

ESCoRTS
EUROPEAN NETWORK FOR THE
SECURITY OF CONTROL AND REAL TIME SYSTEMS
16 June 2008- 15 June 2009

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 completed as its first deliverable a survey of stakeholder needs in SCADA (Supervisory Control And Data Acquisition) security. This survey 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. One US member of the ESCoRTS consortium contributed lessons learned from experiments in their national laboratories.

The questionnaire asked to qualify the respondent security practice with respect to several areas (Security policy, Physical and Cyber Security measures, Incident response and reporting, Security Risk Assessment & Management), and to qualify relevance to their company business of a number of relevant guidelines and standards which were issued or are in an advanced phase of discussion.

In order to obtain further input from the end user, a Stakeholder Advisory Board (SAB) consisting of some 30 representatives of various user industries and security service providers has been established which already met twice. The survey was presented to the Stakeholders Advisory Board (SAB) in a workshop in February 2009. The workshop confirmed the survey conclusions as follows:

- EU industry awareness and readiness lags behind US initiatives.
- There is a growing feeling in Europe that security issues are crucial for reliable critical control system operation, so vendors and users are trying to keep the pace with what emerges as best practice security

- There seems to be the lack of European explicit demand for a comprehensive security solutions. Two related issues emerge as decisive. On the one hand, there is the potential cost of security measures, which might weigh considerably on the overall control equipment cost. On the other hand, there is the lack of adoption in Europe of common security reference or baseline (be them formal or de facto standards, guidelines, or accepted best practices accepted and applicable across all countries).
- Certification is necessary for ensuring the cyber security of industrial processes., but not sufficient. The organizational dimension is the key one in a longer term perspective. To that aim, a long term strategy is to be instantiated. Impact assessment is very important: in that respect process security is definitely the key prospect: no business case of a comparable size can be quoted when looking to disruptions of the mere IT (Information Technology) business network.

The survey concludes by stating that "Although ESCoRTS, alike many similar endeavours, may play a role in increasing the awareness of European stakeholders and in the harmonization of the European market place, by fostering adoption of more uniform security guidelines EU wide, it is evident that Europe must substantially increase its efforts to urgently secure mission critical systms."

The second Deliverable for completion by summer 2009 is an evaluation of the market for SCADA security services. Most input to that evaluation was collected in a second workshop held in May 2009.

The study 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.

The study concludes that there is, beside managed security services, definitely a market also for other security services, especially for security consulting, which includes security assessments, testing, and training. But the readiness of the actors (mainly the operators of critical infrastructure) depends on the sector to which they appertain. There are some sectors -such as energy, chemical or pharmaceutical industry- with a significant security awareness, who are already performing security assessments. However these are often enforced by specific regulations rather than being intrinsically motivated. In addition different methodologies/guidelines are used for these assessments and different amount of effort is spent, which makes a comparison of the security levels achieved very difficult.

With respect to security testing the study concludes that there are two aspects to be considered.

The first aspect is the testing of critical infrastructure installations and of their critical components. This usually is done in relation to a security assessment of the system. Testing of real-live systems is possible but has to be performed with extreme caution in order to avoid discontinuation or breakdown of the system. On the other hand testing of a reference system in a test range would be less dangerous. But building up such facilities for realistically emulating industrial systems would

require important investment. The results of these tests have to be interpreted correctly, but a capable test range can provide the possibility of testing systems before their deployment.

The second aspect is security testing of the components by the vendors themselves. Some vendors (at least the larger ones) already perform security tests of their equipment as part of the quality assurance processes. Special test-beds for evaluating equipment can be justified as a centralised place for operators, vendors and government agencies to collaborate in the search for appropriate security solutions against a full range of threats and security scenarios

The study suggests that Security training, for example on awareness, does not need necessarily to be provided by special teaching companies; governmental organisations can also raise awareness.

As the awareness level for cyber security issues increases, more companies will organise "cyber-security training" for their employees. There are already providers delivering "training sessions" to control system owners. A number of actors address the market for security training: specialized training institutes, universities, public authorities (US-CERT, US-NIST, NL-NICC, UK-CPNI, etc.), IT firms, software vendors, control system vendors (linked to product installation), control system consultants, independent experts/trainers. But these activities also seem to be limited to the security aware industrial sectors mentioned at the beginning of this section. However, this is unsurprising as security training often is an initiative accompanying previous security assessments.

The overall conclusion of the study therefore is that 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.

Work has also started on the deliverable that will provide a "Survey of Existing Methods, Procedures and Guidelines in support of SCADA Security". This survey will address Technical standards (e.g. protocols), Security management standards and Security Evaluation Standards and pay specific attention to important standards from outside EU (especially from US). The standards and guidelines will be categorized following an agreed set of criteria to list and describe them. Safety standards and physical security standards (e.g. fire protection) are not part of the survey's scope. The survey is due for finalization end September 2009.

Further to the SAB, CEN has created a Focus Group on the subject to enable all interested parties to become involved when the standardization aspects such as the standardization road map are discussed. While the SAB is open upon invitation by the Consortium, the Focus Group is open to any interested party.

During its second year, the project will aim to achieve a joint understanding among stakeholders of the way current standardisation efforts are progressing. It will aim to point out and rationalise eventual divergences, and to develop a (draft) strategic standardisation roadmap so as to structure existing and forthcoming actions.

The project will also study and report on any requirements for future cyber security laboratories to be established in Europe.

Public information on the project is at:

<http://www.escortsproject.eu>