclear power industry.

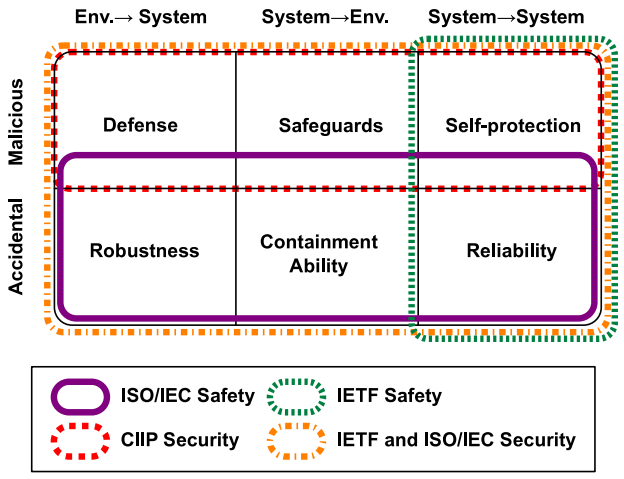

Fig. 7 – Security and safety in the telecommunications and data networks sector.

classical IAEA definition as well as the prevention of and protection against malicious acts and sabotage, and emergency response. This increased scope is expressed using the dotted perimeter in Fig. 6. The differences between the various uses are made explicit when they are projected on the six SEMA sub-notions.

Finally, as in the power grid (Section 4.1) and, more generally, in all critical infrastructures, risks related to cyber attacks on computer systems are also the object of growing attention in the nuclear power generation industry. At the international level, the IAEA and more recently the IEC, are working to tackle this issue [13,16]. In the United States, multiple documents already structure the area (see, e.g., [105, 19]) and others are being prepared. Some of these documents address computer security with slightly different scopes. SEMA makes it possible to render the differences explicit.

4.3. *Telecommunications and data networks*

The telecommunications and data networks sector, like the power grid, has a special place among critical infrastructure sectors because it is a critical infrastructure *per se* as well as an important component of all the other critical infrastructures. In fact, all the critical infrastructures are highly dependent on telecommunications and data networks. The protection of these assets is referred to as critical information infrastructure protection (CIIP) [106]. Consequently, the use of the terms security and safety in this context reflects the pervasiveness of telecommunications and data networks in the various critical infrastructure sectors and varies accordingly.

The Internet Engineering Task Force (IETF), recognized as one of the principal technical bodies in the Internet domain, has published an Internet security glossary [86] with the following definitions:

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

The M–A axis has no relevance in both the IETF definitions. Safety is seen as a system-to-system issue whereas security is potentially much broader. Another differentiation, not captured by SEMA, lies in the nature of the consequences; unfortunately, it is expressed in an ambiguous manner, with harm being closely linked to destruction or loss. Analyzing this set of definitions using SEMA emphasizes the overlaps and ambiguities in the original definitions because clear limits are difficult to draw (Fig. 7).

Definitions of security in the ISO/IEC series of standards on information security also cover malicious and accidental aspects. For example, the ISO/IEC 27005 standard [84] specifies information security risk in terms of threats of a natural or human origin that could be accidental or deliberate. In fact, the domain covered is even broader because it also states that "a threat may arise from within or from outside the organization". Interestingly, the ISO/IEC documents do not mention safety, which may explain the conceptual width given to the term security.

Unfortunately, the IETF and ISO/IEC security definitions are not in line with those that are used in specific CIP sectors. This is the case in the power grid and the nuclear power generation sectors (as discussed in Sections 4.1 and 4.2) as well as others such as the water, chemicals, and oil and gas sectors [107–109]. The pre-existence and importance of safety-related issues and standards (and the use of the term safety) in these domains may explain this situation. However, they may also have contributed to a rather confusing situation in which safety can also be defined in CIP as a very broad concept. The ISO/IEC standards are harmonized in several industrial disciplines around the definition of safety as "freedom from unacceptable risk" [5], whereas one of the most cited documents on dependable and secure computing for critical systems [11] defines safety as the "absence of catastrophic consequences on the user(s) and the environment". In such situations – as for the Internet – SEMA cannot draw clear limits between concepts whose definitions are inherently overlapping. Nevertheless, SEMA is an efficient tool for revealing semantic ambiguities (as illustrated by the lack of readability of Fig. 7); and it can help craft more consistent definitions.

5. Conclusions

Security and safety have different meanings depending on the context in which they are used. The CIP domain is particularly prone to these ambiguities because it involves multiple actors from multiple engineering disciplines. The SEMA framework can help identify and clarify the latent differences in the use of the terms security and safety. The power grid and nuclear power generation sectors provide excellent sector-specific cases for the use of SEMA. However, SEMA can be very useful in other situations such as the recent coordination between the US Federal Energy Regulatory Commission and the US Nuclear Regulatory Commission related to cyber security for nuclear power plants [110]. This is a scenario where security and safety have to be considered from a triple perspective: power grid, nuclear power generation and control systems/telecommunications.

Avoiding ambiguities in the meanings of the terms security and safety is important in system design, risk assessment, policy making and collaborative research. SEMA can be used to clarify inconsistencies and overlaps, helping save time and resources. In addition, SEMA can serve as a mnemonic tool to accommodate the various dimensions of risk and to ensure consistent and holistic risk coverage.

Our current research is proceeding along two avenues. First, we are augmenting the SEMA framework in order to explicitly differentiate between the physical and cyber dimensions [111] involved in computer systems used for security and safety. This would allow for a finer conceptual decomposition and a robust treatment of information security aspects such as confidentiality, integrity, availability and other derived properties. Second, we are investigating how the decompositions of the terms security and safety can support fine-grained analyses of their interdependencies. Security and safety issues are increasingly converging in critical systems, leading to interactions and side-effects ranging from mutual reinforcement to complete conflict. The analysis of such relations is a recurrent but open question [112,113] that is of considerable importance in the CIP domain.

REFERENCES

[1] M. Van Der Meulen, Definitions for Hardware and Software Safety Engineers, 1st ed., Springer, 2000.

[2] M.B. Line, O. Nordland, L. Røstad, 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, 2006.

[3] A. Burns, J. McDermid, J. Dobson, On the meaning of safety and security, The Computer Journal 35 (1) (1992) 3–15.

[4] International Atomic Energy Agency (IAEA), Safety glossary: terminology used in nuclear safety and radiation protection, Ref. STI/PUB/1290, 2007 ed., 2007.

[5] International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), Safety aspects — guidelines for their inclusion in standards, ISO/IEC Guide 51, 2nd ed., Jan. 1999.

[6] European Commission, Council directive 2008/114/EC of 8 december 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union (Dec) (2008).

[7] N. Leveson, Software safety: Why, what, and how, ACM Computing Surveys 18 (2) (1986) 125–163.

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

[9] 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.

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

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

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

[13] International Atomic Energy Agency (IAEA), Computer security of nuclear facilities, Reference manual (draft), 2009.

[14] International Atomic Energy Agency (IAEA), Fundamental safety principles, Safety Fundamentals No. SF-1, 2006.

[15] International Atomic Energy Agency (IAEA), Software for computer based systems important to safety in nuclear power plants, Safety Guide No. NS-G-1.1, Sep. 2000.

[16] International Electrotechnical Commission (IEC), Nuclear power plants – instrumentation and control important to safety – requirements for computer security programmes, IEC New Work Item Proposal (NWIP IEC62645), 2009.

[17] International Atomic Energy Agency (IAEA), Instrumentation and control systems important to safety in nuclear power plants, Safety Guide No. NS-G-1.3, Mar. 2002.

[18] International Atomic Energy Agency (IAEA), Safety of nuclear power plants: design, Safety Guide No. NS-R-1, Sep. 2000.

[19] US Nuclear Regulatory Commission (NRC), Protection of digital computer and communication systems and networks, Regulation 10 CFR73 part 54, Mar. 2009.

[20] International Atomic Energy Agency (IAEA) — International Nuclear Safety Advisory Group (INSAG), Basic safety principles for nuclear power plants, 75-INSAG-3, Rev. 1, Oct. 1999.

[21] US Nuclear Regulatory Commission (NRC), Criteria for use of computers in safety systems of nuclear power plants, Regulatory Guide 1.152, Revision 2, Jan. 2006.

[22] International Electrotechnical Commission (IEC), Nuclear power plants – instrumentation and control for systems important to safety – general requirements for systems, IEC 61513, Mar. 2001.

[23] International Electrotechnical Commission (IEC), Nuclear power plants – instrumentation and control systems important to safety – classification of instrumentation and control functions, IEC 61226, 2nd ed., Feb. 2005.

[24] US Nuclear Regulatory Commission (NRC), Cyber security programs for nuclear facilities, Regulatory Guide 5.71, Jan. 2010.

[25] International Electrotechnical Commission (IEC), Nuclear power plants – instrumentation and control systems important to safety – software aspects for computer-based systems performing category A functions, IEC 60880, 2nd ed., May 2006.

[26] International Electrotechnical Commission (IEC), Nuclear power plants – instrumentation and control important for safety – software aspects for computer-based systems performing category B or C functions, IEC 62138, Jan. 2001.
[27] Institute of Electrical and Electronics Engineers (IEEE), IEEE standard criteria for security systems for nuclear power generating stations, IEEE Std 692-2010, Feb. 2010.
[28] Korea Institute of Nuclear Safety (KINS), Cyber security of digital instrumentation and control systems in nuclear facilities, Regulatory Guidance KINS/GT-N09-DR, Jan. 2007.
[29] Institute of Electrical and Electronics Engineers (IEEE), IEEE standard criteria for safety systems for nuclear power generating stations, IEEE Std 603-1998, Jul. 1998.
[30] Institute of Electrical and Electronics Engineers (IEEE), IEEE standard criteria for digital computers in safety systems of nuclear power generating stations, IEEE Std 7-4.3.2TM-2003, Dec. 2003.
[31] International Electrotechnical Commission (IEC), Power systems management and associated information exchange – data and communications security, IEC 62351 series, 2007–2009.
[32] North American Electric Reliability Council (NERC), Reliability Standards for the Bulk Electric Systems of North America, Nov. 2009.
[33] North American Electric Reliability Council (NERC), Cyber security standards, CIP-002-1 through CIP-009-1, 2006.
[34] European Network of Transmission System Operators for Electricity, UCTE operation handbook — glossary, v2.2, Jul. 2004.
[35] US National Institute of Standards and Technology (NIST), Smart grid cyber security — strategy and requirements, NISTIR 7628 (draft), Sep. 2009.
[36] Institute of Electrical and Electronics Engineers (IEEE), IEEE guide for electric power substation physical and electronic security, IEEE Std 1402-2000, Jan. 2000.
[37] Institute of Electrical and Electronics Engineers (IEEE), IEEE standard for substation intelligent electronic devices (IEDs) cyber security capabilities, IEEE Std 1686–2007, Dec. 2007.
[38] Institute of Electrical and Electronics Engineers (IEEE), IEEE trial use standard for a cryptographic protocol for cyber security of substation serial links, IEEE P1711 (draft), 2007.
[39] European Commission, Regulation (EC) No. 2320/2002 of the European parliament and of the council of 16 december 2002 establishing common rules in the field of civil aviation security, Official Journal of the European Union (Dec.) (2002).
[40] International Civil Aviation Organization (ICAO), Safety oversight audit manual, Doc. 9735, 2nd ed., 2006.
[41] Radio Technical Commission for Aeronautics (RTCA), Software considerations in airborne systems and equipment certification, DO-178B, Jan. 1992.
[42] National Strategy for Aviation Security, US National Security Presidential Directives, Mar. 2007.
[43] European Organisation for the Safety of Air Navigation, ESARR 4 — risk assessment and mitigation in ATM, Apr. 2001.
[44] European Organisation for the Safety of Air Navigation, ESARR 6 — software in ATM systems, Nov. 2003.
[45] European Commission, Regulation (EC) No. 216/2008 of the European parliament and of the council on common rules in the field of civil aviation and establishing a European aviation safety agency, Official Journal of the European Union (Mar.) (2008).
[46] US Department of Homeland Security (DHS) — Transportation Security Administration, Rail transportation security, 49 CFR Parts 1520 and 1580, 2008.
[47] International Electrotechnical Commission (IEC), Railway applications — specification and demonstration of reliability, availability, maintainability and safety (RAMS), IEC 62278, Sep. 2002.
[48] International Electrotechnical Commission (IEC), Railway applications – communications, signalling and processing systems – software for railway control and protection systems, IEC 62279, Sep. 2002.
[49] Code of Federal Regulations, Part 1203 — information security program, Title 14: Aeronautics and Space.
[50] Code of Federal Regulations, Part 1203a — NASA security areas, Title 14: Aeronautics and Space.
[51] Code of Federal Regulations, Part 1203b — security programs; arrest authority and use of force by NASA security force personnel, Title 14: Aeronautics and Space.
[52] European Cooperation for Space Standardization (ECSS), Glossary of terms, ECSS-P-001B, Jul. 2004.
[53] US National Aeronautics and Space Administration (NASA), Standard for integrating applications into the NASA access management, authentication, and authorization infrastructure, EA-STD-0001, Jul. 2008.
[54] US National Aeronautics and Space Administration (NASA), NASA security program procedural requirements w/change 2, NASA Procedural Requirements 1600.1, Nov. 2004.
[55] US National Aeronautics and Space Administration (NASA), Software safety standard, NASA-STD-8719.13B w/Change 1, Jul. 2004.
[56] Norwegian Oil Industry Association (OLF), Information security baseline requirements for process control, safety, and support ICT systems, OLF Guideline No. 104, Dec. 2006.
[57] International Organization for Standardization (ISO), Petroleum and natural gas industries – offshore production installations – basic surface process safety systems, ISO 10418, 2nd ed., Oct. 2003.
[58] American Petroleum Institute (API), Pipeline SCADA security, STD 1164, Jul. 2009.
[59] International Organization for Standardization (ISO), Petroleum and natural gas industries – control and mitigation of fires and explosions on offshore production installations – requirements and guidelines, ISO 13702, Mar. 1999.
[60] International Organization for Standardization (ISO), Petroleum and natural gas industries – offshore production installations – guidelines on tools and techniques for hazard identification and risk assessment, ISO 17776, Oct. 2000.
[61] NORSOK, Technical safety, NORSOK Standard S-001, Jan. 2000.
[62] NORSOK, Safety and automation system (SAS), NORSOK Standard I-002, May 2001.
[63] Norwegian Oil Industry Association (OLF), Application of IEC 61508 and IEC 61511 in the Norwegian petroleum industry, OLF Guideline No. 70, Oct. 2004.
[64] Norwegian Oil Industry Association (OLF), Recommended guidelines: common model for safe job analysis (SJA), OLF Guideline No. 90, Mar. 2006.
[65] US Department of Homeland Security (DHS), Chemical facility anti-terrorism standards; final rule, 6 CFR Part 27, Apr. 2007.
[66] Center for Chemical Process Safety (CCPS), Combined glossary of terms, Mar. 2005.
[67] US Department of Homeland Security (DHS), Risk-based performance standards guidance, Chemical Facility Anti-Terrorism Standards, May 2009.
[68] North Atlantic Treaty Organization (NATO) Standardization Agency (NSA), NATO glossary of terms and definitions (English and French), AAP-6, 2009.
[69] North Atlantic Treaty Organization (NATO), NATO and R&M terminology applicable to ARMPs, AMRP-7, Aug. 2008.
[70] US Department of Defense (DoD), Standard practice for system safety, MIL-STD-882D, Jan. 1993.

[71] UK Ministry of Defence, Safety management requirements for defence systems – part 1 – requirements, Defence Standard 00-56, Jun. 2007.
[72] U.K. Ministry of Defence, Safety management requirements for defence systems – part 2 – guidance on establishing a means of complying with part 1, Defence Standard 00-56-2, Jun. 2007.
[73] International Electrotechnical Commission (IEC), Industrial communication networks – network and system security – part 1-1: terminology, concepts and models, Technical Specification IEC/TS 62443-1-1, Jul. 2009.
[74] International Electrotechnical Commission (IEC), Industrial communication networks – network and system security – part 3-1: security technologies for industrial automation and control systems, Technical Report IEC/TR 62443-3-1, Jul. 2009.
[75] International Electrotechnical Commission (IEC), Functional safety of electrical/electronic/programmable electronic safety-related systems, IEC 61508 series, 1998–2005.
[76] K. Stouffer, J. Falco, K. Scarfone, Guide to industrial control systems (ICS) security, NIST Special Publication 800-82, Sep. 2008.
[77] US National Institute of Standards and Technology (NIST), Information security, NIST Special Publication 800-53, revision 3, Aug. 2009.
[78] American National Standards Institute (ANSI), International Society of Automation (ISA), Security for industrial automation and control systems — part 1: terminology, concepts, and models, ANSI/ISA–99.00.01, Oct. 2007.
[79] UK Centre for the Protection of the National Infrastructure (CPNI), Process control and SCADA security, Good practice guide (version 2), 2008.
[80] International Electrotechnical Commission (IEC) & International Organization for Standardization (ISO), Information technology – security techniques – information security management systems — overview and vocabulary, IEC 27000, May 2009.
[81] International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC), Information technology – security techniques – information security management systems, ISO/IEC 27001, Dec. 2007.
[82] International Electrotechnical Commission (IEC), Information technology equipment – safety – part 1: general requirements, IEC 60950-1, 2nd ed., Dec. 2005.
[83] International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC), Information technology – security techniques – code of practice for information security management, ISO/IEC 27002, Jun. 2005.
[84] International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC), Information technology – security techniques – information security risk management, ISO/IEC 27005, Jun. 2008.
[85] International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC), Information technology – security techniques – management of information and communications technology security — part 1: concepts and models for information and communications technology security management, ISO/IEC 13335, Nov. 2004.
[86] R. Shirey, Internet security glossary, version 2, Internet Engineering Task Force (IETF), RFC 4949, Aug. 2007.
[87] International Telecommunication Union (ITU-T), Information technology – security techniques – information security management guidelines for telecommunications organizations based on ISO/IEC 27002, ITU-T X.1051, 2nd ed., Feb. 2008.
[88] US National Institute of Standards and Technology (NIST), Standards for security categorization of federal information and information systems, FIPS PUB 199, Feb. 2004.
[89] US National Institute of Standards and Technology (NIST), Glossary of key information security terms, NIST IR 7298, Apr. 2006.
[90] US Committee on National Security Systems (CNSS), National information assurance (IA), CNSS Instruction No. 4009, Jun. 2006.
[91] International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC), Guidelines for the inclusion of security aspects in standards, ISO/IEC Guide 81 (draft), Dec. 2009.
[92] International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC), Standardization and related activities — general vocabulary, ISO/IEC Guide 2, 8th ed., Nov. 2004.
[93] International Electrotechnical Commission (IEC), International electrotechnical vocabulary — chapter 191: dependability and quality of service, IEC 60500-191 and first amendment, Mar. 1999.
[94] International Electrotechnical Commission (IEC), Power systems management and associated information exchange – data and communications security part 1: communication network and system security — introduction to security issues, IEC 62351-1, May 2007.
[95] 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) (2009) 1174–1181.
[96] V. Madani, R. King, Strategies to meet grid challenges for safety and reliability, International Journal of Reliability and Safety 2 (1–2) (2008) 146–165.
[97] American Naional Standards Institute (ANSI) & Institute of Electrical and Electronics Engineers (IEEE), National electrical safety code (NESC), Accredited Standards Committee C2-2007, 2007.
[98] US National Grid, Electric safety, Website (last checked 8 June 2010) — http://www.nationalgridus.com/masselectric/safety_electric.asp.
[99] S. Abraham, National transmission grid study, US Department of Energy, May 2002.
[100] CIGRÉ, Institute of Electrical and Electronics Engineers (IEEE), Definition and classification of power system stability, Technical Brochure No. 231, Jun. 2003.
[101] HSPD-7 Homeland Security Presidential Directive for critical infrastructure identification, prioritization, and protection, US Presidential Directive, Dec. 2003.
[102] European Commission, Critical infrastructure protection in the fight against terrorism, COM(2004)702 final, Oct. 2004.
[103] 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 (Jun.) (2006) (in French).
[104] Institut de Radioprotection et de Sûreté Nucléaire, Approche comparative entre sûreté et sécurité nucléaires, Report (in French) 2009/117, IRSN, Apr. 2009.
[105] Nuclear Energy Institute (NEI), Cyber security program for power reactors, Std. NEI04-04, Feb. 2005.
[106] European Commission, Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience, Communications SEC (2009) 399 and SEC (2009) 400, Mar. 2009.
[107] US Department of Homeland Security (DHS), Roadmap to secure control systems in the chemical sector, Chemical Sector Roadmap WG, Sep. 2009.
[108] US Department of Homeland Security (DHS), Roadmap to secure control systems in the water sector, Water Sector Coordinating Council Cyber Security WG, Mar. 2008.

[109] US Department of Homeland Security (DHS), LOGIIC — linking the oil and gas industry to improve cybersecurity, Sep. 2006.
[110] US Federal Energy Regulatory Commission (FERC), Nuclear plant implementation plan for CIP standards, Cyber Security Order 706B, 2009.
[111] E.A. Lee, Cyber physical systems: design challenges, Tech. Rep. UCB/EECS-2008-8, University of Berkeley, EECS, Jan. 2008.
[112] V. Stavridou, B. Dutertre, From security to safety and back, in: Proceedings of the Computer Security, Dependability, and Assurance: From Needs to Solutions, CSDA'98, York, UK, 1998, pp. 182–195.
[113] M. Sun, S. Mohan, L. Sha, 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, 2009.