

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

During its last half year of operation, ESCoRTS finalized the Standards and R&D Roadmap. The main conclusions from the Roadmap are summarized below.

- 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.
- 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.

ESCoRTS further produced a report discussing a general framework for security metrics. 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.

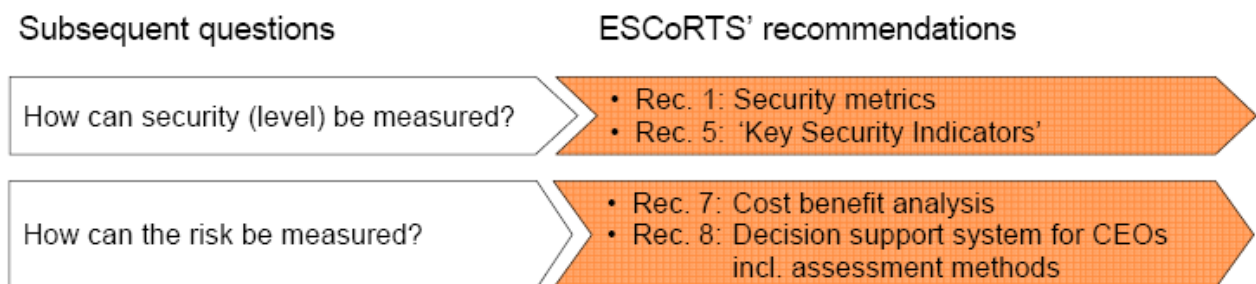
A final deliverable which got finalized was the report on Requirements for future cyber Security laboratories. This report presents a first consideration of the requirements for a laboratory for conducting security experiments with SCADA systems. The main consideration has been that the laboratory would be used by all potential stakeholders, and not only by the SCADA system manufacturers. This puts special conditions, mainly from the standpoint of the target system for the experiments. The field of experimental security of information and communication technologies is just emerging in the last years, and there is a lot to learn yet. Mainly from the methodological perspective, it is clear that there are many gaps. The report tried to highlight some of them.

The report suggests that the development in the future of SCADA security labs will have to pay detailed attention to:

- The extension and details of the target system
- The capacity of the attack resources and sophistication of the attack mechanisms
- The capacity of control and observation of the experiments
- The repeatability and comparison of results

The other results from ESCoRTS during the final half year of operation were the organization of an open meeting on 27 October 2010 at which the results of the project were presented. A special attention was given at the meeting to the Stuxnet malware and how the ESCoRTS findings do relate to this threat.

At the open meeting, the ESCoRTS recommendations in the roadmap were clarified in the context of combating a targeted attack to a SCADA systems (see below).



## Subsequent questions

## ESCoRTS' recommendations

How to increase the current security level?

- Rec. 2: Security Processes Best Practices
- Rec. 3: Definition of skills and competences
- Rec. 6: Testing methodology and testbed
- Rec. 9: Training material
- Rec. 10: Common terminology
- Rec. 11: Joint use of standards
- Rec. 12: Security requirements for configuration tool sets
- Rec. 13: Technical guidelines for the application of generic standards

How can the (overall) damage be limited, in case an attack was successful?

- Rec. 4: Information sharing
- New: Early detection of (targeted) attacks in critical infrastructures

The early detection of (targeted) attacks in critical infrastructures was identified as an additional recommendation to combat targeted attacks (bearing in mind for instance the time line of Stuxnet).

The consortium members also agreed on a plan for talking the results further into 2011 when the project has finished. 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](http://ec.europa.eu/enterprise/sectors/ict/standards/work-programme/index_en.htm).

Public information on the project is at:

<http://www.escortproject.eu>