419

Treatment of Information Security for Electric Power Utilities (EPUs)

Working Group
D2.22

June 2010

Treatment of Information Security for Electric Power Utilities (EPUs)

Working Group D2.22

Members

Göran Ericsson, Convenor (SE), Åge H Torkilseng, Secretary (NO) Giovanna Dondossola (IT), Stuart Duckworth (GB), Andrew Bartels (US), Thomas Kropp (US), Ludovic Piètre-Cambacédès (FR), Marc Tritschler (GB), Andreï Vidrascu (FR), Tor Aalborg (NO)

Corresponding members:
Dennis K. Holstein (US), Rodolfo Pellizzoni (AR), Erik Sandström (SE), Joe Weiss (US),
As of Aug 2008: Robert Evans (Australia)

Expert invited for Risk Assessment:
Gerben Heslinga (NL)

Disclaimer notice

ISBN: 978-2-85873-106-0

SUMMARY

This Technical Brochure (TB) covers the efforts of Working Group WG D2.22 "Treatment of Information Security for Electric Power Utilities (EPUs)". The work has been carried out between 2006 and 2009. The WG D2.22 is the successor of Joint Working Group (JWG) D2/B3/C2-01 on "Security for Information Systems and Intranets in Electric Power System" (2003 – 2006/2007). The WG D2.22 has focussed and deepened the study on the following three issues:

- *Frameworks for EPUs* on how to manage information security,
- *Risk assessment (RA)*: Common models and methods for treating vulnerabilities, threats and attacks, and
- *Security technologies* for SCADA (Supervisory Control And Data Acquisition)/control systems including real time control networks.

As intermediate results, the WG D2.22 has produced the following six papers which are included as appendices:

1. Å. Torkilseng, S. Duckworth: "**Security Frameworks for Electric Power Utilities - Some Practical Guidelines when developing frameworks including SCADA/Control System Security Domains**", Electra, No. 241, December 2008.
2. G. Dondossola: "**Risk Assessment of Information and Communication Systems - Analysis of some practices and methods in the Electric Power Industry**", CIGRÉ Electra, No. 239, August 2008.
3. M. Tritschler, G. Dondossola: "**Information Security Risk Assessment of Operational IT Systems at Electric Power Utilities**", Paper D2-01 D03, Cigré D2 Colloquium, October 21-22, 2009, Fukuoka, Japan.
4. A. Bartels, L. Pietre-Cambacédès, S, Duckworth: "**Security Technologies Guideline – Practical Guidance for Deploying Security Technology within Electric Utility Data Networks**", Electra, No. 244, June 2009.
5. L. Pietre-Cambacédès, T. Kropp, J. Weiss, R Pellizzonni: "**Cybersecurity standards for the electric power industry – a survival kit**" – Paper D2-217, CIGRÉ Paris Session 2008, France
6. G. Ericsson, A. Bartels, D. Dondossola, Å. Torkilseng: "**Treatment of information security for electric power utilities – progress report from Cigré WG D2.22**" Paper D2-213, Cigré Paris 2008 Session, France.

It is concluded that an overall security framework should be based on existing standards and "best practices", taking into account legal and regulatory requirements. A framework should be based on risk assessment. The technical solution should be based on the domain model and the assigned technical security controls. The selection of the "proper" standard(s) is delicate.

It is evident that information security for an EPU will continue to be an important issue, in both the short and long run. As natural further works, the following are proposed: 1) To improve methods for use of security frameworks and deploying risk assessment methods; 2) To more deeply involve and get acceptance from management regarding the importance of information and IT security; 3) To embed information security as a natural and mandatory part through all phases of a project, from specification through acceptance, and throughout the operational life of a system.

KEYWORDS

Electric Power Industry, Electric Power Utility, Information Security, Cyber Security, IT Security, security framework, Risk Assessment, security technology, SCADA, ISO/IEC standard, control systems, industrial control systems, power system control, power systems, governance, security controls.

Contents

1 Introduction

Since the beginning of this new millennium, the need for treating Information Security for Electric Power Utilities (EPUs) has become more evident among utilities, vendors, consultants, governments, standards and regulatory bodies, around the globe. Within Cigré, the first steps were taken in 2002 when the Joint Working Group (JWG) D2/B3/C2-01 – "Security for Information Systems and Intranets in Electric Power Systems" – was launched. The JWG delivered its Technical Brochure (TB) in 2006 [7], where the purpose was to raise the awareness of information/cyber security in Electric Power Systems. Also, the "domain concept" for managing information security was introduced, and it has become a good practice recommended in subsequent publications on cyber security in the Electric Power Industry. The focus of the TB was mostly on the management issues, rather than on technical details. It was concluded that there is a need for a comprehensive Information and Control Systems Security Framework for electric utilities. Management of Information Security must be an essential and natural part of daily operations of various tasks in an EPU.

As a successor of the JWG D2/B3/C2-01, the WG D2.22 "Treatment of Information Security for Electric Power Utilities" was formed in 2006. Here in WG D2.22, the scope has been narrowed, in order to focus on and study certain aspects being raised in the former JWG. The following three issues have been studied: *Frameworks for EPUs, Risk assessment (RA), and Security technologies* for SCADA (Supervisory Control And Data Acquisition) systems.

The term of office for the WG D2.22 has been between 2006 and 2009. The main deliverable is this TB. As intermediate results, the WG has produced the six papers [1-6] which are included as appendices to the TB.

1.1 Why is Information Security important?

Proper treatment of Information Security has received increased attention within the Electric Power Utilities (EPUs) during the last ten years. As providers of life-critical products and services, EPUs need to develop new security systems and procedures that are responsive to the improvements in ICT (Information and Communications Technology) and also recognize the development of threats and attacks. This implies that utilities not only need to deal with physical intrusion, but also with cyber intrusion. Cyber security has become a critical issue, and this is expected to develop even more.

Therefore, Cigré has initiated works within this area. The first effort was carried out by the Joint Working Group (JWG) "Security for Information Systems and Intranets in Electric Power Systems" D2/B3/C2-01, which delivered its Technical Brochure in 2006 [7]. Thereafter in 2006, the WG D2.22 "Treatment of Information Security for Electric Power Utilities" was formed.

The WG D2.22 follows the work delivered by JWG D2/B3/C2-01. The JWG covered Information and Control System Security on a broad basis using a top-down approach. The JWG concluded that no comprehensive information security guidelines exist. The focus was mainly on the management issues, such as raising the awareness of information security and giving some guidance on security problem solving using a domain modelling concept. The key issues of risk assessment methodologies for the security analysis of electric power control sys-

tems were discussed [21]. Also, partial treatment of technical issues for control system security in substation automation was done.

In WG D2.22, the scope has been narrowed compared to the JWG D2/B3/C2-01, in order to focus on and study certain aspects and solve specific questions being raised in the former JWG. The scope has been to study the following three issues:

- Frameworks for EPUs: How to manage information security for all organizational units of the Electric Power Utility including power system operation.
- Risk assessment: Common models and methods for managing vulnerabilities, threats and attacks.
- Security Technologies: Effective strategies for applying appropriate security technologies to secure EPU technical infrastructures.

By having this focus, the WG has striven towards a common understanding and terminology for handling of information and control system security for Electric Power Utilities.

1.2 Reported Cyber Security Incidents

Various cyber security intrusion studies by the U.S. Department of Energy (DOE) and by commercial security consultants have demonstrated the cyber vulnerabilities of control systems to unauthorized access. There have been many real-world cases where control systems have been impacted by electronic means. Events have occurred in electric power control systems for transmission, distribution, generation, as well as control systems for water, oil/gas, chemicals, paper, and agricultural businesses. Some of these events have resulted in damage, e.g., confirmed damages from cyber intrusions have included intentionally opening breaker switches and shutdown of industrial facilities [38]. Very few of the reported incidents have been publicly described and initiatives aimed at creating an open repository of industrial security incidents encounter understandable resistance.

Cyber attackers have a range of capabilities and motives. Threat agents can arise from many groups of people, such as: hackers, employees, insiders, contractors, competitors, traders, foreign governments, organized crime, extremist groups, terrorists, and alliances of all groups. These potential attackers will also have a wide range of capabilities, resources, organizational support, and motivations.

It is also important to recognize that both accidental and malicious cyber threats exist due to the complexities of modern day systems which give rise to increases in:

- Risk of accidental unauthorized logical access to components/devices/equipment;
- Risk of accidental operation of components/devices/equipment through unauthorized logical access;
- Risk of individual component/device/equipment failure (including software and networks);
- Number of failure modes, both directly due to increased component/device/equipment count, and indirectly due to increased (and often unknown) interdependencies between components/devices/equipment;
- Risk of accidental mis-configuration of components/devices/equipment;

- Risk of failure through not implementing appropriate maintenance activities (e.g., patch management, system housekeeping);
- Risk of failure through implementing more complex maintenance activities incorrectly (e.g., patch management, system housekeeping).

1.3 Principal Distinguishing Features of Modern Power Systems

Only a generation ago, the Vertically Integrated Utility (VIU) was the most usual form of organisation in the power supply industry. The adoption of a business model designed to encourage competition and to force the separation of generation, transmission, and distribution and supply businesses has dramatically altered the structure of the power supply industry. In parallel with these structural changes the potential of computer systems to support change has lead to the installation of a multitude of ICT systems, many of which depend on interconnectivity and inter-operability to achieve their objectives.

The power sector is presently characterised by a large and expanding number of participants, each of whom has a requirement to communicate with almost any other participant in the sector. E.g., the following participants are evident: *Transmission System Operators (TSO), Regional or National System Operators, Energy Market Operators, Transmission Companies, Distribution Companies, Generation Companies, Consumers, Industrial Control System Vendors, Regulators,* and now *Cyber Security Solution Providers*. In the upcoming electronic "E-Energy" era, secure ICT solutions are envisaged for the Operation/Maintenance of the Operational Process Layer (with Smart Generation, Smart Grids and Smart Customers), for the Marketplace applications of the Business Layer, as well as for coupling Business Layer and Operational Process Layer ICT infrastructures.

1.4 Purpose of Technical Brochure (TB)

The purpose of the work described in this TB has been to continue the work described in JWG TB [7], and deepen the work on Security Frameworks, Risk Assessment, and Security Technologies. The work has been carried out by producing six papers, and while the highlights are given here, the papers are included as appendices.

1.5 Outline

The Technical Brochure is outlined as follows. In Section 2, Frameworks on Management of Information are treated. Thereafter in Section 3, Risk Assessment is treated. In Section 4, Guidance on Security Technology Deployment is discussed. Section 5 covers standards related to cyber security for SCADA systems. In Section 6, proposals for further works are given. The TB Conclusions are given in Section 7. In Section 8, references are given. Papers 1-6 produced by the WG D2.22 are included as appendices.

2 Frameworks

The objective of this part of work is to provide some practical guidelines when developing frameworks that include SCADA/control system security domains. This is done by elaborating the specific security requirements of these types of domains, and also by giving a view of interrelated domains and high level frameworks that are necessary to manage corporate risks.

2.1 The Selection of Standards, Best Practices, and Guidelines

There has been a general discussion within WG D2.22 about the process of selecting the "right" standards for EPU security. The conclusion is that WG D2.22 should not attempt to select standards on behalf of the Electric Power Industry but aim to support the EPUs in the selection process by analyzing some of the most important approaches and try to achieve a consensus on the best "pieces". The work of [5] gives an overview of relevant standards that support the EPUs in the selection by presenting some of the most important approaches. It is also treated in Section 5. The selection may consider cultural tradition, sometimes bound to specific or international regional standard bodies, but also take into account the technical or business environment.

2.2 Definitions of Security Frameworks

Here, no rigorous and precise definition of "security framework" is used. "Security framework" can here be considered as the skeleton upon which various elements are integrated for the appropriate management of security risk. The elements that are elaborated on are Security Domains, Security Policies and Security Processes. Other framework elements elaborated by WG D2.22 are Risk Assessment and Security Technologies.

2.3 Alignments to other types of Frameworks

First, at the top level an EPU could be using frameworks to manage the overall corporate EPU risk profile, including market, financial and operational risks which encompass Information Technology (IT) and control system risks. Second, the EPU could be using frameworks for IT service management describing in detail the IT processes necessary to deliver high quality IT services that support business processes. Figure 1 shows an example of a layered framework architecture providing an integrated approach to risk management, IT services and information security management that is elaborated [1].

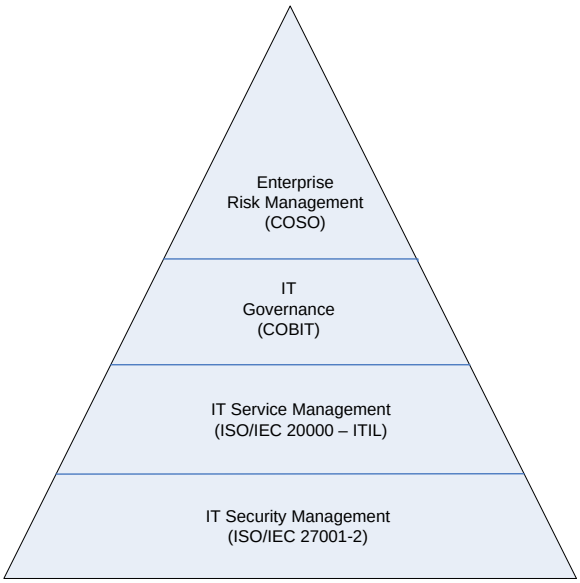


Figure 1 - Example of layered frameworks underpinning IT and information security

However, the EPU must be aware of the unique requirements in those domains relating to power system operations and implement framework elements to fulfil those requirements.

2.4 Framework Elements

2.4.1 Security Domains

The basic security domain definitions that were elaborated on by the former JWG [7] have been adopted by WGD2.22. It should be noted that there is always only one security authority for a domain, but a security authority might be responsible for more than one domain.

2.4.2 Information Security Domain Model

Different domain models have been discussed. An EPU representing one security authority could define each domain according to the level of protection required by the organisation. The domain model should be defined based on the results of a risk assessment process [Section 3]. Figure 2 shows a model for different types of EPUs including examples of interconnections that are elaborated [1]. Appropriate security controls must be assigned to the domains and inter/intra connections [Section 2.4.3]. The EPU systems and data networks supported by IT components like servers, client devices, data communication infrastructure, access and network management devices, operating systems, databases, etc. must be mapped to the domain model as well [Section 4]. This model is suited for a "defence in depth" strategy against cyber risk.

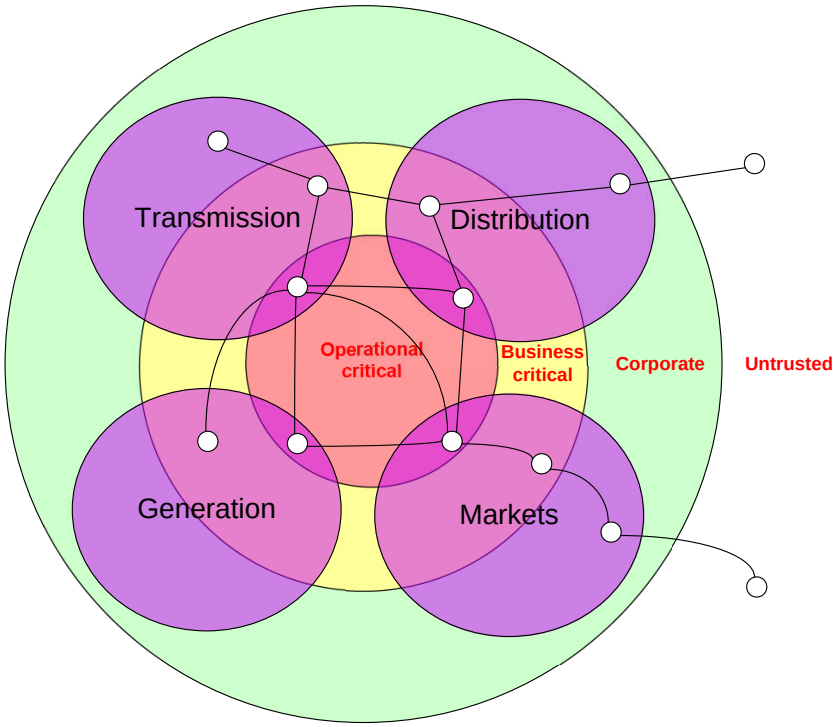


Figure 2 - Information Security Domain Model

2.4.3 Baseline Controls

An EPU needs to define its own selection of security controls for SCADA control systems, based on normative sources such as ISO 27002 [25], NIST SP 800-53[35], NERC CIP [34], ISA [31], or others, and appropriate for the EPU's regulatory regime and assessment of business risks.

The security controls need to be defined within each domain and the information flows between the domains, based on agreed risk assessments. For example, the Corporate domain and Business critical domain controls will depend on an intra-business risk assessment, whereas Operational critical domain controls are likely to require interdependent risk assessments between other operators and possibly Government agencies in addition to an intra-business risk assessment. Many types of IT components are required to support EPU control systems and lists of controls should be elaborated such as [1]:

- System Architecture Security Controls
- IT Support User Security Controls
- User Access Security Controls

2.4.4 Security processes

The establishment of the security framework itself and the execution of the security controls require organization of security activities in a structured manner. ITIL [12] and ISO/IEC 20000 1-2 [10-11] define a structured process model that describes the activities necessary to provide reliable and cost effective IT services. The Information Security Management Process (ISMP); in this context referred to as one process, is part of the model. The interrelationship between the ISMP and processes like incident management, problem management, and change management is elaborated upon.

3 Information/ICT Security Risk Assessment of Operational IT Systems at Electric Power Utilities

Risk Assessment is an integral part of the Risk Management process employed by Electric Power Utilities (EPUs). The objective of Risk Management is to ensure that all risks faced by the EPU are appropriately identified, understood and treated. The decision making process for the treatment of risks relies on accurate information about the threats and vulnerabilities that contribute to the likelihood of the risk occurring and the impact of its occurrence, compared with the cost of mitigating the risk and the risk appetite of the EPU. Thus, risk treatment options range from mitigation to acceptance for any given risk.

Formal Risk Management has become an accepted part of corporate governance for EPUs, and in order to cover all necessary aspects it needs to operate within a framework which facilitates the inclusion of Risk Assessment information from all parts of the EPU. Clearly, this must include Risk Assessment information concerning EPU physical operations, and within physical operations Risk Assessment must include information security/Information and Communications Technology (ICT) security Risk Assessment for operational ICT systems such as SCADA/EMS and power plant process control systems. It is believed that improvements need to be made in this area in order to improve the consideration of these risks within the context of enterprise wide Risk Management.

In ISO Guide 73 [13] Risk Management is defined as *"coordinated activities to direct and control an organization with regard to risk"*. The work of WG D2.22 has focused on three aspects of the co-ordinated activities of Risk Management, the Risk Management Process (generic), a Risk Management Framework (specific to EPUs), and Risk Assessment Methodologies for use in assessing risk on power/ICT infrastructures.

3.1 Risk Management Process

A generic risk management process can be used for risk management in the context of information/ICT security risk assessment for operational ICT systems such as SCADA/EMS and power plant process control systems. This describes the high level steps required for a consistent risk management process. Such a generic process has been used as the basis for the development of the Generic SCADA Risk Management Framework by the Trusted Information Sharing Network for Critical Infrastructure Protection in Australia [15]. In this case, the generic process utilized is the standards-based risk management framework as described in AS/NZS 4360:2004 [16] and ISO/IEC 27001:2005 [24].

The process is essentially generic and can be applied in any scenario where risk management is required. However, it operates at one level only and does not assist in identifying, analyzing and evaluating risks in the context of hierarchical organizations (and business processes and systems within those organizations). In conclusion, it is very useful in the single level in which it is utilized, but requires additional inputs and outputs to fit within a framework for multi-level risk management, and for effective communication of risks including cyber security ones associated with critical SCADA systems to senior management but requires additional inputs and outputs to fit within a framework for multi-level risk management. Moreover, it is not specifically tailored to take into account EPU specificities, but is aimed at the generic risk assessment of SCADA systems used to control any critical infrastructure including energy, water, broadcasting, and transport.

3.2 Risk Management Framework

Risk Management needs to be applied on a hierarchical, multi-level basis to work within the hierarchical and multi-level nature of organizations, business processes and systems that exist in the modern EPU environment, with their complex dependencies. For the purposes of developing an appropriate Risk Management Framework for EPUs, we decompose the organization as shown in Figure 3 below.

The four layers in Figure 3 illustrate the various hierarchical levels of the operations part of a typical EPU which operates power plants and/or electricity networks. Depending on the size and nature of the organization, levels 1 and 2 may be merged (for example in a smaller organization with one operational business unit). However, typically each level will have authority over one or more entities in the level below. Therefore, the single corporate entity will have authority for most business units, and each business unit will have responsibility for one or more power plant and/or electricity network, etc. As each level has authority over the entities in the level below, it will set certain business objectives for them, and monitor the level of achievement of these business objectives. We can use this same concept to elaborate how risk is assessed and managed within the corporate structure of EPU operations, considering the dependencies between each level of the EPU.

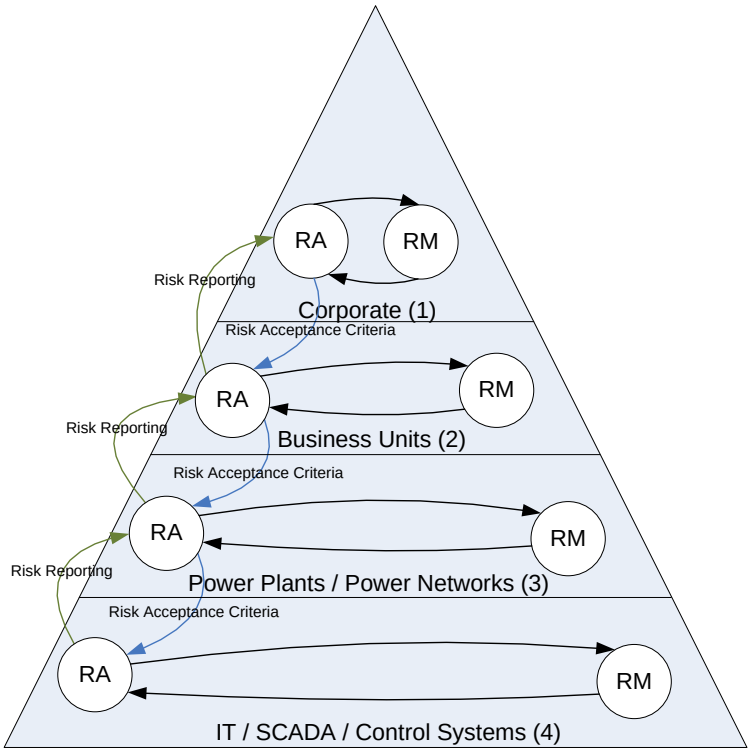


Figure 3 – EPU Risk Management and Risk Assessment Model

At each level within the organization, Risk Assessment activities should take place, and this should result in risks being quantified and Risk Treatment actions being taken to bring certain identified risks down to acceptable levels (where they are not already at or below acceptable levels). In some cases, risks at the higher levels in the organization are managed not within the level itself but by setting objectives for the lower levels of the organization. As shown in Figure 3, this constitutes Risk Acceptance Criteria for Risk Assessment activity at the lower level. Also as shown in Figure 3, the level undertaking the Risk Assessment (RA) and Risk Management (RM) activities reports back up to the higher level (Risk Reporting) in order to demonstrate that it is managing risk appropriately (or perhaps to identify where it needs further investment to manage specific risks). Importantly, this Risk Reporting is based on performance against Risk Acceptance Criteria originally set by the higher level.

There are interdependencies between all adjacent levels in the framework, however it is of critical importance in the framework that it permits the recognition of both potential ICT consequences and power consequences due to the occurrence of risks arising from the existence of threats (including threat agents i.e., individuals, groups or other entities that manifest threats) and vulnerabilities. The framework addresses the relationship between ICT consequences and power consequences, and their impact on the EPU, and proposes a method for assessing these risks and reporting on them against Risk Acceptance Criteria set at appropriate levels within the EPU. This provides an approach which permits the appropriate integration of these risks into an enterprise wide Risk Management process.

Additionally, research [17][18] is being undertaken to develop more comprehensive interdependency modelling techniques and tools for the interdependencies between level 3 and level 4, and also for interdependencies with other level 4 elements such as Telecoms, which are not directly IT, SCADA or Control Systems but are critical components of these systems. Such sophisticated models should be complimentary to this proposed framework.

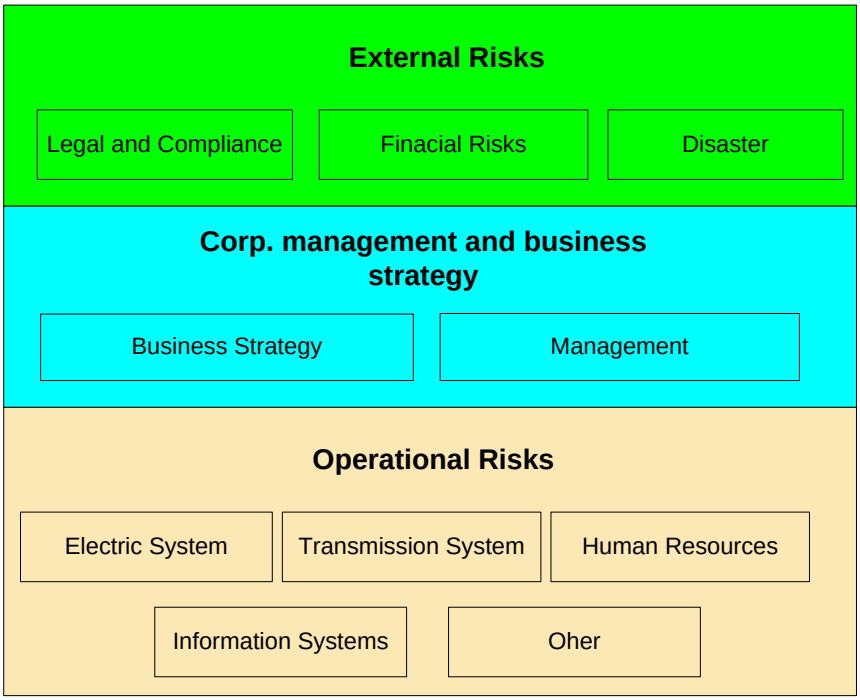


Figure 4 – Risk Categorization

The model described recognizes that dependencies exist between risks at adjacent levels in the organization, and therefore identifies there are links between Risk Assessment and Risk Management activities at adjacent levels. This, however, identifies a further requirement; the need to create a common understanding and means of expressing risk between each level. In order to do this, we first state that risk expressed from one level to another is essentially an abstraction of the risk between the two levels, and we use this to create a taxonomy of risk from the highest level in the organization to the lowest level.

One means of developing a common understanding and means of expressing risk which would be applicable at all levels would be to classify risks into a number of different categories. Figure 4 shows an example risk form, used as part of the Risk Assessment process, which guides participants to classify risks into different categories as part of a risk taxonomy, in this case with three overall higher level risk categories and a total of nine more detailed risk categories. For any risk to be of concern to the EPU, it must be categorized into one or more of these risk categories. Using a common taxonomy of risk, such as this example, throughout the EPU ensures that risk communication uses a common language and provides support for the categorization of risks into appropriate overall risk categories.

3.3 Risk Assessment Methodologies

In each level of the Risk Management Framework, Risk Assessment takes place as part of the Risk Management Process previously described. However, each risk assessment activity may use a different methodology dependent on the target of the risk assessment. A survey of the Risk Assessment practices performed by the members of WG D2.22 [2], particularly at levels 3 and 4 (Figure 3), identified that there are only a few commonalities but a lot of differ-

ences among the WG members` practices. The comparison provides evidence that the frameworks underlying the considered practices differ in terminology, concepts and scales.

The findings of the survey demonstrated the lack of a reference method and confirmed the need of developing a methodology that is widely accepted by most EPUs and integrating both power and ICT security knowledge. This is synonymous with integrating level 3 and level 4 security knowledge in Figure 3. Of the survey sample, 30% are using no defined method and 70% are using some defined method when doing Risk Assessment, 50% use qualitative practices and only 20% make use of some tool support which are either an IT Risk Assessment tool or an ad-hoc test application.

Based on the survey outcome, the following issues have been identified by WG D2.22 as needs to be addressed by tools accounting for the dependencies of power from ICT failures:

(i) Information on ICT threats must be kept updated on a continuous basis.

(ii) Statistical data of ICT component failures affecting power control infrastructures are not available due to both data sensitivity and the continuous evolution of threats: consequently a hybrid approach, combining stochastic analysis with empirical analysis could potentially be pursued.

(iii) Improved estimations on the probability of occurrence of ICT failure could be achieved by considering the threat plausibility and their degree of success.

(iv) The judgment of whether a given ICT component failure requires countermeasures or not requires a deep functional and behavioural analysis of the ICT infrastructure in relation to the control functions. This analysis is needed to understand if a certain threat, affecting a specific component of the ICT infrastructure, is able to impact on some core control functions, resulting in a malfunction from the ICT to the electrical infrastructures.

(v) Classes of power failures have to be analyzed in combination with ICT failures.

(vi) The quantification of the cascading effects of ICT failures on the power infrastructure depends on the duration of the potential power failure, the number of customers affected or the loss of security.

(vii) The Risk Index associated to a given scenario is a function of 1) the probability of combined ICT-power failures given the probability of failures of the adopted security controls 2) the evaluation of the impact of their consequences.

(viii) The impact evaluation is based on a mix of economic, social and quality of service criteria, by distinguishing the size and services from the EPU (power transmission, power distribution, bulk power production, distributed energy generation etc).

(ix) Depending on the risk rating resulting from the evaluation, existing controls are reviewed and new appropriate controls may be submitted for management approval for implementation.

(x) Any measures for counteracting those combined anomalous events must allow the restoration of secure and normal power conditions within the process time delay.

In the absence of established methodologies which address the specific needs of the EPUs, Risk Assessment efforts for level 3 and level 4 tend to use a scenario-based approach which considers threats, likelihoods and impacts across both level 3 and level 4 combined. In order for this to be successful, an excellent knowledge of both the power systems and the ICT sys-

tems and the detailed interaction between them is required, so that realistic scenarios can be developed. Whilst this process is an extremely valuable step for EPUs to take, it must be recognized that it is unlikely to develop a comprehensive Risk Assessment of all possible scenarios, due to the complexity of the interactions between the power system and the ICT infrastructure.

3.4 Remarks on Risk Assessment

In order to address risks due to power systems and ICT systems dependencies, all EPUs should undertake Risk Assessments at level 3 and level 4 as part of a Risk Management Process, in accordance with a Risk Management Framework for the EPU, such that both the Risk Acceptance Criteria and Risk Reporting are integrated into the overall Risk Management activities of the EPU. The language used to communicate risk between the various levels of the EPU should be based on common and agreed terminology.

For level 3 and level 4 Risk Assessment activities, the lack of established methodologies to deal with the unique nature of power systems and ICT systems dependencies mean that the EPUs must bring power systems and ICT specialists together regularly to perform (scenario-based) Risk Assessments as a team, and that these assessments will be limited by the capabilities of these teams until such times as more comprehensive tools becomes available which are specific to the needs of the EPUs. However, bringing such teams together to undertake Risk Assessments is a very positive step in the Risk Management process, and all EPUs should be committed to such activities on a regular basis. Research activities addressing the development of tools for levels 3-4 Risk Assessment are described in [20] and [21].

4 Security Technologies Guideline – Practical Guidance for Deploying Cyber Security Technology within an EPU Data Network

This part of the TB provides guidance on the application of cyber security controls to electric utility networks. Ideally, a formal risk assessment should be already completed and a corporate security domain model defined. With these steps completed, assets within the network can be mapped to security domains. Appropriate security technologies can then be deployed within the network to meet the requirements of each domain. Due to the wide and varying range of EPU data networks, this part generalizes data networks into common elements that are likely to be present within most EPUs. A specific diagram is provided, integrating Transmission and Distribution (T&D) grid data networks, and data networks associated with generation plants. The approach in this section can also be applied to other EPU data networks. In Appendix 4 [4], this is further described.

An essential part of any EPU security deployment process is ensuring compatibility with legacy systems. This part is mindful of both modern IT and legacy SCADA environments, and the technological approach given herein allows for consistent and effective security measures across both.

4.1 Logical Security Domains to Technical Implementation

The security domains covered above are logical. Although security controls can be assigned in general to each security domain, a successful security implementation involves adding cy-

ber controls to the data network, that is, appropriate policies, procedures, segmentation, technology devices, and software. To ensure that devices and software are placed in the data network to enforce security applicable for each domain, physical network assets must be mapped to logical security domains. This assignment can be made based on the following criteria:

- Results of Risk Assessment from the assessment of:
  - Known vulnerable points within the network
  - Impact to operations if a given area of the network is compromised
  - Interconnectedness of the network to networks in less secure domains
  - Reliance on third party communications infrastructures
- Already established Corporate Security Policy requirements

4.2 Transmission, Distribution, and Generation Networks

Identifying security domains and implementing cyber security technology within an EPU is a complex process, and specific details vary according to the data network configuration. Additionally, special consideration must always be given to the impact of cyber security controls on an EPU's operations data network, as these networks are often more sensitive to reliability and latency factors than a typical IT data network. In countries operating deregulated energy markets, and particularly for participants who sell and buy power, business critical ICT used for market participation also requires special performance and security measures nearing those required for operational SCADA systems. They also represent a new source of threats to operational SCADA systems as they need to extract data from these systems in the near real time, and hence special security measures need to be put in place to protect the operational SCADA environment.

4.2.1 Example Data Network with Security Domains

To illustrate the application of cyber security for EPUs, paper [4] provides an example mapping of security domains within a typical EPU data network. The mapping is intended to be representative of the various elements present within an EPU data network; an actual mapping will vary based on Risk Assessment, Security Domain definitions and the specific details of the data network.

Major data network components include the T&D network with substations, one or more generation facilities, and connections to a corporate office. Logical security domains are mapped to the physical EPU data network according to relative criticality and risk (which would be determined by a risk assessment process). The typical EPU network often contains a mixture of Operations Critical, Business Critical, Corporate, and Untrusted domains. See Figure 5.

The Operations Critical Security Domain primarily covers the operations control centre(s), substations, and the control networks directly supporting generation. The Business Critical Security Domain covers assets that support critical operations, but which are not, in themselves, critical to grid operations. The Corporate Security Domain covers data network components which have baseline security requirements, but which are not essential to grid operations. Two domains, the Operations Critical Security Domain and Business Critical Security Domain span areas of the data network that are geographically dispersed. This type of configuration, which is typical, can complicate the implementation of security measures for each domain.

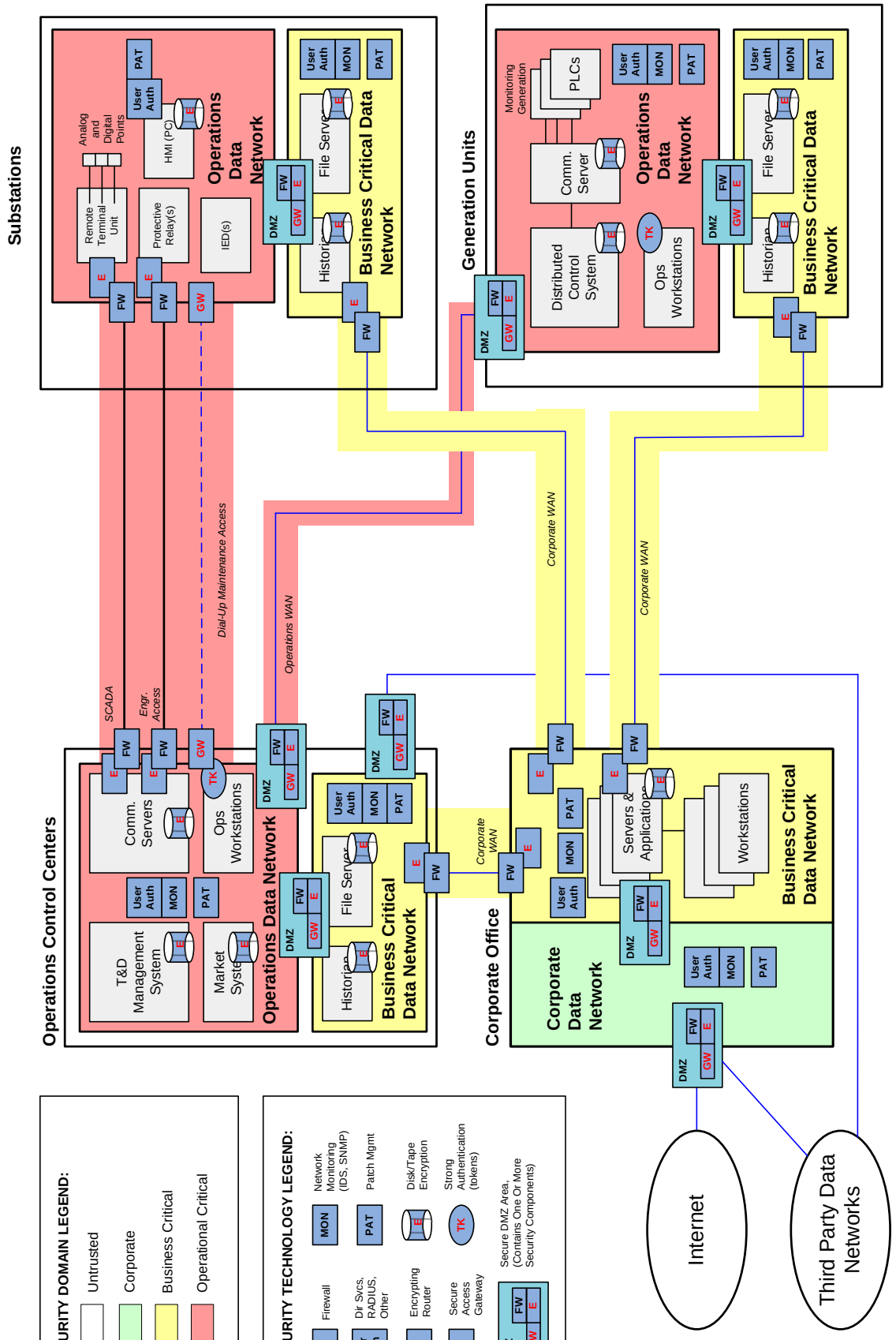


Figure 5 – Example of Cyber Security Technologies Deployed

4.3 Applying Security Technologies to Logical Diagrams

Once logical security domains have been mapped to the physical EPU data network, specific security control implementation details can be worked out. Since each security domain prescribes specific security controls, specific security technologies can be selected for deployment. As stated earlier, the choice of technology should be considered in light of any special reliability and latency requirements of the data network being secured.

Yet, a well researched and careful approach can yield a highly effective security deployment – one that actually enhances electric reliability by protecting critical cyber assets from attack. Paper [4] provides an approach to the crucial step of deploying security technology. However, deployment is in fact the last step in what must become a repeated security review cycle. As other works within the Cigré WG D2.22 shows, EPUs must implement a complete security discipline that includes regular processes:

- Reviewing and analyzing current and evolving cyber security standards [5]
- Assessing risk to the system, using an appropriate methodology [2]
- Maintaining high corporate awareness of possible cyber threat scenarios [22]
- Establishing and maintaining a well documented security frameworks model, as part of a larger corporate security policy [1]
- Maintaining appropriate skills and training program
- Deploying and maintaining security technologies that map to logical security domains.

5 Standards

The purpose of this part of the WG work is not to be exhaustive in the sense of picking the one and only standard, but rather to provide some kind of guidance in the standards "landscape", which is a "moving target", and from the control systems perspective for an EPU.

5.1 A fast-changing landscape

The growing focus on cyber security in the EPU industry and the associated decision-makers have led to an impressive number of standards and guidelines initiatives, among which it is not easy to navigate. The difficulties are not only in the number of documents, but also in the diversity of their scope, the relative recognition and prominence they have, and of course, the speed at which this landscape evolves. Some standards may be relevant only for traditional IT environments, whereas others will be specifically relevant for industrial control systems (ICS). Some may be directly leveraged by operators, others may concern in first place solution providers or government agencies. They can be national, regionally based or explicitly international. They can be structured for compliance testing and validation, or may just be good practices collections or informative documents. In addition to this diversity, new initiatives seem to appear almost every month, and the relative interest is sometimes challenging and always time-consuming to evaluate. The paper [5] reproduced in Annex and presented at the CIGRE Session 2008 had proposed a "survival kit" in the cyber security standards arena, identifying and focusing on the most relevant documents for EPUs. Written around January 2008, it had been presented in August at the Session in Paris; within only the submission, review and presentation time, some of the content was already deprecated. Permanent attention

and regular updates are needed to address accurately this area. The content of this TB section makes no exception.

5.2 The "best pieces"

This part is of course not intended to select standards on behalf of the Electric Power Industry but rather support EPUs in the selection and contribute into achieving consensus about the "best pieces". Hereunder are gathered executive summaries of what has been considered by the working group as a minimum list to consider. Note that only documents relevant for all kinds of utilities have been selected: those targeting specific categories (e.g., regarding nuclear power) have not been included to preserve the general message of the technical brochure.

5.2.1 ISO/IEC 2700x series

This series of standards was prepared in the frame of the ISO/IEC. They cover the requirements, and establish guidelines for implementing, maintaining, and improving information security management systems (ISMS), risk management, metric and measurement in many different types of organizations (commercial enterprises, government agencies, not-for profit organizations, …). As a matter of a consequence, if they have not been specifically developed for EPUs, most of their principles are relevant for our industry, in particular for traditional IT systems and on the business processes point of view. On the other side, there was no ICS community participation in the development of these standards and they do not address many of the unique issues of such systems, which are integral and sensitive part of the EPUs' security issues. Specific approaches proposed by other standard bodies, and presented later, should then be considered.

Within the series, three standards are more particularly relevant and have already gained significance: ISO/IEC 27001 on ISMS requirements [24], ISO/IEC 27002, providing a "Code of practice for information security management" [25] (formerly ISO/IEC 17799), and the ISO/IEC 27005 on "Information security risk management", published in June 2008 [26].

5.2.2 IEC 62351

Working Group 15 of Technical Committee 57 (TC57 WG15) of the International Electrotechnical Commission (IEC) was formed in 1999 to focus on the theme "Power system control and associated communications - Data and communication security." It undertakes the development of standards for "end-to-end" cyber security of the electrical system, and has in particular developed specifications to secure the communication protocols defined within TC 57. Since its creation, WG15 has specified security mechanisms for IEC 60870-6 (TASE.2/ICCP), IEC 60870-5 (and its derivative DNP), and IEC 61850, already published [27-28]. The group has also developed abstract Network and System Management (NSM) data objects for the power system operational environment (currently under final review) and more recently a Role-Based Access Control (RBAC) document aiming at promoting such solutions for the entire pyramid in power system management and enabling interoperability in the multi-vendor environment. This last item is in its initial stage discussions.

5.2.3 IEEE P1686 and P1711

IEEE PES has released the IEEE 1686-2007 Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities [30].

P1711 is a trial use standard which defines a cryptographic protocol to provide integrity, and optional confidentiality, for cyber security of substation serial links. It does not address specific applications or hardware implementations, and is independent of the underlying communications protocol. This trial use standard defines a cryptographic protocol known as Substation Serial Protection Protocol (SSPP) that can protect the integrity and optionally confidentiality of asynchronous serial communications typically used by substation equipment. SSPP is primarily intended to protect serial SCADA communications, but can be applied to other serial communications. SSPP is independent of the underlying communications link and protocol, and is appropriate for serial communications over leased lines, dial-up lines, multi-drop links such as RS-485, radio, power line carrier, fibre optic, etc. SSPP is suitable for implementation in new equipment or for deployment in bump-in-the-wire devices retrofitting protection to existing systems.

5.2.4 ANSI/ISA99 – IEC62443 Technical Reports and Standard Series

The ISA99 committee addresses control systems cyber security [31]; it has numerous North American and international members from end-users (including electric utilities), suppliers, contractors, universities, and government organizations. This includes DCS, PLCs, SCADAs, networked electronic sensing, monitoring or diagnostic systems. ISA99 establishes standards, recommended practices, technical reports, and related information that define procedures for implementing electronically secure control systems and security practices or assessing electronic security performance. The ISA99 may soon gain a more international momentum as they are proposed to become international standards though IEC (62433 series). The process is under way.

5.2.5 North American NERC CIP standards

NERC (North American Electric Reliability) Corporation is the “electric reliability organization” for North American power grid, and relies on the diverse and collective expertise of industry participants. NERC Standards CIP-002 through CIP-009 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the electric power grid [34]. These standards have been approved by FERC (Federal Energy Regulatory Commission) and are enforced by anyone who could adversely impact the transmission grid in North America, including generators, transmission companies, and large load servers. These standards are evolving: Version 2 has been submitted to the FERC for approval and work on Version 3, which will substantially expand the standards, is in progress.

5.2.6 NIST SP800-53 & SP800-82

The National Institute of Standards and Technology (NIST) is non-regulatory agency of the U.S. Department of Commerce, involved in standards development and testing done by the private sector and U.S. government agencies to promote innovation and industrial competitiveness.

NIST SP 800-53 security controls give the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. SP 800-53 was originally written for business IT systems. It has been extended in Revision 2 to specifically address industrial control systems such as those used in EPUs [35].

NIST initiated the ICS Security project [36] in cooperation with the public and private sector ICS community to develop specific guidance on the application of the security controls in NIST SP800-53 Recommended Security Controls for Federal Information Systems to ICS. Consequently, NIST 800-82 was developed to provide specific recommendations and guidance for securing ICS [35]. In addition, SP800-82 provides an overview of the many activities currently ongoing among US government organizations, standards organizations, industry groups, and automation system vendors to make available "best practices" in the area of ICS security.

5.2.7 The CPNI Good Practice Guidelines

The British CPNI (Centre for the Protection of National Infrastructures), formed from the merger of the National Infrastructure Security Co-ordination Centre (NISCC) and a part of MI5 (the UK's Security Service) has published a set of Good Practice Guidelines for Process Control and SCADA Security, through a series of very concise and readable guides [37]. They cover the following topics "Understand the Business Risk", "Implement Secure Architecture", "Firewall deployment for SCADA and process control networks", "Establish Response Capabilities", "Improve Awareness and Skills", "Manage Third Party Risk", "Engage Projects", "Establish Ongoing Governance".

5.3 A "survival kit"

From all standards reviews to date, the NIST and ISA standards seem the most comprehensive standards to use for industrial control systems on a global requirement perspective (specifically including EPU control systems), while IEEE and IEC62351 standards deserve a particular attention for specific devices and technical implementations. CPNI guidelines are pragmatic and synthetic documents covering a large spectrum of security with a specifically SCADA-oriented approach. ISO/IEC 270xx series are more relevant on a global organization point of view and for non-ICS considerations.

Beyond these considerations, to survive in the dense normative jungle of cyber security standards, here are a few general recommendations:

- A first vital step is of course to check if any relevant local and national regulations, standards or recommendations may exist in the organization environment.
- A good global view of the different kind of standards and initiatives existing in the field is also necessary, and this section is intended to constitute a first basis for this.
- Then, it is important to realize that none of the existing references have exactly the same scope and cover the same aspects. There is no unique, right and universal standard to rely on, but several pieces and tools to be used and integrated to build an efficient and coherent enterprise-wide security posture. In this perspective, the presented standards are all valid bases to consider.
- Selection may consider cultural tradition, sometimes bound to specific or international regional standard bodies, but also direct technical or business environment: which stan-

dards do the partners or competitors use? What are the products/solutions available compliant to a given set of standards of interest? How will they fit into the organisation?

This said, the standards presented here, summarized in Table 1, are all prime candidates to consider.

Designation	Nature/scope	State	Focus	Ref.
ISO/IEC 2700x	International standards	27001, 2 & 5 published and widely used	General IT. Sound guidelines and requirements for security management	[23-26]
IEC 62351	International Technical Specifications	Partly published, ongoing work	Power system data and communications protocols. Technology providers oriented.	[27,28]
IEEE P1711	IEEE std. (regional), but worldwide relevant	Advanced Draft	Specifically tailored for SCADA, RTU and IED equipment.	[30]
ANSI/ISA 99 – IEC 62443 Reports & Standards	Initially US based standards, getting "internationalized" through IEC - worldwide relevant	Partly published, ongoing work.	ICS oriented thus relevant for EPUs'. Completing existing standards and identifying new topics (e.g. patch management, metrics,...)	[31,32]
NERC CIP standards	North America	Enforced in the US. Still evolving.	Framework for the protection of the grid Critical Cyber Assets	[34]
NIST SP800-53 & 800-82	US documents, but worldwide relevant	Advanced drafts	Complete framework for SCADA and ICS cyber security	[35,36]
CPNI Guidelines	UK guidelines, but worldwide relevant	Published (2005)	Clear and valuable good practices for Process Control and SCADA security	[37]

Table 1[1] – Prime candidates in the cyber security standards jungle

6 Future Works

The work on information security will continue with CIGRE, also after WGD2.22 is dismantled. Forthcoming issues may include the following. A key question here is: What do the EPUs need?

- To be informed about how to do risk assessments for electricity industry control systems environments.
- To have a way of convincing management to invest in security measures for electricity industry control systems. This could include awareness, quantification of risks, presentation of avoided potential costs and damage, etc.
- To have information about specific security technologies/measures for electricity industry control systems. This is being addressed directly in CIGRE B5.38 for IEC61850, and in D2.24 for 21st century EMS architectures. However, gaps remain which are specific to

[1] All the status information of this section is to be taken as of the date of the TB elaboration, i.e. the first part of 2009.

electrical utilities. What gaps could this future WG contribute to? E.g., analysis/evaluation/comparisons of intrusion detection systems, data diodes, firewalls, etc., all considered in the specific context of the electricity industry control systems environments.

- A security management system/cycle for operations which is appropriate and implemented at levels 3 and 4 of the risk management framework (hierarchy pyramid) described in Section 3 (i.e. the power system and the ICT/control system levels).
- Guidance on the embedding of security into the project lifecycle for the implementation of electricity industry control systems (this may be part of item 4 to provide a whole lifecycle covering both projects and operations)
- What kind of list of information security requirements should an EPU present to a potential vendor of SCADA/control systems?
- What are the most relevant security metrics [39] that can be used by an EPU to quantitatively measure the security of its ICT systems?

7 Conclusions

Based on this work of Cigré WG D2.22, the following can be concluded:

- There is a great and increasing number of works which could both support an EPU but also create a confusing situation, when a Security Framework is to be chosen and the information security issues are to be managed.
- An overall framework should be based on existing standards and "best practices", taking into account legal requirements, culture, and specificities of the EPU. The wheel should not be re-invented. The Security Framework should "fit" into the landscape of other frameworks adopted by the EPU.
- The WG has chosen to focus on domain modelling, risk assessment and definition of baseline controls and work processes, as important elements of a security framework.
- Risk assessment works show that this area could be more mature and be further developed, in order to provide guidance to security management. A survey has shown that IT-based support for risk assessment was only used to a limited extent.
- The technical solution should be based on the domain model and the assigned controls, which are based on the risk assessment work and possible legal requirements imposed by the government. Also, limitations related to the already installed base, such as "legacy systems", must be taken into account in a way that do not hamper the organization security posture.
- The world of standards has been widened. An EPU needs guidance when picking the proper standard(s) for its needs of managing information security.

Based on these and other experiences faced the WG D2.22, it is evident that information security for an EPU will continue to be an important issue, in both the short and long run.

8 References

[1] Å. Torkilseng, S. Duckworth: "Security Frameworks for Electric Power Utilities - Some Practical Guidelines when developing frameworks including SCADA/Control System Security Domains", Electra, December 2008.
[2] G. Dondossola, "Risk Assessment of Information and Communication Systems - Analysis of some practices and methods in the Electric Power Industry", CIGRÉ Electra, August 2008.
[3] M. Tritschler, G. Dondossola: "Information Security Risk Assessment of Operational IT Systems at Electric Power Utilities", Paper D2-01 D03, Cigré D2 Colloquium, October 21-22, 2009, Fukuoka, Japan.
[4] Bartels, L. Pièrre-Cambacédès, S, Duckworth "Security Technologies Guideline – Practical Guidance for Deploying Security Technology within Electric Utility Data Networks", will appear in Electra, 2009.
[5] L. Pièrre-Cambacédès, T. Kropp, J. Weiss, R Pellizzonni, "Cybersecurity standards for the electric power industry – a survival kit" – Paper D2-217, CIGRÉ Paris Session 2008, France.
[6] G. Ericsson, A. Bartels, D. Dondossola, Å. Torkilseng: "Treatment of information security for electric power utilities – progress report from Cigré WG D2.22" Paper D2-213, Cigré 2008 Session, Paris, France.
[7] Cigré JWG D2/B3/C2-1 Technical Brochure TB 317 on "Security for Information Systems and Intranets in Electric Power Systems", 2007.
[8] COSO ERM (The Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management), 2004 URL: www.coso.org
[9] COBIT (Control Objectives for Information and related Technology) URL: www.isaca.org
[10] ISO/IEC 20000-1:2005 Information Technology – Service management – Part 1: Specification
[11] ISO/IEC 20000-2:2005 Information Technology – Service management – Part 2: Code of practice
[12] ITIL (IT Infrastructure Library). URL: www.itil-officialsite.com/home/home.asp
[13] Risk management — Vocabulary, ISO/IEC CD 2 Guide 73, concept, April 2008.
[14] Risk management — Principles and guidelines on implementation, ISO/DIS 31000, concept, April 2008.
[15] Generic SCADA Risk Management Framework for the IT Security Expert Advisory Group (ITSEAG), Trusted Information Sharing Network for Critical Infrastructure Protection, December 2006.
[16] AS/NZS 4360:2004 Risk Management, Standards Australia.
[17] IRRIIS project, http://www.irriis.org
[18] CRUTIAL project, http://crutial.cesiricerca.it
[19] Risk Assessment of Information and Communication Systems - Analysis of some practices and methods in the Electric Power Industry, Giovanna Dondossola CESI RICERCA SpA, Electra, August 2008
[20] Dondossola G., Lamquet O., "Cyber Risk Assessment in the Electric Power Industry", Electra N°224, February 2006, pp. 36-43, http://www.cigre.org/gb/electra/electra.asp
[21] Dondossola G., Lamquet O., Torkilseng A., "Key issues and related methodologies in the security risk analysis and evaluation of electric power control systems", Cigré Session 2006, Paris 27 August – 1 September 2
[22] "Common Vulnerabilities and Exposures List" – available online at http://www.cve.mitre.org/
[23] Standards and projects under the direct responsibility of JTC 1/SC 27 Secretariat http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45306
[24] ISO/IEC 27001:2005, Information technology -- Security techniques -- Information security management systems – Requirements http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103
[25] ISO/IEC 27002:2005, Information technology -- Security techniques -- Information security management systems -- Code of practice for information security management http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297
[26] ISO/IEC 27005:2008, Information technology -- Security techniques -- Information security risk management http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42107
[27] L. Pièrre-Cambacédès, C. Chalhoub, F. Cleveland, "IEC TC57 WG15 – Cyber security standards for the power system", Proc. of CIGRE D2 Colloquium, Luzern, 2007.
[28] IEC, Power system control & associated communications - Data & communication security, 62351 part 1-8, TS
[29] AGA Report 12, Cryptographic Protection of SCADA Communications www.aga.org/Committees/gotocommitteepages/gasctrl/AGAReport12.htm
[30] IEEE, Trial Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links, Draft 3, 2008-08-16. http://grouper.ieee.org/groups/sub/wgc6/wgc6.htm
[31] ISA99 web site, http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821
[32] Technical Report ANSI/ISA-TR99.00.01-2007, Security Technologies for Industrial Automation and Control Systems. http://www.isa.org/Template.cfm?Section=Shop_ISA&Template=/Ecommerce/ProductDisplay.cfm&Productid=9665
[33] The ISA99 Standards Vision, A Roadmap for Developing Secure Industrial Automation and Control Systems, ISA EXPO 2008, Oct 2008
[34] NERC CIP Standards as approved by the NERC Board of Trustees, May 2006. ftp://www.nerc.com/pub/sys/all_updl/standards/sar/Cyber_Security_Standards_Board_Approval_02May06.pdf
[35] NIST, Computer Security Division, Computer Security Resource Centre http://csrc.nist.gov/publications/PubsSPs.html
[36] NIST ICS Security project – website: http://csrc.nist.gov/sec-cert/ics/index.html
[37] CPNI Guidelines : http://www.cpni.gov.uk/ProtectingYourAssets/scada.aspx
[38] J. Weiss: "Control Systems Cyber Security—The Current Status of Cyber Security of Critical Infrastructures", Testimony before the *Committee on Commerce, Science, and Transportation, US Senate,* March 19, 2009.
[39] Andrew Jaquith: "Security Metrics - Replacing Fear, Uncertainty, and Doubt", Addison-Wesley, United States of America, 2007

Appendices

Appendix 1:

Å. Torkilseng, S. Duckworth: "**Security Frameworks for Electric Power Utilities - Some Practical Guidelines when developing frameworks including SCADA/Control System Security Domains**", Electra, No. 241, December 2008

Appendix 2:

G. Dondossola, "**Risk Assessment of Information and Communication Systems - Analysis of some practices and methods in the Electric Power Industry**", CIGRÉ Electra, No. 239, August 2008

Appendix 3:

M. Tritschler, G. Dondossola: "**Information Security Risk Assessment of Operational IT Systems at Electric Power Utilities**", Paper D2-01 D03, Cigré D2 Colloquium, October 21-22, 2009, Fukuoka, Japan

Appendix 4:

A. Bartels, L. Piètre-Cambacédès, S, Duckworth "**Security Technologies Guideline – Practical Guidance for Deploying Security Technology within Electric Utility Data Networks**", CIGRE Electra, No. 244, June 2009

Appendix 5:

L. Piètre-Cambacédès, T. Kropp, J. Weiss, R Pellizzonni, "**Cybersecurity standards for the electric power industry – a survival kit**" – Paper D2-217, CIGRÉ Paris Session 2008, France

Appendix 6:

G. Ericsson, A. Bartels, D. Dondossola, Å. Torkilseng: "**Treatment of information security for electric power utilities – progress report from Cigré WG D2.22**" Paper D2-213, Cigré 2008 Paris Session, France

“Security Frameworks for Electric Power Utilities – Some Practical Guidelines when developing frameworks including SCADA/Control System Security Domains”

Åge Torkilseng, Stuart Duckworth

On behalf of Cigré WG D2.22 “Treatment of Information Security for Electric Power Utilities”.

EXECUTIVE SUMMARY

1 INTRODUCTION

While the first Cigré WG D2.22 paper focused on risk assessment of information and communication systems, this report, number 2 out of 3, focuses on security frameworks for Electric Power Utilities.
The former JWG D2/B3/C2-01 “Security for Information Systems and Intranets in Electric Power Systems”, recommended using a security domain concept as a methodology to analyse and manage the information security problem [1]. They also gave some guidance on how to develop an overall information security framework. In this paper the focus is more on SCADA/control system type of domains but without losing sight of the “big picture”.

The objective is to provide some practical guidelines when developing frameworks that include SCADA/control system security domains. This is done by elaborating the specific security requirements of these types of domains, and also by giving a view of interrelated domains and high level frameworks that are necessary to manage corporate risks.

2 THE SELECTION OF STANDARDS, BEST PRACTICES AND GUIDELINES

There has been a general discussion within WG D2.22 about the process of selecting the “right” standards for EPU security. The conclusion is that WG D2.22 should not attempt to select standards on behalf of the Electric Power Industry but aim to support the EPUs in the selection process by analyzing some of the most important approaches and try to achieve a consensus on the best “pieces”. The paper “Cybersecurity standards for the electric power industry” [3] gives an overview of relevant standards that support the EPUs in the selection by presenting some of the most important approaches. The selection may consider cultural tradition, sometimes bound to specific or international regional standard bodies, but also take into account the technical or business environment.

3 DEFINITIONS OF SECURITY FRAMEWORKS

In this paper no rigorous and precise definition of “security framework” is used. “Security framework” can here be considered as the skeleton upon which various elements are integrated for the appropriate management of security risk. The elements that are elaborated on are Security Domains, Security Policies and Security Processes. Other framework elements elaborated by WG D2.22 are Risk Assessment [4] and Security Technologies [5].

4 ALIGNMENTS TO OTHER TYPE OF FRAMEWORKS

First, at the top level an EPU could be using frameworks to manage the overall corporate EPU risk profile, including market, financial and operational risks (including Information Technology [IT]/control system risks). COSO Enterprise Risk Management [6] is an example of such a framework. On this level we also like to mention the upcoming ISO risk management standard, ISO 31000. Frameworks for IT Governance like COBIT [7] could be used to define IT-processes to fulfil requirements for core business information like Quality requirements (Effectiveness, and Efficiency), Security requirements (Confidentiality, Integrity and Availability) and Fiduciary requirements (Compliance and Reliability).

Second, the EPU could be using frameworks for IT service management describing in detail the IT processes necessary to deliver high quality IT services that support business processes. ISO/IEC 20000 [8], [9] that is based on ITIL [10] describes a specification and code of practice for an integrated approach, and demonstrates the fact that a security management framework cannot be implemented in a separate vacuum. Fig. 1 shows an example of a layered framework architecture providing an integrated approach to risk management, IT services and information security management.

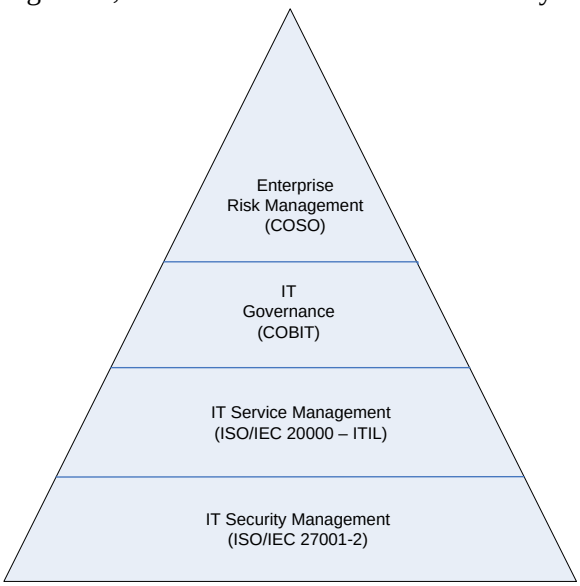


Fig. 1 Example of layered frameworks underpinning information security

However, the EPU must be aware of the unique requirements in those domains relating to power system operations and implement framework elements to fulfil those requirements.

6 FRAMEWORK ELEMENTS

6.1 Security Domains

Definitions of security domains made by ISO/IEC that were elaborated on by the former JWG [1] are adopted by WGD2.22. It should be noted that there is always only one security authority for a domain, but a security authority might be responsible for more than one domain.

6.1.2 Information Security Domain Model

Different domain models have been discussed. An EPU representing one security authority could define each domain according to the level of protection required by the organisation. Fig. 2 shows a

model for different types of EPUs including examples of interconnections. Table 1 gives a short description of the domains, their protection levels and examples of systems.

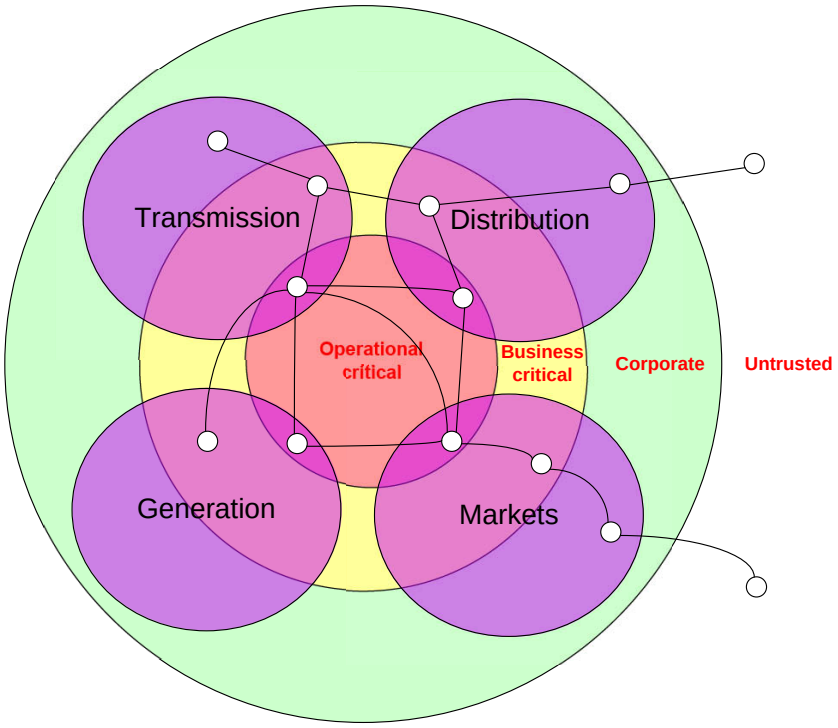


Fig. 2 Information Security Domain Model

Protection Level (relative to operations)	**Domain**	**Colour in Fig. 2**	**Example Systems**
Low	Untrusted	White	Vendor / 3rd party networks, internet
Medium	Corporate	Green	Office level business network
High	Business Critical	Amber	Finance, human resource systems
Very High	Operation Critical	Red	Controls systems, SCADA networks

Table 1: Domain Descriptions

It is important to note that these domains are abstract security domains, which contain elements of logical controls and physical security architecture; the actual security perimeters for these domains can be quite complex to define. For example, for a single organisation, if the control centres, substations, power plants, and the SCADA data communications are all considered to be Operation Critical, then all these separate physical systems, their locations, and the data networks between them will be within a single “red” security domain governed by a single security policy and security authority.

The situation is further exacerbated by the need to establish a comprehensive security policy that recognizes the legitimate interaction of organizations not under the control of the utility. Such organizations include EPU partners, system solution providers, independent system operators, government oversight agencies, first responders, and the list goes on. Clearly, a federated approach, rather than a hierarchical approach, is needed to effectively manage such a comprehensive security policy.

6.2 Baseline Controls

An EPU needs to define its own selection of security controls for SCADA control systems, based on sources such as ISO 27002 [11], NIST SP 800-53[12], NERC CIP [13], ISA [14], or others, and appropriate for the EPU's regulatory regime and assessment of business risks.

The security controls need to be defined within each domain, and the information flows between the domains, based on agreed risk assessments. For example, the Corporate domain and Business critical domain controls will depend on an intra-business risk assessment, whereas Operational critical domain controls are likely to require interdependent risk assessments between other operators and possibly Government agencies in addition to an intra-business risk assessment.

The following IT components are typically required to support EPU control systems:

a) servers supporting SCADA and telemetry systems,

b) client devices (e.g. workstations, PCs, printers),

c) data communications infrastructure (e.g. LANS, WANS, routers, switches),

d) access and network management devices (e.g. firewalls, IDS, access control servers, Active Directory[AD] servers, Domain Name Servers[DNS], patch and anti-virus servers),

e) operating systems, databases, and software applications.

Security should also be viewed as a personal responsibility, so human behavior must be considered. For example, EPU human resources departments estimate that 20% of the employees are subject to compromise. Thus, the situation is very prone to social engineering by a determined adversary. Furthermore, complex security policies can be counter-productive, resulting in less security assurance and system reliability, not more.

The following list of security controls should be considered:

System Architecture Security Controls

a) EPU Control Systems must be protected from other networks by being hosted on a logically separate data network using firewall / DMZ security controls.

b) The corporate data network and the control system network should not communicate directly with each other.

c) Certain standard business services (e.g. email and internet services) should be excluded.

d) EPU Control Systems should be installed at control centres, not at corporate data centres, to. benefit from the enhanced physical security at these sites.

e) Physical separation of control system IT infrastructure away from corporate business infrastructure is preferred.

IT Support User Security Controls

It is well known that within IT environments the threat of attack from insiders is real and substantial. To minimise this insider risk the following controls should apply to the IT support function:

a) IT support personnel (including contractors) should under normal circumstances be onsite within secure control centres.

b) Clear guidelines for the recruitment, selection, accreditation, and security clearance of IT support personnel.

c) Security clearance should include pre- employment background checks, e.g. identification (ID) verification, previous employment history, criminal record checks, etc, compliant with the local laws and regulations.

d) Strict change management control for all joiners, movers, and leavers.

User Access Security Controls

a) External (remote) access to be authorised, time-limited, use strong 2-factor authentication, and be encrypted up to the network access point.

b) Direct access to the control system data network should be limited to Control Room staff and their immediate support.

c) Other business users requiring access should use 'proxy' services (e.g. Citrix).

d) Access to control system applications should require further ID/password authentication.

e) Data historian servers should be used to provide read-only data views and management information services to obviate the need for wider access to the control systems.

6.3 Security processes

The establishment of the security framework itself and the execution of the security controls require organisation of security activities in a structured manner. ITIL[10] and ISO/IEC 20000 1-2 [8][9] define a structured process model that describes the activities necessary to provide reliable and cost effective IT services. The Information Security Management Process (ISMP); in this context referred to as one process, is part of the model. The interrelationship between the ISMP and processes like incident management, problem management, change management etc. is elaborated on.

As part of the security framework, the EPU should describe its security processes and control services in the SCADA/control system domains and their relationship to other processes necessary to provide reliable IT services. The applicability of using ITIL or ISO/IEC 20000 in the SCADA/control system domains needs however further studies.

7 CONCLUSIONS

This paper has provided some practical guidelines for EPUs to implement baseline information security controls for SCADA / Control Systems within the context of a security domain framework. These guidelines draw on the practical experience of members of the WG D2.22, and the need to control the increasing exposure to electronic security risks that this industry faces. A security domain model is presented providing a layered approach of different security levels or domains appropriate for the protection of SCADA / Control Systems embedded within the business environment of an EPU, whilst acknowledging the integrated nature of EPU operations and the interrelationships between EPUs. Ref-

erence is made to existing standards and governance frameworks and how these can be adapted or extended to meet the needs of SCADA / Control Systems security management.

8 REFERENCES

[1] Cigré JWG D2/B3/C2-1 Technical Brochure TB 317 on "Security for Information Systems and Intranets in Electric Power Systems", 2007

[2] G. Ericsson, Å. Torkilseng, G. Dondossola, A. Bartels, " Treatment of Information Security for Electric Power Utilities – Progress Report from Cigre WG D2.22," – D2-213 , Cigre Paris Session 2008

[3] L. Pietre-Cambacedes, T. Kropp, J. Weiss, R Pellizzonni, "Cybersecurity standards for the electric power industry – a survival kit" – D2-217 , Cigre Paris Session 2008

[4] Dondossola G., "Risk Assessment of Information and Communication Systems - Analysis of some practices and methods in the Electric Power Industry", submitted to Electra 2008

[5] Bartels, A, L. Pietre-Cambacedes, Stuart Duckworth " Security Technologies Guideline – Practical Guidance for Deploying Security Technology within Electric Utility Data Networks", submitted to Electra 2008

[6] COSO ERM (The Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management), 2004. URL: www.coso.org

[7] COBIT (Control Objectives for Information and related Technology). URL: www.isaca.org

[8] ISO/IEC 20000-1:2005 Information Technology – Service management – Part 1: Specification

[9] ISO/IEC 20000-2:2005 Information Technology – Service management – Part 2: Code of practice

[10] ITIL (IT Infrastructure Library). URL: www.itil-officialsite.com/home/home.asp

[11] ISO/IEC 27002:2005, Information Technology - Code of practice for Information Security Management

[12] NIST (National Institute of Standards and Technology) Special Publication 800-53 – Recommended Security Controls for Federal Information Systems. URL: www.nist.gov

[13] NERC CIP (North American Electric Reliability Corporation – Critical Infrastructure Protection). URL: www.nerc.com

[14] ISA99 web site, http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821

Risk Assessment of Information and Communication Systems - Analysis of some practices and methods in the Electric Power Industry

Giovanna Dondossola CESI RICERCA SpA
Power System Development - Department, Milan - Italy

On behalf of Cigré WG D2-22 "Treatment of Information Security for Electric Power Utilities (EPUs)".

Abstract
The paper presents the outcome of a survey activity of the Risk Assessment practices performed within the Cigré Working Group (WG) D2.22 "Treatment of Information Security for Electric Power Utilities (EPUs)". The WG decided to approach the Risk Assessment issues by starting to survey the status of the practices of the WG members with the aim of setting up an initial, shared view of the state-of-practices.
By following an anonymous style of reporting, the core aspects of the considered best practices are first described and then evaluated on a common base. Only a few commonalities but a lot of differences were found among the WG members` practices. The findings demonstrate the lack of a reference method and confirmed the need of developing a electricity-specific methodology that is widely accepted by most Electric Power Utilities and integrating both power and ICT (Information and Communication Technologies) security knowledge.
Preliminary recommendations from the state of these practices as well as open issues to be addressed in future developments are derived from the analysis. The presented overview on Risk Assessment practices constitutes a first step towards the final WG objective of developing practical recommendations addressed to both chiefs of EPU Security Programs and managers of Control Centers.

1 Introduction

During the efforts of the previous Cigré Joint Working Group D2/B3/C2-01 "Security for Information Systems and Intranets in Electric Power Systems" [1], one method referred to the Electric Power Cyber Security Assessment methodology was presented [2], [3]. It supports the security evaluation of power utility information systems, as complex interacting infrastructures involving process knowledge, advanced control and information and communication technologies.

Building up on the background knowledge of the previous JWG a working task has been activated on the Risk Assessment (RA) topic within the scope of the current Cigré Working Group D2.22 "Treatment of Information Security for Electric Power Utilities (EPUs)".

The aim of the RA activity is to i) find out what the utilities really are doing today for managing vulnerabilities, threats and attacks whose successful occurrence provokes a relevant impact on the operational status of the power processes, ii) to suggest improvements to the currently practiced matrix-based risk assessment methods, and iii) to foster the development and adoption of common advanced methods usable in the EPU practice.

The WG has proposed to follow a "best practice track" rather than a "research track" and to to approach the Risk Assessment issues by starting to survey the status of the practices of the WG members with the aim of setting up an initial, shared view of the state-of-practices. The presented

overview on Risk Assessment practices is a first step towards the final WG objective of developing practical recommendations addressed to both chiefs of EPU Security Programs and managers of Control Centers.

The paper presents the outcome of the survey activity by following an anonymous style of reporting. The section 2 summarizes the characteristics of the contributions under analysis; the section 3 describes the core aspects of the practices described in the contributions; the section 4 evaluates the status of the analyzed practices against an identified common base and section 5 concludes with the final remarks and the next steps.

2 Summary of the contributions under analysis

The survey is based on the contributions provided by a representative sample of ten WG members composed by well-recognised power system operators and engineering service providers at international level.
The results are depicted in Figure 1, which shows that 30% of the contributors are using no method and 70% are using some method when doing Risk Assessment, 50% use qualitative practices and only 20% make use of some tool support: an IT (Information Technology) Risk Assessment tool and a beta (test) application.

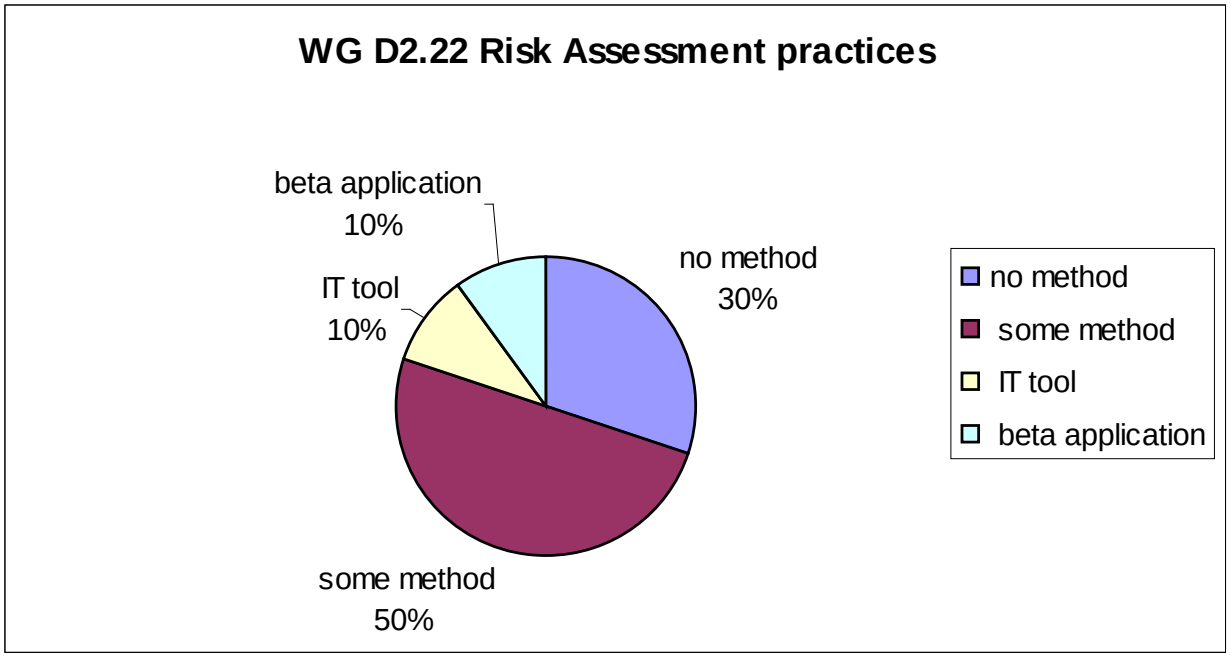


Figure 1: Risk Assessment practices from the WG members

The descriptions of practices were very heterogeneous and referred to different-level RA methods, covering an electricity sector-specific method, some Information Security Management System (ISMS)-level methods, a scenario-based method and a graphical methodology for IT security analysis based on standard Unified Modeling Language (UML) profiling.

By considering the non-homogeneous content of the contributions, the identification of the common criteria and items to be used in conducting a full comparative analysis was non trivial. However, some core aspects that emerged by each single-method analysis will be described, together with a few considerations related to the IT Security Management Framework and by the evaluation of some common and distinguishing factors from the whole set of the analysed contributions.

3 Core aspects of the practices described in the contributions

The availability of a reference electricity-specific methodology supporting the Risk Assessment activity and widely accepted by most Electric Power Utilities is highly desirable.

To this aim, a risk analysis of the electricity supply sub-sector (of the energy sector) has been conducted in 2005 by InfoSurance from an economic and social point of view.
This methodology covers ICT risks on major services in electricity production, transmission and distribution, with focus on cross-company and cross-sector risks, whilst excludes risks associated with energy trading as well as environmental risks (like storms, natural disaster and acts of war). A treatable set of 15 critical scenarios have been analysed and mapped onto a risk matrix combining risks from ICT failures with standard power failures.

In the analysis an ICT failure is considered relevant only if it has the potential to cause a power failure lasting at least four hours and affecting at least 10.000 customers.
Two classes of power failures (i.e. abnormal events) are considered to assess ICT failures [4]: loss of n-1 security and loss of 3000 MegaWatt production capacity in the power grid. In both cases it must be possible to restore secure and normal power and frequency conditions within 15 minutes.
ICT and power failures are assumed to be independent events: this implies that threat probability is achieved by multiplying respective ICT and power failure probabilities.
Occurrences probability of power failures has been estimated on the base of statistical data.

The following considerations may be summarised on the electricity sector analysis.

i) At the aim of identifying critical scenarios, some relevance criteria should be applied to ICT failures, based on the quantification of the cascading effects on the power infrastructure. Actually the judgment if a given ICT component failure is to be accounted for countermeasures or not requires a deep functional and behavioural analysis of the ICT infrastructure in relation to the control functions, in order to understand if a certain threat, targeting a specific component of the ICT infrastructure, is able to propagating to some core control functions, finally provoking a cascading malfunction from the ICT to the electrical infrastructures.
ii) Given classes of power failures have to be considered concurrently to ICT failures and any measures for counteracting those combined anomalous evolution must allow to restore secure and normal power conditions within a time delay of the order of 15 minutes.
iii) The mutual independency assumptions between power and ICT failures does not allow to account for the different functional dependencies existing between the two infrastructures [5].
iv) The Risk Probability Number associated to a given threat should be a function of the frequencies of combined ICT-power failures, their consequences on the system economy and security, and the probability of failures of adopted security controls.
v) Statistical data of ICT component failures affecting power control infrastructures may be not available due to both data sensitivity and threat continuous evolution: consequently an hybrid approach, combining stochastic analysis with empirical scenarios is the only possible.

3.1 Alignment with the framework issues

Currently the risk management activities for the Power System and for the ICT systems are separately managed, even if with some relationships between power and ICT teams. Since Power System origin the electrical security is being approached by means of static and deterministic methods that analyse a set of highly probable power contingencies during the system design phase, at the aim to implement sufficient system redundancies and reserves able to guarantee the power provision in case those con-

tingencies occur. Recently probabilistic approaches to the power risk assessment that take into account the operational state of the power system are under development [6].

With reference to the ICT risks the assessment activity within an EPU should be performed in the context of the enterprise ISMS [7]. Currently security management activities for control systems and for the IT systems are experiencing a graceful integration process.
Depending on the specific utility, the enterprise security management process may have reached different level of maturity both in IT and control systems, being developed on an empirical base or with the graceful introduction of a well structured methodology like ISO/IEC 27001-2 [8] [9]. According to the currently applied practices, a risk assessment session should start whenever a major change to some business, information system or threat and vulnerability hypothesis is contemplated. Depending on the risk rating resulting from the evaluation the current set of applied controls may be reviewed and new appropriate controls may be submitted to the management approval for implementation.

In a singular case control and teleoperation applications were subjected to an experimental activity consisting in the application of the CRAMM risk assessment methodology [10], originated in the IT domain, to the control system domain. CRAMM includes a comprehensive range of risk assessment tools that are fully compliant with BS7799 and which address tasks such as: asset dependency modelling, business impact assessment, threats and vulnerability analysis, risk assessment, security control identification.
Results from this experience revealed that these IT tools were not adequate to the context of control systems: the lack of tool flexibility for the SCADA systems and the high complexity in mapping the information assets required to perform some simplification in order to make the method applicable to the typical information assets and flows of SCADA architectures.

A mention was made about the possibility of using the CORAS language [11] for the risk assessment of the power system, a UML-based graphical notation for threat and risk assessment of ICT systems. Five distinct phases of brainstorming security analysis sessions have been identified by the CORAS method: (1) context identification, (2) risk identification, (3) risk estimation, (4) risk evaluation and (5) treatment identification. Each of these phases is documented using: asset overview diagrams, threat diagrams, risk overview diagrams, treatment diagrams and treatment overview diagrams.

In absence of a Risk Assessment practice, a more empirical approach to the management of ICT risks is singularly applied:

- due to the un-trustiness of the Corporate network, the corporate and operational services are rigorously separated in two independent networks;
- the Operational network is being installed with several security policies to be accessed and also protection devices as firewalls and IDSs (Intrusion Detection Systems);
- in the Corporate network the security politics must be followed by all employees; its security requirements were recently increased due to need to adequate to the Sarbanes-Oxley requirements.

Depending on the enterprise network adopted technology, hardening activities for both corporate and operational networks may be supported by the application of commercial products.

4 Common and distinguishing factors

Only a few commonalities but a lot of differences were found among the WG members` practices. In three out of six practices the following commonalities have been found:

- Assets, threats and vulnerabilities are well known dimensions;
- The threat assessment is conducted before of the vulnerability analysis;
- Deliberate as well as accidental types of threats are taken into account;
- The level of threat is judged without considering the controls already in place to counter the threats;
- The level of vulnerability is judged considering the controls in place to counter the threat.

Concerning the differences the comparison put in evidence that the frameworks underlying the considered practices differ in terminology, concepts and scales. For instance:

- different concepts like weaknesses, impacts or consequences are used to evaluate the failure effect in the risk measure;
- Different types of threats are considered;
- From 3 to 5 levels are used for the evaluation of both threats and vulnerabilities;
- From 3 to 11 levels are used for the impact evaluation.

5 Conclusions

A survey based on the contributions provided by a representative sample of ten WG members composed by well-recognised power system operators and engineering service providers at international level has been carried out.

The ICT risk assessment activity within an EPU should be performed in the context of the enterprise Information Security Management framework compliant with the appropriate standards [12]. According to the currently applied practices, a risk assessment session should start whenever a major change to some business, information system or threat and vulnerability hypothesis is contemplated.

The availability of a reference electricity-specific methodology widely accepted by most Electric Power Utilities is highly desirable. This methodology should cover Information and Communication Technology (ICT) risks on major services in electricity production, transmission and distribution, with focus on cross-company and cross-sector risks. A treatable set of critical scenarios should be analysed and mapped onto a risk matrix, combining risks from ICT failures with standard power failures. Classes of power failures have to be considered concurrently to ICT failures and any measures for counteracting those combined anomalous evolution must allow to restore the secure and normal system state within the process time delays.
Depending on the risk rating resulting from the evaluation the current set of applied controls may be reviewed and new appropriate controls may be submitted to the management approval for implementation.

Only a few commonalities but a lot of differences were found among the WG members` practices. The level of contributions confirmed that the ICT risk assessment in the electric power industry needs a lot of advancements. The findings demonstrate the lack of a reference method and confirmed the emergent need of a methodology integrating both power and ICT security knowledge. The nodal topics of Risk Assessment will be further investigated along the WG D2.22 activity.

6 Acknowledgments

I would like to explicitly acknowledge all the WG D2.22 members who contributed to the risk assessment survey: Werner Meier - Swissgrid (CH), Giancarlo Caroti – Italian National Grid (I), Stuart Duckworth – UK National Grid (UK), Marc Tritschler – Kema (NL), Goran Ericsson Swedish National Grid (SE), Age Torkilseng – Salten Kraftsamband (NO), Erik Sandstrom – Vattenfall (SE), Tor Aalborg – Statnett (NO), Claudio Trigo de Loureiro – FURNAS Centrais Electricas (BZ), Andrei Vidrascu - French National Grid (FR).

7 References

- Cigré JWG D2/B3/C2-1 Technical Brochure TB 317 on “Security for Information Systems and Intranets in Electric Power Systems”, 2007
- Dondossola G., Lamquet O., “Cyber Risk Assessment in the Electric Power Industry”, Electra N°224, February 2006, pp. 36-43, http://www.cigre.org/gb/electra/electra.asp

- Dondossola G., Lamquet O., Torkilseng A., "Key issues and related methodologies in the security risk analysis and evaluation of electric power control systems", Cigré Session 2006, Paris 27 August – 1 September 2006
- UCTE Operation Handbook. Union for Co-ordinatin of Transmission of Electricit UCTE, July 2004 – September 2007
- Kaaniche M. and oth., "Methodologies synthesis", Critical Utility InfrastructurAL Resilience, CRUTIAL European Project IST-FP6-027513, Deliverable D3, January 2007.
- Ciapessoni E., Cirio D., Gaglioti E., Liliana T., Massucco S, Pitto A., "A probabilistic approach for operational risk assessment of power systems", – C4-114, Cigré Paris Session 2008
- Ericsson G., Torkilseng A., Dondossola G., Bartels A., "Treatment of Information Security for Electric Power Utilities – Progress Report from Cigré WG D2.22" – D2-213, Cigré Paris Session 2008
- ISO/IEC 27001:2005, Information Technology - Security techniques - Specification for an Information Security Management System

- ISO/IEC 27002:2005, Information Technology - Code of practice for Information Security Management

- http://www.cramm.com/

- Aagedal J., den Braber F., Dimitrakos T., Axel Gran B., Raptis D., Stolen K., „Model-based risk assessment to improve enterprise security", EDOC'02, pages 51-64, IEEE Computer Society, 2002.

- L. Pietre-Cambacedes, T. Kropp, J. Weiss, R Pellizzonni, "Cybersecurity standards for the electric power industry – a survival kit" – D2-217, Cigre Paris Session 2008

http: //www.cigre-d2.org
http://www.cigre2009-d2.jp/

CONSEIL INTERNATIONAL DES GRANDS RESEAUX ELECTRIQUES
INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS

STUDY COMMITTEE D2
INFORMATION SYSTEMS AND TELECOMMUNICATION

2009 Colloquium
October 21-22, 2009
Fukuoka - Japan

D2-01 D03

INFORMATION/ICT SECURITY RISK ASSESSMENT OF OPERATIONAL IT SYSTEMS AT ELECTRIC POWER UTILITIES

by

Marc Tritschler

KEMA Limited

(UK)

and

Giovanna Dondossola

CESI RICERCA

(ITALY)

SUMMARY

Risk Assessment is an integral part of the Risk Management process employed by Electric Power Utilities (EPUs). The objective of Risk Management is to ensure that all risks faced by the EPU are appropriately identified, understood and treated. The decision making process for the treatment of risks relies on information about the threats and vulnerabilities that contribute to the likelihood of the risk occurring and the impact of its occurrence, compared with the cost of mitigating the risk and the risk appetite of the EPU. Thus, risk treatment options range from mitigation to acceptance for any given risk.

Formal Risk Management has become an accepted part of corporate governance for EPUs, and in order to cover all necessary aspects it needs to operate within a framework which facilitates the inclusion of Risk Assessment information from all parts of the EPU. In the context of this paper, this must include Risk Assessment information concerning EPU physical operations, and within physical operations Risk Assessment must include information security/Information and Communications Technology (ICT) security Risk Assessment for operational ICT systems such as SCADA/EMS and power plant process control systems. It is believed that improvements need to be made in this area in order to improve the consideration of these risks within the context of enterprise wide Risk Management.

Definitions of risk and Risk Management are provided, based on the ISO 31000 Risk Management standard currently under development, and relevant to EPUs. Further to this, a Risk Management framework for EPUs is proposed, particularly to facilitate the incorporation of information/ICT security Risk Assessment for operational ICT systems into the overall, enterprise wide, Risk Management process. The proposed framework and methods are aligned with already published Risk Management methodologies specific to SCADA systems.

Of critical importance in the framework is the recognition of both potential ICT consequences and power consequences due to the occurrence of risks arising from the existence of threats and vulnerabilities. The framework addresses the relationship between ICT consequences and power consequences, and their impact on the EPUs, and proposes a method for assessing these risks and reporting on them against Risk Acceptance Criteria set at appropriate levels within the EPU. This provides an approach which permits the appropriate integration of these risks into an enterprise wide Risk Management process.

KEYWORDS

Risk Assessment, Risk Management, Security, SCADA, ICT, Dependencies

1. DEFINITIONS

Risk is defined in ISO Guide 73 [1] as ***"the effect of uncertainty on objectives"***. This is being expanded by the developers of the upcoming ISO 31000 Risk Management standard [2] as follows:

- The effect is some deviation from the expected, which can be positive and/or negative.
- Objectives can have different aspects such as financial, health and safety, and environmental goals and can apply at different levels such as strategic, organization-wide, project, product, and process.
- Risk is often characterized by reference to potential events, consequences, or a combination of these and how they can affect the achievement of objectives.
- Risk is often expressed in terms of a combination of the consequences of an event or a change in circumstances, and the associated frequency and probability of occurrence.

It important to stress that this definition of risk does not only cover a negative outcome, i.e. the definition is broadened to potential positive outcomes in order to cope with the aspect of companies taking risks for commercial reasons, for example making uncertain investments with the intention to obtain a positive outcome.

In ISO Guide 73 Risk Management [1] is defined as ***"coordinated activities to direct and control an organization with regard to risk"***. This paper focuses on three aspects of the co-ordinated activities of Risk Management, the Risk Management Process (generic), a Risk Management Framework (specific to EPUs), and a discussion of Risk Assessment Methodologies for use in assessing risk on power/ICT infrastructures..

2. RISK MANAGEMENT PROCESS

A generic risk management process can be used for risk management in the context of information/ICT security risk assessment for operational ICT systems such as SCADA/EMS and power plant process control systems. This describes the high level steps required for a consistent risk management process. Such a generic process has been used as the basis for the development of the Generic SCADA Risk Management Framework by the Trusted Information Sharing Network for Critical Infrastructure Protection in Australia [3]. In this case, the generic process utilized is the standards-based risk management framework as described in AS/NZS 4360 [4] and shown in Figure 1 below.

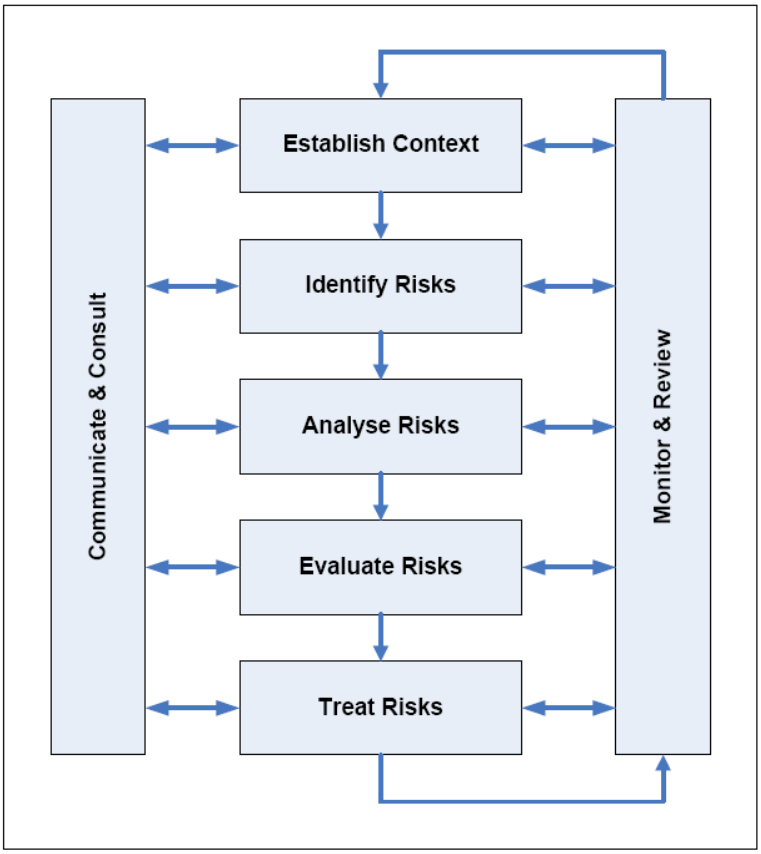


Figure 1 - Risk Management Framework (Source: AS/NZS 4360:2004)

The steps represented in the diagram above are as follows:

- Establish Context involves defining the scope of the assessment process and, in particular, identifying the assets that are potentially at risk.
- Identify Risks, Analyse Risks and Evaluate Risks are the core risk assessment steps.
- Treat Risks covers the plans and activities to address the levels of risk identified by the core risk assessment steps.
- Communicate and Consult comprises the engagement of stakeholders associated with the assets assessed.
- Monitor and Review comprises the governance controls to ensure enduring effectiveness of the process.

The process is essentially generic and can be applied in any scenario where risk management is required. However, it operates at one level only and does not assist in identifying, analyzing and evaluating risks in the context of hierarchical organizations (and business processes and systems within those organizations). In conclusion, it is very useful in the single level in which it is utilized, but requires additional inputs and outputs to fit within a framework for multi-level risk management.

3. RISK MANAGEMENT FRAMEWORK

Risk Management needs to be applied on a hierarchical, multi-level basis to work within the hierarchical and multi-level nature of organizations, business processes and systems that exist in the modern EPU environment, with their complex dependencies. For the purposes of developing an appropriate Risk Management Framework for EPUs, we decompose the organization as shown in Figure 2 below.

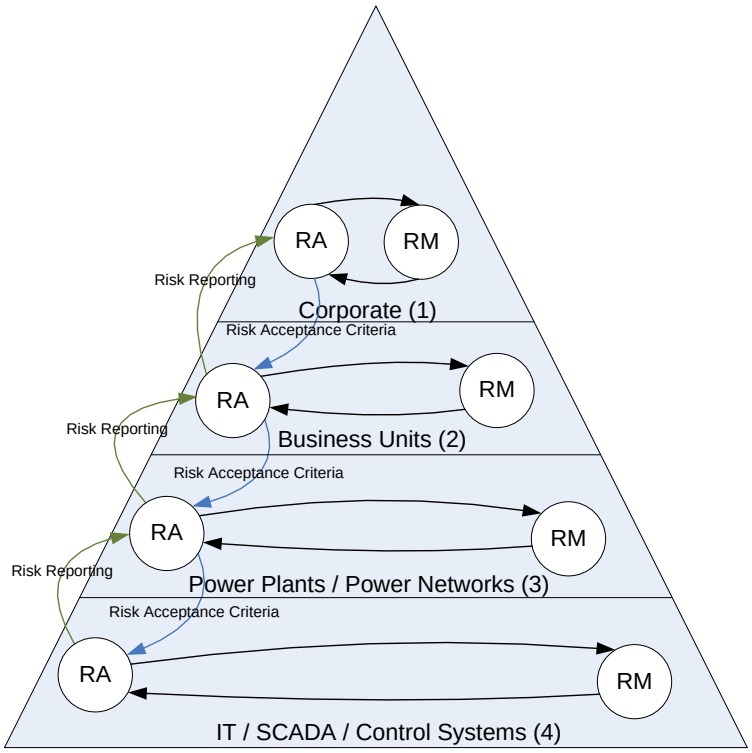


Figure 2 – EPU Risk Management and Risk Assessment Model

The four layers in Figure 2 illustrate the various hierarchical levels of the operations part of a typical EPU which operates power plants and/or electricity networks. Depending on the size and nature of the organization, levels 1 and 2 may be merged (for example in a smaller organization with one operational business unit). However, typically each level will have authority over one or more entities in the level below. Therefore, the single corporate entity will have authority for most business units, and each business unit will have responsibility for one or more power plant and/or electricity network, etc.

As each level has authority over the entities in the level below, it will set certain business objectives for them, and monitor the level of achievement of these business objectives. We can use this same concept to elaborate how risk is assessed and managed within the corporate structure of EPU operations.

Each level of the organization has a different set of objectives, and is therefore exposed to different sets of risks. However, as there are dependencies between each level in terms of objectives, there are also dependencies between each level in terms of risk. In order to take a holistic approach to risk management, it is important that these dependencies are recognized, and linked unambiguously through the use of a common framework or language for the identification and management of risks.

At each level within the organization, Risk Assessment activities should take place, and this should result in risks being quantified and Risk Treatment actions being taken to bring certain identified risks down to acceptable levels (where they are not already at or below acceptable levels). In some cases, risks at the higher levels in the organization are managed not within the level itself but by setting objectives for the lower levels of the organization. As shown in Figure 2, this constitutes Risk Acceptance Criteria for Risk Assessment activity at the lower level. Also as shown in Figure 2, the level undertaking the Risk Assessment (RA) and Risk Management (RM) activities reports back up to the higher level (Risk Reporting) in order to demonstrate that it is managing risk appropriately (or perhaps to identify where it needs further investment to manage specific risks). Importantly, this Risk Reporting is based on performance against Risk Acceptance Criteria originally set by the higher level.

There are interdependencies between all adjacent levels in the framework, however it is of critical importance in the framework that it permits the recognition of both potential ICT consequences and power consequences due to the occurrence of risks arising from the existence of threats and vulnerabilities. The framework addresses the relationship between ICT consequences and power consequences, and their impact on the EPU, and proposes a method for assessing these risks and reporting on them against Risk Acceptance Criteria set at appropriate levels within the EPU. This provides an approach which permits the appropriate integration of these risks into an enterprise wide Risk Management process.

Additionally, research [5][6] is being undertaken to develop more comprehensive interdependency modelling techniques and tools for the interdependencies between level 3 and level 4, and also for interdependencies with other level 4 elements such as Telecoms, which are not directly IT, SCADA or Control Systems but are critical components of these systems. Such sophisticated models are outwith the scope of this paper but should be complimentary to this proposed framework.

The model described recognizes that dependencies exist between risks at adjacent levels in the organization, and therefore identifies there are links between Risk Assessment and Risk Management activities at adjacent levels. This, however, identifies a further requirement; the need to create a common understanding and means of expressing risk between each level. In order to do this, we first state that risk expressed from one level to another is essentially an abstraction of the risk between the two levels, and we use this to create a taxonomy of risk from the highest level in the organization to the lowest level.

One means of developing a common understanding and means of expressing risk which would be applicable at all levels would be to classify risks into a number of different categories. Figure 3 below shows an example risk form, used as part of the Risk Assessment process, which guides participants to classify risks into different categories as part of a risk taxonomy.

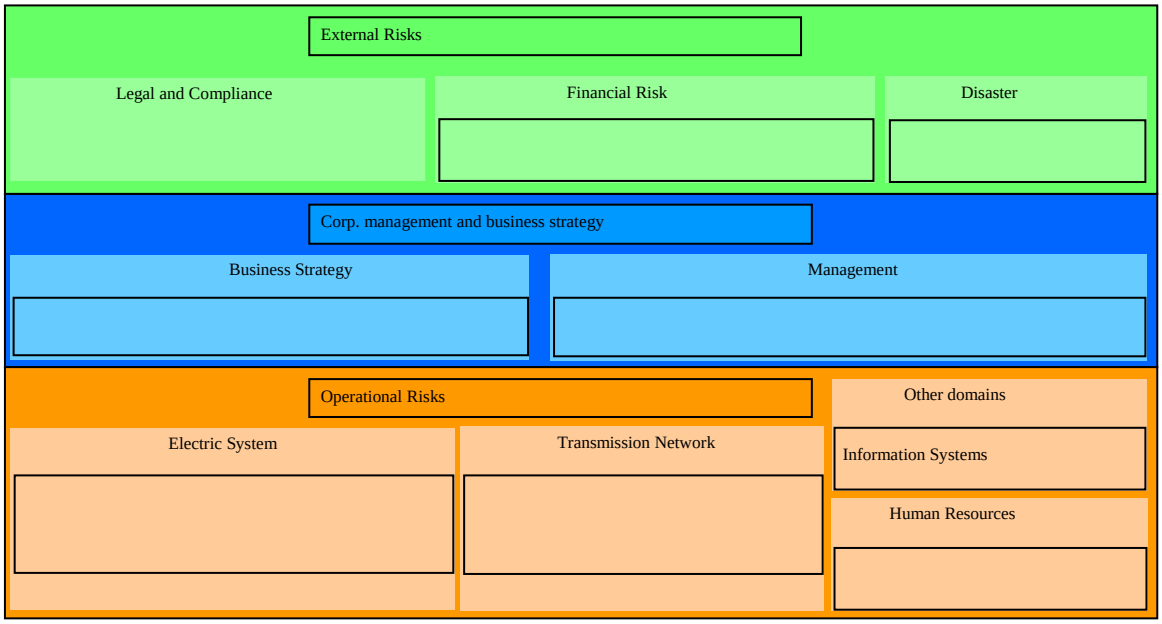


Figure 3 – Risk Categorisation (Source: Andrei Vidrascu, RTE)

In Figure 3, the higher level risk categories are External Risks, Corporate Management and Business Strategy, and Operational Risks, and there are a total of nine lower level risk categories (Electric System, Transmission Network Assets, Human Resources, Information Systems, Business Strategy, Management, Finance, Natural Disaster, and Legal). For any risk to be of concern to the EPU, it must be categorised into one or more of these risk categories. Using a common taxonomy of risk such as this throughout the EPU ensures that risk

communication uses a common language and that only risks which can be identified in the appropriate categories are addressed.

4. RISK ASSESSMENT METHODOLOGIES

In each level of the Risk Management Framework, Risk Assessment takes place as part of the Risk Management Process previously described. However, each risk assessment activity may use a different methodology dependent on the target of the risk assessment. A survey of the Risk Assessment practices performed by the members of the Cigré WG D2.22 [7], particularly at levels 3 and 4, identified that there are only a few commonalities but a lot of differences among the WG members` practices. The comparison provides evidence that the frameworks underlying the considered practices differ in terminology, concepts and scales, including:

- Different concepts like weaknesses, impacts or consequences are used to evaluate the failure effect in the risk measure;
- Different types of threats are considered;
- Different levels are used for the evaluation of threats, vulnerabilities and impact evaluation.

The findings demonstrated the lack of a reference method and confirmed the need of developing an electricity-specific methodology that is widely accepted by most EPUs and integrating both power and ICT security knowledge. This is synonymous with integrating level 3 and level 4 security knowledge in Figure 2. Of the survey sample, 30% are using no defined method and 70% are using some defined method when doing Risk Assessment, 50% use qualitative practices and only 20% make use of some tool support which are either an IT Risk Assessment tool or an ad-hoc test application.

Among Risk Assessment tools originating from the IT domain, the CRAMM risk assessment methodology [8] has been evaluated against the control system domain. CRAMM includes a comprehensive range of risk assessment tools addressing tasks such as: asset dependency modelling, business impact assessment, threats and vulnerability analysis, risk assessment, security control identification. From this experience the tool has been judged not adequate to the context of control systems: the lack of flexibility and the high complexity in mapping the information assets required to perform several simplifications in order to make the method applicable to the typical information assets and flows of SCADA architectures.

The CORAS language [9] for the risk assessment of the power system has also been mentioned in the survey. CORAS is a UML-based graphical notation for threat and risk assessment of ICT systems. Five distinct phases of brainstorming security analysis sessions are contemplated in CORAS: context identification, risk identification, risk estimation, risk evaluation and treatment identification. Each of these phases is documented using: asset overview diagrams, threat diagrams, risk overview diagrams, treatment diagrams and treatment overview diagrams.

A more complete inventory of Risk Assessment Methods and Tools can be found in the Risk Management section of the ENISA Website [10], however this does not provide any information specific to the application of the tools to level 3 and level 4 of the model in Figure 2.

Based on the survey outcome, the following issues have been identified by the WG as needs to be addressed by tools accounting for the dependencies of power from ICT failures:

(xi) Information on ICT threats must be kept updated on a continuous basis.

(xii) Statistical data of ICT component failures affecting power control infrastructures are not available due to both data sensitivity and the continuous evolution of threats:

consequently a hybrid approach, combining stochastic analysis with empirical analysis could potentially be pursued.

(xiii) Improved estimations on the probability of occurrence of ICT failure could be achieved by considering the threat plausibility and their degree of success.

(xiv) The judgment if a given ICT component failure requires countermeasures or not requires a deep functional and behavioural analysis of the ICT infrastructure in relation to the control functions, in order to understand if a certain threat, affecting a specific component of the ICT infrastructure, is able to impact on some core control functions, resulting in a malfunction from the ICT to the electrical infrastructures.

(xv) Classes of power failures have to be analysed in combination with ICT failures.

(xvi) The quantification of the cascading effects of ICT failures on the power infrastructure depends on the duration of the potential power failure, the number of customers affected or the loss of security.

(xvii) The Risk Index associated to a given scenario is a function of 1) the probability of combined ICT-power failures given the probability of failures of the adopted security controls 2) the evaluation of the impact of their consequences.

(xviii) The impact evaluation is based on a mix of economic, social and quality of service criteria, by distinguishing the size and services from the EPU (power transmission, power distribution, bulk power production, distributed energy generation etc).

(xix) Depending on the risk rating resulting from the evaluation, existing controls are reviewed and new appropriate controls may be submitted for management approval for implementation.

(xx) Any measures for counteracting those combined anomalous events must allow the restoration of secure and normal power conditions within the process time delay.

In the absence of established methodologies which address the specific needs of the EPUs, Risk Assessment efforts for level 3 and level 4 tend to use a scenario-based approach which considers threats, likelihoods and impacts across both level 3 and level 4 combined. In order for this to be successful, an excellent knowledge of both the power systems and the ICT systems and the detailed interaction between them is required, so that realistic scenarios can be developed. It must be recognised that this process is unlikely to develop a comprehensive Risk Assessment of all possible scenarios, due to the complexity of the interactions between the power system and the ICT infrastructure.

5. CONCLUSIONS

In order to address risks due to power systems and ICT systems dependencies, all EPUs should undertake Risk Assessments at level 3 and level 4 as part of a Risk Management Process, in accordance with a Risk Management Framework for the EPU, such that both the Risk Acceptance Criteria and Risk Reporting are integrated into the overall Risk Management activities of the EPU. The language used to communicate risk between the various levels of the EPU should be based on common and agreed terminology.

For level 3 and level 4 Risk Assessment activities, the lack of established methodologies to deal with the unique nature of power systems and ICT systems dependencies mean that the EPUs must bring power systems and ICT specialists together regularly to perform (scenario-based) Risk Assessments as a team, and that these assessments will be limited by the capabilities of these teams until such times as more comprehensive tools becomes available which are specific to the needs of the EPUs. However, bringing such teams together to undertake Risk

Assessments is a very positive step in the Risk Management process, and all EPUs should be committed to such activities on a regular basis.

8.1.1.1 BIBLIOGRAPHY

[1] Risk management — Vocabulary, ISO/IEC CD 2 Guide 73, concept, April 2008.

[2] Risk management — Principles and guidelines on implementation, ISO/DIS 31000, concept, April 2008.

[3] Generic SCADA Risk Management Framework for the IT Security Expert Advisory Group (IT-SEAG), Trusted Information Sharing Network for Critical Infrastructure Protection, December 2006.

[4] AS/NZS 4360:2004 Risk Management, Standards Australia

[5] IRRIIS project, www.irriis.org

[6] CRUTIAL project, http://crutial.cesiricerca.it

[7] Risk Assessment of Information and Communication Systems - Analysis of some practices and methods in the Electric Power Industry, Giovanna Dondossola CESI RICERCA SpA, Electra, August 2008.

[8] http://www.cramm.com/

[9] Aagedal J., den Braber F., Dimitrakos T., Axel Gran B., Raptis D., Stolen K., Model-based risk assessment to improve enterprise security“, EDOC’02, pages 51-64, IEEE Computer Society, 2002.

[10] http://www.enisa.europa.eu/rmra/rm_home.html

"Security Technologies Guideline - Practical Guidance for Deploying Cyber Security Technology within Electric Utility Data Networks"

Andrew Bartels, Ludovic Pietre-Cambacedes, and Stuart Duckworth

On behalf of Cigré WG D2-22 "Treatment of Information Security for Electric Power Utilities (EPUs)".

ABSTRACT

Electric Power Utilities (EPUs) are increasingly becoming aware of the need to secure critical data networks. The challenges faced here are daunting, given the extreme complexity of EPU data networks, the vast number of cyber attacks possible [1], and the high reliability requirements naturally associated with power delivery. The paper presents practical guidance in this area, and gives illustrated examples of an effective approach to identifying cyber controls and deploying cyber security technologies that are both compatible with, and appropriate for use within EPU data networks.

This guide is the third part of the work of Cigré WG D2.22 "Treatment of Information Security for Electric Power Utilities" [2], to be presented at the Cigré 2008 Paris session. The approach outlined has best application after an EPU has taken prerequisite steps (previously addressed by WG D2.22), such as establishing an internal corporate awareness of existing cyber security standards [3], establishing appropriate security frameworks [4], and performing risk assessment [5].

1 INTRODUCTION

This paper provides guidance on the application of cyber security controls to electric utility networks. To make best use of this material, the reader should be familiar with the preceding WG D2.22 Security Frameworks [4] and Risk Assessment [5] papers. Ideally, a formal risk assessment should be already completed and a corporate security domain model defined.

With these steps completed, physical assets within the network can be mapped to security domains. Appropriate security technologies can then be deployed within the network to meet the requirements of each domain.

Due to the wide and varying range of EPU data networks, this paper generalizes data networks into common elements that are likely to be present within most EPUs. Specific diagrams are provided for Transmission and Distribution (T&D) grid data networks, and data networks associated with generation plants. The approach in this paper can also be applied to other EPU data networks.

Note: this paper is focused on cyber security technologies; nevertheless, it is well understood that organizational and policy issues, physical security, and redundancy and disaster recovery plans are also of paramount importance to ensure an appropriate and consistent level of security, and a precondition for an efficient use of the discussed technical solutions.

1.1 SENSITIVE CONTROL SYSTEMS AND SECURITY TECHNOLOGY

Supervisory Control and Data Acquisition (SCADA) and other types of control systems are a key part of critical operations for EPUs. Due to the industrial environment, timing sensitivity, and unique technology characteristics of control systems, standard IT security products are often incompatible or ineffective to deploy. An essential part of any EPU security deployment process is ensuring compatibility with legacy systems. This paper is mindful of both modern IT and legacy SCADA environ-

ments, and the technological approach given herein allows for consistent and effective security measures across both.

2 EFFECTIVE DEPLOYMENT OF SECURITY TECHNOLOGY

2.1 RELATIONSHIP OF RISK ASSESSMENT AND SECURITY DOMAINS TO TECHNICAL SECURITY CONTROLS

In the preceding Frameworks paper [4], an example security domain model is given. The model given is adopted within this paper as an initial starting place.

Briefly, this model defines security controls for four security domains. Each domain represents a different level of security. A summary of the levels and associated domains is provided here for reference:

Protection Level (relative to operations)	**Domain**	**Colour in Fig. 1**	**Example Systems**
Low	Untrusted	White	Vendor / 3rd party networks, internet
Medium	Corporate	Green	Office level business network
High	Business Critical	Amber	Finance, human resource systems
Very High	Operation Critical	Red	Controls systems, SCADA networks

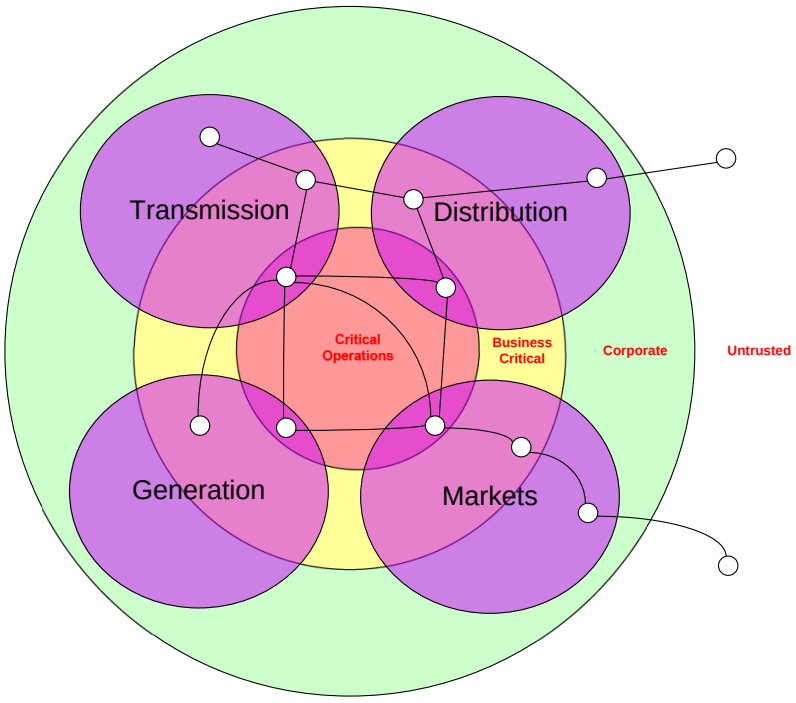


Fig. 1 Information Security Domain Model

When combined with risk assessment results, the security domains model can be extended to include specific cyber security controls. For illustration purposes, security controls for the Corporate, Busi-

ness Critical, Operation Critical domains might reasonably include the measures in Tables 1, 2 and 3. Although this is a summary list, more detailed information on appropriate controls can be found in the major industry cyber security standards [3].

Table 1 - Corporate Security Domain (Baseline Controls)

Cyber Security Controls:
Access Control
✓ Logical access control (when possible based on least-privilege; RBAC)
✓ Security gateways as unique interfaces between adjacent domains (control, log)
✓ Remote access controls
✓ Physical access control to cyber assets
Monitoring & Logging
✓ Maintenance and monitoring of computer and network security components
✓ Anomaly/intrusion detection systems and procedures
✓ Reporting and review of unused and expired accounts
Vulnerabilities Monitoring and Management
✓ Patch management (manual and automated, as appropriate)
✓ Vulnerability awareness and acceptance program

Table 2 - Business Critical Security Domain

Cyber Security Controls:
Corporate Security Domain controls (listed in Table 1)
✓ Some controls enhanced (i.e. restricted Internet access, remote maintenance strict controls)
Integrity and Confidentiality Protection (*)
✓ Minimum protection level for in-flight data (during communications) between geographically dispersed data networks Minimum protection level for stored data (i.e. disk, tape)
Monitoring & Logging
✓ Logged application access, including user ID, event time, and all user activity while logged in
✓ Auditing / logging of all automated / scripted login sessions

Table 3 - Operations Critical Security Domain

Cyber Security Controls:
✓ **Corporate Security Domain controls (listed in Table 1)**
✓ **Business Critical Security Domain controls (listed in Table 2)**
Vulnerabilities Monitoring and Management
✓ Patch management (manual testing and deployment)
Advanced Authentication
✓ Device-to-device authentication, ensures communications only flow between authorized data network devices
✓ Strong user-to-device and user-to-application authentication

* Integrity and confidentiality are highlighted. Availability must also be addressed, though it is not explicitly included in the examples due to limited space.

2.2 LOGICAL SECURITY DOMAINS TO TECHNICAL IMPLEMENTATION

The security domains covered above are logical. Although security controls can be assigned in general to each security domain, a successful security implementation involves adding cyber controls to the data network, in the form of cyber security technology devices and software. To ensure that devices and software are placed in the data network to enforce security applicable for each domain, physical network assets must be mapped to logical security domains. This assignment can be made based on the following criteria:

- Results of Risk Assessment, i.e. the Risk Probability Numbers [5] from the assessment of:
  - Known vulnerable points within the network
  - Impact to operations if a given area of the network is compromised
  - Interconnectedness of the network to networks in less secure domains
  - Reliance on third party communications infrastructures
- Already established Corporate Security Policy requirements

3 TRANSMISSION, DISTRIBUTION, AND GENERATION NETWORKS

Identifying security domains and implementing cyber security technology within an EPU is a complex process, and specific details vary according to the data network configuration. Additionally, special consideration must always be given to the impact of cyber security controls on an EPU's operations data network, as these networks are often more sensitive to reliability and latency factors than a typical IT data network.

3.1 EXAMPLE DATA NETWORK WITH SECURITY DOMAINS

To illustrate the application of cyber security for EPUs, we provide an example mapping of security domains within a typical EPU data network (see Figure 2). While this example mapping is intended to be representative of the various elements present within an EPU data network, an actual mapping will vary based on Risk Assessment, Security Domain definitions and the specific details of the data network.

Major data network components in Figure 2 include the T&D network with substations, one or more generation facilities, and connections to a corporate office. Logical security domains have been mapped to the physical EPU data network according to relative criticality and risk (which would be determined by a risk assessment process). The logical security domains are illustrated with color coded regions. As can be seen, the typical EPU network often contains a mixture of Operations Critical, Business Critical, Corporate, and Untrusted domains.

In Figure 2, the Operations Critical Security Domain primarily covers the operations control center(s), substations, and the control networks directly supporting generation. The Business Critical Security Domain covers assets that support critical operations, but which are not, in themselves, critical to grid reliability. The Corporate Security Domain covers data network components which have baseline security requirements, but which are not essential to grid reliability.

Notice that two domains, the Operations Critical Security Domain and Business Critical Security Domain span areas of the data network that are geographically dispersed. This type of configuration, which is typical, can complicate the implementation of security measures for each domain. The next section identifies how this problem can be overcome.

3.2 APPLIYING SECURITY TECHNOLOGIES TO LOGICAL DIAGRAMS

Once logical security domains have been mapped to the physical EPU data network, specific security control implementation details can be worked out. Since each security domain prescribes specific

security controls, specific security technologies can be selected for deployment. As stated earlier, the choice of technology should be considered in light of any special reliability and latency requirements of the data network being secured.

In considering Tables 1 through 3, it's possible to identify security technologies that can be deployed to meet the security control requirements. Tables 4 through 6 provide such a mapping (although the list of technologies may be expanded upon, according to applicability to the environment).

Table 4 - Corporate Security Domain (Baseline Controls)

Cyber Security Controls / Technology:
Access Control
✓ Directory services, remote access authentication, two-factor authentication technology, application security models, single sign-on technologies
✓ Firewalls, remote user access gateways
Monitoring & Logging
✓ SNMP v3 monitoring technologies, system event log auditing technologies, reporting tools
✓ IDS (intrusion detection systems)
✓ Security reporting tools
Vulnerabilities Monitoring and Management
✓ Automated patch management downloading tools, manual patch evaluation and testing, enterprise patch deployment tools
✓ Subscriptions to security alert services

Table 5 - Business Critical Security Domain

Cyber Security Controls / Technology:
Corporate Security Domain controls (listed in Table 4)
Integrity and Confidentiality Protection
✓ Encrypting routers, security appliances Online disk encryption technology, tape backup encryption technology
Monitoring & Logging
✓ Application gateway technology
✓ Firewalls, deep packet inspection

Table 6 - Operations Critical Security Domain

Cyber Security Controls / Technology:
✓ **Corporate Security Domain controls (listed in Table 1)**
✓ **Business Critical Security Domain controls (listed in Table 2)**
Vulnerabilities Monitoring and Management
✓ Manual patch management downloading, manual patch testing, careful deployment
Secure Protocols
✓ Use secure versions of SCADA and ICS protocols
Advanced Authentication
✓ Network authentication appliances, VPN tunnels
✓ Strong authentication (tokens)

Figure 3 depicts the deployment of these security technologies in response to the requirements of each security domain, using the example EPU data network in Figure 2 as a basis.

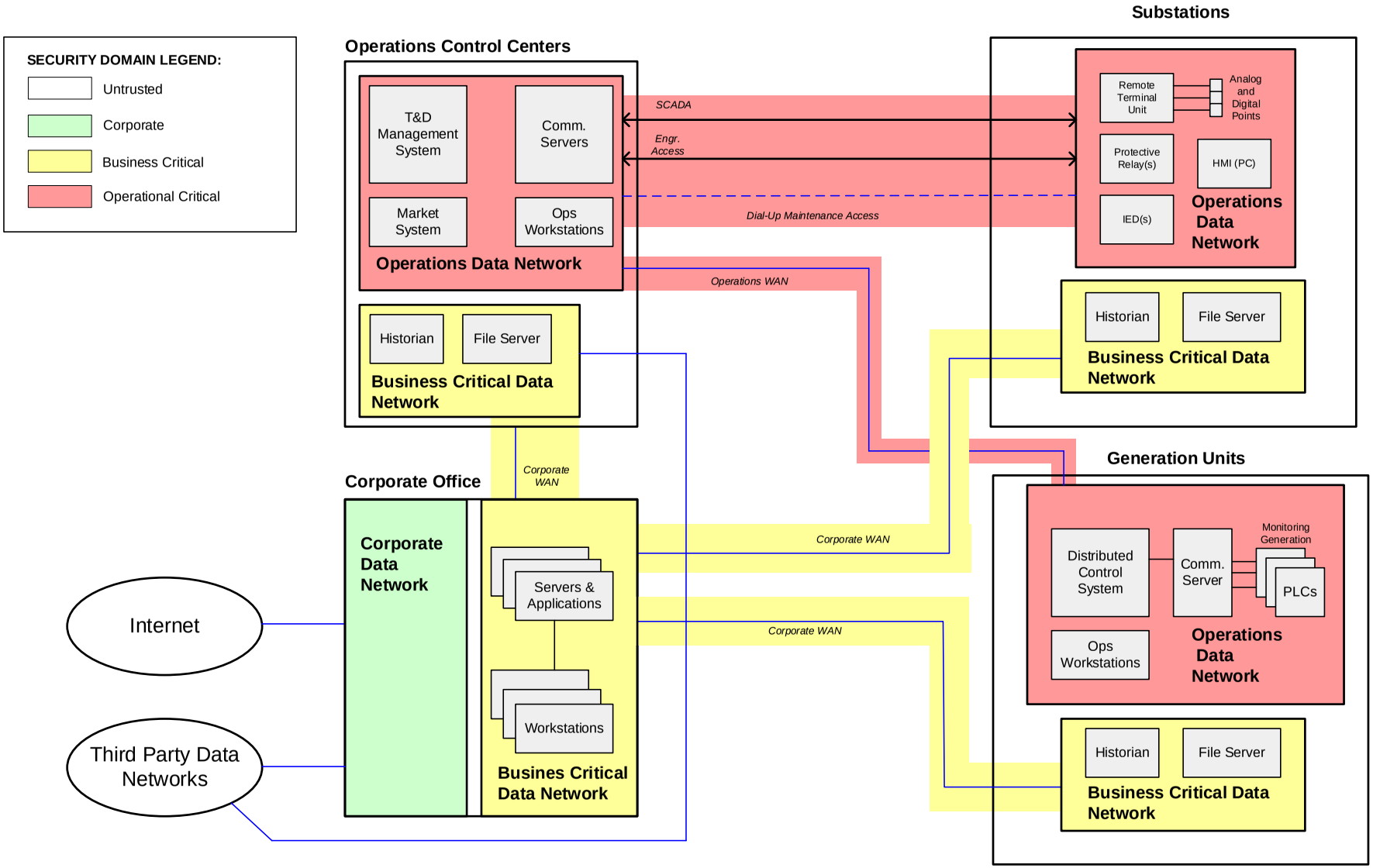


Figure 2 – Example of Logical Security Domains for T&D and Generation

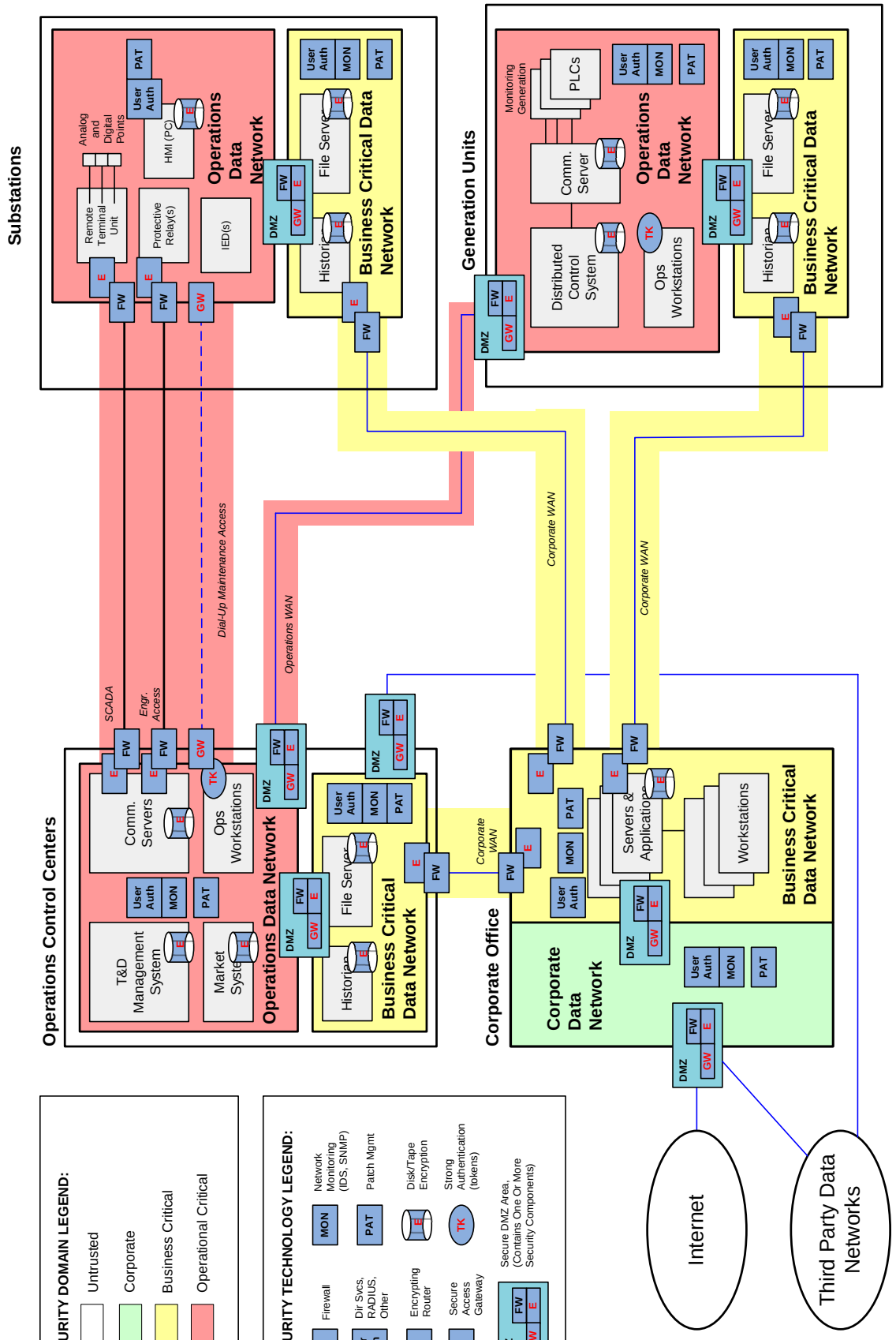


Figure 3 – Example of Cyber Security Technologies Deployed

4 SUMMARY

The special challenges that EPUs face in securing data networks are complex. Yet, as this paper demonstrates, a well researched and careful approach can yield a highly effective security deployment – one that actually enhances electric reliability by protecting critical cyber assets from attack.

This paper provides an approach to the crucial step of deploying security technology. However, deployment is in fact the last step in what must become a repeated security review cycle. As previous work from Cigré WG D2.22 shows, EPUs must implement a complete security discipline that includes regular processes:

- Reviewing and analyzing current and evolving cyber security standards [2]
- Assessing risk to the system, using an appropriate methodology [5]
- Maintaining high corporate awareness of possible cyber threat scenarios [1]
- Establishing and maintaining a well documented security frameworks model, as part of a larger corporate security policy [4]
- Deploying and maintaining security technologies that map to logical security domains.

5 REFERENCES

[14] "Common Vulnerabilities and Exposures List" – available online at http://www.cve.mitre.org/

[15] G. Ericsson, Å. Torkilseng, G. Dondossola, A. Bartels, " Treatment of Information Security for Electric Power Utilities – Progress Report from Cigre WG D2.22," – D2-213 , Cigre Paris Session 2008

[16] L. Pietre-Cambacedes, T. Kropp, J. Weiss, R Pellizzonni, "Cybersecurity standards for the electric power industry – a survival kit" – D2-217 , Cigre Paris Session 2008

[17] Torkilseng, Å., Duckworth, S, "Security Frameworks for Electric Power Utilities – Some Practical Guidelines when developing frameworks including SCADA/Control System Security Domains", submitted to Electra 2008.

[18] Dondossola G., "Risk Assessment of Information and Communication Systems - Analysis of some practices and methods in the Electric Power Industry", submitted to Electra 2008.

[19] ISO/IEC 27002:2005, Information Technology - Code of practice for Information Security Management

Cybersecurity standards for the electric power industry – a "survival kit"

L. PIETRE-CAMBACEDES[1], T. KROPP[2], J. WEISS[3], R. PELLIZZONI[4]
[1]Electricité de France, [2]Dyonyx, [3]Applied Control Systems, [4]Transba
[1]France, [2,3]U.S.A., [4]Argentina

SUMMARY

As Electric Power Utilities (EPUs) have automated their operational computing systems, cybersecurity has become a critical issue. Systems used to monitor and control the electric system as well as to manage their core business and administrative tasks, face new threats and vulnerabilities along with the performance improvement provided by their growing networked interconnections and standardization. Many EPUs are aware of this evolution and are structuring their approaches accordingly. Common cybersecurity frameworks, that is to say, comprehensive approaches to manage risks adequately and create a common ground to build adapted defences and security processes, are necessary to adopt an efficient and coherent enterprise-wide response. The establishment of such frameworks can be based on several existing standards, which differ in their nature (informational, regulatory, compliance-oriented, etc.), in their form (guidelines, reports…), and also in their scope (e.g., general IT, process control-oriented, electrical transmission and distribution-oriented).

This paper is not intended to select standards on behalf of the Electric Power Industry but rather support EPUs in the selection process by presenting some of the most important approaches, and contribute into achieving consensus about the best "pieces". The following set of standards has been considered as particularly relevant: the ISO/IEC 2700x series, the IEC 62351 technical specification, the IEEE P1711 & P1689 drafts, the ANSI/ISA 99 Technical Reports and Standards series, the NERC CIP standards, the NIST SP800-53 (annex 1) & SP800-82 special publications and the CPNI Guidelines. The provided information for each of them is tailored to give an executive summary, but also allow some comparisons and relevance analysis for the reader's organization and situation. Wrapped-up with some general recommendations, the whole is intended to constitute a "survival-kit" into the fast moving landscape of cybersecurity standards for Electric Power Utilities.

KEYWORDS

Cybersecurity, computer security, information security, SCADA, Industrial Control Systems, Standards, Guidelines.

ludovic.pietre-cambacedes@edf.fr

1. INTRODUCTION: A FAST EVOLVING SITUATION

As Electric Power Utilities (EPUs) have automated their operational computing systems, cybersecurity has become a critical issue. Systems used to monitor and control the electric system as well as to manage their core business and administrative tasks, face new threats and vulnerabilities along with the performance improvement provided by their growing networked interconnections and standardization [1]. Many EPUs are aware of this evolution and are structuring their approaches accordingly. Common cybersecurity frameworks, that is to say, comprehensive approaches to manage risks adequately and create a common ground to build adapted defences and security processes, are necessary to adopt an efficient and coherent enterprise-wide response [2]. The establishment of such frameworks can be based on several existing standards, which differ in their nature (informational, regulatory, compliance-oriented, etc.), in their form (guidelines, reports…), and also in their scope (e.g., general IT, process control-oriented, electrical transmission and distribution-oriented).

Standards are a powerful mean to promote uniformity in equipment design, implementation, maintenance, and procurement. They promote interoperability of systems and minimize costs of new developments. Additionally, consensus standard bodies undergo a thorough vetting by end-users, equipment suppliers, contractors, and government organizations to assure technical validity.
The importance of the topic and the growing awareness of the industry and the decision-makers have led to an impressive number of initiatives, among which it is not easy to navigate, and identify which references or parts may be of interest. A rapid and non exhaustive inventory by the authors has listed more than forty relevant documents and initiatives. Of course, in some case, regulations may apply and lead naturally to focus on specific standards (e.g. in North America with the NERC CIP standards [3]). Nevertheless, in other regions, standards are chosen and followed on a due-diligence basis. This situation is in itself rapidly evolving. This paper is not intended to select standards on behalf of the Electric Power Industry but rather support EPUs in the selection by presenting some of the most important approaches, and contribute into achieving consensus about the best “pieces”.

2. DIFFERENT KINDS OF RELEVANT STANDARDS

In order to select the best “pieces” it is important to recognize what pieces are appropriate for which specific applications. Some standards may be relevant only for traditional IT environments, components of EPUs’ business and office systems, whereas others will be specifically relevant for industrial control systems (ICS), which manage EPUs’ industrial infrastructures. Other aspects should also be considered to characterize the different existing standards, and see how they can serve the organisation interests and security posture. Among them:

- standards may be directly aimed at operators and end-users, and leveraged by them, but may also concern in first place other types of actors like solution providers, government agencies etc.;
- standards can be national, regionally based or explicitly international. However, the equipment and/or concerns being addressed are often either similar or the same regardless of geography.
- standards can be structured for compliance testing and validation, whereas other may just be good practices collections or informative.

Cyber security standards have been originally developed for the IT community (e.g. ISO/IEC 27002 or 27001 presented later on in the paper), without the benefit of control system expertise. Consequently, these standards are not sufficient to address the unique aspects of industrial equipments and architectures (SCADA, smart meters, intelligent field devices, etc.). This has resulted in the need to extend the IT security to address the unique aspects of control systems.

Several attempts have been made to list and compare the existing cyber security standards, in particular for the ICS domain [4, 5, 6, 7, 8]. The following part proposes a short summary for a selected set of standards, ICS or IT oriented, national, regional or international, but all particularly relevant for our industry.

3. SELECTED ZOOMS[2]

3.1 International standards

ISO/IEC 2700x series

This series of standards was prepared in the frame of the ISO/IEC joint technical committee JTC 1 on Information Technologies (IT), by the Subcommittee SC 27 on IT Security techniques [9]. They cover the requirements, and establish guidelines for implementing, maintaining, and improving information security management systems (ISMS), risk management, metric and measurement in many different types of organizations (commercial enterprises, government agencies, not-for profit organizations…). As a matter of a consequence, if they have not been specifically developed for EPUs, most of their principles are relevant for our industry, in particular for traditional IT systems and on the business processes point of view. On the other side, there was no ICS community participation in the development of these standards and they do not address many of the unique issues of such systems, integral and sensitive part of the EPUs' security issues. Specific approaches proposed by other standard bodies, and presented later, should then be considered. The series will comprise seven standards of which three have been published, the others being in different draft conditions, as CD (Committee Draft) or FCD (Final Committee Draft):

- ISO/IEC 27000, "Overview and vocabulary" related to ISMS, is currently still a CD
- ISO/IEC 27001 on ISMS requirements, has been published [10]. This standard adopts the "Plan-Do-Check-Act" (PDCA) model to produce the information security outcomes meeting the organization's security requirements and expectations. As described in its abstract, it "specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the overall business risks of the organization". "The standard ensures the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties". This standard is gaining more and more importance in the process of ISMS certification.
- ISO/IEC 27002, a "Code of practice for information security management", is published [11]. Formerly ISO/IEC 17799, it has been incorporated in the new 2700x numbering scheme. It contains best practices of control objectives and controls in the main areas of information security management (policy; organization; asset management; human resources; physical and environmental security; communication operations management; access control; systems acquisition, development & maintenance; incident handling; business continuity, compliance).
- ISO/IEC 27004 "Information security management measurements", is still a CD.
- ISO/IEC 27005 on "Information security risk management" is a FCD, it should be published soon.
- ISO/IEC 27006, setting the requirements for bodies providing audit and certification of ISMS, has been published in 2007.
- ISO/IEC 27011 "Information security management for telecommunications" is presently a FCD.

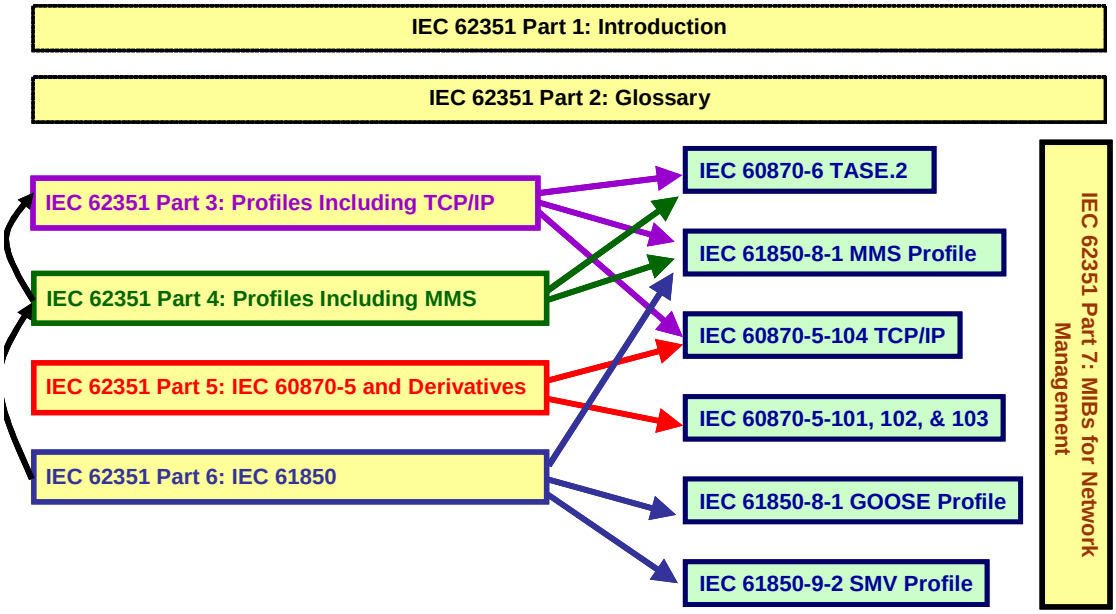
IEC 62351

Working Group 15 of Technical Committee 57 (TC57 WG15) of the International Electrotechnical Commission (IEC) was formed in 1999 to focus on the theme "Power system control and associated communications - Data and communication security." It undertakes the development of standards for end-to-end cybersecurity of the electrical system, and has in particular developed specifications to secure the communication protocols defined within TC 57. Since its creation, WG15 has specified security mechanisms for IEC 60870-6 (TASE.2/ICCP), IEC 60870-5 (and its derivative DNP), and

[2] all the status information of this section is to be taken as of the date of the article submission, i.e. mid January 2008.

IEC 61850, already published [12]. The associated security standards were designed to meet different security objectives according to the protocols, how they are used, and their environmental constraints (bandwidth, delay…). The group has also recently developed abstract Network and System Management (NSM) data objects for the power system operational environment (currently under review). The results are regrouped under a Technical Specification referenced IEC62351 [13], which is presently divided into 7 parts as presented in Figure 1.

Figure 1: Correlation between IEC 62351 Parts and TC57 Standards [12]



Future planned work includes Role-Based Access Control, Conformance and interoperability testing and Security for Access to CIM Interfaces.

3.2 Regional standards examples

IEEE P1711 & P1689

WG C4 of the Power Engineering Society Substations Committee is currently working on P1689, a "Trial Use Standard for Retrofit Cyber Security of Serial SCADA Links and IED Remote Access" [14]. This work adapts to the electric power industry work by the American Gas Association for Cryptographic Protection of SCADA Communications [15]. IEEE P1689 sets forth high level requirements to protect serial communications between SCADA master stations and RTUs (Remote Terminal Units) from cyber attack. The standard is designed to strengthen authenticated remote access to maintenance ports in RTUs and other IEDs (Intelligent Electronic Devices). Requirements are intended to retrofit existing communications equipment while minimizing the changes required to installed devices. Key management is integral to this standard. EPUs can use the requirements of this standard in a procurement specification for the retrofit of existing communications to protect against attacks without changing existing master stations, RTU or other IED software. It provides manufacturers with requirements to design and build open system cyber security modules to protect existing SCADA serial communications and dial-up communication systems from cyber attack.

The retrofit cyber protection requires SCADA cryptographic modules (SCMs) on the communication links between the master station and each remote station. The retrofit cyber protection of existing remote dial up access to the maintenance ports of IEDs (including RTUs) requires the installation of Maintenance cryptographic modules (MCMs) upstream of those maintenance ports. The cyber protection also requires a key management system for the storage and maintenance of the master cryptographic keys used to permit secure communications between the master and remote stations.

IEEE P1711 [16] is a companion standard to IEEE 1689 which sets forth the cryptographic protocol to be used to implement cyber security required by IEEE 1689 on serial links connecting SCADA systems to master stations. The standard specifies a cryptographic protocol that will protect serial communications from cyber attacks. This standard has evolved also from [15]. It can be used in procurement specifications to ensure that solution providers deliver interoperable cyber security devices to protect installed asynchronous serial communications from cyber attack.

ANSI/ISA 99 Technical Reports and Standard Series

ISA99 committee addresses control systems cyber security [17]; it has over 300 North American and international members from end-users (including electric utilities), suppliers, contractors, universities, and government organizations. This includes DCS, PLCs, SCADAs, networked electronic sensing, monitoring or diagnostic systems. ISA99 establishes standards, recommended practices, technical reports, and related information that define procedures for implementing electronically secure control systems and security practices or assessing electronic security performance.

Technical Report ANSI/ISA-TR99.00.01-2007 provides a current assessment of cyber security tools, mitigation countermeasures, and technologies that may be applied to industrial automation and control systems []. In ISA99 standard series, Part 1 has been released in late 2007; ANSI/ISA-99.00.01-2007, "Security for Industrial Automation and Control Systems: Concepts, Terminology and Models", serves as the foundation for all subsequent standards in the ISA99 series. Work underway includes:

- Part 2 standard, "Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program". The most recent committee voting was in October 2007.
- Part 4 standard, "Technical Requirements for Industrial Automation and Control System".
- a Technical Report addressing patch management for ICS. In particular, efforts are also put to identify the status of control system specific Microsoft patches, their availability, and cost.

Note that ISA99 is working with ISA100 on the cyber security of industrial wireless applications, ISA100 addressing industrial wireless instrumentation and control systems. Moreover, ISA has recently undertaken a new initiative closely related to the work of the ISA99 committee: The ISA Security Compliance Institute will identify and promote security standards-compliant products and systems in industrial control systems applications. Compliant elements will carry the "ISASecure" designation, as a recognition of the security characteristics to asset owners, integrators.

3.3 National standards examples

North American NERC CIP standards

NERC (North American Electric Reliability) Corporation is the "electric reliability organization" for North American power grid, and relies on the diverse and collective expertise of industry participants. NERC Standards CIP-002 through CIP-009 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the electric power grid. These standards are currently being reviewed by FERC (Federal Energy Regulatory Commission). Several experts have recommended that the CIP standards should undergo substantial technical modifications in scope and technical content and move in the direction of the NIST cyber security standards.

The standards recognize the differing roles of each entity in the operation of the grid, the criticality and vulnerability of the assets needed to manage grid reliability, and the risks to which they are exposed. The standards state that "responsible Entities should interpret and apply CIP-002 through CIP-009 using reasonable business judgment." However, the US Federal Government has stated that business judgment cannot be used as a reason to avoid implementing the standards. The major requirements are [3]:

- CIP-002 - Critical Cyber Asset Identification - requires the identification and documentation of the Critical Cyber Assets (CCA) associated with the Critical Assets that support the reliable operation of the grid. These Critical Assets are to be identified through the application of a risk-based assessment. No risk based assessment methodology is currently specified.
- CIP-003 - Security Management Controls - requires that Responsible Entities have minimum security management controls in place to protect CCA. This includes a formal program for categorizing critical information and a formal set of roles and responsibilities for the access, use, and handling of critical information as well as a formal testing and change control program.
- CIP-004 - Personnel & Training - requires that all personnel having authorized cyber or unescorted physical access to CCA have an appropriate level of personnel risk assessment, training, and security awareness.
- CIP-005 - Electronic Security Perimeter(s) - requires the identification and protection of the Electronic Security Perimeter(s) inside which all CCA and access points on the perimeter reside.
- CIP-006 - Physical Security of CCA - is intended to ensure the implementation of a physical security program for the protection of CCA.
- CIP-007 (Systems Security Management) requires Responsible Entities to define methods, processes and procedures for securing those systems determined to be CCA, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s).
- CIP-008 (Incident Reporting and Response Planning) ensures the identification, classification, response, and reporting of Cyber Security Incidents related CCA.
- CIP-009 (Recovery Plans for CCA) ensures that recovery plan(s) are put in place for CC and that these plans follow established business continuity and disaster recovery techniques and practices.

These standards are currently directed toward anyone who could adversely impact the transmission grid in North America, including generators, transmission companies, and large load servers. They will probably be strengthened over the next few years. Since NERC uses an ANSI Standards development process, revised standards will require 18 – 24 months. As these standards evolve over the coming years, the industry will develop methods to effectively implement them. Companies in other parts of the world could benefit from observing this process and its challenges and successes.

NIST SP 800-53 & SP800-82

The National Institute of Standards and Technology (NIST) is non-regulatory agency of the U.S. A. Department of Commerce, involved in standards development and testing done by the private sector and U.S.A. government agencies to promote innovation and industrial competitiveness.

NIST SP 800-53 security controls give the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. SP 800-53 was originally written for business IT systems. It has been extended in Revision 2 to specifically address industrial control systems such as those used in EPUs (Appendix I) [18]. NIST has performed a line-by-line mapping of SP 800-53 to the NERC CIP standards. SP 800-53 was found to be more comprehensive than the NERC CIPs [7]. NIST will be performing a similar mapping between ISA 99 Part 2 and the NIST SP 800-53 management and operational security controls. No significant difference is expected.

NIST initiated the ICS Security project [19] in cooperation with the public and private sector ICS community to develop specific guidance on the application of the security controls in NIST SP 800-53 Recommended Security Controls for Federal Information Systems to ICS. Consequently, NIST 800-82 was developed to provide specific recommendations and guidance for securing ICS. In addition, SP800-82 provides an overview of the many activities currently ongoing among US government organizations, standards organizations, industry groups, and automation system vendors to make available “best practices” in the area of ICS security.

National relevant guidelines

Considering the growing concerns regarding critical infrastructure cyber security, a growing number of national agencies and governments propose frameworks or guidelines to help operators protecting themselves against cyber attacks. In addition and in complement of the standards previously presented, many of them can in fact be helpful for any EPUs trying to enhance its security level.

For example, the British CPNI (Center for the Protection of National Infrastructures), formed from the merger of the National Infrastructure Security Co-ordination Centre (NISCC) and a part of MI5 (the UK's Security Service) has published a set of Good Practice Guidelines for Process Control and SCADA Security, through a series of very concise and readable guides [20]. They cover the following topics "Understand the Business Risk", "Implement Secure Architecture", "Firewall deployment for SCADA and process control networks", "Establish Response Capabilities", "Improve Awareness and Skills", "Manage Third Party Risk", "Engage Projects", "Establish Ongoing Governance". The US Department of Homeland Security has prepared a draft Catalog of Control System Security Requirements during 2007, which is also worth considering [8].

4. GENERAL COMMENTS AND RECOMMANDATIONS

Several attempts have been made to identify and integrate efforts on control system cyber security. For example, the US DHS has held two Control System Cyber Security International Standards Coordination Meetings – in August 2005 and August 2006. The meetings identified the gaps and inconsistencies in many of the standards [a], but did not result in reconciling the differences. As already mentioned, there have been several studies comparing standards [4, 5, 6, 7, 8].

In the US debate context, ref. [7] was a line-by-line comparison of NIST SP800-53 to the NERC CIPs. NIST SP800-53 was found to be significantly more comprehensive. In preparing congressional testimony [21], the same standards were compared to determine if either could have prevented four actual control system events. Applying the NERC CIP standards would not have prevented any of the four events, while NIST SP800-53 could have prevented the events. Additionally, the FERC issued a staff assessment of the NERC CIPs [22] that found it technically lacking and the Notice of Proposed Rulemaking [23] reiterated FERC's technical and administrative concerns. From all standards reviews to date, the NIST and ISA standards seem the most comprehensive standards to use for industrial control systems on a global requirement perspective (specifically including EPU control systems), while IEEE and IEC62351 standards deserve a particular attention for specific devices and technical implementations. ISO/IEC 2700x series are more relevant on a global organization point of view and for non-ICS considerations.

Beyond these considerations, to survive in the dense normative jungle of cybersecurity standards, here are a few general recommendations:

- A first vital step is of course to check if any relevant local and national regulations, standards or recommendations may exist in the organization environment.
- A good global view of the different kind of standards and initiatives existing in the field is also necessary, this article is intended to constitute a first basis for this
- Then, it's important to realize that none of the existing references have exactly the same scope and cover the same aspects. There is no unique, right and universal standard to rely on, but several pieces and tools to be used and integrated to build an efficient and coherent enterprise-wide security posture. In this perspective, the presented standards are all valid basis to consider.
- Selection may consider cultural tradition, sometimes bound to specific or international regional standard bodies, but also direct technical or business environment: which standards do the partners or competitors use? What are the products/solutions available compliant to a given set of standards of interest? How will they fit into the organisation?

This said, the standards presented in this paper, summarized next page in Table 1, are all sure-shots to consider.

Table 1 – Sure-shots in the cyber security standards for EPUs jungle

Designation	Nature/scope	State	Focus	Ref.
ISO/IEC 2700x	International standards	27001 & 2 published and widely used	General IT. Sound guidelines and requirements for security management	[9][10] [11]
IEC 62351	International Technical Specifications	Partly published, ongoing work	Power system data and communications protocols. Technology providers oriented.	[13] [12]
IEEE P1711 & P1689	IEEE std. (regional), but worldwide relevant	Drafts	Specifically tailored for SCADA, RTU and IED equipment.	[14] [16]
ANSI/ISA 99 Reports & Standards	US based standards with international participation - worldwide relevant	Partly published, ongoing work	ICS oriented thus relevant for EPUs'. Completing existing standards and identifying new topics such as patch management	[17]
NERC CIP standards	North America	Proposed in the US. Will evolve soon	Framework for the protection of the grid Critical Cyber Assets	[3]
NIST SP800-53 (annex 1) & SP800-82	US documents, but worldwide relevant	Available drafts	Complete framework for SCADA and ICS cybersecurity	[18] [7] [19]
CPNI Guidelines	UK guidelines, but worldwide relevant	Published	Clear and valuable good practices for Process Control and SCADA security	[20]

5. CONCLUSION

Standards are a powerful tool to ensure interoperability of systems, minimize costs of new developments or maintenance, and ensure high technical and organizational level of quality. This is particularly true when it comes to cyber security issues for Electric Power Utilities. Nevertheless, their multitude and fast evolution in this specific field can lead to a confusing situation, where EPUs may not be able to leverage and use them properly to build and maintain their security posture. In fact, several initiatives have been identified as particularly relevant, but they have to be considered holistically, rather than on an individual system basis.

6. BIBLIOGRAPHY

[1] US General Accounting Office, Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems, Report to Congress, GAO-04-354, 2004.

[2] Cigré JWG D2/B3/C2-1 Technical Brochure TB 317 on "Security for Information Systems and Intranets in Electric Power Systems", 2007.

[3] NERC CIP Standards as approved by the NERC Board of Trustees, May 2006. ftp://www.nerc.com/pub/sys/all_updl/standards/sar/Cyber_Security_Standards_Board_Approval_02May06.pdf

[4] Carlson RE, Dagle JE, Shamsuddin SA, Evans RP, A summary of control system security standards activities in the energy sector, 2005 National SCADA testbed.

[5] Evans RP, Hill RC, Rodriquez JG, A comparison of cross-sector cyber security standards. Idaho national laboratories, Idaho National Labs Report ref. INL/EXT-05-00656, 2005.

[6] Weiss, Joseph, "Approaches to International Standards Coordination for Cyber Security of Control Systems", ISA Expo 2005, Chicago, IL , October 2005.

[7] Katzke, Stuart, Stouffer, Keith, Abrams, Marshall, Norton, David, Weiss, Joseph, "Applying NIST SP 800-53 to Industrial Control Systems", ISA Expo 2006, Houston, TX, October 2006.

[8] DHS Catalog of Control System Security Requirements (DRAFT), INL/EXT-07-12332, 2007

[9] Standards and projects under the direct responsability of JTC 1/SC 27 Secretariat http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45306

[10] ISO/IEC 27001:2005, Information technology -- Security techniques -- Information security management systems -- Requirements http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

[11] ISO/IEC 27002:2005, Information technology -- Security techniques -- Information security management systems -- Code of practice for information security management http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297

[12] L. Pietre-Cambacedes, C. Chalhoub, F. Cleveland, "IEC TC57 WG15 – Cyber security standards for the power system", Proc. of CIGRE D2 Colloquium, Luzern, 2007.

[13] IEC, Power system control & associated communications - Data & communication security, 62351 part 1-6, TS, 2007.

[14] IEEE, Trial Use Std. for Retrofit Cyber Security of Serial SCADA Links and IED Remote Access, P1689 Draft, 2007.

[15] AGA Report 12, Cryptographic Protection of SCADA Communications www.aga.org/Committees/gotocommitteepages/gasctrl/AGAReport12.htm

[16] IEEE, Trial Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links, P1711 Draft, 2007.

[17] ISA99 web site, http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821

[18] NIST, Computer Security Division, Computer Security Resource Center http://csrc.nist.gov/publications/PubsSPs.html

[19] NIST ICS Security project – website: http://csrc.nist.gov/sec-cert/ics/index.html

[20] CPNI Guidelines : http://www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

[21] Weiss, Joseph, "Control Systems Cyber Security—The Need for Appropriate Regulations to Assure the Cyber Security of the Electric Grid", Testimony to the Committee on Homeland Security's Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, U.S. House of Representatives, October 17, 2007, http://homeland.house.gov/SiteDocuments/20071017164638-60716.pdf

[22] US Federal Energy Regulatory Commission Staff Preliminary Assessment of the North American Electric Reliability Corporation's Proposed Mandatory Reliability Standards for Critical Infrastructure Protection, RM06-22-000, December 11,2006, http://www.ferc.gov/industries/electric/indus-act/reliability/12-11-06-cip.pdf

[23] US Federal Energy Regulatory Commission, 18 CFR Part 39, Docket Number RM06-22-000, Mandatory Reliability Standards for Critical Infrastructure Protection, July 20, 2007, http://www.ferc.gov/whats-new/comm-meet/2007/071907/E-4.pdf

21, rue d'Artois, F-75008 PARIS
CIGRE 2008
http : //www.cigre.org

D2-213

Treatment of Information Security for Electric Power Utilities – Progress Report from Cigré WG D2.22

G. ERICSSON[1], Å. TORKILSENG[2], G. DONDOSSOLA[3], A. BARTELS[4]
[1]Swedish National Grid, [2]Salten Kraftsamband AS, [3]Cesi Ricerca SpA,
[4]Aegis Technologies, Inc.
[1]Sweden, [2]Norway, [3]Italy, [4]USA

SUMMARY

Since the beginning of this new millennium, the need for treating Information Security for Electric Power Utilities (EPUs) has become more evident among utilities, vendors, consultants, standards and regulatory bodies, etc., around the globe. Within Cigré, the first steps were taken in 2002 when the Joint Working Group (JWG) D2/B3/C2-01 – "Security for Information Systems and Intranets in Electric Power Systems" – was launched. The JWG delivered its Technical Brochure (TB) in 2006, where the purpose was to raise the awareness of information/cyber security in Electric Power Systems. Also, the "domain concept" for managing information security was introduced. The focus of the TB was mostly on the management issues, rather than on technical details. It was concluded that there is a need for a comprehensive Information and Control Systems Security Framework for electric utilities. Management of Information Security must be an essential and natural part of daily operations of various tasks in an EPU.

As a successor of the JWG D2/B3/C2-01, the WG D2.22 "Treatment of Information Security for Electric Power Utilities" was formed in 2006. Here, the scope is narrowed in order to focus on and study certain aspects and solve specific questions raised in the former JWG. The following three issues are studied: *Frameworks for EPUs*, *Risk Assessmen*t, and *Security Technologies*.

The purpose of this paper is to provide an intermediate progress report on work of WG D2.22. The WG will deliver its Technical Brochure in 2008/2009 and about five papers will be published, where this paper is one of them. So far, the results are mostly in the areas of security frameworks and risk assessment. The security technologies part will be covered more in the later parts of the WG. In the paper, it is concluded that among the various security approaches, an EPU must be competent to select and implement the best and adequate pieces and have in-depth knowledge of SCADA/Control domain requirements. The findings of a risk assessment survey show a clear lack of a reference method and it confirms the need for methodologies combining power and information security knowledge.

KEYWORDS
Electric Power Industry, Electric Power Utility, IT Security, Information Security, SCADA, Framework, Risk Assessment, Security Technology.

INTRODUCTION

Proper treatment of Information security has received increased attention within the Electric Power Utilties (EPUs) during the last five years. And this is expected to develop even more. Therefore, Cigré has initiated works within this area. The first effort was carried out by the Joint Working Group (JWG) (Security for Information Systems and Intranets in Electric Power Systems) D2/B3/C2-01, which delivered its Technical Brochure in 2006 [1]. Thereafter in 2006, the WG D2.22 "Treatment of Information Security for Electric Power Utilities" was formed.

The WG D2.22 follows the work delivered by JWG D2/B3/C2-01. The JWG covered Information and Control System Security on a broad basis using a top-down-approach. The JWG concluded that no comprehensive information security guidelines exist. The focus was mainly on the management issues, such as raising the awareness of information security and giving some guidance on security problem solving using a domain modeling concept. The key issues of risk assessment methodologies for the security analysis of electric power control systems were discussed [12]. Also, partial treatment of technical issues for control system security in substation automation was done.

In WG D2.22, the scope is narrowed compared to the JWG D2/B3/C2-01, in order to focus on and study certain aspects and solve specific questions being raised in the former JWG. The scope is to study the following three issues:

- Frameworks for EPUs on how to manage information security for all organizational units of the Electric Power Utility including power system operation.

- Risk assessment: Common models and methods for managing vulnerabilities, threats and attacks.

- Security Technologies: Effective strategies for applying appropriate security technologies to secure EPU technical infrastructures.

By having this focus, the WG strives towards a common understanding and terminology for handling of information and control system security for Electric Power Utilities.

8.2 Purpose

The purpose of this paper is to intermediately report on the progress from the Cigré WG D2.22 "Treatment of Information Security for Electric Power Utilities". The WG was formed in 2006 and it has a duration of three years. Hence, it is expected to deliver results by 2009.

Frameworks for Eletric POwer utilities on how to manage information security

Management of Information Security must be done in an ordered way, within a framework. This approach is prevailing within the more administrative IT oriented arenas, and it is natural to introduce a framework approach also here, for EPUs.

This task has two purposes. The first is to find information security approaches for an EPU on how information security should be managed. In order to not re-invent the wheel, a number of existing approaches from the area of Information Security Management are elaborated on. In this context we try to make an updated list of standards, best practices and guidelines, do some comparisons and give some recommendations for EPUs to make the rights choices [2].

There has been a discussion within WGD2.22 about the process of selecting the "right" standards in general. The conclusion is that WGD2.22 should not have the intention to select standards on behalf of the Electric Power Industry but rather support the EPU's in the selec-

tion process by analyzing some of the most important approaches and try to achieve consensus of the best "pieces".
The second purpose of this task is to provide some practical guidance to the EPU on how to adapt and implement a framework in its own environment. Two main questions are raised: 1) How could the security framework be aligned with other kind of frameworks like frameworks for IT Governance or IT Service Management? 2) How could "top down or enterprise" security framework be adapted to meet the specific security requirements for SCADA/Control system domains?

8.3 Alignment to other type of frameworks

It is important to be aware that there might be other kinds of frameworks that the EPU's information security framework has to be aligned to. Even if the EPU has not implemented those frameworks, it should be aware of its own work processes that have to align with the security management process.

First, on the top level an EPU could be using frameworks to face the overall corporate EPU risk problem related to market-, financial and operational risks (including IT/ICS risks). COSO ERP [3] is an example of such a framework. Frameworks for IT Governance like COBIT [4] could be used to define IT-processes to fulfil requirements for core business information like Quality requirements (Effectiveness, and Efficiency), Security requirements (Confidentiality, Integrity and Availability) and Fiduciary requirements (Compliance and Reliability).

Second, the EPU could be using frameworks for IT service management describing in detail the IT processes necessary to deliver high quality IT services that support business processes. ISO/IEC 20000 [5], [6] that is based on ITIL[7] describes a specification and code of practice of an integrated approach that demonstrate the fact that a security management framework cannot be implemented in a separated vacuum. Security Management must to be aligned and interfaced with many other processes to obtain a successfully execution of security policies and procedures. Fig. 1 shows this layered framework architecture that affects information security.

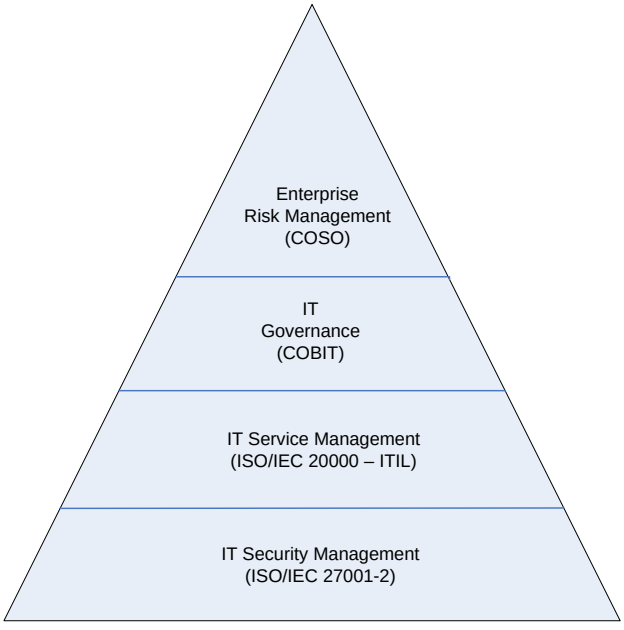


Fig. 1 Layered frameworks that affect information security

2.2 Enterprise security frameworks and SCADA/Control system domains

An EPU could use ISO 27001 [8] and ISO 27002 [9] or NIST SP 800-53 [10] to build a corporate enterprise framework including the SCADA/Control domain. However, "bottom up"

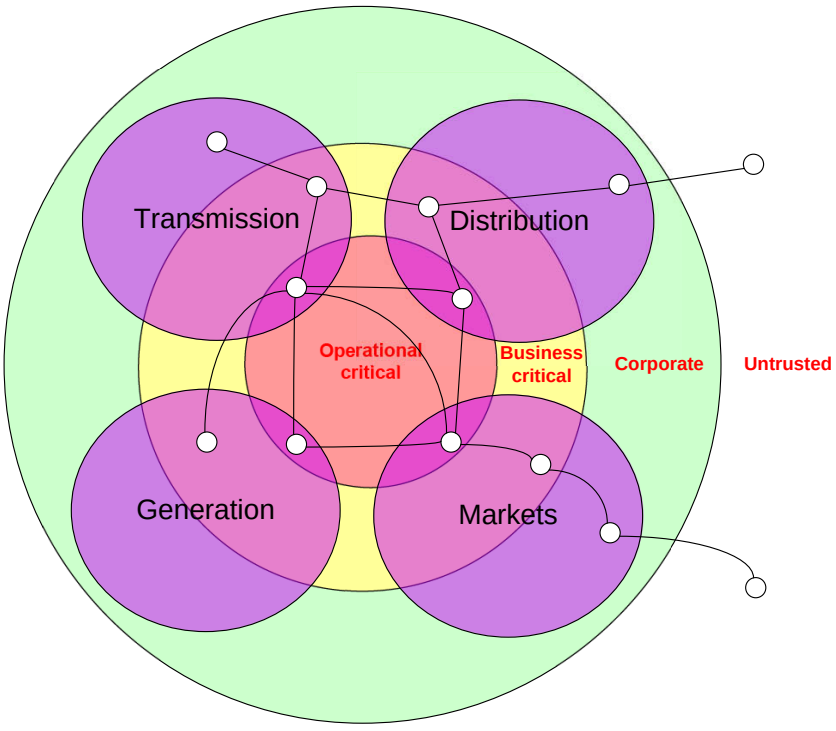
frameworks, which include the unique requirements for power system operations like NERC CIP [11], are being developed.
Depending on the choices made for standards, best practices and guidelines the roadmap for establishing a security framework will be different from one EPU to another. However a security framework could be established by adopting some basic tools, such as security domains, risk assessment methodologies (See Section 3), security program loops, and baseline controls. It could be implemented by involving IT service management staff in an integrated environment (See Section 2.1) and by using appropriate technology (See Section 4). A challenge is to make a coherent concept that includes the specific requirements for the SCADA/Control system domains. To achieve this, the WGD2.22 is discussing the different tools with the view not to repeat the material written for and used in the corporate administrative domains, but look for differences, interpretations and enhancements for the SCADA/Control system domains.

2.2.1 Information Security Domain Model

Different domain models have been discussed. One model would be to use different levels for different degrees of criticality:

Level 1: Untrusted zones (the "white" zone), e.g., vendor / 3rd party networks, internet
Level 2: Corporate zone (the "green" zone), e.g., office level business network
Level 3: Business critical zone (the "amber" zone), e.g., finance, human resource systems
Level 4: Operational critical zone (the "red" zone), e.g., controls systems, SCADA networks

Fig. 2 shows this model for different types of EPUs including examples of interconnections.



It is important to note that these domains are abstract security zones, which contain elements of logical zones; as the actual physical security perimeters for these zones can be quite complex to define. For example, for a single organisation if the control centres, substations, and the SCADA data communications are all considered to be at Level 4, then all these separate physical systems, their locations, and the data networks between them will be within a single "red" zone.

The model could be used as a tool for making security analysis, the definition of security controls as well as building an appropriate technological architecture.

2.2.2 Baseline Controls

An EPU needs to define its own selection of adequate security controls for its information systems and SCADA control systems. As starting points or foundations in this definition process, the EPU could use security control baselines taken from sources like ISO 27002 [9], NIST SP 800-53[10] or NERC CIP [11] or others. The final determination of the appropriate set of security controls necessary to provide adequate security is a function of the EPU's assessment of risks.

The security controls need to be defined within each domain as does control of information between the zones, based on level of risk and agreed with the key stakeholders. For example, the Corporate zone and Business critical zone controls will depend on an intra-business risk assessment, whereas Operational critical zone controls are likely to require interdependent risk assessments between other operators and possibly Government agencies.

The controls listed in existing standards that apply to corporate IT systems (i.e., those found in Levels 1, 2, and 3) will not be repeated, but focus will be on the enhanced controls appropriate for EPU control systems (Level 4).

Risk Assessment

During the efforts of the JWG [1], one method referred to the Electric Power Cyber Security Assessment (EPCSA) methodology was presented. It supports the security evaluation of power utility information systems, as complex interacting infrastructures involving process knowledge, advanced control and information and communication technologies.
Building up on the background knowledge of the previous JWG, the aim of the work to be conducted under Risk Assessment (RA) within the current D2.22 is to i) find out what the utilities really are doing today, ii) to suggest improvements to the currently practised matrix-based risk assessment methods, and iii) to foster the development and adoption of common advanced methods usable in the EPU practice.
The WG has proposed that we shall follow a "best practice track" rather than a "research track". It has been decided to approach the Risk Assessment issues by starting to survey the status of the practices of the WG members with the aim of setting up an initial, shared view of the state-of-practices. The presented overview on Risk Assessment practices is a first step towards the final WG objective of developing practical recommendations addressed to both chiefs of EPU Security Programs and managers of Control Centers.

3.1 Summary of the contributions under analysis

The survey is based on the contributions provided by a representative sample of ten WG members composed by well-recognised power system operators and engineering service providers at international level.

The results are depicted in Fig. 3, which shows that 30% of the contributors are using no method and 70% are using some method when doing Risk Assessment, 50% use qualitative practices and only 20% make use of some tool support (an IT Risk Assessment tool and a beta (test) application).

The descriptions of practices were very heterogeneous and referred to different-level RA methods, covering an electricity sector-specific method, some Information Security Management System (ISMS)-level methods, a scenario-based method and a graphical methodology for IT security analysis based on standard Unified Modeling Language (UML) profiling.

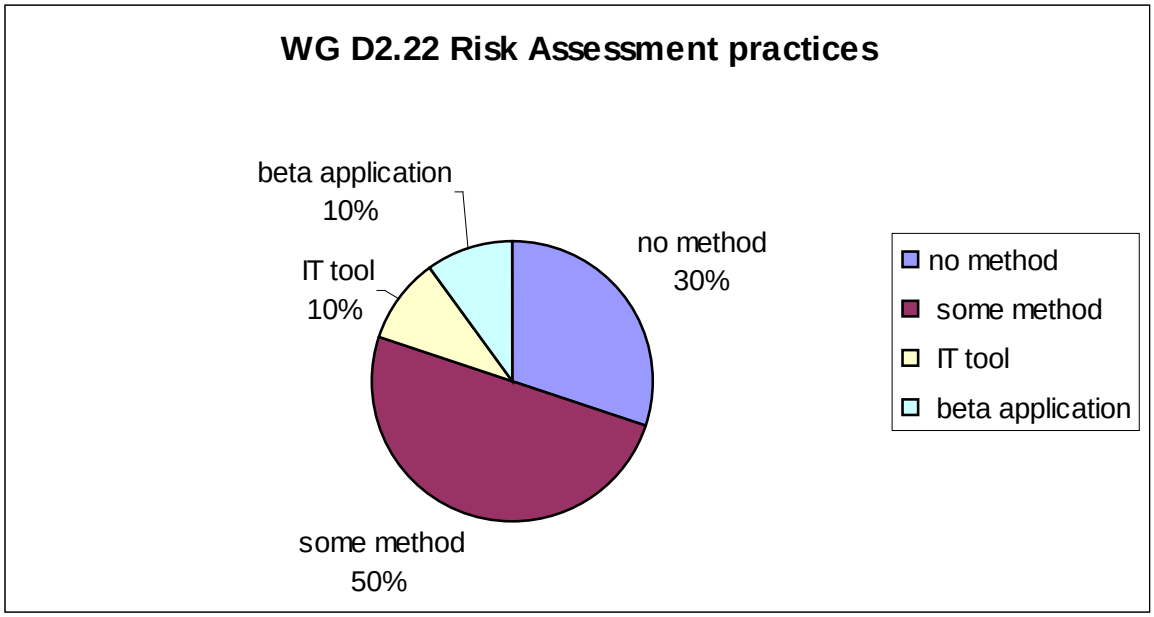


Fig. 3 Risk Assessment practices from the WG members

By considering the heterogeneous content of the contributions, the identification of the common criteria and items to be used in conducting a full comparative analysis was non-trivial. However, a few considerations related to the frameworks issues and by the evaluation of some common and distinguishing factors from the whole set of the analysed contributions are described herein.

The availability of a reference electricity-specific methodology, supporting the Risk Assessment activity and widely accepted by most EPUs, is highly desirable. This methodology should cover Information and Communication Technology (ICT) risks on major services in electricity production, transmission and distribution, with focus on cross-company and cross-sector risks. Possibly the scope may also include risks associated with energy trading as well as environmental risks (like storms, natural disaster and acts of war). A treatable set of critical scenarios should be analysed and mapped onto a risk matrix, combining risks from ICT failures with standard power failures.

3.2 Alignment with the framework issues

The risk assessment activity within an EPU should be performed in the context of the enterprise security framework. With specific reference to ICT risk analysis, it should be part of the IT Security Management framework depicted in the bottom part of the Fig. 1. Currently security management activities for control systems and for the IT systems are separately managed, with some relationships established between corresponding teams.

Depending on the specific case, the security management process may have reached different level of maturity both in IT and control systems, being developed on an empirical base or with the graceful introduction of a well structured methodology like ISO/IEC 27001-2 [8], [9]. In a singular case control and teleoperation applications are being subjected to an experimental activity consisting in the application of a risk assessment methodology, originated in the IT domain and compliant with the ISO/IEC 27001-2 standard, to the control system domain. Results from this experience are not encouraging: the lack of tool flexibility for the SCADA context and the high complexity in mapping the information assets required to perform some simplification in order to make the method applicable to the typical information assets and flows of SCADA architectures.

According to the currently applied methods, a risk assessment session should start whenever a major change to some business; information system or threat and vulnerability hypothesis is contemplated.

Depending on the risk rating resulting from the evaluation, the current set of applied controls may be reviewed and new appropriate controls may be submitted to the management approval for implementation.

3.3 Common and distinguishing factors

Only a few commonalities – but a lot of differences – were found among the WG members' practices. In three out six practices, the following commonalities have been found:

- Assets, threats and vulnerabilities are well known dimensions;
- The threat assessment is conducted before the vulnerability analysis;
- Deliberate as well as accidental types of threats are taken into account;
- The level of threat is judged without considering the controls already in place to counter the threats;
- The level of vulnerability is judged considering the controls in place to counter the threat.

Concerning the differences, the comparison put in evidence that the frameworks adopted by the considered practises differ in terminology, concepts and scales. For instance:

- Different concepts, such as weaknesses, impacts, or consequences, are used to evaluate the failure effect in the risk measure;
- Different types of threats are considered;
- From 3 to 5 levels are used for the evaluation of both threats and vulnerabilities;
- From 3 to 11 levels are used for the impact evaluation.

The findings demonstrate the lack of a reference method and confirm the need of risk assessment methodologies integrating both power and ICT security knowledge.

Security Technologies

The third part of the WG D2.22 to tackle is to deal with "security technologies." As such, it is a vast area, and of course the EPUs are "technology users" and not a "technology inventors" in this case. Hence, the EPUs would gain considerably by having support when choosing among the different technical solutions.

Therefore, the purpose of this task of the WG D2.22 is to provide a practical guide and make possible assessment of current available appropriate security technologies, with the focus on the Transmission, Distribution, Generation and Commercial Market domains. The aim of the WG is to identify most common EPU architectures, and thereby identify leads to security technology recommendations that apply directly to EPU networks.

The WG D2.22 has found three interesting works that aim to provide practices and guidance for utilities, when security technologies are to be chosen:

- The CPNI (Centre for the Protection of National Infrastructure) Good Practices which include "NISCC (National Infrastructure Security Coordination Centre) – Good Practice Guide, Process Control and SCADA Security" [14]. Here, seven separate guides are given together with a firewall deployment guide for SCADA.
- NIST (National Institute of Standards and Technology) SP 800-82 Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security- Last public draft released September 2007 [15].
- The DHS "Catalog of Control System Security Requirements (Draft)" [16], which is "a compilation of practices that various industry bodies have recommended to increase the security of control systems from both physical and cyber attacks".

It was also suggested that, when authoring the Frameworks issues and the Technologies issues, the same security domain model should be referred to. The part on Frameworks issues should in this context concentrate on the management part (security program) elements required to protect the Domain Model domains. And the part on Technologies issues should concentrate on the technical elements required to protect the same domains, i.e., the selection of technology and how to build network architecture and technical solutions.

Concluding remarks

The WG D2.22, succeeding the former JWG D2/B3/C2-01, on Information Security for Electric Power Utilities, was created in 2006 and will deliver its Technical Brochure during 2008/2009. Also in between, about five papers will be authored, where this paper is one. The WG D2.22 focuses on three parts: Frameworks for EPUs on how to manage information security; Risk assessment; and Security Technologies.

Based on the work carried out so far in the WG, the following can be concluded:

- For Frameworks: The EPUs should be aware that various security approaches exist and are being developed. An EPU must be competent to select and implement the "best pieces". The implementation requires knowledge of and alignment to other frameworks that might be used within the EPU and that are affecting information security. In-depth knowledge of SCADA/Control domain requirements is a must. Here, an Electra paper on this issue is planned for May 2008.
- For Risk Assessment: A survey based on the contributions provided by a representative sample of ten WG members composed by well-recognised power system operators and engineering service providers at international level is carried out. Only a few commonalities, but several differences, were found among the WG members` practices. The findings demonstrate the lack of a reference method and confirmed the need of methodologies integrating both power and ICT security knowledge. Here, a paper is submitted for Electra in February 2008 [13].
- For Security Technologies: Sources of information that deal with Security Technologies necessary to fulfil the specific SCADA/Control system requirements are found. A common Information Security Domain Model will be used to demonstrate a technical implementation. Here, a paper will be submitted to Electra for September 2008.

BIBLIOGRAPHY

[20] Cigré JWG D2/B3/C2-1 Technical Brochure TB 317 on "Security for Information Systems and Intranets in Electric Power Systems", 2007

[21] L. Pietre-Cambacedes, T. Kropp, J. Weiss, R Pellizzonni, "Cybersecurity standards for the electric power industry – a survival kit" – D2-217 , Cigre Paris Session 2008

[22] COSO ERM (The Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management), 2004. URL: www.coso.org

[23] COBIT (Control Objectives for Information and related Technology). URL: www.isaca.org

[24] ISO/IEC 20000-1:2005 Information Technology – Service management – Part 1: Specification

[25] ISO/IEC 20000-2:2005 Information Technology – Service management – Part 2: Code of practice

[26] ITIL (IT Infrastructure Library). URL: www.itil-officialsite.com/home/home.asp

[27] ISO/IEC 27001:2005, Information Technology - Security techniques - Specification for an Information Security Management System

[28] ISO/IEC 27002:2005, Information Technology - Code of practice for Information Security Management

[29] NIST (National Institute of Standards and Technology) Special Publication 800-53 – Recommended Security Controls for Federal Information Systems. URL: www.nist.gov

[30] NERC CIP (North American Electric Reliability Corporation – Critical Infrastructure Protection). URL: www.nerc.com
[31] Dondossola G., Lamquet O., Torkilseng A., "Key issues and related methodologies in the security risk analysis and evaluation of electric power control systems", Cigré Session 2006, Paris 27 August – 1 September 2006.
[32] Dondossola G., "Risk Assessment of Information and Communication Systems - Analysis of some practices and methods in the Electric Power Industry", to be submitted to Electra.
[33] CPNI (Centre for the Protection of National Infrastructure) Guidelines. URL: www.cpni.gov.uk/
[34] NIST (National Institute of Standards and Technology) Special Publication 800-82 – Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security. URL: www.nist.gov
[35] Catalog of Control System Security Requirements (DRAFT), DHS INL/EXT-07-12332, 2007