

ESCoRTS
EUROPEAN NETWORK FOR THE
SECURITY OF CONTROL AND REAL TIME SYSTEMS
16 June 2009- 15 June 2010

Publishable summary

ESCoRTS is a European Coordination Action (June 2008 – December 2010) to foster progress towards cyber security of industrial control systems 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 standardisation.

A Survey of Existing Methods, Procedures and Guidelines in support of secure Supervisory Control And Data Acquisition (SCADA) applications was produced. The survey 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).

In total 37 standards, guidelines or regulations relevant for operators or manufacturers in the area of control system (cyber) security, were identified:

- international standards or guidelines (13),
- produced US committees (14)
- defined by European groups, or by groups of European countries (10)

The identified standards and guidelines were been 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 is 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, Transeletrica and Mediterranea delle Acque) where the companies' security processes were evaluated against these standards/guidelines.

In its report on a Taxonomy of Security Solutions for the SCADA Sector, security vulnerabilities (see extract below), threats and solutions are listed and classified.

Protocol	Vulnerability/Threat	Description
Modbus	Unauthorized Command Execution	Since Modbus does not implement any authentication mechanism, an attacker can forge Modbus packets. These can maliciously interact with the normal operative behavior of a target PLC (e.g. a PLC could start to send wrong commands to the field devices). Indicatively, candidate commands for this type of threat are all the commands allowing to write values into the PLC registers, such as FC5 (force single coil), FC6 (preset analog reg.), FC15 (force multiple coils), FC16 (preset multiple analog reg.)
Modbus	Brute Force DOS	A side effect of the lack of authentication mechanisms is that the PLC will try to execute every "Modbus command" received, using part of its computational resources. An attacker sending meaningless Modbus commands to a PLC, could consume all its resources, leaving the PLC unable to process its own routines.

Figure - extract of D22 –Taxonomy of Security Solutions for the SCADA Sector

The consortium found security for control systems to be a complex subject due to at least the three following reasons. A first reason is that the architecture of control systems, while getting complex for functional and topological reasons, is rarely designed with security goals in mind. Secondly, the technologies employed (such as most prominently the SCADA protocols) are often insecure by nature. And thirdly, because the business benefits from security are not immediately evident, the practices employed by the companies, rarely consider security among their goals.

In terms of countermeasures, the report addresses:

- Communication Protocol countermeasures
- Filtering and Monitoring countermeasures
- Architectural Good Practices and
- Organizational Countermeasures

The consortium also developed a secure ICT pilot platform for the exchange of relevant data among stakeholders. Indeed, as any other engineering field, the security of SCADA and control systems heavily depends upon empirical data for guiding its evolution and for indicating the lacks and shortcomings of the solutions implemented. However, all security data is sensitive by nature, and so the system operators are not keen on openly sharing them.

A solution to this conundrum has been the constitution of trusted communities, where the exchange of information is done among partners that agree on strict confidentiality rules. Trust among the participants is a key element. Such a trusted community exists in the European SCADA

and control systems Information Exchange (E-SCSIE), whose participants are national authorities and agencies, and critical infrastructure operators.

In the context of ESCoRTS, it is recognised the need for a broader and parallel exchange of information involving other actors, such as the vendors and integrators of SCADA and security technologies. At the same time, it is accepted that due to commercial and procurement-related issues, the exchange with the latter actors might have to be differentiated from the work in the national/European information exchanges.

The report on a Secure ICT platform for the exchange of relevant data among stakeholders describes the requirements that such a trusted platform should meet. It further discusses from the communication and technical point of view, the basic elements that should be taken into account in the implementation of such information exchange. A pilot implementation of the platform exists at JRC.

Public information on the project is at:

<http://www.escortsproject.eu>