# 2022. January, Industrial Control Systems security feed

Black Cell is committed for the security of Industrial Control Systems (ICS) and Critical Infrastructure, therefore we are publishing a monthly security feed. This document gives useful information and good practices to the ICS and critical infrastructure operators and provides information on vulnerabilities, trainings, conferences, books, and incidents on the subject of ICS security. Black Cell provides recommendations and solutions to establish a resilient and robust ICS security system in the organization. If you're interested in ICS security, feel free to contact our experts at info@blackcell.io.

## List of Contents

# ICS good practices, recommendations

## The 4 Pillars of Industrial Cybersecurity

The U.S. government has been warning us for a few years by now about attackers targeting the nation's critical infrastructure. The targeting of these entities are obvious; easier to find the weak spot of a legacy OT system then an up-to-date IT system, and those stakeholders have the money to pay ransom in a case of a ransomware attack. The downtime of these operators can easily collapse complete sectors. To avoid the downtime and losses due to these attacks, the OT systems also needs to be hardened, not just the IT ones.

To properly harden the OT infrastructure, one should take a loot at the following four pillars:

1. Reveal
   Every stakeholder must create an accurate **OT network map**, because "you can't protect what you can't see". It is always hard to map these via security scope, as the OT systems are mostly legacy systems, with low tolerance for downtime, proprietary protocols and remote user activity. The providers must create attributes to help to find a solution that supports a large library of industrial protocols and employs different asset-discovery techniques to create and maintain a comprehensive and enriched asset database. On the other hand, full visibility of the OT network must be created to monitor all the normal behaviour of the system and human entities and activities to identify misconfigurations, traffic overloads, and other issues that pose risks to reliability, availability, and safety.

2. Protect
   The risk of connecting OT systems to IT systems is high. Due to the fact that the OT (legacy) systems are more vulnerable than the IT systems the connection of those to IT systems are highly inadvisable. In the last few months two huge critical infrastructure provider (Colonial Pipeline and JBS) went down for days due to a ransomware attack. To avoid these attacks the providers must have an always up-to-date asset inventory, you can tackle inherent critical risk factors, from vulnerabilities and misconfigurations to poor security hygiene and untrustworthy remote access mechanisms. After this mapping all the risks must be overviewed. You have to **know your risks** to mitigate them. Because no organization has the resources, bandwidth or permissible downtime required to fully mitigate every risk it faces the organizations must **prioritize** the risks. The prioritizing of the risks in OT systems are quite simple; just calculate with the maximum tolerable downtime of these systems or assets. The last step of pillar 2 is the **mitigation (reducing) of risks**. It could be done by applying the Zero Trust model (policy). All the operators must implement and enforce authentication policies along these guidelines can drastically reduce the risk of unintentional or malicious actions. And always keep your systems up to date.

3. Detect
   The protection is about creating policies and procedures (controls) but even the most advanced protective controls and processes you implement can't eliminate risk completely. The detection of threats is basically easy in IT systems with sophisticated firewall settings, but threat detection is significantly more difficult within industrial networks due to the fact these legacy systems are incompatible with IT security tools, the size and complexity of OT

environments, the digitization of industrial networks, and lack of industrial cybersecurity expertise. Since every OT environment is different, a one-size-fits-all approach isn't effective. That's why operators must **tailor threat detection and alerts** to the unique needs of their networks based on an extensive database of signatures and indicators of compromise. The handling and mitigation of the threat detection alerts could be hard without **prioritizing** them.

4. Connect

   Connecting or disconnection IT/OT infrastructure and systems? Should you find experts to your team of IT, or OT or should you have two separate team? Double all the resources? Double the SOC team as well? The key is the holistic approach.

   The operators must **centralize responsibility and accountability** for securing the industrial environment with the CISO. The planning and controlling of the security should be in one hand to tailor all the controls, to maintain the safe and continuous operation of the IT and OT systems. Appoint **additional leadership team members** for **IT and OT security**. The two side have two different approaches of the security and safe operation. Operator also need to designate a cybersecurity site leader for each OT site who could liaison between on-site OT personnel and the SOC team in a case of an incident. The **resources must be integrated** with existing IT security resources. These integrations should cover a broad range of use cases, including security information and event management (SIEM), workflow management, security orchestration, automation, and response (SOAR), and network infrastructure tools.

Source and more information are available on the following link:

https://www.securityweek.com/reveal-first-pillar-industrial-cybersecurity
https://www.securityweek.com/protect-second-pillar-your-journey-improve-industrial-cybersecurity-posture
https://www.securityweek.com/detect-third-pillar-industrial-cybersecurity
https://www.securityweek.com/connect-fourth-pillar-industrial-cybersecurity

## ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in February 2022:

NEW!

O'Reilly provides a 10-day free trial training course. In this Industrial Cybersecurity training you get O'Reilly members experience live online training, plus books, videos, and digital content from 200+ publishers.

More details can be found on the following website:

https://www.oreilly.com/library/view/industrial-cybersecurity/9781788395151/60f43e9e-1d7b-4fe8-89de-87b70052da85.xhtml

SANS provides online ICS security courses. The details of the trainings and courses are available on the following link:

https://www.sans.org/course/ics-scada-cyber-security-essentials#results

**Periodic online courses:**

The Coursera (https://www.coursera.org/) website provides an opportunity to take advantage of online trainings regarding ICS security. The trainings provide video instructions, and the candidates could demonstrate their knowledge in the field of ICS and IoT and the related cloud security. After the course, the University of Colorado, Boulder issues a certificate to the graduates. The following courses are available:

- Developing Industrial Internet of Things Specialization
- Development of Secure Embedded Systems Specialization
- Industrial IoT Markets and Security

More details can be found on the following website:

https://www.coursera.org/search?query=-%09Developing%20Industrial%20Internet%20of%20Things%20Specialization&

ICS CERT offers the following courses:

- Introduction to Control Systems Cybersecurity
- Intermediate Cybersecurity for Industrial Control Systems (201), (202)
- ICS Cybersecurity
- ICS Evaluation

More details can be found on the following website:

https://www.us-cert.gov/ics/Training-Available-Through-ICS-CERT

ICS-CERT Virtual Learning Portal (VLP) provides the following short courses:

- Operational Security (OPSEC) for Control Systems (100W) - 1 hour
- Differences in Deployments of ICS (210W-1) – 1.5 hours
- Influence of Common IT Components on ICS (210W-2) – 1.5 hours
- Common ICS Components (210W-3) – 1.5 hours
- Cybersecurity within IT & ICS Domains (210W-4) – 1.5 hours
- Cybersecurity Risk (210W-5) – 1.5 hours
- Current Trends (Threat) (210W-6) – 1.5 hours
- Current Trends (Vulnerabilities) (210W-7) – 1.5 hours
- Determining the Impacts of a Cybersecurity Incident (210W-8) – 1.5 hours
- Attack Methodologies in IT & ICS (210W-9) – 1.5 hours
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 1 (210W-10) – 1.5 hours
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 2 (210W-11) – 1.5 hours
- Industrial Control Systems Cybersecurity Landscape for Managers (FRE2115) - 1 hour

VLP courses are available on the same website, like the other ICS-CERT courses.

SANS online courses in the field of ICS security:

- ICS410: ICS/SCADA Security Essentials
  - anytime, on demand.

- ICS515: ICS Active Defense and Incident Response
  - anytime, on demand.

More details can be found on the following website:

https://www.sans.org/find-training/search?types=10&coursecode=ICS410,ICS515

Udemy provides online courses in ICS and SCADA security. From the basics of ICS and SCADA security principles to the technological solutions and governance questions, the below course could help to understand the essence of the ICS/SCADA security.

- ICS/SCADA Cyber Security
- Learn SCADA from Scratch to Hero (Indusoft & TIA portal)
- Fundamentals of OT Cybersecurity (ICS/SCADA)

More details can be found on the following website:

https://www.udemy.com/ics-scada-cyber-security/

The Department of Homeland Security's two days training is useful for the ICS/SCADA operators:

- SCADA security training

The courses are available live online.

More details can be found on the following website:

https://www.tonex.com/training-courses/scada-security-training/

The SCADAhacker.com website provides ICS security online courses:

- Fundamentals of Industrial Control System Cyber Security

The training takes 40-120 hours, and 8 modules can help to understand the ICS cybersecurity issues. The training focuses on the „Blue teaming" activities, for ICS and SCADA systems.

If you have a certificate, like CISSP, CEH, the course can help to add some ICS and SCADA specific knowledge.

More details can be found on the following website:

https://scadahacker.com/training.html

INFOSEC-Flex SCADA/ICS Security Training Boot Camp gives the possibility for ICS/SCADA operators to get ready for external and internal threats.

The 4 days course guarantees the "Certified SCADA Security Architect" certification for the candidates (93% exam pass rate).

The basics of the ICS/SCADA security, governance, security controls, penetration testing and other topics can help the participants to become an ICS/SCADA security expert.

More details can be found on the following website:

https://www.infosecinstitute.com/courses/scada-security-boot-camp/

Industrial Control System (ICS) & SCADA Cyber Security Training

This is a three day course, what is designed for:

- IT and ICS cybersecurity personnel
- Field support personnel and security operators
- Auditors, vendors and team leaders
- Electric utility engineers
- System personnel & System operators
- Independent system operator personnel
- Electric utility personnel involved with ICS security.
- Technicians, operators, and maintenance personnel
- Investors and contractors in the electric industry
- Managers, accountants, and executives of electric industry

More details can be found on the following website:

https://www.tonex.com/training-courses/industrial-control-system-scada-cybersecurity-training/

## ICS conferences

In February 2022, the following ICS/SCADA security conferences and workshops will be organized (not comprehensive):

### 13th SCADA World Summit

Industry 4.0, Growth in adoption of cloud-based SCADA systems, urban development projects such as smart cities, energy & utilities infrastructure growth & transportation development, and high penetration of mobile SCADA systems drive the growth of the global SCADA market. However, cyber threats and the requirement of high investment for setting up the SCADA systems are expected to impede the SCADA market growth. Furthermore, among the other key issues that need to be managed include real time data management from multiple sources, overcoming challenges such as redundancy and design & communication network management, the need to integrate SCADA within current business systems for improved business decision making as well as implementing advanced applications and IoT applications within SCADA to manage the increasingly complex business environment.

Equip Global's 13th SCADA World Summit 2022 is the industry's leading SCADA conference and will provide an exclusive platform that brings together cross-industry SCADA Leaders and Project Owners to discuss the implementation of highly effective and energy efficient SCADA systems in order to accommodate the ever-growing business needs, whilst developing solutions to mitigate security risks and challenges associated with SCADA implementation.

Live Online; February 7-10, 2022

More details can be found on the following website:

https://www.equip-global.com/13th-scada-world-summit-online

### Critical Infrastructure Protection & Resilience North America

After a long year of restrictions and lost opportunities due to the pandemic and highlighting new challenges and threats to our critical infrastructure, we need to get back to the business of building better resilience for future continuity and sustainability for economic prosperity.

Critical Infrastructure Protection and Resilience North America provides a unique opportunity to meet, discuss and communicate with some of the most influential critical infrastructure protection and security policy makers and practitioners.

New Orleans, Louisiana, USA; February 1-3, 2022

More details can be found on the following website:

https://www.ciprna-expo.com/wp-content/uploads/2021/12/CIPRNA-2022-PSG.pdf

# ICS incidents

## Industrial Organizations Targeted by Log4Shell Attacks

Eduard Kovacs published an article on the SecurityWeek's website, where he shows the Log4Shell threats for industrial organizations.

CVE-2021-44228, also dubbed as Log4Shell and LogJam, came to light in late November, and it was patched on the 6th of December. According to the information, there are some attacks where the exploitation of the vulnerability was successful.

The vulnerability is exploitable remotely, and remote code execution is possible after the successful attack. "This cross-cutting vulnerability, which is both vendor agnostic and affects both proprietary and open-source software, will leave a wide swathe of industries exposed to remote exploitation, to include electric power, water, food and beverage, manufacturing, transportation, and more," Dragos said.

"Log4j is found in popular open-source repositories used in numerous industrial applications, such as Object Linking and Embedding for Process Control (OPC) Foundation's Unified Architecture (UA) Java Legacy. Additionally, adversaries can leverage this vulnerability in proprietary Supervisory Control and Data Acquisition (SCADA) and Energy Management Systems (EMS) which make use of Java in their codebase," it added.

IT/OT segmentation is a good recommendation, and the experts said, that in case of segregated IT/OT networks, the exploitation of the vulnerability is more complicated.

Products confirmed to be affected include E-Car OC, EnergyIP, Geolus, Industrial Edge Management, Logo! Soft Comfort, Mendix, MindSphere, Operation Scheduler, Siguard DSA, Simatic WinCC, SiPass, Siveillance, Solid Edge, and Spectrum Power.

Many ICS vendors responded to the Log4Shell situation with notices, but many vendors still analyse the vulnerability.



CISA (Cybersecurity & Infrastructure Security Agency) published an Alert (AA21-356A), which contains technical details and give some advice how to mitigate the negative impacts.

https://www.cisa.gov/uscert/ncas/alerts/aa21-356a

The source and more information available at the following links:

https://www.securityweek.com/industrial-organizations-targeted-log4shell-attacks

# Book recommendation

## Cybersecurity - Ambient Technologies, IoT, and Industry 4.0 Implications

It is becoming increasingly important to design and develop adaptive, robust, scalable, and reliable security and privacy mechanisms for IoT applications and for Industry 4.0 related concerns. This book serves as a useful guide for researchers and industry professionals and will help beginners to learn the basics to the more advanced topics.

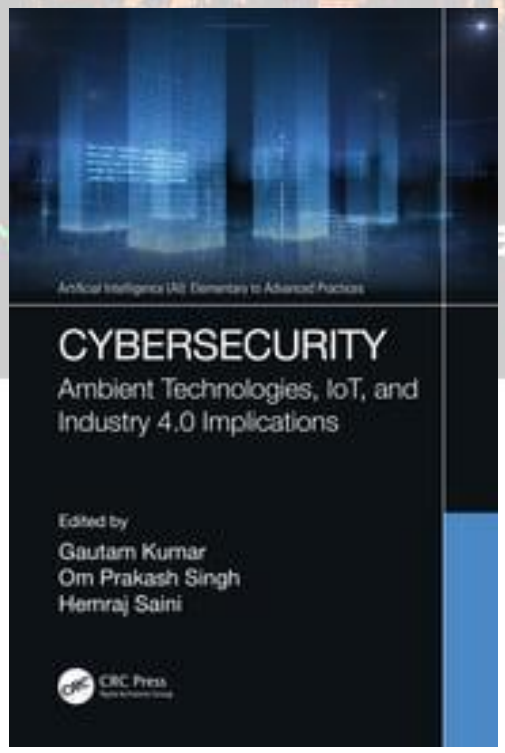
Along with exploring security and privacy issues through the IoT ecosystem and examining its implications to the real-world, this book addresses cryptographic tools and techniques and presents the basic and high-level concepts that can serve as guidance for those in the industry as well as help beginners get a handle on both the basic and advanced aspects of security-related issues. The book goes on to cover major challenges, issues, and advances in IoT and discusses data processing as well as applications for solutions and assists in developing self-adaptive cyberphysical security systems that will help with issues brought about by new technologies within IoT and Industry 4.0.

Authors/Editors: Dr. Gautam Kumar; Dr. Om Prakash Singh; Hemraj Saini.

Year of issue: 2021

The book is available at the following link:

https://www.routledge.com/Cybersecurity-Ambient-Technologies-IoT-and-Industry-40-Implications/Kumar-Singh-Saini/p/book/9780367702168



## Black Cell recommendations

### Water Security Plan - Implementation Manual for Drinking Water Systems

ERNCIP published (January 11, 2022) a document what is very useful for the water system operators to establish a comprehensive security. ERNCIP (European Reference Network for Critical Infrastructure Protection) aims at providing a framework within which experimental facilities and laboratories will share knowledge and expertise in order to harmonise test protocols throughout Europe, leading to better protection of critical infrastructure against all types of threats and hazards.

The implementation of security measures to counter hostile actions against the physical and cyber integrity of water supply systems and deliberate waterborne contamination requires an appropriate planning process incorporating risk assessment surveys, establishment of communication strategies, protocols and screening methods. This manual provides a detailed basis for the creation and implementation of a Water Security Plan for drinking water systems, supporting water utility operators with the information and tools they need to develop a plan specifically for the security of their water supply systems.

The document mentions many relevant things, for example the importance of redundancies, SCADA security and other related security aspects. The part most interesting from the OT perspective is in the 2nd point.

2.1 security planning and preparation
2.2 protection: event detection and analysis
2.3 response and cooperation

This document is very important for the operators of drinking water systems and we strongly recommend studying it, especially as it's downloadable for free.

Source and more details available on the following link:

https://erncip-project.jrc.ec.europa.eu/documents/water-security-plan-implementation-manual-drinking-water-systems

## ICS vulnerabilities

In January 2021, the following vulnerabilities were reported by the National Cybersecurity and Communications Integration Center, Industrial Control Systems (ICS) Computer Emergency Response Teams (CERTs) – ICS-CERT:

ICSMA-21-355-01: **Fresenius Kabi Agilia Connect Infusion System** (Update A)

High level vulnerabilities: Uncontrolled Resource Consumption, Use of a Broken or Risky Cryptographic Algorithm, Insufficiently Protected Credentials, Improper Access Control, Plaintext Storage of a Password, Files or Directories Accessible to External Parties, Exposure of Information Through Directory Listing, Cross-site Scripting, Injection, Use of Hard-coded Credentials, Use of Client-side Authentication, Use of Unmaintained Third-party Components.
https://www.cisa.gov/uscert/ics/advisories/icsma-21-355-01

ICSA-21-334-02: **Mitsubishi Electric MELSEC and MELIPC Series** (Update A)

High level vulnerabilities: Uncontrolled Resource Consumption, Improper Handling of Length Parameter Inconsistency, Improper Input Validation.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-334-02

ICSA-22-025-01: **GE Gas Power ToolBoxST**

High level vulnerabilities: Improper Restriction of XML External Entity Reference, Path Traversal.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-025-01

ICSA-22-020-01: **ICONICS and Mitsubishi Electric HMI SCADA**

Critical level vulnerabilities: Cross-site Scripting, Incomplete List of Disallowed Inputs, Plaintext Storage of a Password, Buffer Over-read.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-020-01

ICSMA-21-187-01: **Philips Vue PACS** (Update A)

Critical level vulnerabilities: Cleartext Transmission of Sensitive Information, Improper Restriction of Operations within the Bounds of a Memory Buffer, Improper Input Validation, Improper Authentication, Improper Initialization, Use of a Broken or Risky Cryptographic Algorithm, Protection Mechanism Failure, Use of a Key Past its Expiration Date, Insecure Default Initialization of Resource, Improper Handling of Unicode Encoding, Insufficiently Protected Credentials, Data Integrity Issues, Cross-site Scripting, Improper Neutralization, Use of Obsolete Function, Relative Path Traversal.
https://www.cisa.gov/uscert/ics/advisories/icsma-21-187-01

ICSA-21-131-02: **Mitsubishi Electric GOT and Tension Controller** (Update A)

Medium level vulnerability: Buffer Access with Incorrect Length Value.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-131-02

ICSA-20-343-02: **Mitsubishi Electric GOT and Tension Controller** (Update B)

High level vulnerability: Out-of-bounds Read.
https://www.cisa.gov/uscert/ics/advisories/icsa-20-343-02

ICSA-22-013-01: **Mitsubishi Electric MELSEC-F Series**

High level vulnerability: Lack of Administrator Control Over Security.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-013-01

ICSA-22-013-02: Siemens SICAM A8000
Critical level vulnerabilities: Use of Hard-coded Credentials, Improper Access Control.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-013-02

ICSA-22-013-03: Siemens Energy PLUSCONTROL
High level vulnerabilities: Type Confusion, Improper Validation of Specified Quantity in Input, Buffer Access with Incorrect Length Value, Integer Underflow, Improper Handling of Inconsistent Structural Elements.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-013-03

ICSA-22-013-04: Siemens SIPROTEC 5 Devices
Medium level vulnerability: Improper Input Validation.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-013-04

ICSA-22-013-05: Siemens COMOS Web
High level vulnerabilities: Basic XSS, Relative Path Traversal, SQL Injection, Cross-site Request Forgery.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-013-05

ICSA-22-013-06: Siemens SICAM PQ Analyzer
Low level vulnerability: Unquoted Search Path or Element.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-013-06

ICSA-22-013-07: Mitsubishi Electric MELSEC-F Series
High level vulnerability: Improper Initialization.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-013-07

ICSA-21-266-01: Trane Symbio (Update B)
High level vulnerability: Code Injection.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-266-01

ICSA-21-103-14: Siemens Nucleus DNS (Update A)
Medium level vulnerability: Use of Insufficiently Random Values.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-103-14

ICSA-20-303-01: Mitsubishi Electric MELSEC iQ-R, Q and L Series (Update B)
High level vulnerability: Uncontrolled Resource Consumption.
https://www.cisa.gov/uscert/ics/advisories/icsa-20-303-01

ICSA-22-011-01: Johnson Controls VideoEdge
Medium level vulnerability: Improper Handling of Syntactically Invalid Structure.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-011-01

ICSMA-22-006-01: Philips Engage Software
Low level vulnerability: Improper Access Control.

https://www.cisa.gov/uscert/ics/advisories/icsma-22-006-01

ICSA-22-006-01: Omron CX-One
High level vulnerability: Stack-based Buffer Overflow.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-006-01

ICSA-22-006-02: Fernhill SCADA
High level vulnerability: Uncontrolled Resource Consumption.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-006-02

ICSA-22-006-03: IDEC PLCs
High level vulnerabilities: Unprotected Transport of Credentials, Plaintext Storage of a Password.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-006-03

The vulnerability reports contain more detailed information, which can be found on the following website:

https://ics-cert.us-cert.gov/advisories

Continuous monitoring of vulnerabilities is recommended, because relevant information on how to address vulnerabilities, patch vulnerabilities and mitigate risks are also included in the detailed descriptions.

## ICS alerts

In January 2022, ICS-CERT has not published alerts.

The previous alerts can be found at the following link:

https://www.us-cert.gov/ics/alerts