EUROPEAN NETWORK FOR THE
SECURITY OF CONTROL AND REAL TIME SYSTEMS

R&D and standardization Road Map, final
Deliverable 3.2

ESCoRTS Consortium
www.escortsproject.eu

The research leading to these results has received funding from the European Community's Seventh Framework Programme, under Grant agreement n°.218217

Contact: Luc Van den Berghe, lvandenberghe@cencenelec.eu

Security and space research

Contents

1. Introduction – background – objectives

ESCoRTS roots are in earlier work of the JRC, which was among others reported to the CEN Technical Board Working Group 161 on Safety and Security of the Citizen, and which led to the following observations:

- Compared to the US, there is less awareness in Europe about cyber security risks and a lack of expertise among technicians in the process control sector.
- Several standardisation efforts exist in Technical Committees of the International Electro-technical Commission (IEC), more particularly in TC 57 and TC65, but standardisation proceeds at a slow pace.
- There exists also an US approach based of producing sector guidelines which is pragmatic and productive.

The observation that Europe lags behind the US in awareness of cyber security risks was also confirmed by the ESCoRTS deliverable "Survey of the stakeholder needs" as part of its work package 1.

The ESCoRTS deliverable "Review of current standardization efforts" under work package 2 confirmed the broad variety of standards and guidelines, at national, regional and international level. The standardization efforts reviewed in this work package did not restrict to formal standards as issued by the European Standards Organizations (such as CENELEC) or their international counterparts (such as IEC).

This is also the approach in this deliverable on a standardization roadmap, where the recommendations for further work include also the production of guidelines, often complementing existing standards, in addition to suggestions for formal standards themselves.

In a number of cases, this roadmap makes detailed suggestions for the follow-up steps (including the acquisition of funding), but in other cases only requirements are identified without detailing the follow-up steps to address these requirements.

In relation to the possibilities for acquiring funding in support of the follow-up steps, the "2010-2013 ICT Standardisation Work Programme ", a rolling work plan with European Commission priorities for standardization actions, is an important opportunity in support of the follow-up of the ESCoRTS recommendations. More information on this 2010-2013 ICT Standardisation Work Programme is in Annex 1.

2. Issues identified in earlier ESCoRTS deliverables

2.1 Deliverable D11

Deliverable D11 contains a survey of stakeholder needs in SCADA security. D11 provides an overview of the current stakeholders' practices regarding the security of control systems, and a summary of their opinions on related industrial needs and requirements. Responses were collected via replies to a questionnaire and targeted interviews.

Deliverable D11 suggests that one of the key factors for EU industry awareness and readiness lagging behind the US one seems to be the lack of European explicit demand for security attributes, which hinders the offer. Two related issues emerge as decisive:

1.) the potential cost of security measures, which might weigh considerably on the overall control equipment cost, and
2.) the lack of adoption in Europe of common security references or baselines (be them formal or de facto standards, guidelines, or accepted best practices accepted and applicable across all countries). The adoption of security measures by the single company might affect its competitive position, without any immediate apparent benefit.

A study that compares the economic cost of critical infrastructure failure and the costs of security measures could increase industry awareness that money spent on security measures is well spent. The ABB/ENEL targeted experiment which was conducted under the ESCoRTS Work Package 2 made it clear that the costs for ENEL becoming ISA99 compliant could not be estimated and that such could be part of a future project.

2.2 Deliverable D12

Deliverable D12 contains an evaluation of the market for SCADA security services. Most input to that evaluation was collected in a workshop with stakeholders held in May 2009.

D12 concentrates on three important aspects of security related services:

- Security assessments help to find deficiencies with respect to the security organization of an operator and with respect to the implementation of technical security measures.
- Security testing which can be regarded as (technical) part of a security assessment (for a infrastructure operator), but it is also relevant for the vendors of control system components or systems.
- Security training and awareness can be seen as an important part of the security assessment with respect to organizational aspects and is the precondition that the implemented technical security measures will have the intended effects. Adequate training is the most important factor to discriminate a security induced event from an everyday operational fault.

D12 confirmed the need for common security references or baselines. Missing commonly accepted guidelines or standards for security testing and/or security assessments currently hinder the providing of such security services. The question "How can the security level of a system be measured?" suggests a common accepted understanding of "What is the metric and what are key indicators? This could be addressed by producing a widely accepted

guideline, produced in a standardization process, based on Deliverable D42 "Security metrics for cyber security assessment and testing".

Any security assessment process has to include a risk assessment process. There is no "official" methodology to conduct a risk assessment (RA). Each RA must be adapted to the specific technical architecture, business nature, and the system operator's objectives, available time and budget. The lack of "best practices" in RA could lead to confusion and inconsistency in the quality of the service. This again could be addressed by producing widely accepted best-practices on RA, produced in a standardization process.

2.3 Deliverable D22

Deliverable D22 "Security solutions taxonomy" lists and classifies security vulnerabilities, threats and solutions. The provision of best practices or possible options to address the vulnerabilities are outside of the project's scope and available resources, and do require therefore further work.

Further work on a control systems security taxonomy is planned to take place during the second half of 2010 and the first half of 2011 under a US DoE contract which will involve the US Sandia National Laboratories (SNL) and the European Commission's Joint Reserach Centre.

The Security solutions taxonomy deliverable identified among others the need for new standards defining robust and secure industrial protocols. While different work is being undertaken in international organizations such as IEC, there is space for many other initiatives, as networking is at the core of control systems. An example of such initiative is a secure version of the Modbus protocol.

2.4 Deliverable D41

Deliverable D41 "Develop and deploy a secure ICT platform for the exchange of relevant data among the stakeholders" describes a prototype of an Information Exchange platform for the secure sharing of information of security-relevant data among stakeholders.such as the critical infrastructure operators and the vendors and integrators of SCADA and security technologies. Such information exchange platform aims to complement the national/European information exchanges between national authorities and agencies.

D41 discussed from the communication and technical point of view, the basic elements that should be taken into account in the implementation of an information exchange platform on the security of industrial control systems. An impediment to information sharing are incompatible terminologies and technologies (such as formats) used for the description and storing of data. Each industrial actor, or at times sector, uses their own approach, and at times standard. Much can be gained from common, standardised approaches for the specification of security-related information (not unique, but at least compatible), including taxonomies, protocols for handling contents and for other tasks (e.g. validation). An agreement of the stakeholders on the exchange of security-related information, in particular which information and in which format, seems a condition to enable information sharing.

3. Recommendations following earlier ESCoRTS deliverables

Following the closure of the ESCoRTS project, detailed project proposals will have to be drafted, including information from this report. Proposals for standardization deliverables (3.2 to 3.5) are suggested to be funded under the ICT 2010 Standardization work programme.

3.1 Which standardization deliverables?

CEN and CENELEC have a range of solutions for delivering standards and related information in a timely manner. This includes 'full' standards (ENs), voted upon by national members of CEN and CENELEC, and other publications, such as Technical Reports or Technical Specifications and CEN and CENELEC Workshop Agreements.

The development of European Standards (ENs), Technical Reports and Technical Specifications takes place in Technical Committees where participants represent their National Standards Body. The Vienna Agreement between ISO and CEN, and the Dresden Agreement between IEC and CENELEC makes it possible to develop and vote in parallel the International and European Standard. There is a preference in general by industry for standards that are internationally applicable. In the case of CENELEC for instance, only 24% of the CENELEC Standards are "homegrown" while 61% are identical to an IEC standard and 15%s are based on an IEC standard. (Source: CENELEC Annual Report 2009°).

CEN or CENELEC Workshop Agreements (CWAs) are developed in groups (called Workshops) where there is direct participation of the stakeholders. A more detailed description of these Workshops is in Annex 2.

3.2 CWA on metrics

A key issue being considered by current efforts to establish generic and SCADA specific security standards is compliance metrics. Compliance metrics would allow to measure the increase of security, and might lead to a cost-neutral approach to implementation of those standards. In light of the interlinks Profit-Revenue-Cost, to avoid depreciating Profit, either Revenue must be increased to cover the Cost of adding security or, savings in other cost items (e.g., liability insurance) must be realized. Either approach will result in a security cost offset which means that security deployment is cost neutral. This will facilitate the take up of security-related standards by industry, and therefore contribute to the growth of the security of industrial systems. On the other hand, appropriate security metrics can contribute to level the security baseline, avoiding the risk of security resulting in unfair market advantages or moral hazard. A CWA on the subject might leverage on the work of the Standards and Practices Committee ISA SP 99 and of the IEC Technical Committee TC 65 which are developing the ANSI/ISA 99 and IEC 62443, respectively.

3.3 CWA: Security Processes Best Practices

A CWA to outline best practices for security processes (organization and management, products and services, and commission and maintenance) is needed for guiding and facilitating the adoption of standards by industry. One reference methodology is Carnegie Mellon University's System Security Engineering Capability Maturity Model, which provides an excellent framework to establish Base Practices and Generic Practices. Other security engineering models should also be considered. Using a tailored framework, requirements for Base Practices and Generic Practices will be defined. Base Practices will define requirements for practices that collectively define security engineering. Generic Practices will define the requirements that indicate the increased level of maturity for process management and institutionalization capability. In response to these security process requirements, Evidence Requirements will be defined to determine if the Base Practices and Generic Practices have been met and adequately documented.

3.4 CWA for definition of skills and competences for people to plan and operate a security programme

Emerging threats to critical infrastructures security are having vast impacts on stakeholders, and demand appropriate approaches for the management of the associated societal risks and the related education and training processes. Companies will have to adapt their internal handling of threats related to security of ICT systems, taken into consideration the potential implications of security failures on the society. Summarising, a general culture of security, including the necessary skills and competences for dealing with all aspects of security, will have to permeate the human, organisational and societal dimension of the power infrastructure, embracing the physical and ICT aspects of the systems. In the short term, there is a strong need to increase awareness of control and ICT vulnerabilities among policy and business circles, technical actors and the public at large. A basic and widespread education on security is lacking, and it is appraised that companies would benefit from clear references. Future developments should focus on the creation of educational tools and structures. These structures should support curricular activities in universities and professional training of current staff.

3.5 CWA outlining an agreement of the stakeholders on how to exchange security-related information, in particular which information and in which format, seems a condition to enable information sharing

There is a need to exchange information relevant to potential threats and vulnerabilities, and to report on actual incidents caused by cyber security attacks. A CWA in these subjects may leverage on several ongoing endeavours, like E–SCSIE, the European SCADA and Control Systems Information Exchange, a working group formed on June 2005 from European industry, government and research, in order to benefit from the ability to collaborate on a range of common issues, and to focus efforts and share resources where appropriate. This initiative has developed model agreements and appropriate forms for cyber security

information exchange. The CWA will have to propose approaches for both physical (face-to-face) and electronic exchanges, in multi-institutional, multi-national environments.

3.6 A Research Project identifying and analysing in a practical experience (technical) 'Key security Indicators' for the monitoring of security level and behaviour

After the first phase of identification of the Security Criteria for the design and implementation of a "secure" control system and infrastructure, it would be important to define some relevant key indicators for the complete life cycle of the system itself.

These key indicators will have to allow the monitoring of the security level of the complete system, in particular after a maintenance or upgrading activity but also during normal operation, taking into account also the threats/vulnerabilities evolution. The objective of such a project will be to identify some Key Performance Indicators (KPI), as usually made for process or production monitoring, applied to security concern (Key Security Indicators).

This project should be constituted by three different phases:

- The first one is based on the state of the art analysis of the current standards or guidelines regarding risk assessment and the definition of some indicators and evaluation criteria that will be used to periodically monitor the effectiveness and the performance of implemented information security controls.
- The second phase is the identification of an industry specific risk model in order to identify the "best" Key Security Indicators, producing a guideline for their evaluation and application.
- The third phase is the practical application of this Indicators through a set of experiments reproduced in a laboratory, in order to validate the method and the result.

3.7 Proposals for accompanying measures

Study on economic cost of security measures and infrastructure failure

Networked computers reside at the heart of critical infrastructures and systems on which people rely, such as the power grid, the oil & gas infrastructure and power, oil and chemical process plants. Today, many of these systems are vulnerable to cyber attacks that can inhibit their operation, corrupt valuable data, or expose private information. Exposure to malicious threats is massively growing, and intelligence sources estimate today a disruptive attack more likely to target Europe than the US. As extensively discussed in chapter 4, an overall approach to ensuring security of the North American bulk power system, known as the NERC CIP standards 002 to 009, was established over 2003-07 and is now coming to mandatory application. However, earlier trials of those standards have shown that they appear defective because their terminology still is to some extent unclear, and they lack a

precise compliance metrics. This makes difficult to estimate the costs related to their adoption, which appear anyway considerably high. All horizon approaches to control system security standardisation, like the ISA S 99, are expected to be completed by year 2012, so that it is still unclear whether they will solve the issues that currently hamper adoption of earlier frameworks such as the NERC standards. In these conditions, there is a need for establishing the economic and organisational impact of the implementation of such emerging cyber security frameworks in Europe, i.e., to identify costs and benefits for industrial stakeholders on an objective basis and outline organisational processes wherever beneficial. Especially concerning the European power system, this is a pre-condition to adoption of emerging control system security approaches to EU critical infrastructures as defined by the Directive 2008/114/EC of 8 December 2008.

Study on a decision support system to CEOs

CEOs take their decision on the basis of a cost-benefit analysis, with the objective to minimize costs and to maximize revenues. If they perceive security only as a cost instead as an investment, they will be led to underestimate the consequences of security failures.

Although many individuals may be risk averse, decision-making bodies, such as governments and law enforcement practitioners, need to distribute risk reduction factors in a consistent and equitable manner to achieve the best outcomes and maximise risk reduction. While risks are hardly ever acceptable, they are often tolerable if the benefits are seen to outweigh the costs. Many risks can be reduced but sometimes at increasing cost.

A cost-benefit analysis provides a means to measure the cost associated with avoiding the risk, to determine whether such a cost is justifiable or excessive thereby maximising societal and/or organisational resources.

From a security response perspective, different situations will require different responses. The development of effective security solution responses, particularly those involving technology, equipment and security systems, will most often require the following to be considered:

- At the strategic level: What is the need and justification for the procurement of technology, equipment and security systems?
- At the tactical/technical level: What is the required capacity, specification and scope of the technology, equipment and security systems?
- At the operational level: How in deployment terms can the return on investment be maximised?

The hypothesis is that if applied within each of the foregoing decision making levels, Cost Benefit Analysis Models can assist in the maximisation of return on investment.

The main aims of this proposed study are to develop robust security governance Cost Benefit Analysis Models (CBAM) for policy makers and practitioners at strategic, tactical/technical and operational levels to facilitate and optimize the decision making process on security related matters at each of the three levels of policing.

- To establish robust CBAM to be applied in strategic decision making considerations to procure or not procure technology, equipment and security systems.

- To establish robust CBAM to be applied in tactical/technical decision making processes around the capacity, specification and scope of the technology, equipment and security systems to be procured.

- To establish robust CBAM to be applied in the operational decision making considerations to most effectively deploy technology, equipment and security systems and maximize the return on the investment.

Through the following work-plan, cross-border practices will be considered and different security scenarios compared, including those involving private business elements and public national policies.

The goal will be to produce a range of sensible and pragmatic Cost Benefit Analysis tools to optimize public expenditure on security, adoptable CEOs of Companies at EU level.

The end users will consequently be in a position to define common security standards, priorities and policies to be implemented at national and European levels.

Develop a testing methodology and a testbed for verifying the security assurance of SCADA protocols

The project will concern the specification of an experimental approach for testing the security attributes of SCADA protocols. These tests should conform to the requirements of different standards, or to accepted security policies. The project shall also develop the tools necessary for conducting the tests, including the testing platform and the instruments. Testing has to be conducted in safe settings, and the project will define the characteristics for the fidelity and precision of the tests:

- Results should be reproducible
- The testbed should be usable for newly proposed protocols, and for new architectures using the protocols
- The testing methodology should be integrated with appropriate security metrics, for indicating the satisfaction of the assurance objectives

Different testing strategies will be defined, with the relative tools: tests of functional characteristics, tests of corrective actions, tests of mitigation activities, tests for identifying vulnerabilities, tests for benchmarking alternative implementations/solutions, tests for tracing the meeting of security requirements, tests for validating security requirements, tests related to cost/benefit analysis, and tests related to certification.

Training: development of training material for awareness raising for operators, field technicians, etc. who have access to the control system

See also CWA in section 3.4

A control system will be well protected against accidents or malicious actions only if all the relevant people are aware of the problem and of the consequences that their behavior could have not only on the infrastructure but also on the people and/or other utilities served by the system.
This proposed project aims at defining tools able to assess the current status and to identify and classify the system vulnerabilities, that, if exploited, could lead to major consequences. For each category of vulnerability, proper training material will be developed, based on solutions provided by national and international standards as well as best practices and countermeasures successfully adopted in similar contexts. A relevant part of the training process will be devoted to the application of security measures on real cases.
The final goal of this project is to provide people having access to a control system the necessary skills and competences to properly carry on the work activities without risking accidents or security leaks that could lead to severe consequences for the company managing the system and all who use the services provided by the system itself.
Specific materials to raise awareness of high-ranking senior managers will be developed, in order to stimulate discussion about security governance mechanisms.

4. Detailed assessment of key relevant standards and guidelines

4.1 Introduction

In deliverable 2.1 “Survey of Existing Methods, Procedures and Guidelines“ standardization activities with respect to cyber security aspects in control systems have been evaluated. A main result was that from high level point of view there exist a lot of “competing” standards and regulations. On the other side these standards and regulations are addressing different branches and often different security relevant aspects.

A first (graphical) impression of the overlaps and gaps is depicted in the following figure. Details of the standards’ content as well as a reasoning of the selection of standards is described in section *4.2 Selected Standards.*

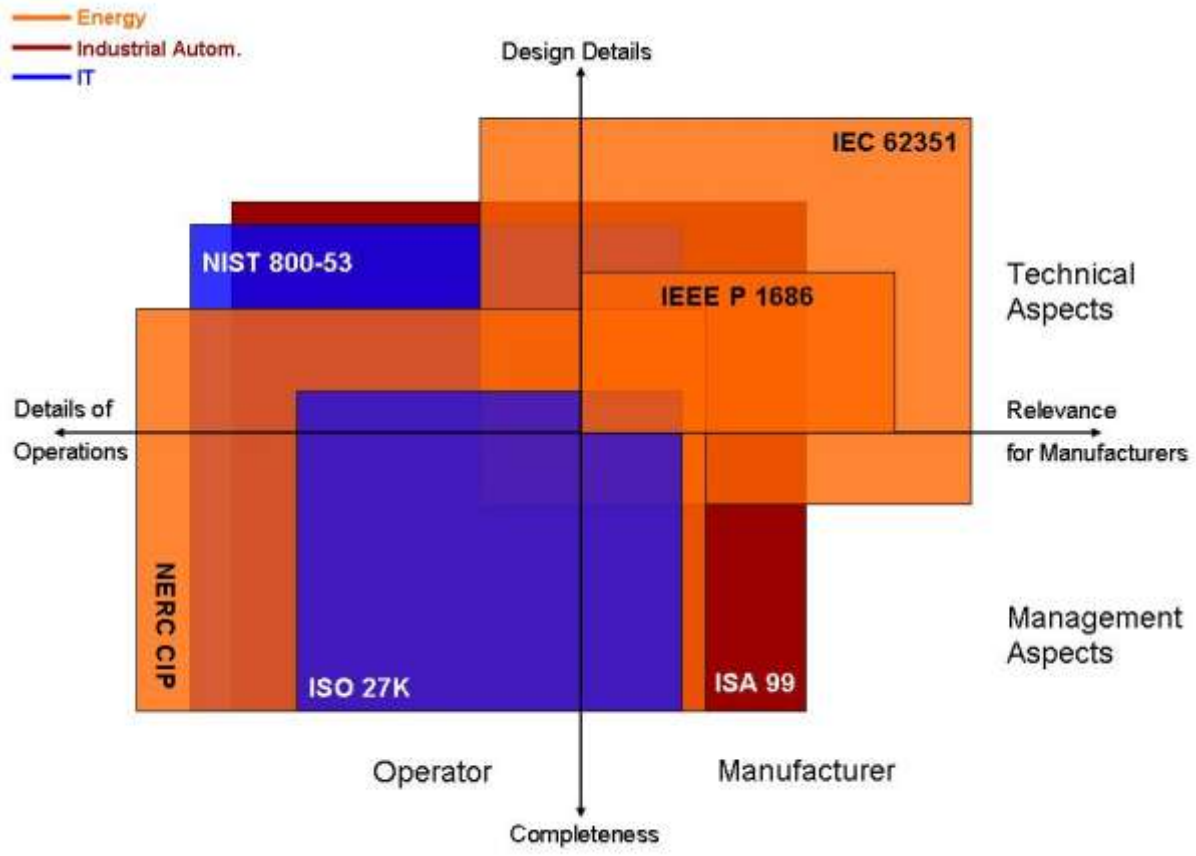

Figure 1: Graphical representation of scope and completeness of selected standards

The different colors indicate the targeted audience. While ISO27K and NIST 800-53 are mainly targeted to IT environments (thus targeted at protecting information), other standards such as ISA 99 are directly addressing Industrial Automation Systems.

While IEC 62351 addresses the energy sector, more specifically substation automation systems and IEEE P1686 intelligent electronic devices, NERC-CIP is generally targeting energy operators.

Standards extending to the right in x-axis direction have relevance for manufacturers. Typically, such standards have detailed technical requirements up to the definition of special security protocols, which must be implemented by the manufacturers.
In contrast, the more a standard extends to the left of the x-axis, the more it is focused on a secure operation. NERC-CIP, for example, prescribes specific actions for operators to do.

Standards extending to the top of the y-axis list precise design details and leave little room for interpretation. IEC 62351, for instance, is intended to list design details in such extend that device interoperability between various manufacturers is guaranteed.
Standards extending to the bottom of the y-axis are covering a broad range of various security areas and thus can be consulted in order to get estimation on the overall security level.

Figure 1 nicely illustrates the broad landscape of standards. This motivates for a closer investigation on the technical overlaps and gaps of the identified standards.

4.2 Selected Standards

In order to get a better view of overlaps and gaps, we decided to choose the most relevant and comprehensive standards, namely

- NERC CIP (Recommendation relevant for bulk energy system operators in the US)
- ISO 27K (Generic standard defining a information security management system)
- ISA 99 / IEC 62443 (Generic standard defining among others a cyber security management system taking into account best practices from industrial automation); note, that ISA and IEC negotiated, that the ISA 99 standards will be adopted as IEC standards as well.

which are compared in more detail.

In addition we choose an additional guideline and a standard addressing industrial information systems in general, which are included in the comparison as well:

- CPNI/NISCC: Good Practice Guides (Best practice recommendations, UK)
- NIST 800-53, Recommended Security Controls for Federal Information Systems and Organizations (US). Note: this standard has not been covered in the standards survey (deliverable 2.1). Although this standard addresses federal information system, it can be applied to industrial control systems (ICS) as well (it encloses an addendum which addresses ICS).

At the end we added two technical oriented standards to the comparison, in order to reflect also standards which mainly define technical measures to be used in control system design:

- IEC 62351 (Technical standard designed to secure the control communication within energy automation systems)
- IEEE 1686 (Technical standard defining security requirements for intelligent electronic devices)

NERC CIP: Reliability Standards for the Bulk Electric Systems in North America

CIP-001-1	**Sabotage Reporting** Disturbances or unusual occurrences, suspected or determined to be caused by sabotage, shall be reported to the appropriate systems, governmental agencies, and regulatory bodies.
NERC Standards CIP-002 through CIP-009 provides a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment. Phased-in Implementation: Please see Implementation Plan for complete list of dates for compliance with the requirements.	
CIP-002-1	**Critical Cyber Asset Identification** Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets. Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.
CIP-003-1	**Security Management Controls** Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.

CIP-004-1	**Personnel & Training** Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.
CIP-005-1	**Electronic Security Perimeter(s)** Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.
CIP-006-1 / CIP-006-1a	**Physical Security of Critical Cyber Assets** Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.
CIP-007-1	**Systems Security Management** Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.
CIP-008-1	**Incident Reporting and Response Planning** Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.
CIP-009-1	**Recovery Plans for Critical Cyber Assets** Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.

ISO 27K Information technology - Security techniques

ISO/IEC 27000	ISO/IEC 27000:2009: Overview and vocabulary. This standard provides an overview of information security management systems, which form the subject of the information security management system (ISMS) family of standards, and defines related terms. As a result of implementing ISO/IEC 27000:2009, all types of organization (e.g. commercial enterprises, government agencies and non-profit organizations) are expected to obtain: 1. an overview of the ISMS family of standards; 2. an introduction to information security management systems (ISMS); 3. a brief description of the Plan-Do-Check-Act (PDCA) process; and 4. an understanding of terms and definitions in use throughout the ISMS family of standards. The objectives of ISO/IEC 27000:2009 are to provide terms and definitions, and an introduction to the ISMS family of standards that: 1. define requirements for an ISMS and for those certifying such systems; 2. provide direct support, detailed guidance and/or interpretation for the overall Plan-Do-Check-Act (PDCA) processes and requirements; 3. address sector-specific guidelines for ISMS; and 4. address conformity assessment for ISMS.

ISO/IEC 27001	ISO/IEC 27001:2005: ISMS Requirements. This general purpose standard covers all types of organizations (e.g. commercial enterprises, government agencies, not-for profit organizations). ISO/IEC 27001:2005 is the main standard of the 27000 family and specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System (ISMS) within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof. ISO/IEC 27001:2005 is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties. ISO/IEC 27001:2005 is intended to be suitable for several different types of use, including the following: - use within organizations to formulate security requirements and objectives; - use within organizations as a way to ensure that security risks are cost effectively managed; - use within organizations to ensure compliance with laws and regulations; - use within an organization as a process framework for the implementation and management of controls to ensure that the specific security objectives of an organization are met; - definition of new information security management processes; - identification and clarification of existing information security management processes; - use by the management of organizations to determine the status of information security management activities; - use by the internal and external auditors of organizations to determine the degree of compliance with the policies, directives and standards adopted by an organization; - use by organizations to provide relevant information about information security policies, directives, standards and procedures to trading partners and other organizations with whom they interact for operational or commercial reasons; - implementation of business-enabling information security; - use by organizations to provide relevant information about information security to customers. Organizations can obtain a formal certification against this standard.

ISO/IEC 27002	ISO/IEC 27002:2005: Code of practice for information security management. This standard establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 27002:2005 contains best practices of control objectives and controls in the following areas of information security management: - security policy; - organization of information security; - asset management; - human resources security; - physical and environmental security; - communications and operations management; - access control; - information systems acquisition, development and maintenance; - information security incident management; - business continuity management; - compliance. The control objectives and controls in ISO/IEC 27002:2005 are intended to be selectively implemented to reach an acceptable level of risk following the process outlined in ISO/IEC 27001:2005. ISO/IEC 27002:2005 is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities.
ISO/IEC 27003	ISO/IEC FDIS 27003: ISMS Implementation guidance (under development) This standard provides detailed step-by-step guidance into the implementation of an information security management system compliant with ISO/IEC 27001:2005 requirements. All critical aspects and activities related to this process are addressed and explained with a very practical perspective.

ISO/IEC 27004	ISO/IEC FDIS 27004: Measurement (under development) This guideline standard is focused on the establishment of a set of metrics, indicators and decision criteria that will be used to periodically monitor the effectiveness and the performance of implemented information security controls, as required by ISO/IEC 27001:2005. An excellent base of examples is provided as Annex.
ISO/IEC 27005	ISO/IEC 27005:2008: Information security risk management. This standard provides guidelines for the information security risk management process. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. Knowledge of the concepts, models, processes and terminologies related to the general risk management discipline is important for a complete understanding of ISO/IEC 27005:2008. It is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that could compromise the organization's information security, also independently from ISO/IEC 27001:2005. The standard also provides valuable annexes with additional guidance on risk management methods and techniques.
ISO/IEC 27006	ISO/IEC 27006:2007: Requirements for bodies providing audit and certification of information security management systems This standard specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS), in addition to the requirements contained within ISO/IEC 17021 and ISO/IEC 27001. It is primarily intended to support the accreditation of certification bodies providing ISMS certification. The requirements contained in ISO/IEC 27006:2007 need to be demonstrated in terms of competence and reliability by any body providing ISMS certification, and the guidance contained in ISO/IEC 27006:2007 provides additional interpretation of these requirements for any body providing ISMS certification.

ISA 99 Manufacturing and Control Systems Security / IEC 62443

ISA 99.01.01	**Terminology, Concepts and Models** This standard presents the basic concepts and terminology that form the basis for the remaining standards in the series. It establishes the scope and context of the ISA99 series of standards by describing it from several different perspectives. It also defines the terminology used and provides a framework within which to position the basic concepts related to Industrial Automation and Control Systems security.
ISA 99.01.02	**Master Glossary of Terms and Abbreviations** This part defines the common terminology which shall be used across all other parts of ISA 99.
ISA 99.01.03	**System Security Compliance Metrics** This standard describes measurable, quantitative security metrics which can be used to assess a given system's compliance with other parts of ISA 99.
ISA 99.02.01	**Establishing an IACS Security Program** This standard provides guidance and direction on how to establish the business case for a security program and how to design the program to meet business needs. It provides the reader with a basic guidebook that can be used to assemble their program, without prescribing details for every industry type.
ISA 99.02.02	**Operating an IACS Security Program** Programs must be effectively transferred from “build mode” to “operate mode” and be regularly renewed in order to be successful in the long term. This standard describes how a security program is run after it is designed and implemented, providing more normative material related to measuring or assessing program effectiveness.

ISA TR99.02.03	**Patch Management in the IACS Environment** The theme of the report is how to address the topic of patch management from both an Asset Owner and Vendor perspective. This includes information to help asset owners develop risk mitigation plans that balance acceptable level of risk in the system and desired level of patching against the process availability requirements of the operation. For vendors, this technical report deals with acceptable practices for notification, documentation, implementation and rollback procedures, and testing procedures for internal or third party supplied patches. The overall goal of this technical report is to provide solid guidance to both communities to ensure that patches are appropriately tested, all impacted systems and functions are documented and evaluated properly, and necessary patches are staged and disseminated in accordance with Service Level Agreements or support plans.
ISA TR99.03.01	**Security Technologies for Industrial Automation and Control Systems** This technical report provides an assessment of various cyber security tools, mitigation counter-measures, and technologies that may effectively apply to the modern electronically based IACSs regulating and monitoring numerous industries and critical infrastructures. It describes several categories of control system-centric cyber security technologies; the types of products available in those categories; the pros and cons of using those products in the automated IACS environments relative to the expected threats and known cyber vulnerabilities; and, most important, the preliminary recommendations and guidance for using these cyber security technology products and/or countermeasures.
ISA 99.03.02	**Target Security Assurance Levels for Zones and Conduits** This standard establishes requirements for defining the zones and conduits of a system under consideration, the technical system target security level requirements for this class of systems used in the industrial automation and control systems environment, and provides informal guidance on how to verify these requirements.

ISA 99.03.03	**System Security Requirements and Security Assurance Levels** This standard defines security requirements on the system level. These requirements are grouped into seven categories: 1) Access Control, 2) Use Control, 3) Data Integrity, 4) Data Confidentiality, 5) Restrict Data Flows, 6) Timely Response to an Event, and 7) Network Resource Availability. For each of the categories, several requirements are defined and for each requirement, requirement enhancements are defined. The requirements and their enhancements are then mapped to target security assurance levels, i.e. for each target security assurance level, the standard defines the requirements a system has to meet to achieve the security assurance level.
ISA 99.03.04	**Product Development Requirements** This standard will address the requirements for a secure development process. The detailed scope of this standard is still to be defined.
ISA 99.04.01	**Component Requirements for Embedded Devices** This standard details the system level requirements as they apply to embedded devices. An embedded device is defined as a special purpose device running embedded software designed to directly monitor, control or actuate an industrial process, e.g. a PLC, a field sensor devices, a SIS controller, or a DCS controller.
ISA 99.04.02	**Component Requirements for Host Devices** This standard details the system level requirements as they apply to host devices. A host device is defined as a general purpose device running a general purpose operating system (e.g. Windows OS, Linux) capable of hosting one or more applications, data stores or functions, e.g. an HMI workstation, an engineering workstation, a historian server, or a domain controller.
ISA 99.04.03	**Component Requirements for Network Devices** This standard details the system level requirements as they apply to network devices. A network device is defined as a device which moves data from one device to another, or restricts the flow of data, but does not directly interact with a control process, e.g. a router, a switch, a firewall, a gateway, an IPS appliance, or a wireless access point.

ISA 99.04.04	**Component Requirements for Application, Data and Functions** This standard details the system level requirements as they apply to applications, data or functions. An application is defined as a software program executing on the infrastructure that are used to interface with the process, e.g. HMI software, historian servers, or PLC ladder logic. Data is defined as any information that is used and/or generated by an application program. There are two types of data, static and dynamic: - Static data rarely changes and is provided as context to dynamic data or used for configuring applications. - Dynamic data is information generated by an application programs, consisting of process values, time stamps and data quality values. Examples of static data include alarm settings, scaling values, units, descriptions, configuration files, password files and filter settings, firmware. Examples of dynamic data include historical or real-time data which is transmitted and stored for further analysis and usage. Function is defined as a procedure involving chemical or mechanical steps to aid in the manufacture of an item or items, usually carried out on a very large scale, e.g. mapping an oil and gas field using models populated by real time data, control functions, safety functions, blending, or unit level control.

CPNI/NISCC: Good Practice Guide - Process Control and SCADA Security, Overview, Parts 1 to 7

This guide is designed to impart good practice for securing industrial control systems such as: process control, industrial automation, distributed control systems (DCS) and supervisory control and data acquisition (SCADA) systems. Such systems are used extensively across the nation's critical national infrastructure. The paper provides valuable advice on protecting these systems from electronic attack and has been produced by PA Consulting Group for CPNI.

The guideline consists of seven short documents (each about 20 pages):

Guide 1: Understand the business risk

Guide 2: Implement Secure Architecture

Guide 3: Establish Response Capabilities

Guide 4: Improve Awareness and Skills

Guide 5: Manage third party risk

Guide 6: Engage projects

Guide 7: Establish ongoing governance

In addition there exists a generic good practice guide on patch management.

NIST 800-53: Recommended Security Controls for Federal Information Systems

The goal of NIST SP 800-53 is to establish an overall security program for industrial Information Systems by establishing a series of security controls that embrace the whole life cycle of the system:

1. well-defined system-level security requirements and security specifications;

2. well-designed information technology products;

3. sound systems/security engineering principles and practices to effectively integrate information technology products into the information system;

4. appropriate methods for product/system testing and evaluation; and

5. comprehensive system security planning and life cycle management

The security controls address the management, operational, and technical safeguards, countermeasures, and/or compensating measures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

IEC 62351: Power systems management and associated information exchange - Data and communications security

IEC 62351-1	**IEC 62351-1: Introduction** Part 1 of the standard is an informative introduction which covers the background of security for power system operations, and provides overview information on the series of IEC 62351 security standards.
IEC 62351-2	**IEC 62351-2: Glossary of Terms** Part 2 includes the definition of terms and acronyms used in the IEC 62351 standards. These definitions are based on existing security and communications industry standard definitions as much as possible, given that security terms are widely used in other industries as well as in the power system industry. When industry standard definitions are used, these are attributed to the source.

IEC 62351-3	**IEC 62351-3: Profiles Including TCP/IP** Part 3 provides security for any profile that includes TCP/IP. It specifies the use of TLS which is commonly used over the Internet for secure interactions, covering authentication, confidentiality, and integrity. This part describes the mandatory and optional parameters and settings for TLS that should be used for utility operations. The purpose of IEC 62351-3 is to provide end-to-end transport security for the communications between software applications. IEC 62351-3 defines mechanisms that protect against: • Eavesdropping through Transport Layer Security (TLS) encryption • Man-in-the-middle security risk through message authentication • Spoofing through Security Certificates (Node Authentication) • Replay, again through TLS encryption. However, TLS does not protect against denial of service.
IEC 62351-4	**IEC 62351-4: Security for Profiles That Include MMS** Part 4 provides security for profiles that include Manufacturing Message Specification (MMS), including TASE.2 (ICCP) and IEC 61850. Security for the Manufacturing Message Specification (MMS) (ISO 9506) provides application-layer security. It requires TLS to configure and makes use of TLS security measures, in particular, authentication: the two entities interacting with each other are who they say they are. If encryption is not employed, then the specific threats countered in IEC 62351-4 include: • Unauthorized access to information If IEC 62351-3 is employed, then the specific threats countered in IEC 62351-4 include: • Unauthorized access to information through message level authentication and encryption of the messages • Unauthorized modification (tampering) or theft of information through message level authentication and encryption of the messages The following security attack methods are intended to be countered by IEC 62351-4. The following list is exclusive of the attack methods countered through IEC 62351-3. In the case that IEC 62351-3 is not employed, the threats countered are restricted to protection during association establishment: • Man-in-the-middle: This threat will be countered through the use of a Message Authentication Code mechanism specified within part 4 • Tamper Detection/Message Integrity: These threats will be countered through the algorithm used to create the Authentication mechanism as specified within part 4.

	• Replay: This threat will be countered through the use of specialized processing state machines specified within IEC 62351-3 and IEC 62351-4.
IEC 62351-5	**IEC 62351-5: Security for IEC 60870-5 and Derivatives** Part 5 provides different security solutions for the serial version (primarily IEC 60870-5-101, as well as parts 102 and 103) and for the networked versions (IEC 60870-5-104 and derivates such as DNP3 over TCP). Specifically, IEC 62351-5 provides application layer authentication which protects against spoofing, replay, modification, and some denial of service attacks. It does not include encryption, so it does not protect against eavesdropping, traffic analysis, or repudiation. Application layer authentication is necessary because site-to-site security and, in some cases, transport layer security, do not address the following: • Security within each local site • Security of serial protocols (such as IEC 60870-5) over unencrypted radios • Security of serial protocols that have been forwarded over IP networks through terminal servers • Protection from “rogue applications” or attacks from within hosts that may be infected by Malware. • Linking role-based authentication to the remote site. Today, the security chain for role-based authentication for users typically stops within the host. Application layer authentication can ensure that only those users authorized to see a particular set of data can access it by preventing it from being transmitted from the remote site until the user is authenticated.

IEC 62351-6	**IEC 62351-6: Security for IEC 61850 Profiles** Part 6 (IEC 62351-6) covers the IEC 61850 profile using MMS over TCP/IP uses IEC 62351-3 and IEC 62351-4. The security threats that are countered include man-in-the-middle, unauthorized modification of data, unauthorized modification of messages, tamper detection, and replay. For those functions where the performance requirements are not as stringent and where confidentiality is required, encryption could be added by other security measures such as “bump-in-the-wire” or VPNs.
IEC 62351-7	**IEC 62351-7: Network and system management (NSM) data object models** Part 7 (IEC 62351-7) addresses security through network and system management of the information infrastructure. Using the concepts developed in the IETF Simple Network Management Protocol (SNMP) standards for network management, IEC 62351-7 defines Network and System Management (NSM) data object models that are specific to power system operations. These NSM data objects will be used to monitor the health of networks and systems, to detect possible security intrusions, and to manage the performance and reliability of the information infrastructure. The NSM data objects use the naming conventions developed for IEC 61850, expanded to address NSM issues. These data objects, and the data types of which they are comprised, are defined as abstract models of data objects. The actual bits-and-bytes formats of the data objects will depend upon the mapping of these abstract NSM data objects to specific protocols, such as IEC 61850, IEC 60870-5, IEC 60870-6, IEC 61968/61970 (CIM), web services, SNMP, or any other appropriate protocol. Those mappings will need to be standardized in separate documents.

IEC 62351-8	**IEC 62351-8: Role-based Access Control (RBAC)** The scope of part 8 is the access control of users and automated agents to data objects in power systems by means of role-based access control (RBAC) similar to what is used by many operating systems to control access to system resources. This specification addresses the exchange of credentials between clients and servers and specifies the format of these credentials as well as the interface to a repository for credential retrieval.

IEEE 1686: Trial Use Standards for Retrofit Cyber Security of Serial SCADA Links and IED Remote Access

IEEE 1686 defines the general requirements to protect serial communications between master stations and remote terminal units from cyber attack, and to strengthen authenticated remote access to maintenance ports in RTUs (Remote Terminal Units and other IEDs (Intelligent Electronic Devices. The standard defines the requirements to retrofit existing communications in such a manner as to minimize the changes needed to existing equipment and software. The test plan defines specific tests and evaluations that should be performed to ensure that the cyber security mechanisms are working properly.

4.3 Gaps and Overlaps matrix

In the following section the selected standards are evaluated with respect to topics which have to be addressed when designing secure SCADA or control systems (manufacturer point of view) or which have to be addressed when operating such a system (operator point of view).

An appraisal of

- **0** means that the topic is either not appropriately addressed in this standard, or there are no clear statements how to address this topic or it is even not addressed at all
- **1** means that the standard includes clear statements, so that the audience (manufacturer or operator) at least can derive actions with respect to this topic.

However, detailed statements on the completeness of the standard would need far more considerations.

		Standards						
		CPNI	NERC CIP	ISO 27 K	ISA 99 IEC 62443	NIST 800-53	IEC 62351	IEEE 1686

Manufacturer	Security aspects within the design phase, e.g.
	• Security requirements
	  ○ Functional
	  ○ Infrastructure
	  ○ Operational
	• Support of SW update process
	• Definition of security features and interfaces (to be implemented)
		0
		
		0
		0
			0
			
			0
			0
				[1] 0
				
				0
				0
					1
					
					1
					1
						[2] 0
						
						0
						0[3]
							1
							
							0
							1
								0
								
								0
								1

	Implementation of security, e.g. • Features and interfaces • Secure coding rules • Code reviews	0 0 0	0 0 0	0 0 0	0 (planned, but not yet available)	0 0 0	1 0 0	1 0 0
	Validation of security implementation, e.g. • Validation of implementation of security requirements • Testing of security features and interfaces • Usability verification	0 0 0	1 1 1	1 0 0	0 0 0	1[4] 1 0[5]	0 0 0	0 0 0

[1] ISO 27001 (And control objectives and controls associated to ISO 27002) focus is on information management security and hence doesn't manage the methods used to produce the means used to manipulate the information, like software, systems, etc. Nevertheless, some relevance exists like ISO9001 does and contribute globally like for example CMM for software development. The ISMS requirement is the aim of ISO 27001 where protective measures are preeminent against feature to embed.

[2] Considered with NIST 800-27, security engineering principles

[3] Mentioned although not specifically addressed

[4] Extensively considered, see 800-17 and req. SI.10 within 800-53

[5] Not explicitly addressed

		Standards						
		CPNI	NERC CIP	ISO 27 K	ISA 99 IEC 62443	NIST 800-53	IEC 62351	IEEE 1686
	Security documentation & guidelines	0	0[6]	0[7]	0	1	1	0
	Support of secure software update (e.g. patches)	0	1[8]	0[9]	1	1	0	0[10]

[6] CIP-007 requires documentation review and maintenance for system security management. Guidelines are not provided.
[7] Security management documentation is mentioned in operational procedures and responsibilities (A10.1) but all other controls shall be documented as per compliance for 4.3.2. Documentation guideline is not provided by the standard.
[8] CIP-007
[9] Patch support is a level not mentioned in ISO 27001. Instead, the standard refers to the treatment of risks to select a control objective. Protection of information and software integrity against malicious and mobile code is the control A.10.4.1 for example.
[10] Firmware change

		Standards						
		CPNI	NERC CIP	ISO 27 K	ISA 99 IEC 62443	NIST 800-53	IEC 62351	IEEE 1686
Asset Owner / Operators	Risk assessment and treatment	1	0	0	0	1	0	0
	Security policy	1	1	1	1	1	0	0
	Organization of security incl. responsibilities	0[11]	1	1	1	1	0	0
	Asset management incl. recovery plans for critical assets	1	1	1	1	0	0	0
	Human resource security	0	1	1	1	0	0	0
	Physical and environmental security	0	1	1	0	0	0	0
	Communications and operations management (incl. handling of cryptographic keys etc.)	0	1	1	1	1	0	0
	Access Control	0	1	1	1	1	0	0
	Systems acquisition, development, and maintenance	0[12]	1	1	1	1	0	0
	Security incident management	1	1	1	1	1	0	0
	Compliance	1	1	1	1	1	0	0
	Training and awareness	1	1	1	1	1	0	0
	Security configuration management /	0[13]	1[14]	0[15]	0	0	0	0

[11] Partely covered, e.g. Part 3 „ Establish response capabilities"
[12] Partly covered in Part 6 „Engage Projects" and "patch management"
[13] Partly covered in Part 6 „Engage Projects"
[14] Covered by CIP-003 R6 requirement, Change control and configuration management but limited to critical cyber asset as per identification stated in CIP-002. Also covered by requirements in CIP-007 Systems Security Management R1, R3, R6
[15] Should be partly covered by A.10.1.1 Documented operating procedures, A.10.1.2 Change management

		Standards						
		CPNI	NERC CIP	ISO 27 K	ISA 99 IEC 62443	NIST 800-53	IEC 62351	IEEE 1686
	Traceability / Reliability and Availability							
	System security architecture	1	0[16]	0[17]	0	0	0	0
	Tool sets for secure configuration	0	0	0	0	0	0	0

Adequately covered=1; not covered or not adequately covered =0 (see detailed explanation at the beginning of this section)

[16] Partly covered by CIP-005 Electronic Security Perimeter

[17] Mentionned in A.11.4.5 Segregation in networks, in A11.6.2 Sensitive system isolation, in A12.1.1 Security requirements analysis and specification

4.4 Main findings and recommendations from the gap and overlap analysis

In the following section the main findings (MF) from the gap and overlap analysis are listed and recommendations (REC) for further actions, projects, or activities are derived.

The various stakeholders involved in the lifecycle of SCADA systems have different requirements regarding the assurance of their security, and this would be reflected in their use and application of the several relevant standards. Therefore, a key point is to analyze the coherence, consistency and overlapping among the standards. So, while there is no requirement to have a single standard covering all aspects regarding the design, implementation and operation of secure control systems, there is a need for a common set of concepts, and it would be desirable to have at least a common terminology. The standard with the largest covering, and that appears to better approach this issue, will be ISA99 respectively IEC 62443 (assuming that all part will be realised as planned). However, even this standard will not cover all aspects, and in addition large parts of this standard are not yet approved or are in a very early stage.

(MF1) No single standard covers all aspects (necessary to design, build and operate secure control systems)

In Europe there is in addition the issue of many national languages. For all these reasons the recommendation is:

(REC1) Define a CEN workshop agreement (CWA) to carry out a thorough assessment of gaps regarding a common terminology and conceptual base (possibly taking as reference ISA 99).

Most of the standards address specific industries and use cases, respectively. The reason is that the specific use cases lead to specific requirements, and this is positive when it provides adequate answers to the sector stakeholders. While diversity can be justified, and in certain occasions can be positive, due to the technological convergence it would be suitable to use common approaches whenever it is not expressly required.
On the other hand, the process and procedure oriented standards (especially) have large overlaps. These are obviously the potential source of disjointed and confusing situations, and even of deep discrepancies affecting the same combined applicability of the standards.

(MF2) Standards partly have large overlaps.

The main purpose of applying security-related standards by vendors, operators/end users, certifiers, and authorities is to gain confidence on the security attributes of the systems. This security depends upon many factors, some technical, some organisational, with relevance in different phases of the lifecycle of the system. Therefore, the assurance of the SCADA security has to consider many elements, considered in technical and general purpose standards.
On the one hand, technical standards are very detailed in some areas with the goal to ensure interoperability, even between various manufacturers. However, they do not suffice for enhancing the overall security level. On the other hand, wide standards allow assessing the general security level and determining missing security controls, but they do not prescribe the exact implementation and configuration of the security controls.

A consequence of the above described situation is that standards will be used in parallel.

(REC2) Start an experiment with respect to the assessment of the joint use of standards. Candidates for those experiments could be generic standards such as ISA 99 or ISO 27k together with branch specific recommendations, guidelines or standards. The proposal is to do this within a CWA which could try to receive funding from the ICT 2010/13 program.

The investigation revealed that there are gaps not covered by any standard especially the topic secure tools for configuration management (this has also already been identified by CIGRE B5.38). Although this is an important topic for secure operation of (distributed) control systems, the other topics are mostly covered. Therefore, the acceptance of any new development activity aiming at the generation of a new overall security standard covering a large area is questionable.

(MF3) Missing security requirements for tool sets used for configuration

(REC3) Define a CEN Workshop Agreement with the goal to develop what security aspects need to be addressed with respect to the definition of tool sets used for configuration. The outcome of this CWA could then be used as a basis for a new work item proposal (NWIP) within IEC.

(MF4) General purpose standards (by nature) do not take into account use case specific requirements.

For the stakeholders the application of the general purpose standards is not always straightforward.

(REC4) Promote (e.g. within ISO/IEC SC27) the production of technical guidelines for the application of general purpose standards to the different technical fields.

5. Conclusions

Awareness of the breadth and fast evolution of cyber security threats is the most important.

ISA99/IEC 62443 is the most promising standard with the largest coverage with respect to control systems. This was confirmed in our targeted experiments. Also, there is no need to wait for a final version to use it for enhancing overall security.

IEC 62351 is the most comprehensive technical specification addressing security of automation systems for the energy sector.

It was concluded in the near term the need for CWAs on the following subjects: metrics, security processes best practices, skills and competences and the exchange of security information (as elaborated in sections 3.2 to 3.5).

A research project is needed to identify Key Performance Indicators for the monitoring of security level and behaviour.

Additional studies are needed (economic cost, a decision support system for CEOs, a testing methodology for verifying security assurance) as well the development of training material for use by staff having access to the control system.

A number of targeted experiments took place. Cross-functional teams (vendors, operators' ICT staff and other functions) were of great benefit. They made it clear that the cost of applying a standard is not well-known.

Further activities will require the continued involvement of all representative stakeholders in order to cover all aspects from product definition to operation.

Annex 1: Some important information on the 2010-2013 ICT Standardisation Work Programme

With their 3-year, rolling ICT standardisation work programme, the Commission services are inviting the ESOs (the European Standards Organizations, CEN, CENELEC and ISO) , where appropriate in cooperation with relevant fora and consortia, to initiate standardisation activities as well as activities supporting the implementation of standards such as interoperability testing, promotional activities, educational initiatives, etc. in the specified policy domains. The policy domains result from legislation or policy initiatives which need standards for effective implementation.

The work programme provides the potential to cover ICT standardisation needs over a 3 years period and each standardisation request clearly indicates which type of standardisation deliverable is needed and the corresponding time frame.

One of the 14 priority domains is eSecurity (Domain 11).

The eSecurity priority domain states explicitly that the ESCoRTS recommendations are eligible for support under the 2010-2013 ICT standardisation work programme.

Below are the relevant extracts from the text:

Cyber-security of industrial control systems

Justification for the standardisation activities

Supervisory Controls and Data Acquisition (SCADA) is the term for security of process control and industrial manufacturing systems. These have increasingly relied on commercial information technologies, but the number of user groups and standardisation activities dealing with security issues in the area of SCADA systems has rapidly grown over the last few years. On the one hand this is a good message, because it underpins that security has become an important issue being taken into account. On the other hand it leads to a jungle of standards and guidelines, because these are often being developed in parallel, with resulting lack of interoperability and other conflicts.

The FP7 ESCoRTS project ("European Network for the Security of Control and Real-Time Systems") has provided an overview of the relevant standards and guidelines. This work should be taken forward in order to provide interoperability specifications and implementation guidance.

Required standardisation actions

In collaboration with interested stakeholders, the ESOs are invited to prepare a programme for the production of the relevant interoperability specifications and related guidance. The programme should be prepared in full collaboration with the relevant TCs in ISO and IEC and with consortia activities as cited in the ESCoRTS overview, and recommend timescales.

The time frame for the required standardisation deliverables

12 months

Note: the full text of the 2010-2013 ICT Standardisation Work Programme is available from

http://ec.europa.eu/enterprise/sectors/ict/standards/work-programme/index_en.htm

Annex 2: Some information on CWAs (CEN or CENELEC Workshop Agreements)

CEN or CENELEC Workshops(they are using the same methodology) are fast, relatively informal consensus-building groups, open to direct participation of any interested party. Participation is thus not based on national delegations. There is no geographical limit on participation and hence participants may come from outside Europe. Workshops are usually created in areas where CEN or CENELEC have no Technical Committee yet operating. They can be organized as part of research project activities - to validate project's standardization outcomes in an open consensus process and publish the results as a CEN or CENELEC deliverable, the CEN or CENELEC Workshop Agreement (CWA).

CWAs are developed along straightforward lines, with a minimum of bureaucratic rules and reflect the consensus of identified companies and organizations responsible for its contents. The CWA's Foreword contains an overview of the companies and organizations who have developed and agreed on the CWA. Upon publication of the CWAs, the corresponding Workshop is disbanded.

More information on Workshops is available from the guidance document "Hands on CWA" which can be accessed from

http://www.cen.eu/cen/Services/Education/Handsonguides/Pages/default.aspx