Cyber Israel
National Cyber Directorate

# Reducing Cyber Risks for Industrial Control Systems (ICS)

## Professional Supplementary Document

# Reducing Cyber Risks for Industrial Control Systems (ICS)

## Professional Supplementary Document

This document is intended to assist the professional and technical bodies within the organization, who are in charge of the OT scene in general and the ICS in particular. This document is not intended to replace the above bodies, but rather to serve as a tool for identifying the key issues related to cyber protection risks at the ICS arena. This document offers professional protection recommendations, based on international standards, research and professional documents, all of which are specified herein. It is understood that the implementation of professional controls in the ICS arena, in a specific organization, requires a dedicated process of risk management and the adjustment of those controls for the organization by suitable professionals.

Cyber Israel
National Cyber Directorate

# Table of Content

# 1. Introduction

## 1.1 Introduction to ICS Environments

Industrial Control Systems (ICS) is a general term for several types of command and control systems, which are used in industry and critical infrastructure. These systems include several subsystems and categories. Some of these systems are designed to control a single component, such as an altitude or temperature sensor, designed to control the opening and closing of a valve or gate. The others are designed to control multiple components, which are distributed in the field. What they all have in common is their capability of communicating with end components, which act as sensors or actuators.

**Common ICS types:**

- SCADA systems
- Distributed Control Systems (DCS)
- Structural Control Systems (BMS)
- Industrial Automation Control Systems (IACS)

In recent years, awareness of cyber events has increased, which has focused on attacking systems in the ICS space network.

Unlike events against computing networks and traditional computing equipment, these events are very likely to directly affect the quality of life and physical safety of citizens. Beyond the potential for **damage to the production line**, damage to such systems can lead to flooding of cities, leakage of gases, poisons, toxins or wastewater into the environment, explosion of containers and disabling essential services such as electricity, gas, water and more.

The trend of cyber attacks against ICS systems has been on the rise in recent years. The main reason for this is due to the attractiveness of the attack and the difficulty of implementing protection and security controls in the operating environment such as those implemented in the IT network.

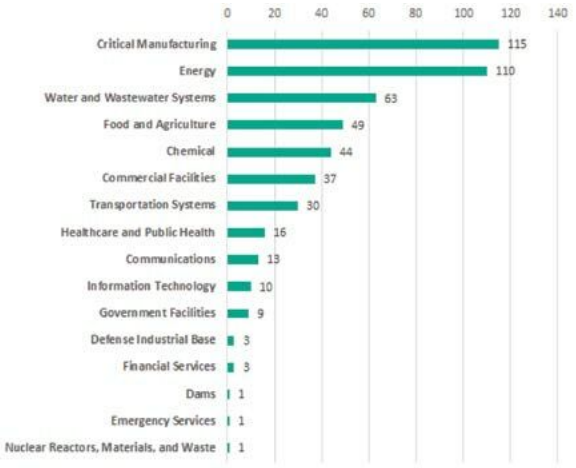


**Figure 1: ICS weaknesses mapping by sectors (from Kaspersky website)[1]**

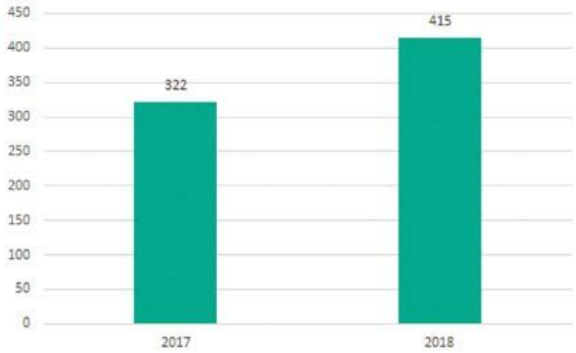


**Figure 2: Number of ICS weaknesses discovered in 2018 versus 2017 (from Kaspersky website)[2]**

## Among the most prominent events that have been published in recent years are[3]:

### TRICONEX attack

A Trojan-based attack from the TRITON family occurred in December 2017 and was directed against an industrial safety system. The attacker gained access to the Engineering Workstation and to the SIS (Safety Instrumented System), and from there used the aforementioned attack platform attempt try to change the operation and programming of the safety system controllers. The purpose of the attacker was to cause damage so as to disable and neutralize the system. Safety in the Manufacturing Process[4].

### Hacking of the Bowman Dam in the US

On March 24, 2016, it was reported that hackers broke into a small dam in the state of New York in the United States. This malicious takeover could have led to a flood in the city, damage to critical systems and significant financial damage to the city.

### BlackEnergy - Power plants disabled in Europe

On December 23, 2015, power outages occurred in European electricity companies, disabling entire regions. It was found that an attacker implanted a malware and sent it via Spear Phishing. Spoofing and Air gap jumping ability from the IT systems to the OT systems led to BlackEnergy running in the organization. In this event, the attacker took advantage of the ability to jump from the IT systems to the OT systems[5].

1 https://ics-cert.kaspersky.com/media/KL_ICS_CERT_H2_2018_REPORT_EN.pdf

2 https://ics-cert.kaspersky.com/media/KL_ICS_CERT_H2_2018_REPORT_EN.pdf

3 https://ics.sans.org/media/SANSICS_DUC4_Analysis_of_Attacks_on_US_Infrastructure_V1.1.pdf - Additional incidents

4 https://www.gov.il/BlobFolder/reports/sis/he/SIS-CERT-IL-W-400.pdf *In Hebrew

5 https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01

## 1.2 Purpose of this document

This document aims to provide the professional audience with the basic knowledge required for better protection of ICS systems. The document shall import knowledge along with methods and workflows to increase resilience in the production line. At the same time, it includes representative examples and risks, ways of defense, recommendations and controls to mitigate risks in the operating environment. The document constitutes a professional extension in the ICS arena to the cyber defense methodology for an organization.

## 1.3 Target Audience

This document is relevant to those engaged in the protection & defense of industrial control systems, including the CISO, the cyber defense personnel in the organization and the operations and control personnel, and in some parts is also intended for other parties within the organization, such as risk managers and procurement personnel, who are also responsible for computing equipment for the OT environment. The target audience for this document includes the following parties:

- **ICS engineers/technicians -** those who are in charge of ICS system installation and maintenance processes
- **ICS Operators -** those who are involved in the ongoing and ongoing operations of the systems
- **Network security personnel in ICS systems**
- **ICS Security Trustees -** as part of their responsibilities (most often appointed by the CISO or a management body)
- **Integration companies, consulting companies and ICS service providers**
- **IT professionals**

**Figure 3: Operator in production line**

# 2. Technology background overview of ICS environments (Topology and Main Components)

## 2.1 Subsystems, Protocols and Key Components in the ICS Environment:

**Supervisory Control and Data Acquisition (SCADA)**

A communication-based system that enables control, control and process control. This is through sending dedicated commands to controllers. These processes are usually production, production, refining, energy generation and product assembly. The systems include a computerized layer for monitoring and controlling the accessories.

**Industry processes** include, among others, production, production, refining, energy generation and product assembly processes.

**Processes in public or private infrastructures** include, inter alia, outdoor lighting systems (urban and inter-urban), water supply systems, waste water collection and purification systems, oil and gas transmission pipeline monitoring, electricity grid, alarm systems, and large communications systems.

**Processes in public or private facilities**, including Building Management Systems (BMS), airports, ports, ships and space stations. SCADA systems monitor and control HVAC systems (Heating, Ventilation And & Air Conditioning) operating in the facility.

**Industrial Network Protocols -** Industrial network protocols are real-time communication protocols developed to link systems, interfaces, and devices that together constitute an industrial control system. Most of them were initially designed for serial communication over serial connections, but later they were adapted to work on Ethernet networks using a communication protocol such as TCP/IP.

The weaknesses of industrial networks are mostly known and are due to a lack of awareness, knowledge, weaknesses in the system configuration, software weaknesses, a lack of protection against malwares, encryption problems and more.

SCADA usually includes these components:

- **Human-Machine Interface (HMI) -** A human-machine interface that displays process data & information to the operator, enabling the operator to monitor and monitor the process.
- **Master Terminal Unit (MTU) -** A centralized control system designed to monitor, monitor, and operate the end components.
- **Programmable Logic Controllers (PLC)**
- **Logic controllers** designed to receive input, run preloaded logic (and logic based on the transfer of commands to end equipment).
- **Remote Terminal Unit (RTU) -** Remote monitoring units, which are involved in the process and in the process are connected to sensors and located on the process site.
- **Historian -** A system that stores the props from the field over time and shows trends in changing the parameters measured in the process. The system is usually used by the control engineers to improve and fine-tune the process.
- **Sensors -** Devices that measure physical conditions and are capable of activating actuators and transmitting to control systems.
- **Actuators -** Actuated by the sensors and trigger the required change (such as valve opening).
- **Communication infrastructure -** connects the control system to units (communications: wired, radio, cellular, Wi-Fi, satellite).
- **Intelligent Electronic Device** (IED) - These devices form part of the control systems such as sensors, motors, transformers, pumps, etc. and are also equipped with a tiny reporting processor. These devices are typically communicated via the Fieldbus protocol, function as Slaves and are controlled by remote end units.
- **Internet of Things (IOT) -** dedicated, communication-based components and the ability to exchange data & information over the Internet.
- **Industrial Internet of Things (IIOT) -** Designed components for the communications-based manufacturing industry.

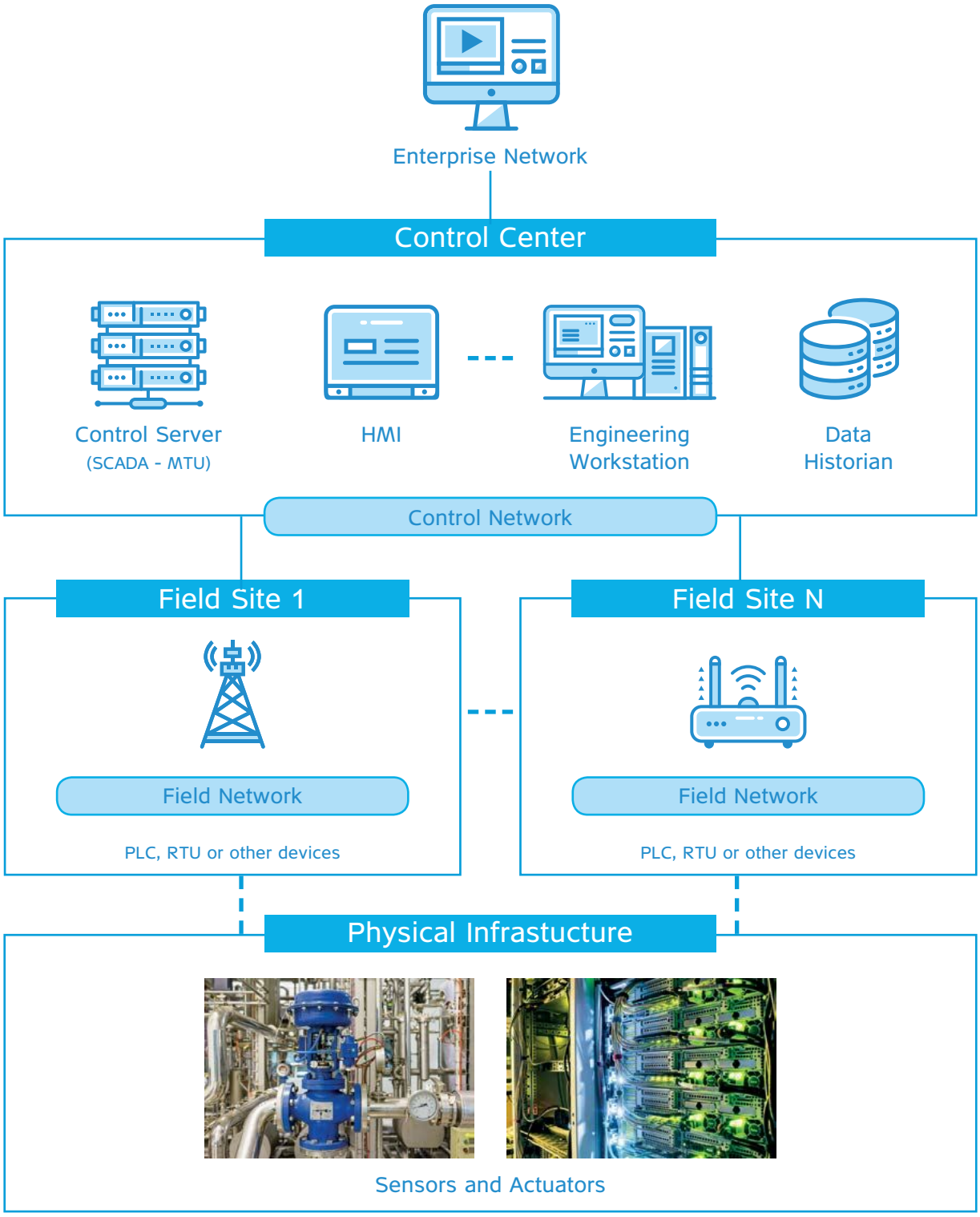


**Figure 4: Description of components in the ICS environment**

**Distributed Control System (DCS) -** This system differentiates the DCS from non-distributed systems that use a single centralized controller.
The DCS system typically uses process-optimized processors (hierarchical) and linked by communication networks for monitoring and control.

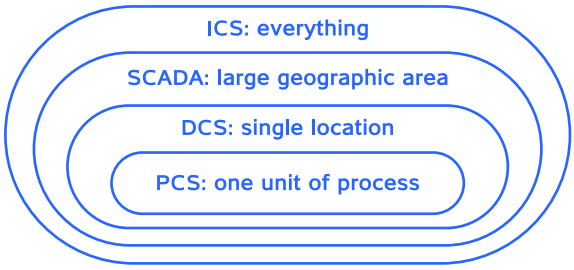


**Figure 5: The main subsystems in the ICS world**

## 2.2. Classical topology in ICS environment

The ICS environment is a complex environment. The environment incorporates a management environment, sometimes linked to ERP and such other systems, operating environment, computer positions, sensors and controllers (see classic environment in Figure 4). There are two models, which can assist in the planning and implementation stages of architecture in the ICS environment:

- **The Triangle Model (based on ISA 95**)
- **PURDUE model**

These models allow for structural reference by hierarchy and control system layer layers. In the Triangle model, the systemic description presented through the five levels in a triangle (Including the Air Gap) is more simplistic and suitable for complex systems. The PURDUE model has a six-level distribution and is suitable for larger organizations/ more complex environments.
As a general rule, both models separate the IT domain - which manages the organization's business system - from the OT and the domain in which physical components are also managed, which receive instructions through commands of electricity power changes.

### 2.2.1. The Triangle Model (suitable mainly for simple environments and small organizations):

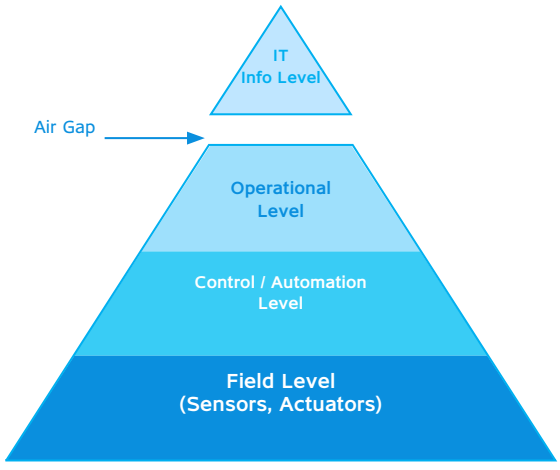


**Figure 6: The triangle model**

Separation of the triangle after IT differentiation inputs[6]:

- **Business environment and IT involvement in the organization.** This network is sometimes directly connected to the internet.
- **Management environment in the manufacturing network** (Air GAPPED).
- **The command and control servers and controllers themselves,** which make up the heart of the system - an area where processes run for all local and remote devices.
- **In the lowest 2 layers of the model,** the PLC, RIO, IED industrial controllers are listed. This is in accordance with the system structure. These components are connected to sensors and actuators via relays that control the manufacturing process.


Purdue Model for Control Hierarchy logical framework

## 2.2.2. Purdue Model

**Figure 7: Distribution of the model by regions[7]**

**This model presents an extended description of the triangular model and contains six levels (0-5).** This structure model is suitable for medium and large organizations, which have an interface to the IT network.

- **Levels 5 and 4 -** This area is dedicated to a business process management environment, and as such, it is based on the

6 The Airgap separation and primarily practiced on critical infrastructure. There are organizations where the separation between environments is based upon VLAN, dedicated FW etc.

7 https://www.encompass-inc.com/top-10-automation-trends-in-2018

enterprise IT systems and services (Enterprise). This area includes enterprise Internet connection, ERP systems, etc[8].

- **Level 3 –** This area includes a production network management environment, materials, manpower, inventory, availability of machines (such as the MES systems, etc.). The Connection between layer 3 and layer 2 will be done by firewall devices, or those where communication is one-way and separated by a device to create one-way traffic (diode)
- **Level 2 –** In this environment there is the control system in the HMI interface, and its role is to enable the monitoring and control of the SIP processes as well as to enable the operator's intervention as needed and according to his/her permissions. Malicious to program or change controller commands (complex systems have several operators' positions (HMI), enabling operators to focus on different areas of the system, or to intervene as needed.
- **Level 1 –** In this environment, processes are managed using control computers (Automation Server) for all devices running RTU, PLC controllers, etc.
- **Level 0 –** represents the lowest layer in the PURDUE model. This layer is connected to the sensors and actuators, which operate the machine.

8 https://www.gov.il/BlobFolder/policy/protection_of_erp_systems/he/Protection%20of%20EPR%20systems_576699_4_WEB.pdf *** In Hebrew**

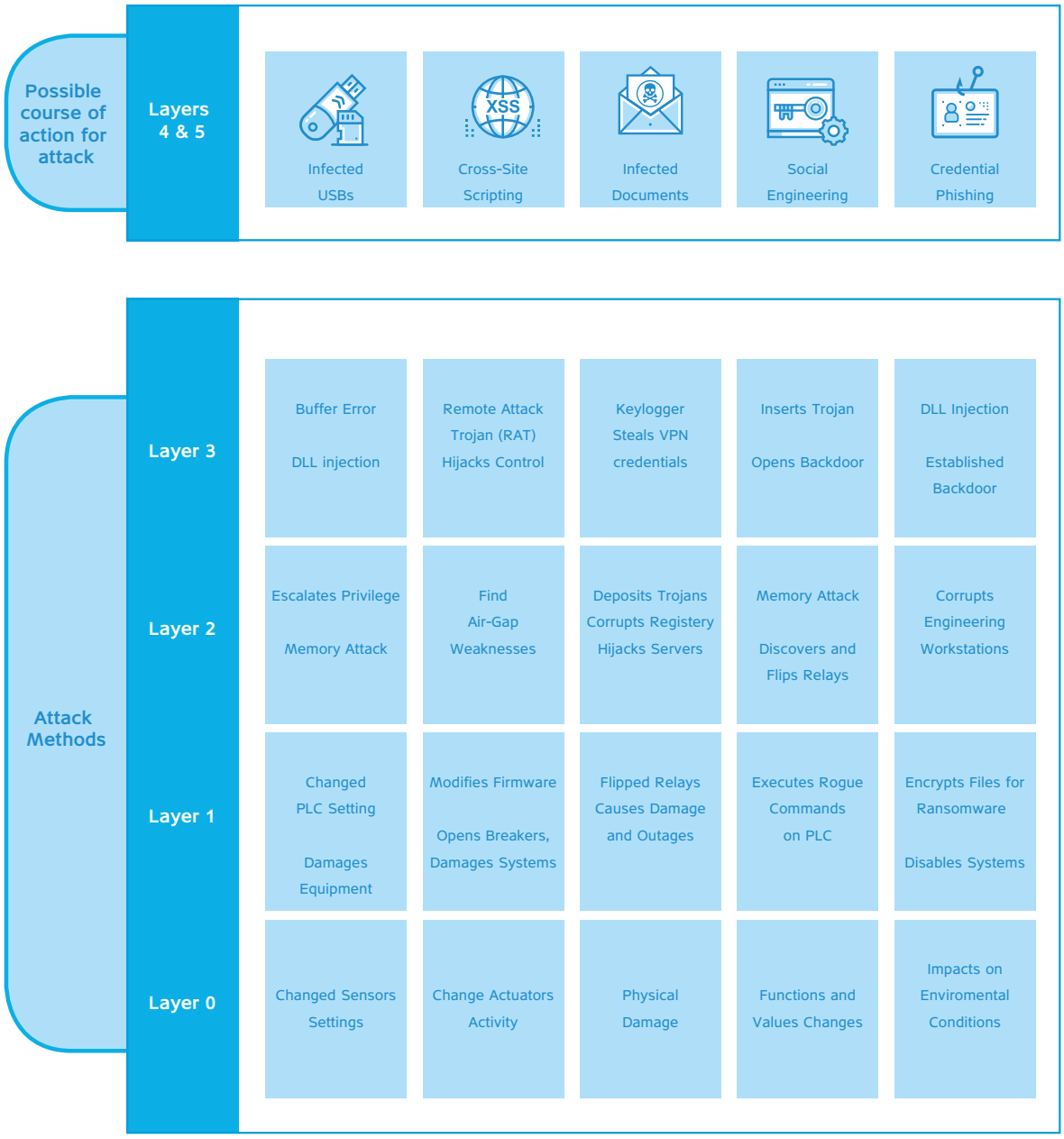


**Figure 8: Mapping of possible attacks according to the Purdue model**

## 2.3. Programming and communication between controllers and HMI

This paragraph describes the background process in controller programming with the aim of understanding the opportunities from the attacker's point of view and risks in the controller loading process (and programming ability). Over the years, PLC controllers have been developed by different manufacturers, all of whom have developed a unique user interface and unique functions. Changing environments and needs - leading to increased operational and security difficulties in communication between programmed controllers by various manufacturers.

Mixed Controls Environment: Despite the need and manufacturer's recommendations to use single controllers (from the same manufacturer and the same family of products), there are also mixed environments that incorporate several controllers, produced by different vendors. Standard and Programming Methods As described in IEC 61311-3, the standard version, published in 2013, defined five programming languages.
Each family of controllers, produced in a particular Vendors has a unique graphical interface that "compiles" the configuration file uniquely to the same controller type (from the same vendors).

In a mixed environment, control engineers are required to become familiar with some graphics software. In modern systems, the controller programming is carried out in one of the five languages defined in the above standard, enabling application transfer and integration "relatively easily" when working with various manufacturers' controllers.
Controller Programming: In the past, it was customary to program controllers using a single method called Ladder Logic, and Control Computers (HMI) - using HMI provider software. This process is done by an Engineering Station.

**Most Common Programming Languages:**

- **Ladder Logic**
  A classic method, which allows a programmer to translate the logical thinking process into a drawing and diagram. The programming process is carried out through translation A business process is desirable to sequence operations represented by illustrations from the electricity

sector simulating switch, digital input, time counter and more.

- **Function Blocks**
  The function allows one software component to be used in several different places, while maintaining the uniformity of the operations and optimizing the writing of the software.
  **Note:** It is important to note that controllers developed using these measures are more immune to making changes to the software process in a way that would impair the process.
- **More languages**
  IL (Instruction List), Structure Text (STFC), Sequential Function Chart (SFC).

## 2.4. Trends and Challenges Common in ICS Environments

### Production environment

- **Standardization –** Use of standard operating systems that include cyber exploitable vulnerabilities.
- **Need for connectivity –** Linking networks or linking to IT and the internet increases visibility and attack surface.
- **Unsecured connectivity –** Modems, remote maintenance approaches, wireless communication (such as Wi-Fi)
- **Information Security and Architecture –** Availability of information about architecture, installation and maintenance practices, structure of interconnection configuration with controllers, controllers on controllers, and famous and known cyber-attacked victims across the Internet.
- **Using IoT Devices & Capabilities**

### App layer

- Obsolete apps, written in an unsecured way.

### Configuration layer

- The systems have been built for years running, without booting, so updates are very difficult to implement.
- Many times, the passwords are burned in the Factory Default Passwords code and sometimes difficult to change.
- There is usually difficulty in encrypting (sensitive) fields.
- Antivirus systems cannot always be installed on equipment (for operational and contractual reasons), or systems that prevent unknown code execution.
- Difficulty in managing and identifying users, as this is an operating environment.

### Network layer

- The development of technology has led to a trend of linking isolated operational networks to an administrative environment, creating many vulnerabilities that expose them to a wide range of threats.
- Focusing on real-time performance makes it difficult to introduce network information security components (Latency).
- Difficulty performing network scanning (Asset Management) due to the fear and risk of delaying production processes (such as Ping Sweep that caused past failures).
- Operational and legal difficulties in conducting classic and active intrusion tests on the network and equipment for fear of dropping the system.
- Difficulty in encryption and network segmentation.

# »»»» 3. Presenting cyber risks on ICS systems

## 3.1. Introduction to Cyber Risks on ICS Environments

As operating systems and production line, ICS systems are systems that have been designed and used for years. Sometimes these are networks without controls or security mechanisms (physical or logical) and without inputs against cyber attacks. In recent years, the realization of attacks on ICS systems has become even easier. The trend stems, among other things, from the ability to detect volnerabilities, identify loopholes, obtain and use hacking tools, and these have led to an increase in the attack trend[9]. Using existing tools and capabilities, such as using the SHODAN website, enables mapping of Internet-connected ICS environments.

An analysis of the history of ICS events published, shows that the threats to these environments are not significantly different from the threats to IT environments. In both cases, the threats can be categorized as those seeking to compromise credibility/reliability, availability and confidentiality (CIA). These threats include attempts to damage business continuity through a DDoS attack, listening to communications, disrupting and/or changing a component's function, data theft, Ransomware attacks etc. Sometimes the production network attack starts with an advance attack on IT networks (such as the energy infrastructure attack event in Ukraine - BLACKENERGY)[10]. The big risk in ICS attacks is that the process of balancing and material damage, such as boiler, turbine, etc., can cause significant damage in providing essential service or harming human life.

9 https://www.nozominetworks.com/downloads/US/Nozomi-Networks-TRITON-The-First-SIS-Cyberattack.pdf

10 https://www.us-cert.gov/ncas/alerts/TA18-074A#revisions

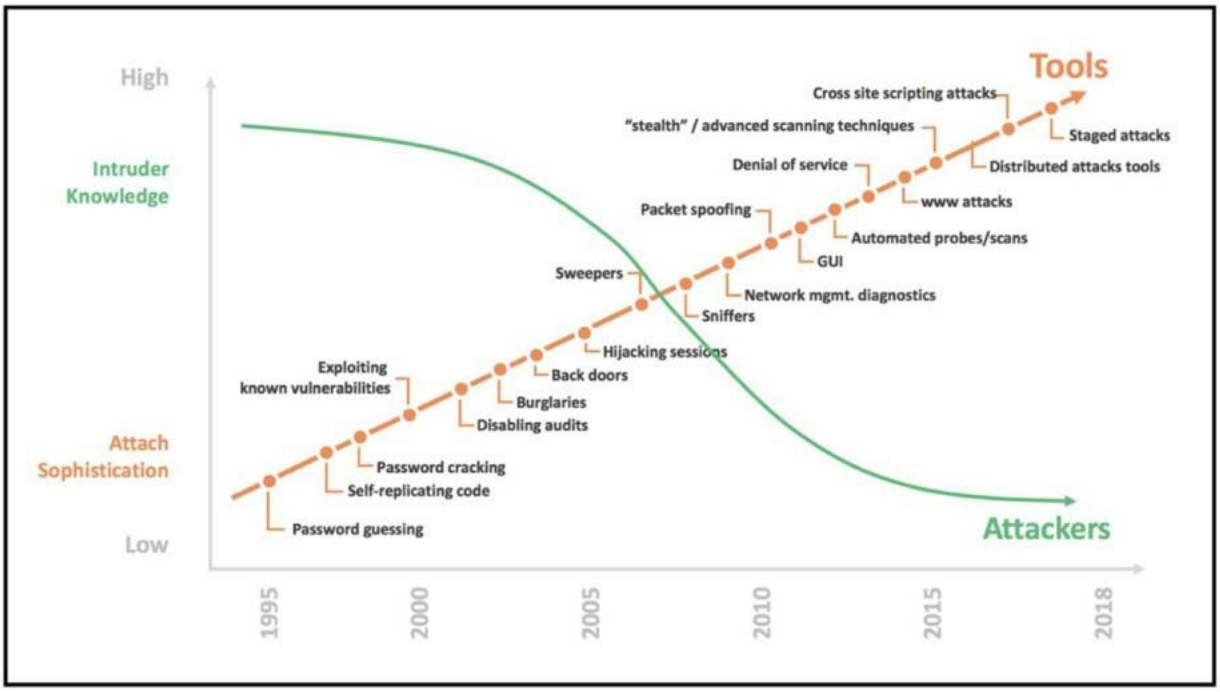


**Figure 9: The development of attack tools for ICS environments in recent years**[11]

## Popular attack methods for ICS networks are based, among others Permit, on[12]:

- **Utilizing Weak Authentication Mechanisms**
- **Network Scanning/Probing (Port Scanning) -** As part of the attack process to locate open ports in the organization and gathering stage
- **Removable Media -** as part of a jumping between different environments.
- **Activate Brute Force** password tools and software as part of a hacking experience process.
- **Abuse of Access Authority (legitimate permissions) -** by the user or malware programmed to use the permissions.
- **Phishing Spear phishing attacks** (mainly popular for Internet-connected ICS networks, such as the BLACKENERGY event and an attack of critical infrastructures)[13]
- **SQL Injection.**

## Sample scenarios:

- Utilize default passwords
- Change a controller command
- GPS-based systems or satellite communications attacks

11 https://www.nozominetworks.com/downloads/US/Nozomi-Networks-TRITON-The-First-SIS-Cyberattack.pdf

12 ?https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

13 https://www.us-cert.gov/ncas/alerts/TA18-074A#revisions

- Listen to the Communication
- Inserting a hostile code through an upgrade Hostile code insertion using an external device connection

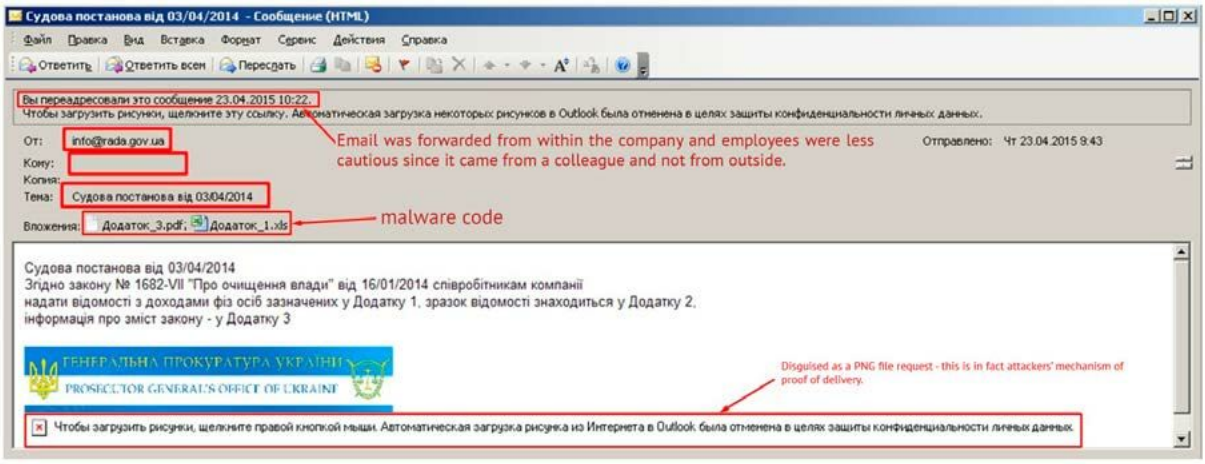


**Figure 10: An attack that began in the IT surface for the purpose of realizing intentions in OT[14]**

In the ranking of the top ten threats on this issue for 2019, published by the German BSI, the following picture emerges:

| Top 10 Threats | Trend since 2016 |
|---|---|
| Infiltration of Malware via Removable Media and External Hardware | ↗ |
| Malware Infection via Internet and intranet | ↗ |
| Human Error and Sabotage | ↑ |
| Compromising of Extranet and Cloud Components | ↑ |
| Social Engineering and Phishing | ↘ |
| (D)Dos Attacks | ↑ |
| Control Components Connected to the Internet | → |
| Intrusion via Remote Access | → |
| Technical Malfunctions and Force Majeure | ↘ |
| Compromising of Smartphones in the Production Environment | → |

**Figure 11: Changes in attack trends in 2019 versus 2016[15]**

14 /https://socprime.com/en/blog/dismantling-blackenergy-part-3-all-aboard

15 BSI: Industrial Control System Security - Top 10 Threats and Countermeasures 2019

In many situations, operating networks are isolated and separated from the Internet. These security arrangements make it difficult to organize and penetrate the process. However, attacking ICS networks as a differentiated network is usually possible in four main axes (and according to their requirements and protection inputs in the design stages below):

- **Internal threat** (an operating incident caused by the employee inadvertently or fraudulently) - and in cases where the attacker had physical accessibility (including exploitation of technicians)[16].
- **Mapping and exploiting opportunities on the supply chain axis** (such as exploiting by spoofing/ activating a party that supports the site or installing malware on the vendor's equipment).
- **Exploitation of input and output channels** and attacking through them (such as Data Sanitization & Content Disarm and Reconstruction -CDR, updates, etc.).
- **Side Channel Attack-based attacks** - exploiting physical & technological environment limitations that exist in the computing environment for data guessing processes, collecting or jamming (such as using electromagnetic inductance).

In recent years, the power of computing has grown and the need for diverse connectivity with other systems, such as business analysis and forecasting, operational performance analysis, output measurement, forecasting failures, fault resolution, etc. These capabilities are designed to leverage organizational activities and provide present and future business and functional needs. This connectivity also rests on the integration of IoT technologies, which also enable attack channels.

Due to the advantages of the development of the above technologies, the concept of a **"differentiated operating network"** is dissolving. Nowadays search engines like SHODAN can find access to operating environments management interfaces.

16 https://www.gov.il/BlobFolder/generalpage/coping_thret/he/Organizational_coping.pdf *** In Hebrew**

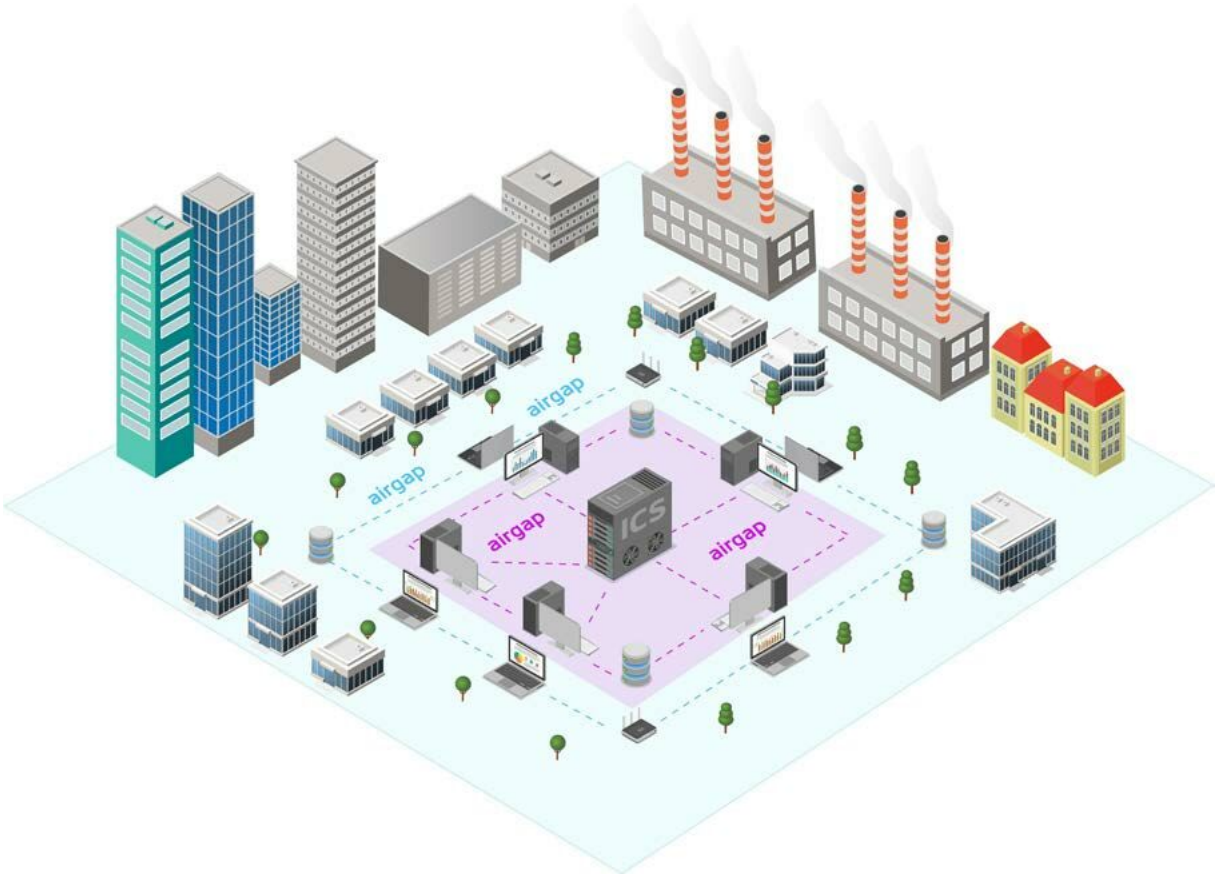


**Figure 12: Isolated network from external network**

## 3.2. Defense Challenges in OT vs. IT Environments

**Differences in IT Systems Protection versus OTs and Industrial Control Systems (ICS) in particular:**

While cyber defense workers are familiar with and experienced in the processes and technologies for protecting the traditional computing environment (IT), the knowledge and ability to realize the same concept and level of protection of the operating environment (OT) is limited. This limitation is due, in part, to the following challenges:

### People:

- **Knowledge -** data, information security and cyber security professionals are most familiar with the protection of IT environments (protocols, products, tools and more). Sometimes they

do not understand the change needed to adapt their knowledge when assessing risks, choosing protection solutions, monitoring and preparing a recovery plan for operating environments.

- **Collaboration -** Most often, the trust that runs the operation and maintenance of the systems in the production environment is a factor that is not hierarchically subject to the Information Security Manager, or to the manager of the information systems and communications networks in the organization. The ability to make reviews/changes and hardening requirements requires deep collaboration between the two different units in the organization.

  While cyber defense professionals usually have the knowledge needed to talk to IT professionals, the knowledge required for dialogue with operations/control professionals is different (sector-specific knowledge, such as a variety of concepts relevant to a production environment such as PAC, which is inexistent in the IT network, **understanding of chemical/engineering processes etc.).**

- **Dependence on external parties**[17] **-** While the IT environment can be used by enterprise employees and local vendors with whom the organization has good familiarity (including background work/ reliability checks), in working with these manufacturers, support and maintenance are often provided by dependent professional parties and are under warranty, and the client's ability to influence them is low (such as a system vendor or expert software from abroad).

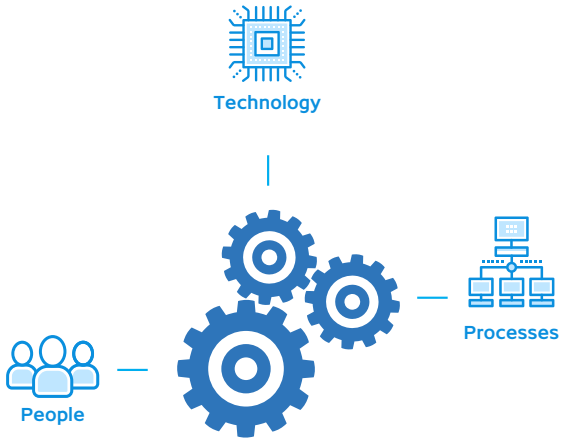


**Figure 13: The synergy, collaboration and synchronization between technology, processes and people**

## Processes:

- **High capability and cost of production line and business operations -** any need for upgrading, updating or downtime

17 http://www.sviva.gov.il/subjectsEnv/Documents/public-comments/2018/toxins-permit-terms-information-and-cyber-protection.pdf *** In Hebrew**

is immediately translated into large amount of money and risk to the control process. As part of risk reduction, a dedicated area for running of files and simulations can be considered as a preliminary process before the network online process.

- **"Halting/Downtime" cost –** Difficulty in balancing risk and locating appropriate controls that prevent stopping the process versus locating compensatory controls that allow risk reduction without stopping & compromising the production line.

**Technology:**

- **Limited supply of dedicated protection solutions –** While solutions such as code analysis, vulnerability detection and more are available and embedded in many systems around the world, they may not always be compatible with dedicated ICS environments. In addition, these tools are not always approved for use by the manufacturer or by the equipment's operators, due to concerns about operational damage, liability coverage, etc.
- **Equipment Lifecycle –** While IT equipment is replaced relatively frequently in organizations and proportionately (in relation to the organization's financial cycle), the replacement of a controller or component of SCADA involves significant efforts, resources, and financial cost to the organization. This leads to a reality in the area where equipment is 10-20 years old or more, which is required to protect it with the existing tools (which are limited and often never fit into this content).
- **Use of old and unchangeable technologies –** such as a network that has not been given security inputs in the characterization and construction process, the use of old controllers, protocols and traditional communication based on old, unsupported classic technologies. Hence, there are difficulties running antivirus or security updates, etc.

## 3.3. Adapting the CIA Model as the AIC Model to the Operating Environment

In the world of data protection, the subject of protection is information. Damage to it may lead to loss of trade secrets and/or sensitive data, impairment of data availability/data & information as well as incidents of data

breach (the disruption of information). These events are classified into the following categories:

**C -Confidentiality**
**I -Integrity**
**A -availability**

In the operating world, most of the focus of the defense is not just on confidentiality information & sensitive data but more on safety aspects and business operational implications related to the production line process, which can be caused by a cyber-attack, which can result in human life, environmental damage, and major economic damage (in case Of business continuity injury). In view of this, the recognized CIA model is required to be adapted to a dedicated language, which is suitable for the operating environment, the operating personnel, the production engineers, the process engineers, etc.

When performing a risk assessment process, we can work, for example, with one of these two models:

### AIC model

- This model changes the order of parameters of the recognized CIA model. The change reflects the importance of availability and business continuity in the production line. Since the object of defense in the OT world is the operational process, the first priority is the ability of the organization to continue producing. Confidentiality of data & information takes on a slightly different level of prioritization. It should be noted that sometimes the reliability of the data can be compromised in cases of human life risk and safety incidents. In these cases, many entities will prefer parameter I over business continuity (parameter A). Inputs will also be applied to maintain the logic of the controller and to examine the field and truth indicators.

## 3.4. The Star Model - Based on NISTIR 8183

- This model focuses on the consequences of the injury. These consequences are aimed at the potential damage as a result of the realization of a cyber event on operational continuity, conservation of human life, environmental protection, quality control and trade secrets. This model is represented by the following diagram:


**Figure 14: A star model**

## 3.5. Summary of the differences between the IT environment and the OT environment:

| Category | Industrial Control Network | IT Network |
|---|---|---|
| Performance requirements | Accuracy in time synchronization | Exact synchronization can be compromised on (and updated in different frequency) |
| Availability Requirements | There must be continuous availability, any downtime must be planned well in advance | Maximum availability is desirable (sometimes subject to availability - depending on risk management) |

| Category | Industrial Control Network | IT Network |
|---|---|---|
| Risk Management | Human life risk is a top priority, alongside physical, operational, regulatory and environmental risks | Maintaining critical information and privacy, and business risk (financial, image) |
| The focus on defense | Protection of endpoint equipment, manufacturing processes and finished product (in case the produce can be disrupted, such as food doses, pharmaceuticals) | Protecting your IT assets and information & data stored in your organization |
| Running software and updates | Running software and updates must first be tested outside the production environment in order not to impair system performance, high costs in setting up a lab environment. On the other hand, many systems installed in redundancy and redundancy configuration reduce the risk by changing PLC'S 1 and after entering work, the controller 2 controller can be made. Planning inputs for configuration and modification and hardening of DEFALT settings must be ascertained | Software and updates are built into the IT environments and therefore more tailored |
| Emergency Interactions | Supplier/manufacturer capability for operator response and emergency operations are critical. Sometimes this approach is also routinely required in support of providing support (for example, for an event that occurred, or for data monitoring for operational purposes) | Ability to close an emergency communication approach, the ability to respond to the incident through various and independent parties. |

| Category | Industrial Control Network | IT Network |
|---|---|---|
| System operation | Careful change management, operation of a variety of dedicated systems | Systems adapted to change, most commonly known systems |
| Resource constraints | The systems are adapted to operational work. Security systems cannot always be added due to a lack of processing and memory resources | System planned for the addition of resources (increase memory, CPU and disk space) |
| Communication | A variety of protocols | Standard communication in familiar protocols |
| Change management | Comprehensive testing is required in test environments, careful planning is required for any change | Standard changes, regulated and common processes |
| Managed support | Support of each manufacturer individually | Allows a variety of support capabilities |
| Access to components | The components can be isolated or nationwide, usually additional physical security is required | Components are usually clustered in the site in server rooms and are accessible |
| Equipment lifecycle | Decades | Individual years |
| Tolerance for harm to business continuity | Very low | Very little |
| Software updates | Low | Frequent |
| Cyber awareness and knowledge | Usually low | Usually existent |

## 3.6. Cyber risks according to layers of the PURDUE model

Cyber-attacks can exploit vulnerability in each of the model layers (ZONE) and their transitions. This section will review the attacks that utilize the communication/ channel that connects the model layers (such as moving from layer 0 to layer 1 in the model).

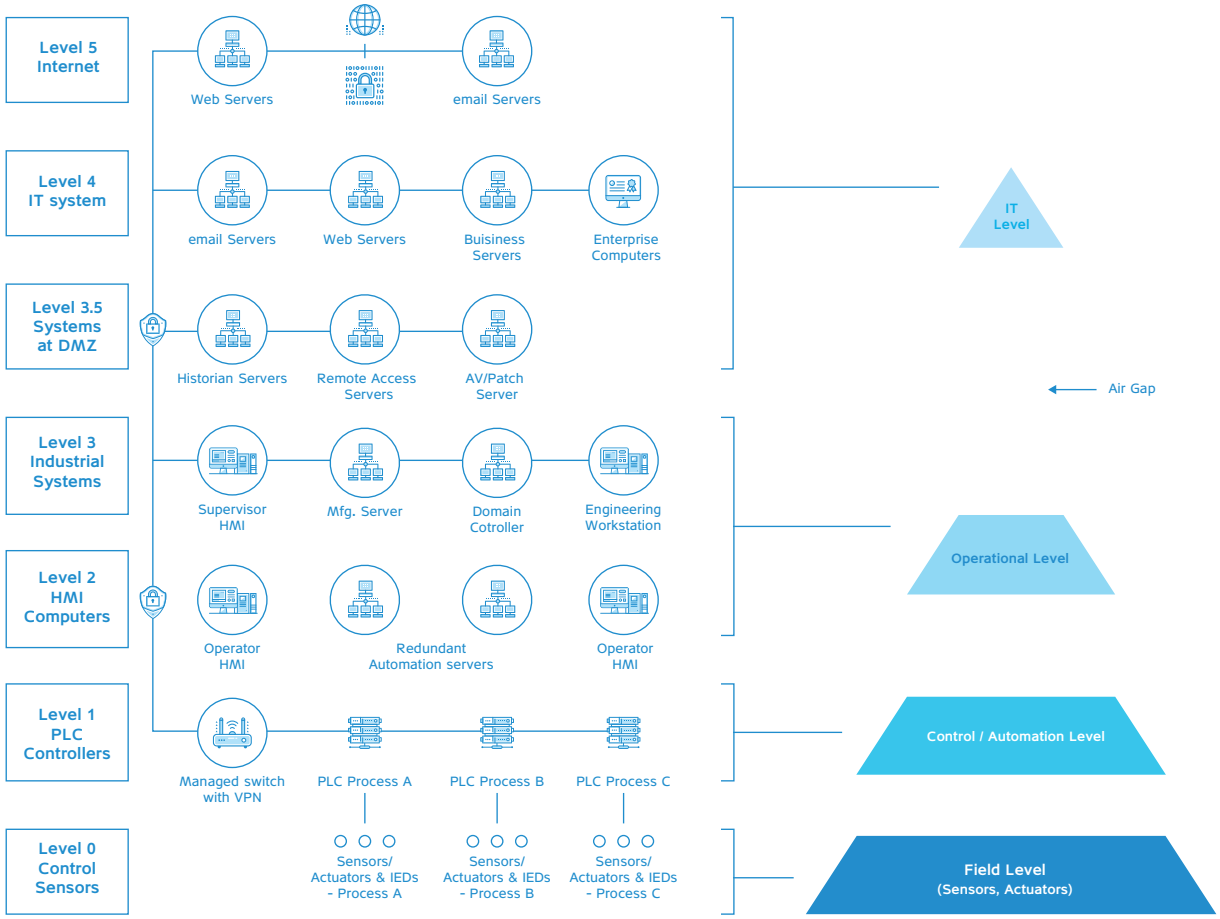


**Figure 15: Overlap zones between the models (PERDUE and the triangle model)**

### 3.6.1 Layer 0 cyber risks:

- There are sensors and controllers in this layer that monitor the operation of machines or active means of operation, such as contacts, analog sensors and more. The risk at this level is manifested in the potential of physical or logical attack, which will lead to changes in some component (sensor, pressure regulator, temp, taps, etc.), which will incorrectly measure and enter incorrect data on the analysis of the processes and the implications thereof.

### 3.6.2 Cyber risks in transition 0-1:

- The connection between the Level 0 devices and the Level 1 controller is conducted through electrical or serial and serial communication connections. The risk at this level is the transmission of fictitious & wrong data, as well as the possibility of tampering with wiring or the replacement of a material component.

### 3.6.3 Layer 1 cyber risks:

- Controller Mapping (PLC/RTU) that manages the controlled process. The main risks for this disabling process are the change of logic, configuration or alternative code implantation into the controller.

### 3.6.4 Cyber risks in transit 1-2:

- This transition is based on network communications (LAN) over protocols (over TCP), such as MODBUS, 3 DNP PROFINET, IEC 60870-5-104, and more. Outdated systems use serial communication (RS-232), including protocols like MODBUS, 1-DF, PROFIBUS, etc.

  **The main risk is the ability to connect to the system, especially if the communication is wireless (unencrypted) and also the ability to bridge networks and intervene in the process. Poor configuration of the protection systems (such as the Firewall) between layers and components will allow an attacker to exploit open ports for continued network expansion and propagation.**

### 3.6.5 Layer 2 cyber risks:

- In this layer is the center/control server, which manages the process and includes the HMI computers. It should be taken into consideration that there are HMI systems that do not receive software updates (Windows XP), mainly due to the fear of systems crashing after the update. These systems are in the control room, and there is a risk that an unauthorized party will

take unauthorized action, such as inserting a USB device into one of the computers and causing the damage to spread. This layer also contains an engineering server, which has operational information about the software in the controller and also the control center software.

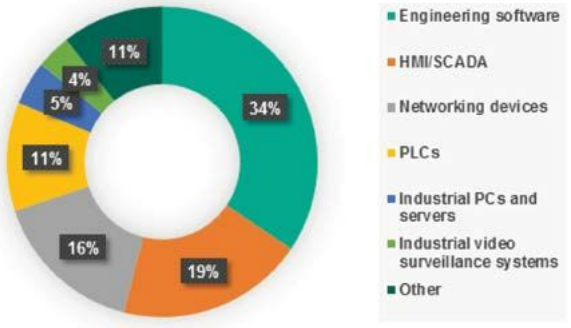


**Figure 16: Mapping weaknesses by components in ICS environment (Kaspersky site)[18]**

### 3.6.6 Additional layers of model:

- Layer 3: The operating layer in which the computers and operating servers are located.
- DMZ-3 Transition: This network transmits data from the control system in the IP/TCP protocol
- DMZ layer: This network has computing systems whose role is to be found within DMZ
- DMZ-4 Transition: In this network, data from the control system in the IP/TCP protocol is transferred to the management environment, the engineer positions and workstations.
- Layer 5: This network contains the IT systems that serve the OT systems (sometimes these stations are connected to the Internet).

18 https://ics-cert.kaspersky.com/media/KL_ICS_CERT_H2_2018_REPORT_EN.pdf

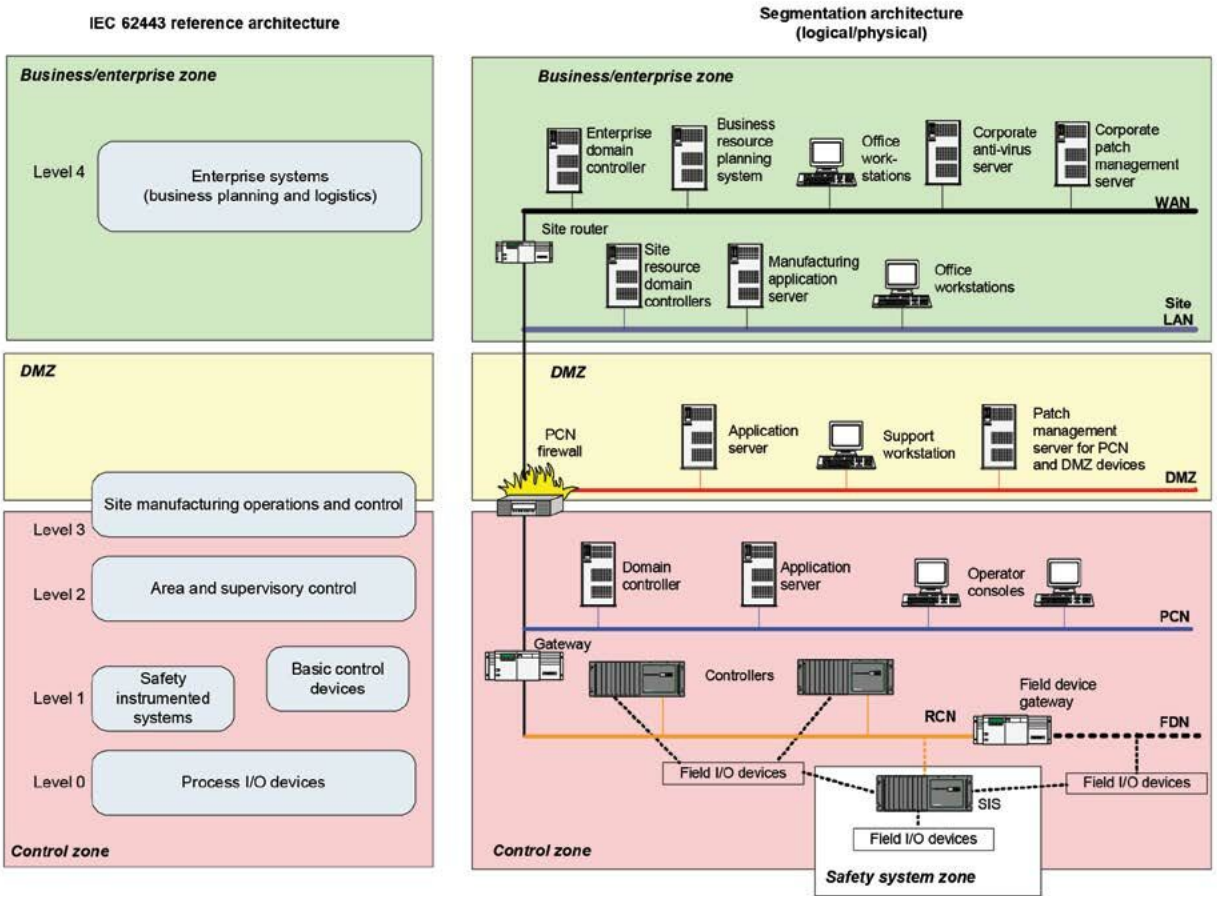


**Figure 17: Component Mapping in the Layer Model (Standard IEC-62443-3-1)**

Firewall (FW) setting & realization in the ICS environment is a complex event in an operating environment, sometimes for security reasons, etc.

The distribution and settings should be in accordance with the PURDUE model and in accordance with these guidelines:

- The FW design will address the data movements between the OT and IT environment and the classic incidents and problems with the ICS environment, including targeted attacks, APT attacks, etc[19].
- Define rules for preventing internal and external unauthorized communication
- Restrict access from the enterprise network (the administrative

19 https://www.energy.gov/sites/prod/files/Good%20Practices%20Guide%20for%20Firewall%20Deployment.pdf

network) to the operational network in a manner that prevents queries or direct commands to controllers.
- Ensure that settings are adjusted and the ability to detect and detect threats in OT protocols.
- FW settings are suitable for vendor support outside the organization.
- Related FW settings for wireless connectivity (as needed and after an organization approval process) - To prevent illegitimate communication and exploiting attack opportunities on these channels.
- Process for collecting and analyzing attack IDs and defining definitions accordingly
- Inputs for managing strong privileges for changes in the FW system.
- As part of the process of ensuring compliance with safety requirements, make sure that the protective measures and FW settings do not create failure points.

**Highlights for dedicated FW settings based on the PURDUE model**

- Layers 4-5 - Sometimes, it is an environment that is connected to the Internet or the Internet-connected systems, and therefore, in this layer, the implementation and definition of rules for the prevention of direct and open (outbound and inbound) communication to the Internet must be ensured - in order to prevent unwanted communication, Denial-of-Service (DoS) attacks, Corrupting or preventing internal messaging.
- Layer 3 - Dedicated inputs for differentiation versus Layer 4[20] will be provided.
- Layers 0-2 - The control systems layer, the HMI and its role to enable the monitoring and control of command and control processes, to enable the operator's intervention as needed and the permissions given to him. The definitions and rules of FW that must be applied are against bypass of communications, possible actions involving the risk of causing harm and unauthorized actions (both in laws and restricting unwanted communication from the up and down layers).

20 https://www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327

### 3.6.7 Attention to the overall system structure in the organization

Differently from the PURDUE model, as well as from other models, four areas connected to each other are addressed:

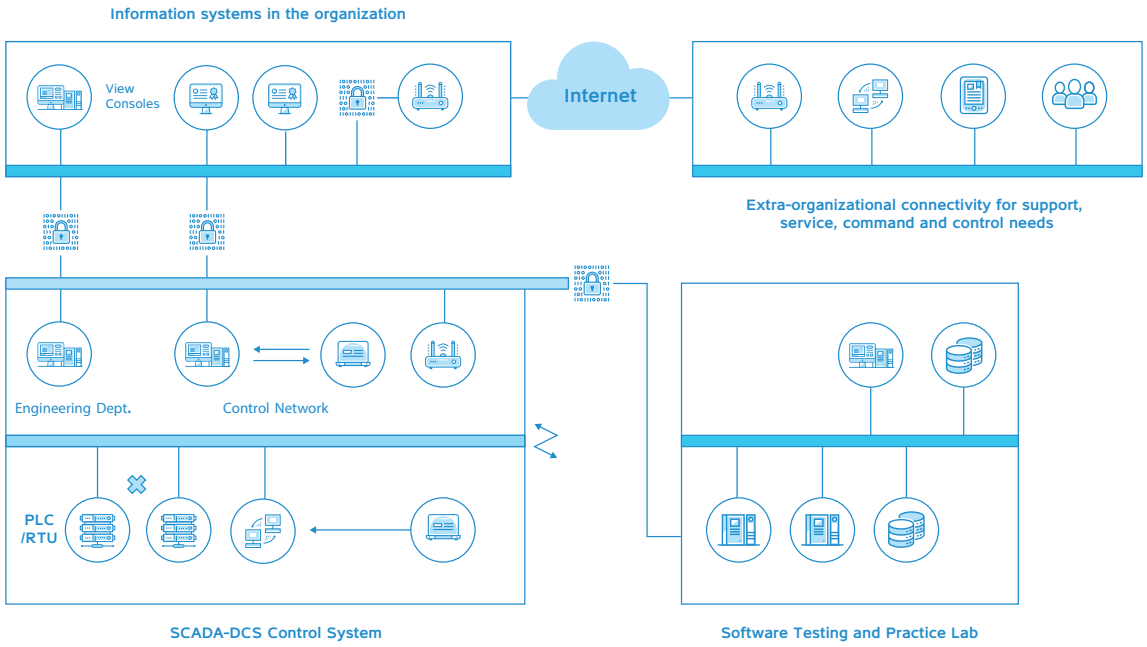


**Figure 18: Interfaces in the connection areas**

**Regarding IT connectivity**

- The connectivity between the IT environment and the OT environment also exists in industrial environments. This is to enable a management environment to perform the work. The connectivity to IT infrastructure (and sometimes the Internet connection) exposes the network to many dangers.

**System Test Lab**

- This system includes a control system that simulates the real system (Digital Twin). This environment is securely connected to the control system and is used for software testing, operator training, and device testing. Although secure security and interconnection mechanisms exist, there is a risk of infringement from this environment.

**Extra-organizational connectivity for support, service, Command and Control needs**

- This area includes the external parties which are required to connect to systems, including suppliers, support service providers, employees supporting outside the organization, etc. The concern and danger are for exploiting this connection for attack purposes (including Man in the Middle (MITM) threats, Denial of Service attack (DoS), exploitation by hostile parties, and more).
  The operating and control systems environment (production line) - This includes the production process, the engineers' computers, the HMI systems and the controllers.

# 4. Risk assessment and management in ICS systems and principles for addressing in a work plan

## 4.1. Cyber risk management process as part of risk assessment and management

The purpose of the cyber risk management process is to examine organizational risks and subsequently reduce the impact of exceptional events on the organization. The process includes formulating risk scenarios that may harm the organization, assessing the potential for damage during its realization, assessing the likelihood of scenario realization, prioritizing scenarios to handle scenarios according to intensity, which is a combination of risk impact and probability of realization, and finally characterizing a risk mitigation plan[21].

Risk management process in ICS systems is an important and complex process. ICS systems are differentiated critical systems, which use different and sometimes mixed protocols, hardware and software. On the other hand, the knowledge available to the IT professionals, operating costs, maintenance, upgrades and avoiding continuous damage to the production process (such as the patchwork update dilemma in a production environment) is challenging and unique in the risk management process in the ICS environment compared to the IT environment.

This process is carried out cyclically according to technological, organizational changes, threats and new attack capabilities, etc. The purpose of the process **is to carry out a proper assessment of the risk in a manner that is acceptable by all parties within the organization** (management, production line personnel and computing entities) and subsequently - translate into a dedicated work plan to reduce the impact of exceptional events and prevent damage such as safety incidents, injury to life or damage to the production line.

21 https://pdfs.semanticscholar.org/cb14/b23b9d0d4242edb1057b722e7a6f923d4885.pdf

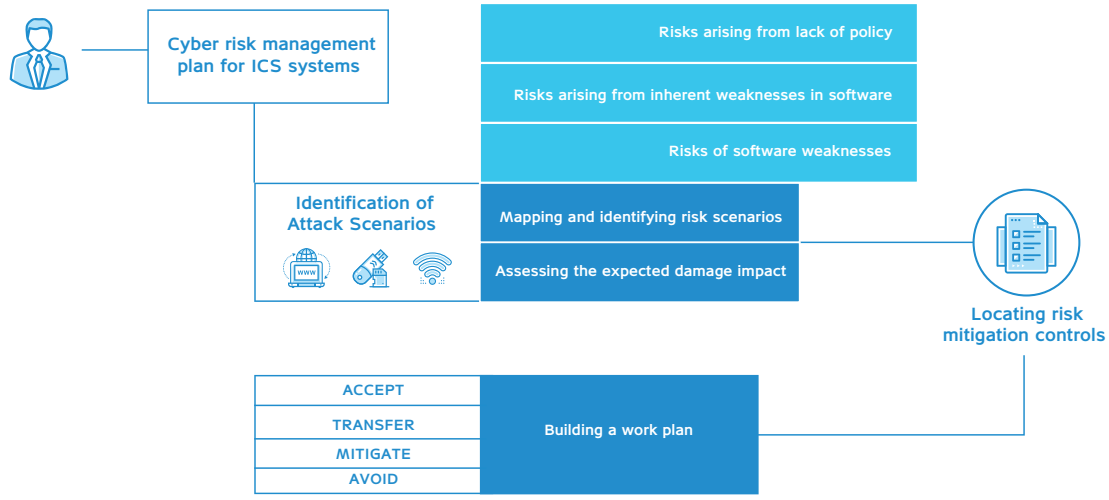


**Figure 19: Cyber risk management process and work plan for IC environment**

## 4.2. Mapping the Risks

Risk mapping is based on the following processes (and their synergy):

- Asset Mapping - The mapping phase also links IT/OT assets (see Chapter 5.2 in Defense Theory)[22].
- Risk mapping resulting from a lack of policy (by mapping regions and issues without policy).

Figure 20 on the next page allows to formulate policies by activity areas on the one hand, and on the other hand to identify risks in areas where there is no policy.

22 Organizational Cyber Defense Doctrine - https://www.gov.il/BlobFolder/policy/cyber_security_methodology_for_organizations/he/Cyber1.0_418_A4.pdf *** In Hebrew**

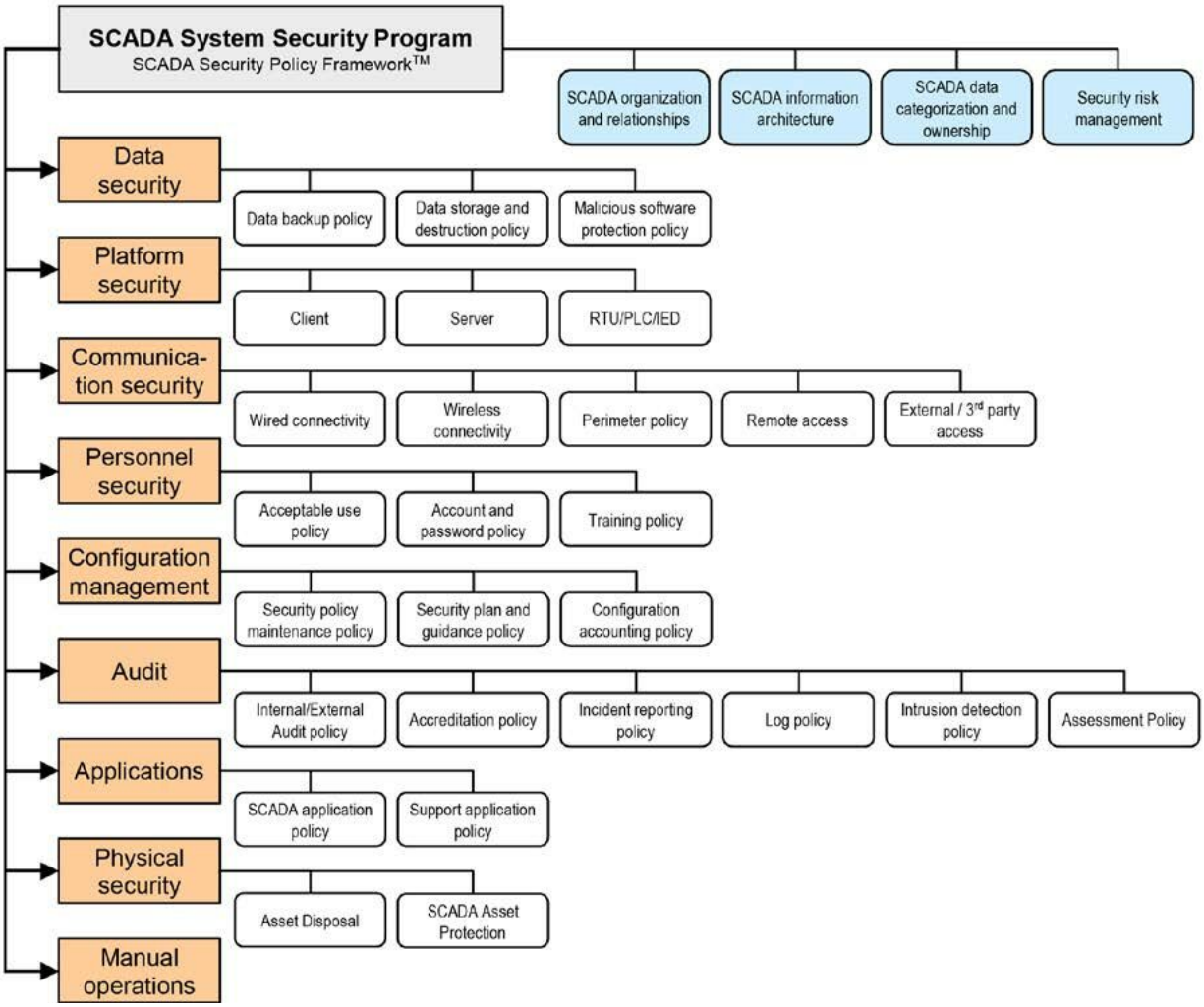


**Figure 20: Framework for SCADA Security Policy in the Organization**

The mapping process will be as follows: System architecture description and component interface description - which will **allow a visual snapshot of the network environment and dependence on various components** and of different types (for instance, several different controllers) - communication and protocols, and pointing out **risks arising from policies, hardware and software weaknesses, and so on.**

**The process of risk mapping in relation to these processes requires:**

- Knowledge of the business process and the components used (including mapping sensors, networks and subnets, communication type, participant components, and logical topology of the environment).

- **Identification of risk scenarios, which are also based on intelligence and event history in the organization and in the sector** – a process that is also accompanied by a review of critical processes of the organization and how feasibility can affect these processes. The risk scenarios depend, among other things, on: those with an interest in attacking the organization, their capabilities and tools at their disposal, and past attacks.

**A scenario bank can be used, or a common risk table, such as the one included in the review in this document, or a table such as this one.**

| | |
|---|---|
| 1. Risk arising from the use of older unsupported systems that do not have advanced security capabilities, and the lack of availability of end-of-life security updates | 6. Cyber risks arising from supply chain processes (such as backdoors and processes with risk potential on the supply chain axis, such as using a computer technician shared by several different customers) |
| 2. Risks in connecting components with wireless interfaces | 7. Security gaps and backdoors built into the software (inability to integrate third-party protection solutions) |
| 3. Increasing attack surface due to frequent use of unsecured interconnection (takeover channels, support and update downloads) | 8. Opportunities for physical penetration and lack of inputs for prevention |
| 4. Personnel shortage of cyber experts in the production line (planning, support, risk management, etc.) | 9. Irregular policies on antivirus and patch updates (security and operations) |
| 5. Unregulated environments, which allow Air-Gap jumping and spreading between networks | 10. Human error (operator), which can cause security gaps and attractive opportunities for attacker |

- **Assess the impact of the expected damage, if any,** on the operating process, safety events, operational damages such as disabling a unique system or controller in a way that would damage the production line, financial damages, etc.
- **Define defensive response and necessary compensatory controls.**

  **Please note:** For a sample template for conducting a risk survey in operational environments and for raising awareness of the issue within the organization's management, see Supplemental Documents on the **Israel National Cyber Directorate**[23] website.

## 4.3. Risk management in the ICS environment versus risk management in the IT environment

Risk management process in ICS environment is different from risk management process in IT environment:

| Factor | IT | OT/ICS | Notes |
|---|---|---|---|
| Connection to business processes | Important | Mandatory | Risk assessment for such an environment cannot be performed without the process being recognized as it arises from conversations with the process engineer and the operational parties. Detecting threats and vulnerabilities is not possible without a thorough understanding of the information flow and process components in depth. |

23 https://www.gov.il/he/departments/topics/organization_cyber_protection * **In Hebrew**

| Factor | IT | OT/ICS | Notes |
|---|---|---|---|
| Defense Capabilities | Commercial protection solutions exist, and a great deal of professional knowledge is available in the field | Many protection solutions are not suitable, cumbersome and/or irrelevant to this environment. The legal and operational ability to install a defense solution and monitoring tools to perform scanning etc. in this environment is very limited | There are dedicated commercial solutions to the ICS world, but they are less time-consuming than solutions for the IT environment where the supply is wider and more experienced in the field. In addition, operators' resistance to interference and impact on operational processes is greater than resistance that sometimes exists to install server and network protection component in the IT environment. The solution usually depends on the control provider. External solution cannot be inserted. |

| Factor | IT | OT/ICS | Notes |
|---|---|---|---|
| Considerations of complex environment variability | Unified environment | Complex environment | There are differences between the environments and complex considerations of the OT environment that have equipment with a lifespan of 15 years, as well as an environment where there are no regular software updates and protocols. These characteristics are due, in part, to the operational needs of the production line [24], which are sometimes not supported by traditional security solutions and are not well known to IT professionals. |
| Damage Potential | Most of the damage will be financial, with secondary damages of reputation, privacy and more | The damage can also be manifested in the termination of production line and damage to human life | Damages that mean a normal lifestyle injury (also at a state level) |
| Conclusion | Protecting ICS Environments: The organization is faced with a very limited defense capability vis-a-vis resource-owning parties which with interests that can cause immense damage. This reinforces the need for organizations to primarily strengthen their monitoring and response capability in protecting such environments. | | |

24 Anastasis Keliris Enabling Multi-Layer Cyber-Security Assessment of Industrial Control Systems through Hardware-in-the-Loop Testbeds, New York University School of Engineering

# 5. ICS system controls

Cyber protection for ICS systems requires integrating protection into "security circuits" using several cyber protection methods and technologies. Since no single technology is available for all types of systems, a variety of controls are required, tailored specifically to the level of risk, system implementation, system operation, system structure, communications technologies, geographic space over which the system is deployed (city, factory, building) and more. The control bank presented in the following table is dedicated and suitable for the ICS environment. The controls presented below were selected based on the ICS environment, computing components, interfacing systems, and technologies. The success of implementing and implemention security controls to mitigate risks depends on the organization, size, nature and complexity (in this way, some controls may reduce risks to mixed environments, while in isolated environments some may be dispensed with).

Proper process for selecting and implementing appropriate controls involves appropriate risk management process.

## 5.1. Cyber Protection Controls in ICS Systems

(Suitable for Industrial Controllers - Defense Theory)

| Control ID | Title | The Control | Complementary explanation | Control Implementation Example | Control Depth* |
|---|---|---|---|---|---|
| 12.1 | Industrial Controllers Policy | Organizational policies should be written, managed and audited for the protection of industrial control environments. This policy responds, to the appointment and definition of a role, which includes determining the division of responsibilities between office holders and parties responsible for the OT network and tangent networks. | The organization will define its operating system policy, including reference to remote access policies, version upgrades, software updates, third-party maintenance, and more. | Supportive policy writing and procedures can be implemented and define the unique requirements for the environment of industrial controllers (production/ logistics/ environmental control/power generation and more).<br>Existing regulatory aspects of these environments must be addressed (for example: FDA, Israel National Cyber Directorate).<br>Make sure that the policy document regulates and defines the body responsible for the organization.<br>The division of responsibilities will cover various areas, such as who is responsible for software updates, vendor login, file uploads for upgrades, etc. recommended,<br>Because the ICS environment's cyber protection trust will have an official nomination letter signed and approved by the organization's management. | 2 |

*** Control level complexity from 1- (low) to 4 (complex)**

| Control ID | Title | The Control | Complementary explanation | Control Implementation Example | Control Depth* |
|---|---|---|---|---|---|
| 12.2 | Industrial Controllers Policy | Defined rules for proper use of equipment in the production environment and place signage explaining these rules. | The organization will define, signage explaining the data security practices at the work stations governing and monitoring the production environment. | The signage may include the use of shared workstations, the use of removable media devices, users log off and more. | 1 |
| 12.3 | Industrial Controllers Policy | Define the sensitive processes where industrial control environments exist according to their level of sensitivity. | The organization will map the processes where control environments exist and define the main business processes involving these controls in order to understand the level of business and regulatory damage that could result from such environments. | Document mapping processes and environments according to severity. | 2 |
| 12.4 | Industrial Controller Communication | Separate control networks from other systems and external networks. | The organization will set apart control networks, users' networks or servers into separate networks so as to restrict direct access between networks | The separation can be carried out using firewalls and separate VLANs for every monitoring network. Given the option, it is preferable to separate by one-way diode and allow only the release of data & information out of the organization. | 2 |

| Control ID | Title | The Control | Complementary explanation | Control Implementation Example | Control Depth* |
|---|---|---|---|---|---|
| 12.5 | Industrial Controller Communication | Separate the management system of industrial equipment controllers and the operative components of the system. | Implement adequate separation between the operational controls network and the management system of the controls. | In any cases that the system connects the production floor to other high environments (in accordance with the PURDUE model), for the production of management reports or other needs, and especially in cases where the operating environment is connected to the cloud, controls must be established in accordance with the "Cloud" section of this document or equivalent standard. | 2 |
| 12.6 | Industrial Controller Communication | Do not connect devices that are not production environment controls, to the production controls network. | The organization will not install equipment that is not part of the Industrial Control System in the controls network. Equipment which is required to be connected, will be connected to separate network, and communication will be enabled individually. | If necessary, to connect different equipment for interfaces with production systems, it must be connected by separate network segment behind the firewall. | 1 |

| Control ID | Title | The Control | Complementary explanation | Control Implementation Example | Control Depth* |
|---|---|---|---|---|---|
| 12.7 | Industrial Controller Communication | Support providers access to the production network will be possible with prior authorization as well as by using secure and identified communication, which allows recording of the provider's actions. | The organization will implement secure communications network for suppliers' access and will review the supplier's access to the organization by providing preauthorization for any provider connection to the control network. | Can be applied using VPN server management system for dedicated users for each provider (user priority for every employee of the provider), which will be usually locked and open only when necessary. | 2 |
| 12.8 | Industrial Controller Communication | Direct or indirect Internet access will not be allowed from industrial controllers as well as from humanmachine interfaces environment interfaces. | | Control networks on the firewall can be restricted and Internet access is not allowed from these networks, as well as integrate file whitening systems for a secure process in environmental transfer. | 2 |
| 12.9 | Industrial Controller Communication | Unnecessary services will be limited in the production environment and support systems, such as humanmachine interfaces and smart sensors. | The organization will cancel and. or limit unnecessary services for all systems in the control environment, whether at the level of operating system, communications level and application level. | It is possible to be based on the manufacturers hardning documents of the operating system and applications, and shut down services, block ports, limit applicative access to certain functions and more | 2 |

| Control ID | Title | The Control | Complementary explanation | Control Implementation Example | Control Depth* |
|---|---|---|---|---|---|
| 12.10 | Industrial Controller Communication | Use reliable communication between industrial controls and terminal equipment if possible. | Use protocols that allow the source and destination authentication and encryption of the medium supporting the equipment. | In an event that it is possible to use secure versions of these protocols, use these versions (SFTP, HTTPS, SNMPv3 and others). | 2 |
| 12.11 | Industrial Controller Communication | A one-way communication system will be setting to the OT environment. | | Tools for one-way communication between sensors and systems must be defined in sensitive environments. | 4 |
| 12.12 | Wireless Communication | Wireless networks in the production environment will be separated from Enterprise wireless networks. | The organization will implement. dedicated wireless network separate from the enterprise wireless network, to be used solely for control network communications. This network will not redirect to the enterprise network and vice versa. | It is preferable to avoid using wireless network in the control networks, but if necessary for business, this network will be set up separately, and its management will be also separate and it will not be linked to any VLAN's internal network. | 1 |
| 12.13 | Wireless Communication Wireless | communication in the production environment will be limited by using secure protocols. | | WPA-2 PSK should be used, where possible, we recommend using a digital certificate-based version for these wireless networks. | 1 |

| Control ID | Title | The Control | Complementary explanation | Control Implementation Example | Control Depth* |
|---|---|---|---|---|---|
| 12.14 | Wireless Communication | A separate user will be defined for each end client using. wireless network in the production environment. | | It's recommended to connect the wireless network to a dedicated Radius Server, which will authenticate users to and manage them. | 2 |
| 12.15 | Man-machine controllers management | Access to Man-machine interfaces will be enabled by personal users, for each operator. | The organization will define a personal user for each person working in front of a human-machine interface. If the station is a shared station, smart card identification can be used. | If and for safety reasons the position cannot be locked, compensatory controls (such as camera placement/ room access documentation, etc.) should be considered. | 2 |
| 12.16 | Man-machine controllers management | Access to human-machine interfaces will be enabled by using strong authentication. | The organization will establish strong authentication with access to human-machine interface. | A variety of measures can be used, such as biometrics, smart cards, OTP and more.<br>Also, make sure that sensitive equipment interfaces, such as the management/ engineering position, man-machine interfaces, etc., make use of unique and managed user names.<br>It is desirable that use of these accounts will be based, as much as possible, on strong identification. | 4 |

| Control ID | Title | The Control | Complementary explanation | Control Implementation Example | Control Depth* |
|---|---|---|---|---|---|
| 12.17 | Man-machine controllers management | Monitoring systems will be installed and activity recording will be carried out on the management servers. | The organization will set up activity recording systems/ logging with emphasis on the management environment of the production environment. | A variety of measures and tools can be used, such as screen recording user activity tools, application logs, etc. | 2 |
| 12.18 | Malicious code control | Install utilities such as intrusion detection tools in the management networks' environment of the production environment. | | Can be applied using tools such as IPS, honeypot traps and more. It should be noted that for safety and functional reasons, these tools cannot always be installed in operating environments. In such cases, sometimes using tools such as IDS may be a partial/ alternative answer. | 3 |
| 12.19 | Malicious code control | Install tools for file signature verification (Integrity Checking) to scan files being transferred to the management environment or installed in the management environment. | | Can be implemented using a variety of File Integrity Checking tools. | 3 |
| 12.20 | Malicious code control | Install dedicated anti-malware tools in human-machine interfaces | | Can be implemented using dedicated anti-malware tools, appropriate to the type of system. | 1 |

| Control ID | Title | The Control | Complementary explanation | Control Implementation Example | Control Depth* |
|---|---|---|---|---|---|
| 12.21 | Software Updates | Manufacturer software updates will be installed on lower environments (test before installing in the production environment. | The organization will ensure the installation of updates in test environment and will run them over time, in order to test the stability of the system and the process. | Can be realized by establishing lower environment (at least partially), diverting communication to this environment during maintenance Window in the production environment, and testing the process. | 2 |
| 12.22 | Software Updates | Install operating system updates that are supported by the provider in the production environment. | The organization will implement within reasonable time operating system and application updates as received from the system vendor and will demand from the vendor security updates for serious flaws as they are published. | As part of this process, reference should be made to the safe method of income of new equipment (such as devices and machines for the OT network and operating environment). Given the sensitivity of the issue, the ability to restore the operating system and software to initial state (state 0) must be ascertained by using firmware/ OS from a reliable source and rewriting of historical data that came with the equipment. | 2 |

| Control ID | Title | The Control | Complementary explanation | Control Implementation Example | Control Depth* |
|---|---|---|---|---|---|
| 12.23 | Software Updates | 'Lock Configuration' tools will be installed on End of Life systems, including obsolete operating systems. | The organization will implement tools that lock the system configuration into a "clean" configuration, if there is no other options to update the equipment. | | 3 |
| 12.24 | Detachable media in the production environment | The ability to connect removable media to production equipment, including controllers, human-machine interfaces and sensors will be limited. | Designated data warehousing bedding should be allocated for use of the OT network to minimize the exposure area and reduce the risk of network and Air Gap jumping. Attention should be paid to cases where private equipment of employees connects For positions, such as in the case of workers in the production line, connect for charging, telephony, etc. for charging or for version upgrades, etc. Management will be done through device management mechanisms. Any component that connects will be identified and pre-approved (White-list). | Can be implemented by disabling USB devices physically (port lock) or logically by operating system policy - GPO. Generally, detachable media connection that does not belong to the organization should be avoided, reviewed and approved by the cyber teams within the organization. | 2 |

| Control ID | Title | The Control | Complementary explanation | Control Implementation Example | Control Depth* |
|---|---|---|---|---|---|
| 12.25 | Detachable media in production environment | Removable media file transfer to the production systems will be carried out after data sanitization the transmitted files. | The organization will implement a set of "whitening" files and examine them in depth using several tools before transferring them to the controller environment.<br>For example, can be based on built-in technology or work process for checking and pre-registering: of the file source (user or site), date and time, documentation and reason for bringing the file, unique identification for each whitening, ability to investigate file transfer events. | Can be realized through the acquisition of specialized data sanitization station, or, alternatively, by establishing dedicated station, which includes several different scan engines. | 2 |
| 12.26 | Redundancy in the production environment | There will be a redundancy system array for critical components in the production environment. | The organization will implement a redundancy system of server and sensor redundancy critical to the control environments for the continuity of the process.<br><br>The organization will implement system of servers and critical sensors in the control environment for the purpose of process continuity. | In order to build redundancy it is recommended to consult with the control system vendor. | 2 |

| Control ID | Title | The Control | Complementary explanation | Control Implementation Example | Control Depth* |
|---|---|---|---|---|---|
| 12.27 | Physical access to the production environment | Physical access will be restricted according to business need only to the industrial controller environment as well as to the communication equipment in this environment | The organization will restrict physical access to media cabinets, hubs and management positions of the controller environment. It should be noted that even when legitimately connected (such as for the benefit of POC execution), the external component connection process is performed safely. | Can be realized by converting dedicated rooms to concentrated communications and servers, and perform access control using access tags and Biometrics for this environment. | 2 |
| 12.28 | Separation of logical approach and networks | Logical access will be limited for business needs only to the industrial controls environment as well as to communications equipment in this environment.. | The organization will limit the access of corporate users who have no business relevance to the control system and will prevent their access to these networks and equipment. | | 2 |
| 12.29 | Separation of logical approach | Logical access will be limited, to the extent possible, (functional) to the production systems, including control interfaces, sample interfaces and human-machine interfaces. | Access to the management systems will be limited according to user profiles. system controller will not change settings and parameters of. system. Changing the parameters will be carried out by an administrative user. | It is possible to verify the system's manufacturer whether the system can use different user profiles. | 3 |

| Control ID | Title | The Control | Complementary explanation | Control Implementation Example | Control Depth* |
|---|---|---|---|---|---|
| 12.30 | Robustness tests | Carry out information security testing in the production and management environments and interface, including penetration tests. | The organization will define comprehensive tests, outline for tests including the variety of control network components, with an emphasis on comprehensive information security tests for all components, in order to maintain the continuity of the business process. | Can be realized by checking the configuration of the environment, running simulations during downtime windows and performing penetration tests in these networks if possible and. or during maintenance operations. | 2 |
| 12.31 | Information Security Monitoring | Set up unique monitoring scenarios in the production environment and monitor them through an organizational monitoring arr. | The organization will define a variety of dedicated monitoring scenarios for the control environment according to the threat outline and the importance of the system to the business process. It should be ensured that monitoring and active registration systems are installed on critical assets, such as management servers/engineering positions. | Network monitoring in control networks is different from ordinary systems monitoring since the sensitivity threshold is lower. Any deviation from the amount of normal communication between the controls and the management interfaces and sensors may indicate. potential cyber-incident, since the activity in these environments is continuous and monotonous. monotonous. | 2 |

| Control ID | Title | The Control | Complementary explanation | Control Implementation Example | Control Depth* |
|---|---|---|---|---|---|
| 12.32 | Information Security Monitoring | The organization will have independent monitoring capability in the operating network and/or IT network. | This monitoring examines a change in the physical space, which is an indication that is independent of the organization's architecture and constitutes an anomaly, which requires an examination of the operating personnel for the exception. | This can be realized, for example, with the ability to read values (analog and digital) to measure changes from sensors and actuators (level 0) in a completely disconnected configuration that is independent of the operating network (out of band) and unaffected. These changes can be detected by measuring electricity, pressure, temperature, etc. | 4 |
| 12.33 | Equipment decommissioning | When removing equipment, or removing it from an external source, file deletion processes and sensitive data (such as logic files, passwords, etc.) from computing systems and computing equipment must be verified. | When removing equipment, or removing it from an external source, file and data deletion processes (such as logic files, passwords, etc.) from computing systems and computing and transfer equipment must be ascertained, including interchange processes at intersections, changing environments, and so on. | | 2 |

| Control ID | Title | The Control | Complementary explanation | Control Implementation Example | Control Depth* |
|---|---|---|---|---|---|
| 12.34 | Cyber Intelligence | A regular gathering of cyber intelligence and attacks in the OT world (visible information, publications, etc.). | Suitable inputs for dedicated monitoring of professional publications for the protection of computer systems and operating systems - ensuring a regular process for the collection and analysis of relevant information from internal and external sources, to serve as a platform for attacks; Actions taken (publications by the CERT, manufacturers, suppliers, etc.) This monitoring will help the organization to strengthen security and harden systems in order to minimize the attack surface. | | 3 |

| Control ID | Title | The Control | Complementary explanation | Control Implementation Example | Control Depth* |
|---|---|---|---|---|---|
| 12.35 | Emergency Preparedness | Write, implement, review, and update. business continuity policy, regarding Cyber-Defense | A dedicated IR team should be set up to handle cyber incidents in operational and industrial environments. This team will include representatives from a variety of disciplines and will be trained accordingly in the exercises. As part of the training, significant cyber events should be reviewed. If such staff cannot be trained, these capabilities should be hired from specialized companies that specialize in this. | A fast recovery position, including an engineering position, including licenses and applications installed on a laptop/stationary network that is not connected to the network (must be updated once every six months and ensure operational and readiness for service). | 3 |

| Control ID | Title | The Control | Complementary explanation | Control Implementation Example | Control Depth* |
|---|---|---|---|---|---|
| 12.36 | Preparedness for disaster recovery | Appropriate inputs should be devoted to creating business continuity and preventing cyber risks in the time synchronization process. | A process will be performed to analyze the level of accuracy effects between the components within the network and between the components of other networks and the outside networks. Ensuring the existence of a time clock synchronization process on the OT network and securing the process with the degree of reliability and accuracy, redundancy compensates on the network. | | 4 |

# 6. Bibliography and accompanying reading material


1. תורת ההגנה הארגונית גרסה 1.0 (In Hebrew - Organizational Defense Methodology for Organizations Version 1.0)
2. Clint E. Bodungen, Bryan Singer, (+3) Hacking Exposed, ICS Secrets and Solutions
3. Andrew Ginter, 13 ways through a firewall: What you do not know can hurt you 2013
4. Mariano Nunez, Cyber-attacks on ERP systems, An analysis of the current threat landscape, 2012 Security, May 2015
5. SP 800-82 R2 Guide to Industrial Control Systems
6. ANSI/ISA 62443 - Partially completed Document
7. NERC-CIP requirements for power utilities - Bulk Power Systems - BPS
8. ISO/IEC 27001-2013 and 27002, Cyber security for Information security management systems -ISMS
9. Andrew Ginter, Secure Operations Technology, Abterra 2018
10. Threat landscape for industrial automation systems, Kaspersky Labs, H2-2018
11. Blake Sobzak, Hackers force water utilities to sink or swim 03-2018
12. https://ics-cert.us-cert.gov/Standards-and-References#conduct

Cyber Israel
National Cyber Directorate

119
INCD@cyber.gov.il
www.cyber.gov.il

Find us at: