

ESCoRTS
EUROPEAN NETWORK FOR THE
SECURITY OF CONTROL AND REAL TIME SYSTEMS
16 June 2008- 15 December 2010

Publishable summary

ESCoRTS is a project with participation from EU process industries, utilities, leading manufacturers of control equipment and research institutes to foster progress towards cyber security of control and communication equipment in Europe. Its main objective is to assist the EU as a whole (i.e. authorities, industry, manufacturers, etc.) in developing informed positions and in shaping current and future efforts related to control systems security standardization. The project methodology is based on a dialogue with the end users of control systems in all relevant industrial sectors such as: power generation, transmission and distribution, oil, water and chemicals. The project makes a number of recommendations in relation to future standardization as well as research activities.

But before making these recommendations, the project set the scene in a number of fact finding reports.

It first produced the "Survey on stakeholders needs" report which confirmed the assumptions underlying the need for the ESCoRTS activities, such as the fact that EU industry awareness and readiness lags behind US initiatives, but also that there is a growing feeling in Europe that security issues are crucial for reliable critical control system operation.

A second report setting the scene evaluated the market for SCADA security services and concluded that the security service market in the area of critical infrastructure is in an early phase. As the awareness to cyber security issues increases continuously the dimension of the security service market will grow accordingly. However, missing commonly accepted guidelines or standards for security testing and/or security assessments currently hinder the providing of such security services.

Another report focussed on standards and other recognized guidance documents. The report called "Survey of Existing Methods, Procedures and Guidelines in support of secure Supervisory Control And Data Acquisition (SCADA) applications" lists existing methods, procedures and guidelines in the area of control system (cyber) security, addressing activities of international organizations, important national activities in Europe and the US, as well as the most important branch specific activities (international and national).

Nearly 40 standards, guidelines or regulations relevant for operators or manufacturers in the area of control system (cyber) security, were identified and categorized along a number of criteria including Status (Draft or Released), Type (Guideline, Regulation/Law or Standard), Geographic Relevance and addressed Industry and Audience. For each standard/guideline, a short description of the content was given.

Among the standards surveyed some are strongly related to evaluation aspects (eg ISO/IEC 27000 series); a few of these standards/guidelines were used in targeted experiments at the location of the ESCoRTS user companies (Enel, Transelectrica and Mediterranea delle Acque) where the companies' security processes were evaluated against these standards/guidelines.

The project performed a more detailed study on a subset of the 39 identified standards, focussing on the most relevant and comprehensive standards. The following 7 standards were chosen for this more detailed study:

- NERC CIP (Recommendation relevant for bulk energy system operators in the US)
- ISO 27000 (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).
- CPNI/NISCC: Good Practice Guides (Best practice recommendations, UK)
- NIST 800-53, Recommended Security Controls for Federal Information Systems and Organizations (US).
- 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)

In the detailed study, the 7 selected standards were 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). The results of this detailed evaluation can be found in the Roadmap deliverable.

A graphical impression of the overlaps and gaps between these standards and guidelines, also indicating their main target audiences and level of design detail or completeness is depicted below.

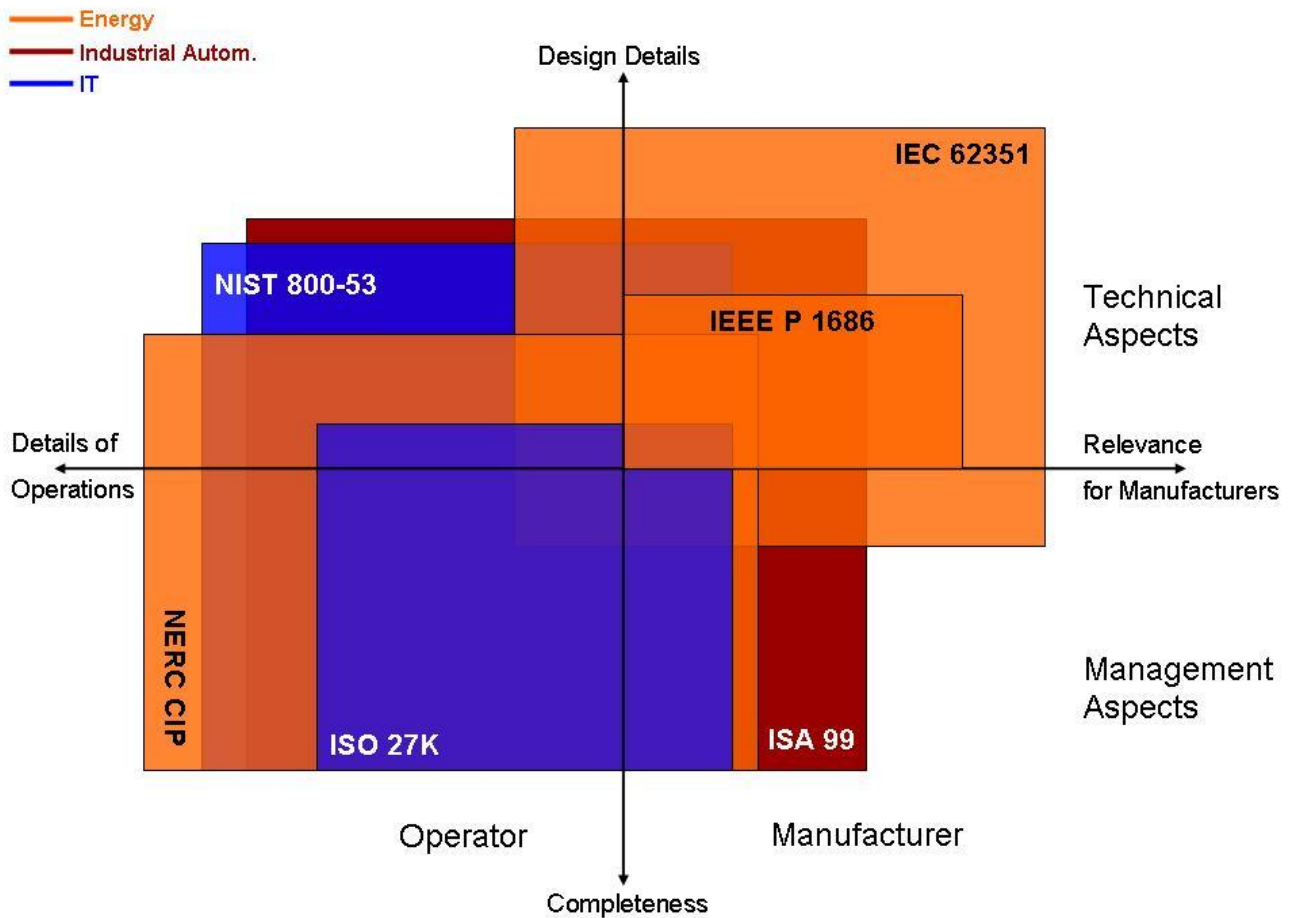


Figure - Graphical representation of scope and completeness of selected standards

The above reports and surveys were complemented by reports showing a comprehensive overview of what has to be secured (delivered as a taxonomy of security vulnerabilities, threats and solutions) and how to measure the security level of installations (delivered as a metrics for cyber security assessment).

The security threats were reported as a "Taxonomy of Security Solutions for the SCADA Sector" which report describes the more typical cybersecurity problems encountered by industrial control systems, and the solutions that can be put in place for countering them. The report classifies and lists security vulnerabilities, threats and solutions, but it does not recommend best practices or possible options. In terms of countermeasures, the report differentiates between Communication Protocol countermeasures, Filtering and Monitoring countermeasures, Architectural Good Practices and Organizational Countermeasures.

The production of a general framework for security metrics was also the subject of a dedicated report.. Security metrics is a key topic for all Information and Communication systems, as all related actors need to take decisions based on appropriate understanding of the security of those systems. In the case of SCADA systems this requirement is particularly stressing, as the consequences of security events onto the controlled systems can have critical effects, with significant safety, environmental and financial impact for the operator of the installation, workers and citizens, and society at large. The report proposes some specific metrics that can be applied

for assessing SCADA systems. These specific metrics were tested on a replication of a specific target application in the energy sector.

Recommendations resulting from all above activities were brought together in a R&D and standardization roadmap. The main conclusions and recommendations from this roadmap are:

- 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. [Note: a technical incompatibility between IEC 62443-2-1 and ISO/IEC 27001:2005 was reported to CEN after the closure of ESCoRTS which may have to be clarified (see the future CEN Workshop Agreement (CWA) on security processes best practices)].
- IEC 62351 is the most comprehensive technical specification addressing security of automation systems for the energy sector.
- CEN Workshop Agreements (CWAs) are suggested on the following subjects: metrics, security processes best practices, skills and competences and the exchange of security information.
- 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.

Other reports produced (in addition to the reports indicated above) were a report on requirements for future cyber security laboratories and a report on requirements for a secure ICT platform for the exchange of relevant data among the stakeholders. A pilot implementation of a secure ICT platform for the exchange of relevant data among the stakeholders is running in the JRC at ISPRA.

ESCoRTS being set up as a "European network for the Security of Control and Real-Time Systems", it is not only the technical contents of its reports that is important. Equally important are the plans for action beyond the project's completion. CEN will seek to launch with the support of the stakeholders a CEN Workshop to deliver some of the CWAs as defined in the Standardization Roadmap. This CEN Workshop will also enable the community of stakeholders to continue and meet during 2011 and beyond.. The intention is to apply during 2011 for project funding under the Commission's ICT Standardization work programme which is available on http://ec.europa.eu/enterprise/sectors/ict/standards/work-programme/index_en.htm.

The public deliverables from the project will remain available from

<http://www.cen.eu/cen/Sectors/Sectors/ISSS/Focus/Pages/FG-ESCORTS.aspx>