Industrial IT Security in Embedded Systems -
What does the standard IEC 62443 perform?

By Dipl. Ing. (FH) Sebastian Schmidt

The networking of computer systems does not stop in front of the industrial systems. The traditional embedded systems are becoming Cyber-Physical Systems. Cyber-Physical systems are systems with software and electronics, which are linked by sensors and actuators with the outside world through the Internet. With the aid of sensors, these systems process data from the physical world and make them available to the virtual outside world, which in turn can have an outcome through the actuators directly to procedures in the physical world. The “internet of things” is formed. This provides the technological basis for the "Industry 4.0" - a future project launched by the German government in 2011. Nowadays, internationally the term "Industry 4.0" is synonymous with the networking of industrial plants.

With the increment of networking and the exchange of information between the systems, however, the standards of security and availability also increases. The recent standardized hardware and software components that have been developed for the simplest possible integration and universal communication, are frequently vulnerable to attacks and manipulations.

A renowned example is the “Stuxnet” virus. The malware was identified in 2010 and it was developed specifically for the Siemens SPS Simatic S7. Thereby, it was attacked in the control of frequency converters, which led to perturbations in Iran's nuclear facilities.

Nowadays, Embedded Systems are used for a variety of tasks and are generally needed to measure, regulate and control all types of devices and systems. Originally developed as autonomous systems, many facilities are not sufficiently protected from attacks.

How can we protect the industrial facilities with your networked control units from enemy attacks, sabotage and espionage? The topic of Industrial IT Security is exactly related to this issue.

The Standard IEC 62443 family offers an integrated approach to the protection of Embedded Systems in industrial facilities.

The Standard IEC 62443 can be seen as an industry-specific reaction by international bodies to this new threat and is specifically addressed to the safety of industrial environments of management and control.
The standard family entails four groups:

1. The documents with the start numbers IEC 63443-1 give an introduction to the philosophy of standards and explicate terms and concepts which are based on the standard.
2. The documents with the initial numbers IEC 62443-2 describe and enlighten a management system for IT security management and control systems in industrial environments. This management system is referred to as Cyber Security Management System (CSMS).
3. The third group (documents with the initial numbers 62443-3) deals with the safety necessities for a so-called Industrial Automation and Control System (IACS). This IT system consists of several components like: the SCADA application, PLC, fieldbus as well as actuators and sensors which is intended to control process or production lines.
4. In the last group, all documents are summarized which are related to the IT security of the individual components of IACS. Both requirements here are defined for the components themselves as well as to the development process.

<table>
<thead>
<tr>
<th>IEC 62443</th>
</tr>
</thead>
<tbody>
<tr>
<td>General 62443-1</td>
</tr>
<tr>
<td>Terminology, concepts and models</td>
</tr>
<tr>
<td>Glossary of terms and abbreviations</td>
</tr>
<tr>
<td>System security compliance metrics</td>
</tr>
<tr>
<td>IACS security lifecycle and use-case</td>
</tr>
</tbody>
</table>

Figure 1: An overview of the standard family IEC 62443

IEC 62443 adopts an integrated approach, since both the CSMS Management System as well as the control system for industrial environments and its components are addressed. Among other things, IEC 62443 accomplishes the following seven areas of work - the "Foundational Requirements”:

- **Access Control (AC):** guarantees that all users (people, software processes and devices) must successfully identify and authenticate so that they are allowed to access the system.
- **Use control (UC):** The use of a certain equipment, information, or both will be monitored so as to prevent unauthorized operation of the device or unauthorized use of information.
- **Data Integrity (DI):** The integrity of data in certain communication channels is safeguarded to prevent unauthorized data exchange.
- **Data confidentiality (DC):** Communication channels are protected from eavesdropping, in order to guarantee the confidentiality of specific data.
• Restricted DataFlow (RDF): The data flow in communication channels is restricted in order to prevent unauthorized lowering before the disclosure of information.
• Timely response (TRE): In case of violations of IT security there will be a reply through a notification within a defined period and corrective activities are initiated.
• Resource availability (RA): The availability of all network resources is ensured for protecting against service attacks denials.

These fields are prepared structurally for example, in IEC 62443-3-3 the Security Requirements for an Industrial Automation and Control System (IACS). The requirements for the IACS are getting higher with an increase in the Security Level (SL). The LS designates the strength of an attacker on a scale with four levels.

These designate the categorised application which begin with an expected attacker:

• SL 1: random misapplication
• SL 2: deliberate attempts with simple means
• SL 3: the same as SL2, but with knowledge and appropriate means
• SL 4: the same as SL but with significant means

According to the stage in the lifecycle, the Security Level can be distinguished among:

• SL-T (target SL): seeking to attain security level is a result of the threat risk analysis. This review is specified generally in the design of an automation solution (ie, in the design phase) to define the appropriate level for ensuring the appropriate operation in terms of security.
• SL-C (SL Capable): Security Level that can attain a device or system theory
• SL-A (SL Achieved): The Security Level that is actually reached in the entire system and is measurable. This level of defence is determined after a system has been considered and configured as a clarification of an automation project, to reach the target SL. If the Capability SLs of components and systems, forming the components of the automation solution, to achieve the desired target SLs are not enough, then there may be necessary additional measures, like, for instance, the use of supplementary security mechanisms for boosting the level of protection.

Further concepts perform IEC 62443 security zones (zones) and communication channels (conduits). Zones represent a set of logical or geographically connected components of the Industrial Automation and Control System (IACS) that share similar security level. Zones are linked to each other through conduits consequently forming a communication channel. Conduits are the only means of communication among the zones.
Collaboration between Safety and Security

There are noticeable the parallels to the concepts of functional safety. One will find here related concepts like, for instance, the access protection of unsafe components to secure data. Though, the similarities are not simply technical in nature. The development processes flows as well similarly in both standards. From an economic standpoint, a certificate in accordance with IEC 62443 to any liability claims for damages is recommended for the future in order to be able to protect yourself from the attacks.

In summary it can be mentioned that the IEC 62443 helps to accomplish a global tactic to the IT security of management and control systems that comprises both the management of IT security and the safety of systems and components.

The protection in the entire life cycle of the automation solution is influenced more by additional actions under the security management, like the physical protection, the management of users and their rights or the consistent operating a Patch Management. Some issues that are associated with the SL-concept are still unclear.

On the whole, though, a manufacturer as well as system integrators and operators will benefit from the developments. It is realistic to anticipate that the need for security in Embedded Systems concepts will continue to increment. Nevertheless, it remains to be seen whether the concepts of IEC 62443 will succeed in the longer run and attain the amplitude in the industry, since a high dynamics of technology often cannot withstand so well with the paper inactivity.
Sebastian Schmidt, Dipl.-Eng. (FH), is the founder of tech-informatik UG and a specialist of the safety and Security applications in Embedded Systems.