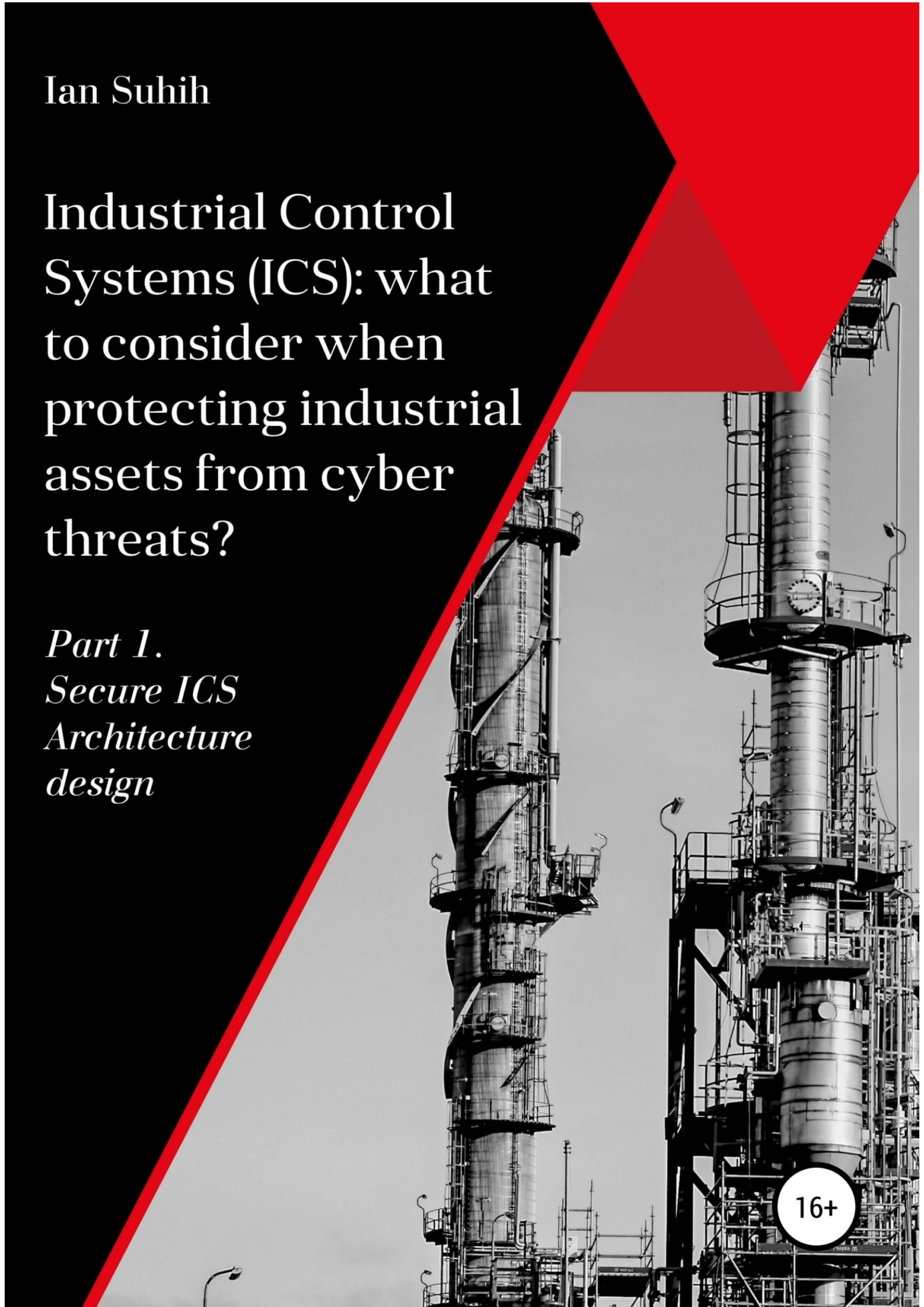
Ian Suhih

Industrial Control Systems (ICS): what to consider when protecting industrial assets from cyber threats?

Part 1. Secure ICS Architecture design



Ian Suhih

Industrial Control Systems (ICS): what to consider when protecting industrial assets from cyber threats? Part 1. Secure ICS Architecture design

«ЛитРес: Самиздат»

2021

Suhih I.

Industrial Control Systems (ICS): what to consider when protecting industrial assets from cyber threats? Part 1. Secure ICS Architecture design / I. Suhih — «ЛитРес: Самиздат», 2021

Currently, the international cybersecurity environment is tense. While until recently, cyber threats were considered primarily in relation to the theft of confidential information and extortion, governments are now increasingly talking about cyber weapons and the possibility of physical damage to critical infrastructure. This can be achieved by attacking industrial control systems (ICS) that connect the world of information technology and real industrial processes. Traditionally, systems of this class were poorly protected from cyber threats, or not protected at all, which now puts entire industries at risk. This paper discusses practical issues of ICS protection and in particular, issues related to the design of secure ICS architectures.

Содержание

Ian Suhih
Industrial Control Systems (ICS): what to consider when protecting industrial assets from cyber threats? Part 1. Secure ICS Architecture design

A Word from the Author

This paper is aimed primarily at managers responsible for the cybersecurity of process control systems, and engineers who are beginning their career in the field of industrial control system cybersecurity. It is designed to help understand the peculiarities of the practical application of international and national standards for the cybersecurity of the industrial control systems to help avoid architectural and gross technical errors at the start of projects, to highlight the main features of the protection of ICS. This paper can also be useful for industry experts as it can offer a new perspective on familiar things.

I sincerely hope that this work will help the reader to better understand the specifics of ICS cybersecurity and make our world a little safer.

The author would like to thank:
• Hubertus Storck
• Alexey Kuzichkin
• Dmitriy Pravikov
• Artem Zhiganov

Without your help, my professional journey would have been much more difficult.

Special thanks for the professional translation:
• Margarita Nazarovskaya

The paper is based on the scientific article " Development of secure architectures for process control systems" DOI: http://dx.doi.org/10.26583/bit.2020.2.08

1. Abbreviations

DCS – Distributed Control System
DMZ – De-Militarized Zone
HIDS – Host-based Intrusion Detection System
NIDS – Network Intrusion Detection System
IDS – Intrusion Detection System
HMI – Human to Machine Interface
IEC–International Electrotechnical Commission
ISO – International Standards Organization
OS – Operating System
SIS – Safety Instrumented System; equivalent to Instrumented Protective System (IPS)
USB – Universal Serial Bus
HDD – Hard Disk Drive
PLC – Programmable Logic Controller
DCS – Distributed Control Systems
PIZ – Process Information Zone
ICS – Industrial control Systems
BPCS – Basic Process Control Systems
IT – Information Technology
OT – Operational Technology
HSE – Health and Safety Executive (United Kingdom)
HMI – Human Machine Interface
SCADA – Supervisory Control and Data Acquisition System
MES – Manufacturing Execution System
APC – Advance Process Control
WSUS – Windows Server Update Services
DPI – Deep Packet Inspection
SIEM – Security Information and Event Management
WAF – Web Application Firewall
DCOM – Distributed Component Object Model
OPC – Open Platform Communications
EPP – End Point Protection
RD – Remote Desktop
NSA – National Security Agency (USA)

2. Introduction

For a long time, industrial control systems were isolated from the outside world and solved local technological process control tasks. In the face of fierce competition, businesses have come to realize that it is possible to achieve greater production efficiency, reduce costs, improve product quality and increase productivity by integrating the process control systems with enterprise systems. Thus, began the fourth industrial revolution, which continues to this day. Today, it is almost impossible to imagine an industrial process without automation and only a small part of these systems operate in isolation from the Internet or the enterprise network (air-gaped).

In the modern world, a lot depends on the operation of control systems: stable power generation, heat and water supply, production of goods, mining, oil and gas extraction, and more. Almost all the services that we use every day are made possible with the use of control systems. Can a modern enterprise work effectively for a long time without a control system? The answer to this question depends on the industry. Some segments are less dependent on control systems and can be managed manually. However, most enterprises are unable to effectively operate for a sufficiently long time without control systems. In this context, the control system can be compared to the Internet, which is used by more than half of the world's population, and majority of us today cannot do our jobs and cannot imagine our lives without Internet access.

The widespread adoption of automated process control systems and their criticality in terms of maintaining business continuity, as well as the reliability and quality of services provided, require special attention to the threats that can lead to disruption of the functioning of these systems.

Traditionally, when it comes to safety in manufacturing industries, functional safety, and some other aspects of the overall safety, which relate to the maintenance operations and occupational safety, are addressed first. For a long time, this was enough, but the fourth industrial revolution brought not only benefits but also new risks associated with cybersecurity. An industrial control system connected to an enterprise network or the Internet is an easy target for an attacker if the connection and protection is not built in accordance with best practices.

Implementing best practices and local and/or international standards to protect ICS is a complex approach where various groups of specialists must be involved. These specialists must overcome several obstacles:

1. **Lack of knowledge.** Traditionally, control engineers do not have sufficient knowledge in the field of cybersecurity or information technology (IT) while IT and cybersecurity engineers do not understand the needs and features of ICS. To create a reliable and secure ICS and/or to appropriately adapt the standards to a specific system, the staff should possess expert knowledge in IT, ICS, and cybersecurity. Simultaneously, the approaches of control engineers and cybersecurity experts in solving problems may have opposite directions. So, a compromise between working staff must be found.

In April 2020, a survey of the expert community was conducted to determine the size of the systems for which the use of centralized cybersecurity management tools becomes justified. The survey has shown that 80 % of the audience were cybersecurity engineers and experts, 20 % were control engineers and middle-level managers. The spread of results was significant, which indicates that there is no consensus among the representatives of the expert community. Based on the survey results, I would like to highlight the following trends that illustrate some differences in approaches:

• Control engineers are less likely to use centralized cybersecurity. On all issues, they voted that services are either not needed at all or are needed for extensive systems. These results indicate the reluctance of control engineers to add new services to classic ICS.

• Cybersecurity engineers are more inclined to use centralized cybersecurity and consider their use justified even for small systems. This is most likely because the use of centralized cybersecurity management tools can significantly reduce labour costs for configuration and management of the system, analysis of incidents, and more.

More information on the results of the survey is provided in Appendix 1.

2. **Complexity of systems and standards.** The IEC 62443 standard considered in this paper has a rather complex structure, and the standard has many requirements that can be interpreted ambiguously and are not always interpreted correctly by users. When it comes to practical applications, users have many questions related to the variety of systems and architectures used, the peculiarities of technological processes, and more. In this work, I will consider some of them and try to help the reader to find the optimal way.

The first problem faced by engineers when designing a secure control system is the development of a secure ICS architecture. This stage is the first and most crucial stage of creating a system. Any errors and shortcomings at this stage can subsequently lead to serious system deficiencies in cybersecurity and/or significant economic losses due to correction of errors on an already implemented system. Thus, qualitative work at this stage will help increase the cybersecurity of control systems and significantly reduce the cost of implementing and maintaining cybersecurity countermeasures.

3. Method of Development of a Secure Industrial Control System Architecture

The concept of "zones and conduits" described in IEC 62443, despite its shortcomings, is an excellent basis for development of the secure ICS architecture. The concept of "zones and conduits" describes how different systems interact with each other, how and in what form information is transmitted between systems and the differences in security requirements in different zones. This concept is initially focused on ICS. In addition, recommendations from the following standards were used in this paper:

– "Cyber Security for Industrial Automation and Control Systems (IACS) EDITION 2", developed by the UK Health and Safety Executive and focused on the practical implementation of IEC 62443.

– "Framework for Improving Critical Infrastructure Cybersecurity" by National Institute of Standards and Technology, which allows a high-level, but structured and comprehensive assessment of the current state of a company's cybersecurity. It also allows to plan improvements to cybersecurity.

– Local standards that are mandatory in the country, but may be inferior to international standards in terms of detail and level of coverage.

I would like to note that despite differences in legislative requirements in different countries, the principles and approaches to ICS cybersecurity are the same everywhere.

4. Inventory

The first step when building a best-in-class secure ICS should be to collect all existing information about assets, including:

- Manufacturing cells and material flow diagrams;
- Location plans for equipment and manufacturing cells;
- Information systems and ICS supporting the operation;
- Dependencies between information systems, industrial control systems, and manufacturing cells;
- General information about information systems and ICS, including vendor names, versions of firmware, hardware and application software, list of, and other data;

Конец ознакомительного фрагмента.