Security protection to industrial control system based on Defense-in-Depth strategy

X. Luo
The College of Mechatronics and Information Engineering, Shanghai Lida Polytechnic Institute, China

Abstract

In this paper, I analyze vital information related to security problems faced by various industrial control systems (ICSs) and introduce the Defense-in-Depth strategy, which is widely used. I especially focus on the structure framework of ICSs based on the Defense-in-Depth strategy and the corresponding protective measures.

Keywords: Defense-in-Depth strategy, industrial control system (ICS), information security.

1 Introduction

German Federal Ministry of Education and Research (BMBF) and Federal Ministry of Economics and Technology (BMWi) put forward the concept of “Industrial 4.0” in HANNOVER MESSE 2013. The Chinese government issued “Made in China 2025” recently. The fusion of industrialization and information will go up to a higher level. In such a new wave, intelligent manufacturing (IM) is one of the most important core content. Industrial control system (ICS) as the key fundamental hardware of IM, along with the application of new technologies – network, embedded, human–computer interaction, and three-dimensional technology – will have broader developing prospects, but meanwhile, inevitably has to face huge information security challenges.

Generally, the safety of ICS includes physical safety and information security [1, 2]. Physical safety refers to whether a system and devices are sound enough to prevent damages, casualties, and social security incidents. IEC62443 defines
information security of ICS as: “The measures that are taken to protect system; the system state that is established and maintained by the protection measures; the ability that avoids unauthorized access or damage to system resources, but enables the authorized personnel and systems working well, etc.”

In recent years, this issue drew remarkable attention from an increasing number of researchers or organizations and gradually saw the development of relatively mature technology norms and standards. For example, the U.S. National Institute of Standards and Technology issued a series of guidelines, including “SP 8000-82,53,” “medium robust environment SCADA system overview,” and other field equipment protection. The U.S. Department of Energy released guidelines including “21 Steps to Improve Cyber Security of SCADA Networks”.

Owing to ICS’s complex architecture, the function of each component is different, the vulnerability of the component to attacks is varied, and demands of security are different from each other. So it is impossible for a single countermeasure or technology to keep ICS secure from attacks. According to the enterprise business process and ICS’s practical security requirements, this paper proposes a security defense structure for ICS based on the Defense-in-Depth strategy.

2 Defense-in-Depth strategy

Defense-in-Depth is the coordinated use of multiple security countermeasures to protect the integrity of the information assets in an enterprise. The strategy is based on the military principle that it is more difficult for an enemy to defeat a complex and multilayered defense system than to penetrate a single barrier.

ANSI/ISA – 99 suggests that ICS should use the Defense-in-Depth strategy to improve its security. It points out that “defense-in-depth refers to layered or stepped method to provide multiple protections.” According to The Guide to Industrial Control Systems Security (GICSS) SP800-82 proposed by National Institute of Standards and Technology (NIST), “defense-in-depth framework includes the application of firewalls, establishment of demilitarized zone, intrusion detection and effective security policy, training program and the time response mechanism.”

2.1 Security requirements and measures in Defense-in-Depth strategy

(1) Security policy

An effective security policy is the first step to protect a control system. But these policies cannot have much impact on production. Managers and system administrators should participate in the development of security policies [3].

(2) Security training

Improving security awareness is crucial to the security of ICS. It was specifically pointed out in NIST SP800-50 to build a training program to improve information technology security awareness [4].
(3) Incident response

Strong incident-response ability is required to fully support the Defense-in-Depth strategy. The system should set up recognition, response, and recovery behaviors when security-related incidents occur [4].

(4) Intrusion detection system (IDS)

Most IDSs are based on signature. Although many current IDS signature files are very robust and can detect a wide range of attacks, it is not enough to detect all malicious connections in a control network. In the special communication protocols of a control system, such as Modbus and DNP3, their special port numbers have not become a part of the current IDS [4]. When deploying an IDS in a control system, special signatures must be added and some default signatures and responding functions that have nothing to do with the control system network should be removed.

(5) Minimization of platform services

Unnecessary services and programs should be removed as much as possible while configuring the operating system of a control system [5].

(6) Minimization of connections

To avoid a direct connection, proxy gateway must be set up based on ICS’s application program and network protocol [5].

(7) Maintenance of backdoor of services

The backdoor of services should be continually maintained to reduce security risks [5].

(8) Evaluation of hardware, software, and their configuration library regularly

Sustainable security is built on the continuous cycle of planning, implementation, review, and enhancement [5].

2.2 Principle of division in Defense-in-Depth strategy

To carry out an effective hierarchical protection, control system architecture should be divided into different regions and the boundaries between them must be clear. The National Security Agency suggests a way to classify regions according to the following basic factors [6]:

(1) External region

External region is the zone connected to the Internet or remote long-distance facilities. It is often considered unreliable, having the lowest priority and the highest risk.

(2) Enterprise region

Enterprise region is the area connected to enterprise communication. It includes email server, DNS server, and IT infrastructure components. Because the number of systems in this region is large, and they connect with the external region, there are significant risks in this region. Its priority is higher than the external region, but lower than other regions.

(3) Manufacturing/data region

A large number of monitoring and controlling behaviors are carried out in this region. It is the midpoint between terminal equipment and business
requirements. Its main risks lie in direct connection with the external region and the enterprise region. Its priority is higher than before regions.

(4) Control region

Control region refers to regions that connect with PLC, HMI, and input/output devices. It has a very high priority because the functions of the equipment in this region affect the physical terminal device.

(5) Safety region

Devices in the safety region can automatically control the security level of terminal equipment. It has the highest priority. In general, this region has less risk because the equipment only connects to terminal devices. But recently, to realize remote monitoring and redundant support, an increasing number of equipment began to support TCP/IP connections.

Each region has different security concerns, so defense-in-depth countermeasures are made up of a collection of effective methods to protect each region.

3 Application of Defense-in-Depth strategy in ICS

3.1 Requirements of security defense measures in ICS

Table 1 lists security precautions put forward by International Industry Standard ANSI/ISA – 99, which are well known in the industrial control field [7].

Table 1: Security precautions put forward by International Industry Standard ANSI/ISA – 99.

<table>
<thead>
<tr>
<th>Name</th>
<th>Main point</th>
<th>Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td>To divide the regions</td>
<td>Equipment with the same function and security requirements is assigned to the same region</td>
<td>To divide security hierarchies</td>
</tr>
<tr>
<td>To establish a pipeline</td>
<td>To execute the pipeline communication between various regions</td>
<td>To ensure the data security is easy to control</td>
</tr>
<tr>
<td>To control communication</td>
<td>To protect equipment by controlling the communication in pipeline between regions</td>
<td>To control data communication</td>
</tr>
</tbody>
</table>

Equipment with the same function and security requirements is assigned to the same region. The pipeline communication is executed between regions. Information security of ICS is ensured by controlling the communicating content in pipeline between regions.
3.2 ICS structure based on Defense-in-Depth strategy

3.2.1 Division of ICS network into three layers in vertical

From the perspective of enterprise business process, the industrial system network can be divided into three layers: Enterprise Management Layer (EML), Data-acquisition Information Layer (DIL), and Industrial Control Layer (ICL) [7] (Fig. 1).

EML mainly refers to management information service (MIS), which contains many subsystems, such as production management, financial management, quality management, and sales management. It uses Office Automation System to extract relevant production data from DIL for management decisions through the general Ethernet [8].

DIL mainly receives data from ICL to complete various control, monitor operating parameters, warn against abnormal data and analyze trends, etc.

ICL is made up of all types of automatic control components, real-time data-acquisition and process control components. This layer is in charge of completing the tasks of data-acquisition, A/D conversion, etc.

3.2.2 Division of ICS network into security regions at same layer

Security region refers to the subnet that has the same security protection requirements. They trust each other, and have the same security access control and border control strategy in a system [8]. For additional security and reliability requirements, the main security region can be further divided into subregions according to the operation function.

According to ANSI/ISA – 99, combined with the security needs of ICS, the industrial system network can be divided into five safety regions [7] (Fig. 1):

1. Enterprise IT network region: An office area that meets the needs of office terminals
2. Process information/data region: The DMZ to satisfy the demand of online businesses
3. Administration/HMI region: The management area that meets the needs of management and monitoring to ICS
4. Industrial control region: The control region to fulfill the automatic operation
5. Third-party control system region.

Generally, owing to different application scenarios in different industries, the division of functional region and requirements for security protection are different.

3.3 Security protection between layers

3.3.1 Security protection between EML and MES

The main security problems between EML and DML are the threats while exchanging data between MIS and MES, such as unauthorized and abused authority, operating mistakes, falsifying data maliciously, denial behaviors, illegal intrusion, and malicious code (viruses and worms). Security protection between EML and
MES, therefore, ensures that only the appropriate terminal and server can exchange data safely between the two layers. At the same time, the data exchange should be monitored and audited in the whole process [8].

Traditional IT firewall can be put between EML and DML [7]. It only allows legal data exchange between two networks and blocks unauthorized illegal access from EML to DML. Meanwhile, it can prevent virus infection from EML and prevent their spreading to the whole control network.

3.3.2 Security protection between MES and ICL
The process data usually needs to be sent to the enterprise information network through a data-acquisition server. Depending on its openness, the enterprise information network can be more easily infected by virus than the control network. So OPC communication protocol is often used during data transmission. Because its port number is not fixed, traditional IT firewall protection is not suitable. Therefore, professional industry firewalls must be installed between the data-acquisition layer and the control layer. And permission values are set in order that only the data-acquisition server is allowed to communicate with the lower OPC server in OPC communication mode to avoid effectively spreading virus [8]. Figure 1 describes the security protection between layers.

3.3.3 Security protection between regions
Information assets that have the same or similar value, security level, security environment, and security strategy should be divided into the same security region. And then, the corresponding security protection technology and management measures should be adopted to ensure information security.

In addition, security protection between EML and MES and between MES and ICL is used not only between layers but also between regions.

3.3.4 Protection of key controller
Communication between the management/HMI region and the controller generally uses specific industrial communication protocols, such as Modbus, which should be protected by professional industrial firewall. It is in charge of the network flow and traffic rate, and allows only a proprietary operating station to access the specified controller in order to prevent it from being influenced by network virus or other attacks [7].

3.3.5 Protection of engineer station and APC node
Engineer stations and APC control nodes are located in DML and ICL. They often need to access third-party equipment (such as U disk and notebook PC). So they have higher security risks and are more easily attacked and invaded by virus. Therefore, industrial firewalls must be put in place before engineer stations and APC nodes to isolate them from the rest of the control system. The industrial firewall allows only the APC node to communicate with the control network using specific communication protocol (such as OPC protocol). It can also ban all other illegal communications and prevent the virus from affecting the rest of the network [9].
3.3.6 Security protection between third-party control systems and ICS
Third-party control systems, such as Safety Instrumented System and Digital Electro-hydraulic Control System, communicate with ICS through Modbus communication protocol. Industrial firewall should be used to isolate third-party control systems and other networks. Its main purpose is to ensure that two regions can safely exchange data, only legal credible, authorized access, and communication can pass the communication pipeline.

4 Discussion

According to the general working process and specification of ICS, this paper analyzes the security protection of ICS based on the Defense-in-Depth strategy, namely layered, subregional, hierarchical security protection. It focuses on security protection in the physical structure. But in practical application, the implementation may differ from network to network and application to application in detail.
In addition, as mentioned by NERC [10], “Technical solutions only account for 20% of all the protection methods for ICS. The other 80% is made up of the standard behavior and security sense of personnel. It is even more challenging.”

5 Conclusions

Safety and information security are vital for an ICS. In accordance with the enterprise business process, and combining with network structure and ICS’s security requirements, and in reference to the international industry standard ANSI/ISA – 99, this paper proposes a framework for ICS based on the Defense-in-Depth strategy. The system protects ICS by establishing vertical layers, horizontal regions, and security measures between layers and regions.

The Defense-in-Depth strategy is a safety precaution widely recognized and applied in the industrial control field. But in practical application, unrealistic and blind defense should be avoided in case excessive defense affects the performance of a system and leads to a waste of resources.

References


