IT SECURITY ASPECTS OF INDUSTRIAL CONTROL SYSTEMS

P. Holečko, I. Krbilová

University of Zilina, Faculty of Electrical Engineering, Department of Information and Control Systems
Univerzitna 1, SK 010 26, Zilina, Slovak republic
E-mail: peter.holecko@fel.utc.sk, izabela.krbilova@fel.utc.sk

Summary This paper discusses a set of general network system architectures for industrial process control systems as well as vulnerabilities related to these systems and the IT threats these systems are exposed to from the point of view of Common Criteria methodology and ITU-T recommendation X.805.

1. INTRODUCTION

Real-time control systems used in process control applications have many characteristics different than traditional process information systems. Foremost among these is design for efficiency and time-critical response. Security is generally not a strong design motivation and therefore tends to get out of way of performance. Computing resources available to perform of security functions are often very limited.

2. PROCESS CONTROL SYSTEMS

Digital industrial control systems can be classified into process-based systems or discrete-based systems. Process-based controls are used to control a continuous process such as fuel flow in a power plant or petroleum in a refinery. Discrete-based controls (also known as batch controls) control discrete parts manufacturing or "batches" of material like in a chemical plant. Both types of control utilize the same types of control systems, sensors, and networks.

Figure 1 shows the key control components of an industrial control system, including the control loop, the human – machine interface (HMI), and remote diagnostics and maintenance utilities [1]. A control loop consists of sensors, control hardware, process actuators, and communication of measurement variables. Measurement variables are transmitted to the controller from the process sensors. The controller interprets the signals and generates the corresponding control signals that it transmits to the process actuators. Process changes result in change of sensor signals, identifying the state of the process.

The human – machine interface allows a control engineer or operator to configure set points, control algorithms and parameters in the controller. The HMI also provides displays of process status information, alarms, and other relevant data. Diagnostic and maintenance tools, often available via modem and Internet interfaces, allow control engineers, operators and vendors to monitor and modify controller, sensor, and actuator properties from remote locations.

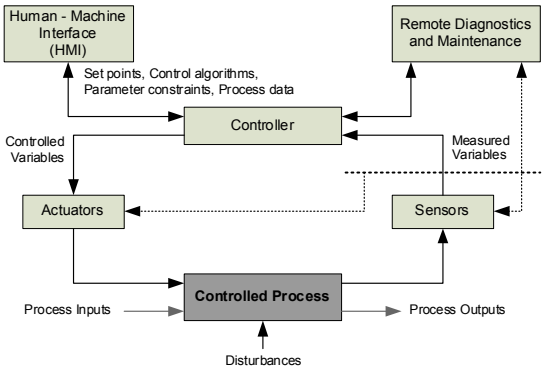

Fig.1 Main control components

A typical industrial control system contains an extension of control loops, HMIs and Remote Diagnostics and Maintenance tools built on an array of network protocols. Supervisory level loops and lower level loops operate continuously over the duration of a process at cycle times ranging on the order of minutes to milliseconds.

In a large enterprise, there may be several geographically distributed industrial plants. Enterprise business operations can access plant information over the Internet or in some cases over a wide area network (WAN).

The local area network (LAN) of a processing plant services all of the operations within the plant while the actual control system of the plant sits on a somewhat isolated peer-to-peer network. At this level the systems can be categorized into two types of supervisory based control schemes, Distributed Control Systems (DCS) and Supervisory and Data Acquisition Systems (SCADA). DCS are used to control large complex processes such as power plants, refineries or chemical plants typically at a single delimited site. By contrast, SCADA are used to control more dispersed assets where centralized data acquisition is as important as control. Examples of SCADA applications are the water, gas, and electrical energy distribution operations.

The general network architectures of DCS and SCADA are shown in Figure 2. By comparison of these schemes we can see that at a higher level of network architecture, the performed plant operations are similar for plants using either DCS or SCADA systems. At this level, everything resides on a local

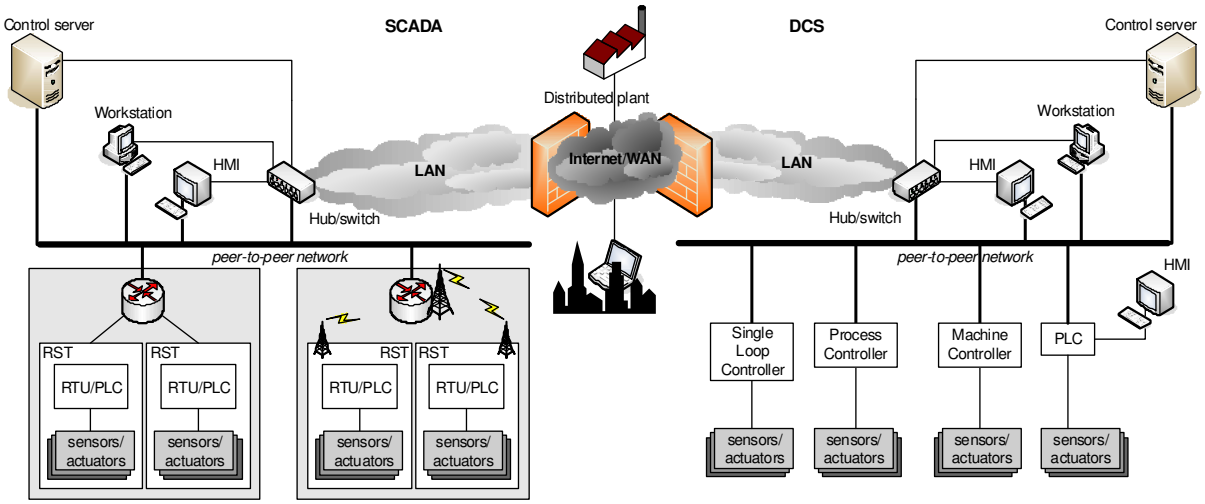

Fig.2 Example of DCS and SCADA architectures

area network. Components include general purpose workstations, printers, databases, application servers and domain controllers. Communication outside the plant is typically established via Internet or WAN using a firewall. The DCS and local SCADA components of a plant typically operate on a peer-to-peer network.

A DCS is comprised of a supervisory layer of control and one to several distributed controller units within the same processing plant. The supervisory controller runs on the control server and communicates with its subordinate units via a peer-to-peer network. The supervisor sends set points and receives data from distributed controllers. The distributed controllers control their associated process actuators based on requests from the supervisor and process sensors feedback. The communication of controller with its sensors and actuators is typically realized using a local field bus eliminating the need of point-to-point connection between the controller and each of these devices. There are several types of control units used in distributed control points of a DCS. In dependence of application the most widespread are machine controllers, programmable logic controllers (PLC), process controllers and single loop controllers.

A typical SCADA consists of a Central Monitoring System (CMS) and one or more Remote Stations (RST). The CMS houses the Control Server and the communication routers via a peer-to-peer network, collects and logs information gathered from by the remote stations and generates necessary actions. A remote station consists of either a Remote Terminal Unit (RTU) or a PLC which controls actuators and monitors sensors. In most cases the RST has a capability of diagnostic and repair functions interfaced via some type of portable computer. The communication channel between remote stations and the CMS is realized using metallic line, optical line or radio frequency with repeaters, where necessary.

Networked control system architectures which include continuous operations of transformation of raw materials into usable products, follow the DCS scenario. On the other hand, the network architectures supporting distribution operations of usable products, copy the structure of SCADA.

3. VULNERABILITIES AND IT THREATS

As we said before, in the sphere of process control, the IT security has been of minimum importance. Systems were primarily designed to meet performance, reliability, safety, and flexibility requirements and were typically physically isolated and based on proprietary hardware and communication systems. The introduction of Internet based information technology within the process controls industry has increased vulnerabilities to the industry's computer systems. Centralized operation and remote maintenance of industry systems performed over public telecommunication networks provides potentialities for threatening influences of this critical infrastructure. DCS and SCADA systems that operate on commercial hardware and software, combined with connections to external networks, allow a simplified invasion and possible devastation of these systems. In the survey [2] which has been performed on a sample of organizations with 100 and more employees in different sections of industry, business, services, and state administration, 75% of respondents pointed the occurrence of security incidents caused by viruses, 28% caused by LAN failure, and 24% due to WAN failure. The treats can originate in different sources: despiteful invader, terrorist group, disgruntled employer, hostile government, but also accident and natural disaster.

4. THE COMMON CRITERIA (CC) PROJECT

The goal of the Common Criteria (CC) project was to develop a standardized methodology for specifying, designing, and evaluating IT products that perform security functions which would be widely recognized and yield consistent, repeatable results independently of technology and implementation [3].

The three-part CC standard ISO/IEC 15408, and the CEM are two major components of the CC methodology, as shown in Fig. 3.

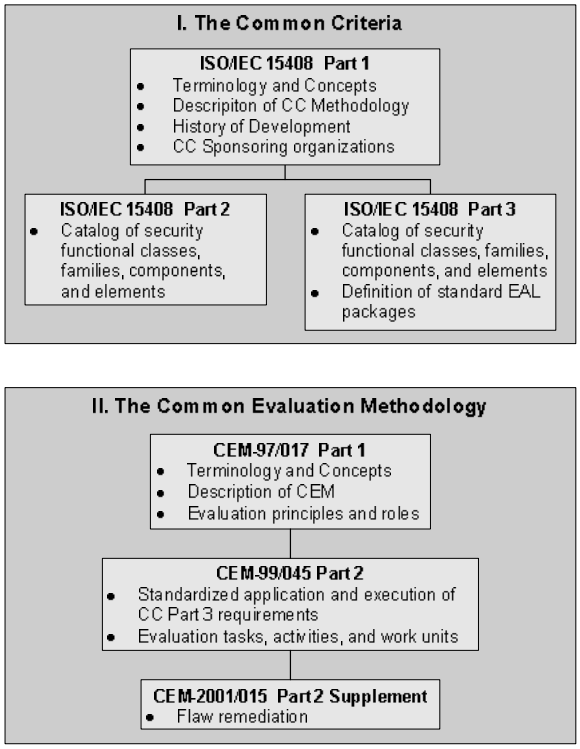

Fig.3 Major components of the CC/CEM

Four key concepts are presented in Part 1 of the standard:

1. Protection Profiles (PPs),
2. Security Targets (STs),
3. Targets of Evaluation (TOEs),
4. Packages.

A Protection Profile is an implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs [4]. Security Target denotes a set of security requirements and specifications to be used as the basis for evaluation of an identified TOE. Target of Evaluation is an IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation. A package is a reusable set of either functional or assurance components (e.g. an Evaluation Assurance Levels), combined together to satisfy a set of identified security objectives.

5. ITU-T RECOMMENDATION X.805

The Recommendation defines general security-related architectural elements that appropriately applied can provide end-to-end network security [5].

The architecture shown in Fig. 4 can be used with different network elements, services, and applications in order to detect, predict, and correct security vulnerabilities.

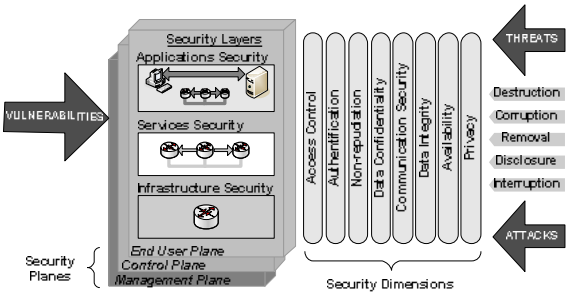

Fig. 4 Security architecture for network security

A Security Dimension is a set of security measures designed to address a particular aspect of the network security. The Recommendation X.805 identifies eight such sets that protect against all major security threats: 1. Access Control, 2. Authentication, 3. Non-repudiation, 4. Data Confidentiality, 5. Communication Security, 6. Data Integrity, 7. Availability, and 8. Privacy.

In order to offer the flexibility of countering the potential threats there are three security layers defined: the Infrastructure Layer, the Service Layer, and the Application Layer. The security Layers identify where security must be addressed in elements and systems by providing a sequential perspective of network security.

The Management Security Plane, the Control Security Plane, and the End-User Plane are a certain type of network activity protected by Security Dimensions. Networks should be designed in such a way that events occurred on one Security Plane are kept totally isolated from the other Security Planes.

The architecture identifies security issues that need to be addressed in order to prevent both intentional as well as accidental threats. The following threats are described [6]:

- destruction of information and/or other resources,
- corruption or modification of information,
- theft, removal or loss of information and/or other resources,
- disclosure of information,
- interruption of services.

The intersection of each Security Layer with each Security Plane represents a security perspective

where Security Dimensions are applied to counteract the threats. Table 1 shows mapping of Security Dimensions to the designated security threats.

Table 1 Mapping Security Dimensions to security threats

SECURITY DIMENSION	SECURITY THREAT				
	Destruction	Corruption, Modification	Theft, Removal, Loss	Disclosure	Interruption
Access Control	■	■	■	■	
Authentication			■	■	
Non-Repudiation	■	■	■	■	■
Data Confidentiality			■	■	
Comm. Security			■	■	
Data Integrity	■	■			
Availability	■				■
Privacy				■	

6. CONCLUSION

Previously we introduced the issue of securing distributed industrial process control systems build on DCS or SCADA system architecture with WAN or Internet connectivity. Such connectivity to public accessible networks makes these systems potential targets of attacks on their vulnerabilities.

The objective of ITU-T Recommendation X.805 is to give developers a comprehensive top-down basis for creation of detailed recommendations for the end-to-end network security independently of the network's underlying information technology or protocol stack.

The Common Criteria project is applicable as a guide for the evaluation of systems with IT security functions and IT security measures implemented in hardware, firmware, or software. The specific Target of Evaluation can be a particular network element but also an entire subsystem or network.

Usage of combination of these frameworks in design, implementation and evaluation of distributed control systems applied in today's industry will lead to minimization of security threats impacts.

Further work in field of application and development of methodologies for increasing security of distributed industrial control systems will continue.

REFERENCES

[1] Falco, J., Stouffer, K., Wavering, A., Proctor, F.: *IT Security for Industrial Control Systems.* National Institute of Standards and Technology, Gaithersburg (2002).

[2] *Information Security Survey in the Slovak Republic 2004.* KPGM Slovensko, DSM – data security management, NSA SR (2005).

[3] Herrmann, D.S.: *Using the Common Criteria for IT Security Evaluation.* Auerbach Publications (2003).

[4] *Common Criteria for Information System Security Evaluation, Version 2.1,* (1999).

[5] *Draft ITU-T Recommendation X.805 (Formerly X.css), Security architecture for systems providing end-to-end communications.* ITU (2003).

[6] *CCITT Recommendation X.800, Security architecture for Open Systems Interconnection for CCITT applications.* CCITT, Geneva (1999).