Analysis of ICS and Corporate System Integration Vulnerabilities

K. ES-SALHI1, N. Cuppens-Boulahia1, D. Espes2 and F. Cuppens1
1LabSTICC, Telecom Bretagne, Cesson sevigne, France
2LabSTICC, University of Western Brittany, Brest, France

Abstract—Integrating industrial control systems (ICS) with Corporate system (IT) is becoming a necessity in the current industrial business world. The benefits of this integration are numerous but not without a strong risk. Indeed, the integration of ICS and IT systems exposes both to many security problems. Hence, securing this interconnection becomes one of the major priorities of the industrial sector. In this paper, we present a summarized overview of integrated ICS vulnerabilities, we evaluate the state of art of existing countermeasures and we suggest some research subjects that may be necessary to ensure integrated ICS security. For this purpose, we have studied several known security standards such as ISA, NIST and other papers on ICS systems convergence.

Keywords: Cyber security, Vulnerabilities, ICS, SCADA, ICS Corporate systems Integration.

1. Introduction

Industrial control system (ICS) is a general term that encompasses several types of control systems used in industrial production, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations often found in the industrial sectors and critical infrastructure [1].

The industrial business world presently has a real need to integrate industrial control systems (ICS) with Corporate systems [2]. The benefits of this integration include increased visibility of industrial control system activities, ability to use business analysis to optimize production processes and gaining more responsiveness to the business requirements and decisions. For example, ERP 1 and CRM systems 2

Interconnecting the two networks introduces multiple security problems. Indeed, industrial systems have been designed without security in mind because they have usually been isolated. This is reflected by the use of insecure industrial equipment (devices, protocols ...), the lack of clear security policies and the lack of human resources security training. Therefore, integration exposes both ICS and Corporate systems to major security threats. Moreover, ICS and Corporate systems are different by their nature and have different security requirements in terms of confidentiality, integrity and availability. ICS security focuses on availability, plant protection, plant operation, control complexity and time-critical systems response while Corporate security focuses on protecting information. Hence, responding to the integrated system security’s needs cannot be accomplished using only known IT security skills. In addition, ICS teams have unfortunately no knowledge about cyber security and, on the other side, IT security specialists have insufficient knowledge about industrial systems.

This paper presents an overview of Integrated ICS systems vulnerabilities and countermeasures identified by other studies and security standards trying to answer the following questions:

- What are the identified problems and needs?
- What security measures they suggest?
- Are the existing Integrated ICS security countermeasures sufficient and implementable?

We will especially focus on vulnerabilities and countermeasures directly related to the integration between ICS and Corporate network. Internal ICS network vulnerabilities will not be covered by this paper.

Section 2 presents architectural models of integrated ICS systems in order to illustrate ICS and Corporate systems boundary. Defining this boundary was very important to classify integration vulnerabilities. These vulnerabilities will be presented in Section 3. Section 4 discusses the existing countermeasures. It provides an analysis of the sufficiency of these measures as well as some suggestions for future work.

For the rest of this document, we will use the abbreviation IICS to refer to “Integrated ICS”. An IICS is an ICS that is integrated with its organization’s Corporate system.
2. IICS architecture

IICS systems have various architectures and infrastructure compositions depending on different aspects such as the industrial sector, the production activities and the size of the organization. Actually, industrial sector determines the needs within the industrial system and has a direct impact on the infrastructure configuration and architecture of the IICS.

There are two main industry sectors:

- Manufacturing industries including "Continuous manufacturing Processes" (e.g., fuel or steam flow in a power plant) and "Discrete-based manufacturing industries" (e.g., Electronic and mechanical parts assembly),
- and Distribution industries (e.g., water distribution and wastewater collection systems).

The two industry families have different characteristics and needs. For example, in terms of localization, manufacturing industries are usually located within a confined factory or plant-centric area, whereas distribution industries are geographically dispersed. Moreover, communication in manufacturing industry are usually performed using LAN while distribution industry systems usually communicate through WAN [1] [3].

Identifying vulnerabilities of all IICS configurations is unfeasible. Therefore, the goal of the first part of our work was to establish a reference architecture. This will be presented in the next subsection. Besides, ICS and Corporate system integration requires enclosing the boundary between them. This boundary is identified using relevant models that represent functions, physical equipment, information within the whole system.

2.1 Reference architecture

Our study is mainly based on the hierarchical functional model provided by ISA-95 [4]. This model is based on the Purdue Reference Model for CIM on the MESA International Functional Model. It depicts the different functional levels (figure 1) that define hierarchical levels at which decisions are made and underlines the relationship between Business and Industrial activities. In other words, it gives a high level picture of the functional architecture of an IICS. It also outlines ICS and Corporate system functional integration at the interface between Level 4 and Level 3. This interface is between plant production scheduling and operation management and plant floor coordination.

The five functional levels inside an IICS are [4]:

- **Level 4 - Enterprise Business Systems**: This level is described as "business planning and logistics". It includes the functions involved in the business-related activities.
- **Level 3 - Operations Management**: This level includes the functions involved in managing and optimizing the production work flows.
- **Level 2 - Supervisory Control**: It includes the functions involved in monitoring and controlling the physical process.
- **Level 1 - Local or Basic Control**: It includes the functions involved in collecting data and manipulating the physical processes. This level contains process monitoring, safety and protection equipment that monitor the industrial processes and automatically return them to a normal state when unwanted events occur.
- **Level 0 - Process**: It is the actual physical process. It includes sensors and actuators directly connected to the production process.

2.2 IICS main components

IICS functions involved in the 5 levels listed above, are implemented using multiple software and hardware components. Figure 2 provides a quite complete list of these components relating them to the hierarchical model.

1) **Level 4: Enterprise and Business system**
   - ERP: Enterprise Resource Planning is a category of business-management software i.e., typically a suite of integrated applications that an organization can use to collect, store, manage and interpret data from many business activities.

2) **Level 3: Operational Management**
   - MES: Manufacturing Execution System is a computerized system used in manufacturing to track and document a manufacturing process. MES can provide the right information at the right time and show the manufacturing decision maker "how the current conditions on the plant floor can be optimized to improve production output"[1] MES might be seen as an intermediate system between an Enterprise Resource Planning (ERP) system,
and a Supervisory Control and Data Acquisition (SCADA) or process control system.

3) **Level 2: Supervisory Control**
   - **SCADA:** Supervisory control and data acquisition systems integrate data acquisition systems to provide a centralized monitoring and control system for numerous process inputs and outputs. Supervisory control layer contains the top level components of SCADA to which we refer as control centers.
   - **Control Center:** It is the central part of a SCADA system. It collects and logs information received from other SCADA components and may generate actions based upon detected events. It is composed of the following elements:
     - **SCADA control Server** (usually called the master): It is a software service that is connected to field devices using industrial protocols, exposes acquired supervision data, and sends controls.
     - **HMI:** It is an operators interface specifically designed for monitoring and control of other SCADA components.
     - **Historian:** It is a data storage server that is used to store history data.
     - **Engineering workstations:** It is a computing unit, generally an ordinary computer, that industrial engineers mainly use to configure industrial control components (especially PLCs and RTUs...).
     - **OPC:** It is a software interface standard that allows Windows programs to communicate with industrial hardware devices.

4) **Level 1: Control**
   - **Field Sites:** Field sites are local or remote and are composed of devices directly responsible of data acquisition, logical operations and controls. A field site contains generally:
     - One or more **PLC** or **RTU** which are central sophisticated devices that directly interact with sensors and actuators in the site.
     - And sometimes a local computer connected to RTU/PLC for configuration.
     - **PLCs** are digital devices used for automation of industrial electromechanical processes. They connect to sensors in the process and convert their signals to digital data.
     - **RTUs** (remote terminal unit) are microprocessor-controlled electronic devices that interface sensors and actuators by transmitting telemetry data to the SCADA Server, and by using messages from the master supervisory system to control connected objects.

5) **Level 0: Process**
   - **Sensors and Actuators:** Devices involved in the actual physical industrial process.

2.3 **IICS logical architecture**

The previous model also highlights the functional boundary between Enterprise system and Industrial system. It is illustrated by the dashed line between level 4 and level 3. We are especially interested in the exchanges and data flows that cross this line. Our IICS architecture is composed of three zones:

- Enterprise zone: Level 4
- Enterprise, industrial system integration zone: Interface between Level 4 and Level 3
- Industrial system zone (ICS zone): This zone is the actual ICS including all the 4 lower levels of the hierarchical model.

IICS functions involved in the 5 levels listed above, are implemented using multiple software and hardware components. Figure 2 illustrates a logical reference architecture that will constitute the basis of our work. This figure also illustrates the three IICS zones.

Communication across the integration zone is needed for multiple purposes and involves different components. For example, coordination between business and industrial activities usually require connecting Enterprise Resource Planning (ERP) system with Manufacturing Execution System (MES) or SCADA historian. Table 1 gives some examples of flows considered to be necessary between the Industrial system and the Corporate system.

### 3. Vulnerabilities and challenges

By connecting ICS and Corporate networks, a lot of security problems arise. It is mainly because ICS networks are heavily predisposed to be vulnerable. The predisposing...
Table 1: Some examples of flows between ICS and Corporate systems [5].

<table>
<thead>
<tr>
<th>Flow Type</th>
<th>Example</th>
<th>Used protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applicative data flows</td>
<td>-Production scheduling data</td>
<td>JCA, Web Services (Http(s), FTP(s), SQL) TCP;IP</td>
</tr>
<tr>
<td></td>
<td>-Production Cost accounting</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-Industrial Processes supervision data</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-Material and energy management data</td>
<td></td>
</tr>
<tr>
<td>Supervision data flows</td>
<td>Devices supervision and monitoring</td>
<td>PING ICMP, SSH, TELNET, TCP;IP</td>
</tr>
<tr>
<td>Other flows</td>
<td>Emailing</td>
<td>Http(s), SMTP(s), IMAP(s), POP</td>
</tr>
<tr>
<td></td>
<td>DNS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Printing</td>
<td>TCP</td>
</tr>
<tr>
<td></td>
<td>Remote maintenance</td>
<td></td>
</tr>
</tbody>
</table>

conditions range from human and organizational problems such as no training of personnel or lack of security policy, to Infrastructural and Architectural problems such as use of insecure protocols, lack of consideration of security in architecture and design. Moreover, low-cost IP-based devices are now replacing proprietary solutions, which increases the possibility of cybersecurity vulnerabilities and incidents.

IICS systems could be highly vulnerable if no countermeasures are taken. According to many research works [1], [3], [6], [7], [8], [9], a quite exhaustive list of vulnerabilities issued by IICS systems can be provided. We collected, grouped and evaluated these vulnerabilities in order to assess the state of art and identify issues that are not (or not completely) addressed yet. We are particularly interested in vulnerabilities related to ICS integration.

IICS vulnerabilities can be categorized in two categories [1]:

1) **Policy and Procedure vulnerabilities**: This category contains the vulnerabilities that arise because of incomplete, inappropriate, or nonexistent security policy, including its documentation, implementation guides (e.g., procedures), and security enforcement.

2) **System vulnerabilities**: This type of vulnerabilities includes:
   - Architecture and Design vulnerabilities,
   - Communication and Network vulnerabilities,
   - Configuration and Maintenance vulnerabilities,
   - Physical vulnerabilities,
   - Software Development vulnerabilities.

Configuration and Maintenance, Physical and Software Development vulnerabilities already exist in both ICS and Corporate systems even without them being integrated. They are less impacted by the integration process. However, Architecture and Design vulnerabilities, Communication and Network vulnerabilities and Policy and Procedure vulnerabilities can be severely strengthened by the interconnection of the two worlds as they are directly related to the integration process. We particularly focus on these types of vulnerabilities.

For the sake of this study, we made a quite exhaustive list of IICS vulnerabilities that belong to these categories. Below a summary of these vulnerabilities:

1) **Architecture and Design vulnerabilities**

   This category is tightly related to ICS integration process. In fact, integrating an ICS system with a Corporate system consists of interconnecting components from the ICS system to components from the Corporate system for some functional or technical purpose ensuring their communication, their interoperability, their security as well as the whole system security. Unfortunately, ICS architectures are definitely not designed to be integrated with Corporate systems’ architectures from a security perspective. Indeed, most of ICS architectures do not make use of segmentation which means that all the components in the system are on the same low level of security. Besides, authentication, encryption of exchanged and stored data, logging and traceability mechanisms are mostly absent and the majority of adopted technologies represent serious sources of vulnerabilities. For example, some devices are implemented with no security capabilities (authentication and encryption ...) at all. Some others come with hard coded passwords on their firmware and cannot thus be efficiently secured.

   In addition, industrial temporal requirements prevent equipping components with anti-virus and firewalls to optimize resource usage. Moreover, applications and drivers inter-compatibility requires keeping them on very precise not up to date versions. Even for the most carefully designed ICS systems, cyber security is not seriously applied. For example, proprietary protocols are thought to be secure without any verification and architectural choices tend to very quickly be taken without security consideration.

   Therefore, it is really necessary to pay special attention to architectural aspects at the integration design and
build time. Designers should, in particular, take the existing heterogeneity into account and opt for an architecture that protects against vulnerabilities such as:

- Backdoors and "holes" (either intentional or not) in the network perimeter [7],
- Inadequate segregation [8],
- Usage of technologies with known vulnerabilities [10],
- ICS network used for non-control traffic [1].

Cautiousness should also be exercised when applying architecture modifications and configuration updates to an existing integration layer.

2) Communication and Network vulnerabilities

ICS and Corporate networks integration introduces new communication and network security needs that have never been addressed. Indeed, integration puts a lot of heterogeneous protocols together. On one hand, IT protocols heavily focus on data security and can unfortunately not be used in ICS network in which protocols focus more on availability. On the other hand, ICS protocols (e.g., Modbus/TCP, Ethernet/IP, DNP3) are not designed with security in mind and, worse, the most vulnerable among them are sometimes employed despite their known vulnerabilities. For example, DCOM, a protocol used for OPC, uses RPC which opens multiple ports to establish communication making firewalls configuration difficult. More seriously, with the recent trend of using Commercial of the shell technologies (especially open protocols such as TCP/IP protocols stack and ordinary Windows computers), ICS systems are more vulnerable than ever before because these technologies knowledge is easily available to attackers.

3) Policy and Procedure vulnerabilities

The current ICS systems also present a lot of human related security problems. These problems are direct consequences of two main factors:

a) The lack of personnel training and sensitization program.
b) The absence of a well-defined globally applied security policy that establishes suitable security procedures and constrains human resources to adopt convenient security practices.

As examples of these security policy problems, we may list [1]:

- Lack of configuration management policy.
- Lack of adequate access control policy.

- Lack of adequate authentication policy.
- Inadequate security incident detection and response plan.

Dealing with this type of vulnerabilities in an IICS is quite challenging. ICS and Corporate systems have always formed two separate entities managed by different teams. Corporate systems security policies are significantly more mature than ICS’s ones when they exist. The main difficulty is to define a common security policy that takes into account Corporate and ICS specificity. Corporate security management teams are more qualified to define this common security policy but they do not have enough experience with ICS networks. Defining a concise efficient global IICS security policy is hence far from being straightforward.

4. Analysis and suggestions

For each identified vulnerability, we extracted the related countermeasures suggested by the studied documents, we compared them and evaluate their efficiency to achieve security objectives, their maturity, and their implementability.

Each extracted countermeasure belongs to one of the three following countermeasures families [3]:

- Measures on "People": Assuring employees awareness and training,
- Measures on "Process": Defining security policies and procedures as well as identifying the real security needs,
- Measures on "Technology": Securing equipment and technologies.

NIST-800-82 Annex G [1] (for ICS security measures) combined with NIST-SP-800-53 Annex G [11] (for Corporate system security measures) constitutes one of the most valuable resources on IICS security measures. These two annexes are essentially equivalent except that the first adds specific considerations about ICS security measures. When combined, they offer an absolutely exhaustive list of IICS security measures. The documents we studied, especially these two annexes, generally cover very well
"people" and "process" security aspects. Indeed, these annexes define multiple groups of measures for which they provide important guidance on security policies and procedures. At least, they can be used as a check list that helps to select adequate "people" and "policy" measures for the system to be secured.

Concerning "Technology" vulnerabilities, especially architecture and communication vulnerabilities, the studied documents recommend a set of countermeasures that should be applied to the integrated system. As regards architecture and design vulnerabilities, it is recommended that security be considered from the beginning of any integration project in order to respond more efficiently to both security and operation requirements. This should be done on a case by case basis during the definition phase in which the security perimeter has to be precisely defined. Special attention should be paid to the ICS system temporal and availability requirements as well as risk and safety requirements. Designing the final solution should take into account the existing systems, their components, their communication flows and their heterogeneity. This helps to figure out the upcoming complexity and adequately select measures needed to meet the defined requirements.

Nonetheless, there are still multiple generic security measures that are advocated for IICS systems. Defense-in-depth is one of the most important of them. This very common security technique is mainly based on segmentation and segregation. The latter consists of enforcing a rule-set to control permitted communications through the segments boundaries using firewalls and intrusion detection systems (IDS). Defense-in-depth should be applied at the IICS integration layer by adding a demilitarized zone (DMZ) as a separate segment that only contains the ICS component connected with Corporate system.

Furthermore, multiple other security measures such as using authentication and authorization mechanisms, using secure protocols, monitoring and logging mechanisms, single point of failure, redundancy techniques are also strongly recommended by the studied documents. For a quite exhaustive list of these measures, please refer to the following NIST standards (Annex G) [1] [11].

Despite the amount of useful information provided by the studied documents, there are still several "Technology" vulnerabilities measures that either are absent or need to be completed or detailed. Firstly, most of the suggested countermeasures are directly borrowed from the IT world and do not really take ICS specificity into account. Besides, most of these countermeasures only serve for guidance or as checklist as they lack reference implementation and real application examples. More concisely, the studied documents dictate more what to do than how to do it. That is why we argue that, currently, there are a lot of IICS security requirements that cannot yet be satisfied using the existing solutions. Among the subjects that need more work, we can list:

1) IICS Authentication and Authorization mechanisms:

Authentication and Authorization mechanisms are highly recommended for IICS systems. There are mainly two types of these mechanisms: distributed authorization and authentication solutions and centralized ones. Selecting one solution depends on the organization structures and scalability requirements. However, there are many challenges to integrate authentication solutions, especially centralized solutions, into an IICS [1]. This is because ICS may utilize its own application-specific accounts and authentication mechanisms that are not designed to be integrated with third party servers and protocols. Besides, most industrial equipment do not have any authentication support and even less capability to be integrated with centralized authentication solutions such as AAA architectures.

Using centralized authentication solutions in IICS systems and using AAA architectures and protocols for ICS systems are subjects that still need more work.

2) IICS Segmentation and Segregation:

As explained before, segmentation and segregation are very important security techniques for IICS systems. Unfortunately, we could not find enough details on how to efficiently implement them in an IICS context. Indeed, there are still several questions that remain unanswered [7], [1]. First, no precise explanation was given on how to partition IICS networks into segments. Should the segmentation be based on the components' physical characteristics, on their functions or on their geographical localization? In addition, although segregation rule-sets definition is not trivial, no sufficient explanation was provided.

Furthermore, segmenting large-scale networks is a complicated task for administrators. It is all the more complicated in systems with frequently changing configuration and topology. We did not either find enough information on how to perform segmentation in large-scale networks taking into account architecture changes and configuration updates. This is why we are convinced that IICS Segmentation and Segregation are major elements to
be studied.

3) IICS firewalls:

Segregation ought to employ firewalls to control communication across segment boundaries. To the best of our knowledge, there is unfortunately no firewall fully adapted for all industrial systems configurations [7], [1]. Existing firewalls only support protocols commonly used in Corporate systems especially TCP/IP and, for the best, some industrial protocols such as ModBus and DNP3 (see Tofino Industrial Security Solution [12]). IICS systems are really in need to industrial firewalls that can be used with different industrial systems configurations (distributed, located, wired, wireless...) taking into account industrial technologies and protocols and more importantly industrial timing requirements.

4) IICS IDS/IPS:

Similarly, IDS/IPS are really indispensable for IICS systems. Unfortunately, there is no commercial IDS/IPS solution that is really adapted to IICS systems. This is because existing IDS/IPS solutions do not support industrial protocols, and are not designed to respect ICS requirements. Besides, no precision was given on where to place IDS within an ICS system.

As far as we are concerned, we will, for the next step of our work, focus on IICS Segregation. It is true that ISA99 [3] and ICS-CERT [7] give some guidelines and recommendations on how to implement IICS Segregation. However, we are convinced that the provided information is not enough detailed and precise. Indeed, the given guidelines do not answer our questions about Segregation. Hence, we suggest to further investigate this issue taking into account the multiple aspects of IICS systems division such as geographical localization, business orientation, hierarchical and functional orientation as well as scalability requirements.

5. Conclusion

This paper highlights one of the major challenges of current Industrial world namely how to integrate two completely different networks (ICS and Corporate system) and keep the integrated system secured. It provides a very useful reference architecture that can be used by other works, a summarized overview of identified vulnerabilities, and an analysis of countermeasures evaluating their efficiency and suggesting some research issues to complete the existing solutions panel in order to secure IICS more efficiently.

A lot of work has been done on IICS security. Multiple vulnerabilities have been identified and a lot of countermeasures have been suggested. However, ICS and Corporate systems integration remains very challenging as regards security. Indeed, most of the suggested security measures are borrowed from the IT world and are not refit to take into account industrial systems specificity. Hence, we argue that there is still work to be done on these measures, especially Authentication and Authorization mechanisms, Segmentation and Segregation, Firewalls and IDS/IPS, in order to adapt them to industrial systems.

References

[8] “Classification method and key measures,” ANSSI.