ANALISING SOME OF THE EXISTING RISK ASSESSMENT AND MANAGEMENT STANDARDS APPLIED WORLDWIDE, FOR ENERGY COMPANIES

VORONCA S. L.
CN Transelectrica SA,Bucuresti
simona.voronca@transelectrica.ro

Abstract - The paper reviews and categorizes the most relevant standards, guidelines, frameworks and methodologies about risk assessment and management, that could be useful to enhance energy companies risk assessment practices, allowing further on to determine a holistic, integrated method, applicable to operators of energy critical infrastructures.
It will be presented the criteria used in evaluation methodologies - especially on how to handle threats and vulnerabilities, standards and prescription coverage, along all risk management process - identification, quantification, prioritization, treatment and control, and areas of specific application.

Keywords: risk, energy companies, standards.

1. INTRODUCTION

The objective of this paper is to review and categorize the most relevant standards, guidelines, frameworks and methodologies about risk assessment and management, that could be useful to enhance energy companies risk assessment practices. The paper summarised a survey realised in 2011, in the framework of the EU project, Energy Control Center Risk Assessment and Management Methodology - ECCRAMM, developed by Symantec and Booz & Company, with Transelectrica acting as partner and end-user, project related to the enhancement of risk assessment methodologies against emerging threats for the protection of Energy SCADA systems, with specific focus on Energy Control Centers (ECC).

In performing this analysis, it has been considered and reviewed a great variety of different types of documents and publications, so to have a perspective as comprehensive as possible. It was considered standards and guidelines issued by global, regional and national organizations, consequently, it was signalled the geographic applicability of the various documents.

There were assessed documents which perform analyses at different levels of detail and specificity. Some of the analyzed standards and guidelines have a generalist approach and provide risk management methodologies applicable to virtually every kind of industry. Others focus either on the risks related to a certain type of industry (e.g. energy) or on a specific type of risk (e.g. IT risk).

It was taken into account both more general standards and documents with deeper technical content. Thus, the standards and guidelines analyzed may be directed to different audiences (e.g. manufacturers, operators, security managers) and may have different purposes (e.g. dealing with technical Issues; evaluation and certification).

Focused on risk assessment and management, the analyse presents, for the documents, the areas and the phases of the risk management process that are covered; then are considered whether and to what extent the standards and guidelines assess the threats and vulnerabilities which may affect an energy companies and whether or not they take into account the possible controls which are implemented to reduce the vulnerabilities.

The main results and findings of this review of the existing standards, guidelines and frameworks about risk assessment and management for energy companies, could be summarized, as follows:

1.1. Areas and fields covered, general information over the main topics and areas covered by the analyzed standards and guidelines. The documents are grouped and classified by the industry / field addressed. The standards/guidelines which have a general purpose and that are applicable across industries have been classified as “Global”. The other relevant elements included in the table are the geographic relevance, the type of risk covered and the audience targeted which allow having a first understanding of the relevance and of the applicability of the documents analyzed.

1.2. Risk management process coverage: analyzes for each document the phases of the risk management process (i.e. risk analysis, risk evaluation, risk reporting and risk monitoring & control) that it covers and whether it addresses them through qualitative or quantitative methodologies. Thus, allows to quickly find information on what documents may be relevant for dealing with a certain aspect of the risk management process and what standards/guidelines propose mitigation strategies and tools to deal with different types of risks and it also indicates the documents which may be used for auditing purposes.

1.3. Threats and vulnerabilities coverage, allowing to go more in detail in the process of risk assessment. The survey signals what documents presented categorizations or at least examples of threats and vulnerabilities which are relevant for energy companies. It is indicated whether the documents provide only a general categorization of threats and vulnerabilities or whether they cover more in depth some specific types of threats and vulnerabilities; also analysed what standards and guidelines evaluate the possible controls which are in place to reduce the vulnerabilities.

2. MAIN ORGANIZATIONS DEFINING STANDARDS OR GUIDELINES RELEVANT FOR ENERGY COMPANIES RISK ASSESSMENT AND MANAGEMENT

The following section lists and gives a short description of the main institutions relevant for energy critical infrastructures risk assessment and management. Beside international activities, also national activities of the United States and of some European countries are reported.

Table 1. Main institutions relevant for energy companies risk assessment and management

Institution	Geographic Relevance
CIGRE (International Council on Large Electric Systems)	Global
IEC (International Electrotechnical Commission)	Global
IEEE (Institute of Electrical and Electronics Engineers	Global
IRGC (International Risk Governance Council)	Global
ISA (International Society of Automation	Global
ISACA (Information Systems Audit and Control Association	Global
ISO (International Organization for Standardization	Global
ACC (American Chemistry Council)	United States
AGA (American Gas Association)	United States
API (American Petroleum Institute)	United States
COSO (Committee of Sponsoring Organizations of the Treadway Commission	United States
DOE (US Department of Energy)	United States
DHS (US Department of Homeland Security)	United States
ES-ISAC (Electricity Sector - Information Sharing and Analysis Center)	United States
Idaho National Laboratory	United States
NERC (North American Electric Reliability Corporation)	United States
NIST (National Institute of Standards and Technology)	United States
BSI (Bundesamt für Sicherheit in der Informationstechnik)	Europe
CPNI (Centre for the Protection of National Infrastructure)	United Kingdom
ENTSO-E (European Network of Transmission System Operators for Electricity)	Europe
EURELETRIC (Union of the Electricity Industry)	Europe
SEMA (Swedish Emergency Management Agency)	Sweden
ITSEAG (Information Technology Security Expert Advisory Group)	Australia

The institutions were classified according to this template:

Table 2. Template

Name	
Organizational form	e.g. non-profit organization; industry association; government agency/department
Geographic relevance	e.g. International, EU, US
Year of foundation	e.g. 2002
Composition	Number and type of members; sponsors; main bodies/organizational units
Key executives	e.g. President, CEO, General Secretary, General Director
Industry / field	e.g. oil and gas; cross industry; automation; risk governance; security
Areas of activity	Short description of the main activities

Table 3. An example

Name	**ISO (International Organization for Standardization)**
Organizational form	non-governamental organization
Geographic relevance	Global
Year of foundation	1947
Composition	Members are the national standards institutes of 163 countries.
Key executives	Alan Morrison (President); Rob Steele (CEO); Jacob Holmblad (Vice-President, technical management); Sadao Takeda (Vice-President, policy).
Industry / field	Cross industry
Areas of activity	ISO is the **world's largest developer and publisher of International Standards**. It has developed over 17500 International Standards on a variety of subjects and more than 1000 new ISO standards are published every year. ISO also publishes technical reports, technical

ISSN 2067-5534 © 2012 JSE

	specifications, publicly available specifications and guides. ISO, together with IEC, created the ISO/IEC Joint Technical Committee which deals with all matters of information technology. Its purpose is to develop, maintain, promote and facilitate IT standards required by global markets, meeting business and user requirements. **Among the standards published by ISO, the series ISO 2700x defined a set of standards for information security management, while ISO 31000 established general principles for risk management.**

3. LIST OF IDENTIFIED STANDARDS AND GUIDELINES

Standards, guidelines and other publications relevant for energy companies are reported in the following table:

Table 4. Relevant documents

Institution	Title	Type
ACC	Guidance for Addressing Cyber Security in the Chemical Industry Version 3.0	Guideline
AGA	AGA Report No. 12, Cryptographic Protection of SCADA Communications	Guideline
AIRMIC, ALARM, IRM	A risk management standard	Standard
API	Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries	Guideline
API	API Std 1164 - SCADA Security, First Edition	Standard
API	Security Guidelines for the Petroleum Industry	Guideline
Austrian Federal Chancellery	Austrian IT Security Handbook	Guideline
British Office of Government Commerce	CRAMM (CCTA Risk Analysis and Management Method	Frame-work
BSI	IT-Grundschutz	Guideline
CIGRE	Management of Information Security for an Electric Power Utility - On Security Domains and Use of ISO/IEC17799 Standard	Guideline
CLUSIF	Méthode Harmonisée d'Analyse de Risques Informatiques (MEHARI)	Frame-work
COSO	COSO - Enterprise Risk Management - Integrated Framework	Frame-work
CPNI	Good Practice Guide - Process Control and SCADA Security, Overview, Parts 1 to 6	Guideline
DOE	Roadmap to Secure Control Systems in the Energy Sector	Guideline
DOE	Risk Management Guide	Guideline
DOE / ES-ISAC	DOE Vulnerability and Risk-Assessment Methodology	Guideline
DOE / ES-ISAC	Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities	Guideline
DHS	Catalogue of Control Systems Security: Recommendations for Standards Developers	Guideline
DHS	Risk Analysis and Management for Critical Assets Protection	Guideline
Dutch Government	DHM Security Management	Guideline
Dutch Ministry of the Interior and Kingdom Relations	NRB	Guideline
EURAM	European Risk Assessment Methodology	Guideline
EURELECTRIC	Operational Risk Methodology - Scenario Analysis	Frame-work
French Government	EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)	Guideline
HM Treasury	The Orange Book - Management of Risk - Principles and concepts	Frame-work
IEC	IEC 62531 Data and Communication Security	Standard
IEC	IEC 61508 Functional safety of electrical/electronic/ programmable electronic safety related systems	Standard
IEC	IEC 62210 - Power system control and associated communications - Data and communication security	Standard
IEEE	IEEE Guide for Electric Power Substation Physical and Electronic Security	Standard
IRGC	Risk governance - Toward an integrative	Frame-work

	approach	
ISA	ISA TR99.03.01 - Security Technologies for Industrial Automation and Control Systems	Standard
ISA	ISA 99.02.01 - Establishing an IACS Security Program	Standard
ISACA	The Risk IT Framework	Frame-work
ISO	ISO 31000 - Risk management – Principles and guidelines	Standard
ISO	ISO/IEC 27005:2008 Information technology - Security techniques - Information security risk management	Standard
ISO	ISO 15408 Common criteria for information technology security evaluation	Standard
ISO	ISO/IEC 13335-1:2004 Information technology – Guidelines for the Management of IT security	Standard
ITSEAG	Generic SCADA Risk Management Framework	Frame-work
NAVI	Good Practices for Risk Analysis	Guideline
NERC	CIP 001-009 - Reliability Standards for the Bulk Electric Systems in North America	Regulation
NERC	Security Guidelines for the Electricity Sector	Guideline
NIST	NIST 800-30 Risk Management Guide for Information Technology Systems	Guideline
NIST	NIST 800-82 Guide to Industrial Control Systems (ICS) Security	Guideline
NIST	System Protection Profile - Industrial Control Systems	Specifica-tion
ENTSO-E	Octavio Control Center Security	Workshop
SEMA	Guide to Increased Security in Process Control Systems for Critical Societal Functions Guideline	Standards
Australia/ Standards New Zealand Commit-tee	AS/NZS 4360:2004: Risk Management	Standard

4. RISK RELATED CRITERIA

Standards and guidelines were categorized by considering:

Process coverage: Evaluation of whether or not the document covers one or more of these three main processes: Risk Management; Audit; Maintenance & Alignment. Risk management is further divided in sub-phases:

- Risk assessment: It includes risk analysis and risk evaluation which be qualitative or quantitative;
- Risk reporting: Covered or not;
- Risk Monitoring & Control: Covered or not;
- Mitigations: Covered or not; just examples or more detailed mitigation strategies.

Risk Type: Type of risk addressed by the standard or guideline. E.g. general, IT-related, SCADA-related;

Area coverage: Considers whether the document treats or at least gives examples of the following aspects:

- Threats: They may be classified in Categories; Categories+ list; Natural hazard; Manmade /fraudulent; Cyber Attacks;
- Vulnerabilities: They may be classified as: Personal; Information; ICT assets; Physical assets;
- Controls: Mechanisms already in place to reduce the vulnerabilities.

5. EXAMPLES OF DETAILED DESCRIPTION OF A STANDARD / GUIDELINES

Further on, we present some examples of detailed description form some of the standards analysed:

ISSN 2067-5534 © 2012 JSE

COSO (Committee of Sponsoring Organizations of the Treadway Commission)

Institution	COSO
Identifier	
Title	COSO - Enterprise Risk Management - Integrated Framework
Status	Final
Type	Framework
Latest update	Sept 2004
Geographic relevance	International
Addressed Industry	Generic
Addressed Audience	Manufacturer: X Operator: X Security Management: X Technical Issues: Evaluation/Certification: X
Cross References	
Short Description	The document is thought for auditing purposes. It provides a very detailed framework for dealing with the various aspects of risk management, ensuring compliance with applicable laws and regulations. It provides also application techniques to put in practice the framework. It identifies eight components of risk management which should be adequately applied at different organizational levels.

Process coverage	**Risk Management**	Risk assessment	Risk analysis	X
			Risk evaluation	X
		Risk reporting		*Process*
		Risk monitoring & control		X
		Mitigations		
	Audit			*Specific for audit*
	Maintenance & Alignment			X
Risk Type				*General*
Area Coverage	**Threats**	Categories		
		Categories+list		
		Natural Hazard		
		Manmade/fraudulent		
		Cyber		
	Attacks			
	Vulnerabilities	Personal		
		Information		
		ICT Assets		
		Physical Assets		
	Controls			

HM Treasury

Institution	HM Treasury
Identifier	
Title	The Orange Book - Management of Risk - Principles and concepts
Status	Final
Type	Framework
Latest update	Oct 2004
Geographic relevance	UK, International
Addressed Industry	Generic
Addressed Audience	Manufacturer: Operator: X Security Management: X Technical Issues: Evaluation/Certification:
Cross References	COSO ERM - Integrated Framework, 2004; AS/NZS 4360:2004; ARMS, 2002
Short Description	Provides a general framework for dealing with the different phases of the risk management process. It is applicable to virtually every industry and type of risk. Regarding risk identification, it offers a summary of the most common categories of risk and of the related issues. It does a quite detailed analysis of risk appetite at different organizational levels.

Process coverage	**Risk Management**	Risk assessment	Risk analysis	*Qualitative*
			Risk evaluation	*Qualitative*
		Risk reporting		*Process*
		Risk monitoring & control		X
		Mitigations		
	Audit			
	Maintenance & Alignment			X
Risk Type				*General*
Area Coverage	**Threats**	Categories		
		Categories+list		
		Natural Hazard		
		Manmade/fraudulent		
		Cyber		
	Attacks			
	Vulnerabilities	Personal		
		Information		
		ICT Assets		
		Physical Assets		
	Controls			

ISO (International Standards Organization)

Institution	ISO
Identifier	ISO 31000
Title	Risk management – Principles and guidelines
Status	Final
Type	Standard
Latest update	2009
Geographic relevance	International
Addressed Industry	Generic
Addressed Audience	Manufacturer: Operator: Security Management: X Technical Issues: Evaluation/Certification: X
Cross References	ISO Guide 73:2009; ISO/IEC 31010
Short Description	Provides principles and generic guidelines on risk management and is not specific to any industry or sector. ISO 31000:2009 can be applied to any type of risk, whatever its nature, whether having positive or negative consequences.

Process coverage	**Risk Management**	Risk assessment	Risk analysis	X
			Risk evaluation	X
		Risk reporting		*Process*
		Risk monitoring & control		X
		Mitigations		
	Audit			
	Maintenance & Alignment			X
Risk Type				*General*
Area Coverage	**Threats**	Categories		
		Categories+list		
		Natural Hazard		
		Manmade/fraudulent		
		Cyber		
	Attacks			
	Vulnerabilities	Personal		
		Information		
		ICT Assets		
		Physical Assets		
	Controls			

AIRMIC, ALARM, IRM

Institution	AIRMIC, ALARM, IRM
Identifier	AIRMIC, ALARM, IRM: 2002
Title	A risk management standard
Status	Final
Type	Standard
Latest update	2002
Geographic relevance	International
Addressed Industry	Generic
Addressed Audience	Manufacturer: Operator: Security Management: X Technical Issues: Evaluation/Certification: X
Cross References	ISO/IEC Guide 73:2002
Short Description	Provides principles and generic guidelines on risk management and is not specific to any industry or sector. It can be applied to any type of risk, whatever its nature, whether having positive or negative consequences.

Process coverage	**Risk Management**	Risk assessment	Risk analysis	X
			Risk evaluation	X
		Risk reporting		*Process*
		Risk monitoring & control		X
		Mitigations		
	Audit			
	Maintenance & Alignment			X
Risk Type				*General*
Area Coverage	**Threats**	Categories		
		Categories+list		
		Natural Hazard		
		Manmade/fraudulent		
		Cyber		
	Attacks			
	Vulnerabilities	Personal		
		Information		
		ICT Assets		
		Physical Assets		
	Controls			

CIGRE (International Council on Large Electric Systems)

Institution	CIGRE Joint Working Group D2/B3/C2-01
Title	Management of Information Security for an Electric Power Utility - On Security Domains and Use of ISO/IEC17799 Standard
Status	Final
Type	Guideline
Latest update	
Geographic relevance	France, Europe
Addressed Industry	Energy
Addressed Audience	Manufacturer: Operator: X Security Management: X Technical Issues: Evaluation/Certification:
Cross References	ISO/IEC 17799
Short Description	The guideline presents the work of the Cigré Joint Working Group D2/B3/C2-01 "Security for Information Systems and Intranets in Electric Power Systems". The paper focuses on the following subjects: stressing the importance of handling information security within an electric utility, the dealing with various threats and vulnerabilities, the evolution of Power Utility Information Systems from isolated to fully integrated systems, the concept of using security domains for dealing with information security within an electric utility, and the use of the ISO/IEC 17799 standard.

Process coverage	**Risk Management**	Risk assessment	Risk analysis	X
			Risk evaluation	X
		Risk reporting		
		Risk monitoring & control		
		Mitigations		
	Audit			
	Maintenance & Alignment			
Risk Type				*IT risks*
Area Coverage	**Threats**	Categories		X
		Categories+list		
		Natural Hazard		
		Manmade/fraudulent		
		Cyber		X
	Attacks			
	Vulnerabilities	Personal		
		Information		X
		ICT Assets		X
		Physical Assets		
	Controls			

DOE (US Department of Energy)

Institution	DOE
Identifier	DoE / DHS Roadmap
Title	Roadmap to Secure Control Systems in the Energy Sector
Status	Final
Type	Guideline
Latest update	Jan 2006
Geographic relevance	US
Addressed Industry	Energy
Addressed Audience	Manufacturer: X Operator: X Security Management: X Technical Issues: Evaluation/Certification:
Cross References	
Short Description	The Roadmap outlines a plan for improving cyber security in the energy sector, and provides a strategic framework for guiding industry and government efforts based on a vision supported by goals and time-based milestones. It addresses the energy sector's most urgent challenges as well as longer-term needs and practices.

Process coverage	**Risk Management**	Risk assessment	Risk analysis	X
			Risk evaluation	
		Risk reporting		
		Risk monitoring & control		
		Mitigations		X
	Audit			
	Maintenance & Alignment			
Risk Type				*IT risks*
Area Coverage	**Threats**	Categories		
		Categories+list		
		Natural Hazard		
		Manmade/fraudulent		
		Cyber		
	Attacks			
	Vulnerabilities	Personal		
		Information		
		ICT Assets		
		Physical Assets		
	Controls			X

ISSN 2067-5534 © 2012 JSE

Institution	DOE
Identifier	DOE G 413.3-7
Title	Risk Management Guide
Status	Final
Type	Guideline
Latest update	16/09/2009
Geographic relevance	US, International
Addressed Industry	Energy
Addressed Audience	Manufacturer: Operator: X Security Management: X Technical Issues: X Evaluation/Certification:
Cross References	
Short Description	Provides a comprehensive guide for all the phases of the risk management process. Initially, it gives a method for breaking down the overall risk of a project and establishing the responsibilities for risk management. It suggests both qualitative and quantitative methods for risk assessment. It proposes a matrix combining the probability and consequences of risks, rating risks as low, moderate and high. Quantitative analysis is mainly based on Monte Carlo simulations. The attachments propose practical tools for the various phases of the risk management process.

Process coverage	**Risk Management**	Risk assessment	Risk analysis	***Qualitative & quantitative***
			Risk evaluation	***Qualitative***
		Risk reporting		***Process***
		Risk monitoring & control		***X***
		Mitigations		
	Audit			
	Maintenance & Alignment			***X***
Risk Type				***General***
Area Coverage	**Threats**	Categories		
		Categories+list		
		Natural Hazard		
		Manmade/fraudulent		
		Cyber		
	Attacks			
	Vulnerabilities	Personal		
		Information		
		ICT Assets		
		Physical Assets		
	Controls			

6. FINDINGS

In total were identified 47 relevant standards, guidelines or frameworks in the area of energy companies risk assessment and management. The survey has included both more general publications and documents dealing with more specific aspects of risk management and security.

Classification based on general criteria

Geographic relevance: 15 standards / guidelines were developed by global organizations, 15 by US ones, 5 by EU ones, 3 by UK ones, 3 by Dutch, 2 by Australian, 2 by German and 2 by French. Even if some standards were created by national or regional institutions on the basis of their geographical specificities, they have a broader relevance and are applicable also to other countries.

Industry / field addressed: 17 standards / guidelines are generic and so can be applied across industries and fields; 9 address information and communication technology; 11 are about energy; 5 are about critical infrastructure; 4 are about oil & gas; 1 is about the chemical industry.

Classification based on risk related criteria

Risk assessment: Virtually all the standards/guidelines address risk analysis and risk evaluation through qualitative methodologies. One of the few exceptions is represented by EURELECTRIC - "The Operational Risk Methodology - A Scenario Analysis" which provides a detailed methodology to estimate in a quantitative way the operational risk for the electricity industry. DOE - "Risk Management Guide" also covers some quantitative techniques for risk assessment, but does not go so much in depth in its analysis.

Mitigations: 12 standards/guidelines give concrete examples of mitigations and suggest applicable mitigation tools and strategies. Some standards (e.g. ISA 99.02.01) propose an integrated mitigation system, others (e.g. IRGC - "Risk governance - Toward an integrative approach") present a variety of mitigation techniques which may be suitable for dealing with different types of risks. In any case, the mitigation strategies illustrated in these standards are not thought to be exhaustive; rather they aim at providing the organizations with some practical examples and suggestions in order to help them define the mitigation system which is more suitable for their specific characteristics and operational context.

Audit: 5 standards/guidelines are suitable for auditing purposes. They are developed by institutions that deal specifically with audit such as COSO (Committee of Sponsoring Organizations of the Treadway Commission) and ISACA (Information System Audit and Control Association). These standards provide organizations with a detailed guidance to implement a risk management methodology and a security system which are perfectly compliant with the existing regulations. They also help the organizations clearly define responsibilities and the accountability for the different phases of the risk management process.

Risk Type: 21 standards/guidelines cover general risks, while 26 address IT-related risks. Some standards (e.g. ISO 31000) consider generic risks across industries, while other standards (e.g. DOE - "Risk Management Guide") look at generic risks for a specific sector (e.g. energy). EURELECTRIC - "The Operational Risk Methodology – A Scenario Analysis" estimates operational risk (which may come in a variety of forms) for the electricity industry.

Regarding IT-related risks, some standards (e.g. ISO/IEC 27005:2008) focus on IT risk in general, while others (e.g. AGA - "Cryptographic Protection of SCADA Communications") deal specifically with SCADA security.

Threats: 26 standards/guidelines provide some kind of categorization, description and practical examples of threats. They present a different level of detail: some standards just identify some general typologies of threats, while some others (e.g. ISA TR99.03.01) describe more in depth a specific type of threat (e.g. cyber threats).

Vulnerabilities: 14 standards/guidelines provide some kind of categorization, description and practical examples of vulnerabilities. Some standards present cases of vulnerabilities just to better illustrate their general framework using some practical examples. For instance,

ISO/IEC 27005:2008 develops a general methodology widely applicable across industries and then, in one its annexes, it gives many examples of vulnerabilities together with the threats which may exploit them. Other guidelines (e.g. DOE - "Vulnerability and Risk Assessment Methodology") follow a bottom-up approach and start from a list of possible vulnerabilities to create a risk assessment framework.

Controls: 15 standards/guidelines examine the control mechanisms which organizations may have in place to reduce the likelihood of a negative event and its possible impact. DHS - "Catalog of Control Systems Security" gives the most detailed list of recommended security controls that organizations from various industries may have implemented to counteract various types of threats.

7. CONCLUSIONS

Some of the analyzed standards and guidelines have a **generalist approach** and provide risk management methodologies applicable to virtually every kind of industry (e.g. HM Treasury - "The Orange Book-Management of Risk - Principles and concepts"; ISO 31000. They could be used in the energy sector, but they would not be able to fully capture its peculiarities. In developing a specific methodology for energy companies, they might be utilized as a reference to make sure to proceed in a rational and systematic way.

Some standards and guidelines (e.g. DOE - "Risk Management Guide"; NERC - "Reliability Standards for the Bulk Electric Systems in North America"; NERC - "Security Guidelines for the Electricity Sector") offer a guidance to deal with **risk in the energy sector**, covering various aspects and types of risk. However, they lack a clear focus on energy companies to be considered as the ideal methodologies for performing energy critical infrastructure risk assessment and management. Moreover, most of them focus on the US context rather than on the European one.

The key finding of this paper, resulting from the review of the existing standards and guidelines, is that, at the moment, there is not a comprehensive methodology for risk assessment and management for energy companies. There are general frameworks which are not able to fully address the needs of the Transmission System Operators and to capture all the specificities of energy critical infrastructures. There are more technical standards that lack the broader perspective which is required to perform an adequate risk assessment and management for energy companies.

CN Transelectrica is participating in many international projects, financed under EU Seventh Framework Programme for Research and Technological development FP7: Energy Control Center Risk Assessment and Mitigation Methodology ECCRAMM, Securing the European Electricity Supply Against Malicious and Accidental Threats SESAME, Critical Response in Security and Safety Emergencies CRISYS, European Risk Assessment and Contingency Planning Methodologies for Interconnected Energy Networks EURACOM. Reviewing the most relevant standards, guidelines, frameworks and methodologies about risk assessment and management, is a common baseline in developing, in international projects, more integrated and comprehensive risk assessment methodologies for energy critical infrastructures, useful to enhance energy critical infrastructure companies risk assessment practices.

REFERENCES

[1]. EURACOM, European Risk Assessment and Contingency Planning Methodologies for Interconnected Energy Networks, Common areas of Risk Assessment Methodologies, FP7, 2010;

[2]. ECCRAMM, Energy Control Center Risk Assessment and Mitigation Methodology, Symantec, Stefano BUSCHI, Booz&Co, 2011;

[3]. Energy Control Centers & SCADA Protection Against Emerging Information Security Threats, Symantec, Booz&Co, 2011;

[4]. Generating a European risk assessment methodology for critical infrastructures, EURAM, European Risk Assessment Methodology, 2008;

[5]. EURELECTRIC Working Group on Risk, Risk Management în the Electricity Industry – White Paper, 2007;

[6]. HM Treasury The Orange Book - Management of Risk - Principles and concepts, 2004;

[7]. Australia/Standards AS/NZS 4360:2004: Risk Management New Zealand Committee, 2004;

[8]. A risk management standard, AIRMIC, ALARM, IRM, 2002;

[9]. CIGRE Management of Information Security for an Electric Power Utility - On Security Domains and Use of ISO/IEC17799 Standard, 2005;

[10]. COSO - Enterprise Risk Management - Integrated Framework, 2004;

[11]. DOE, Risk Management Guide, 2009;

[12]. DOE/ES-ISAC, DOE Vulnerability and Risk-Assessment Methodology, 2002;

[13]. DOE/ES-ISAC, Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities, 2002;

[14]. IRGC, Risk governance - Toward an integrative approach, 2006;

[15]. ISO ISO 31000 - Risk management – Principles and guidelines, 2009;

[16]. ISO ISO/IEC 27005:2008 Information technology - Security techniques - Information security risk management.

 ISSN 2067-5534 © 2012 JSE