INDUSTRIAL CYBERSECURITY:
Monitoring & Anomaly Detection

www.outcomex.com.au

sales@outcomex.com.au   1300 875 469

outcomex

CISCO
Partner
Gold Integrator

INTRODUCTION

Industrial control systems (ICS) are all around us: in water, in gas, and electricity distribution networks, running power plants and critical infrastructure, in production lines and transportation networks, and more.

They have been created and implemented over the past few decades to help industrial organizations pilot their production infrastructure and critical installations. They follow international standards established by cross-vertical (ISA, IEC) or sector-based organizations (IAEA in nuclear, CENELEC in railway, etc.).

Their structure is represented by the following model, defined by the ISA95/IEC-62264 standard:
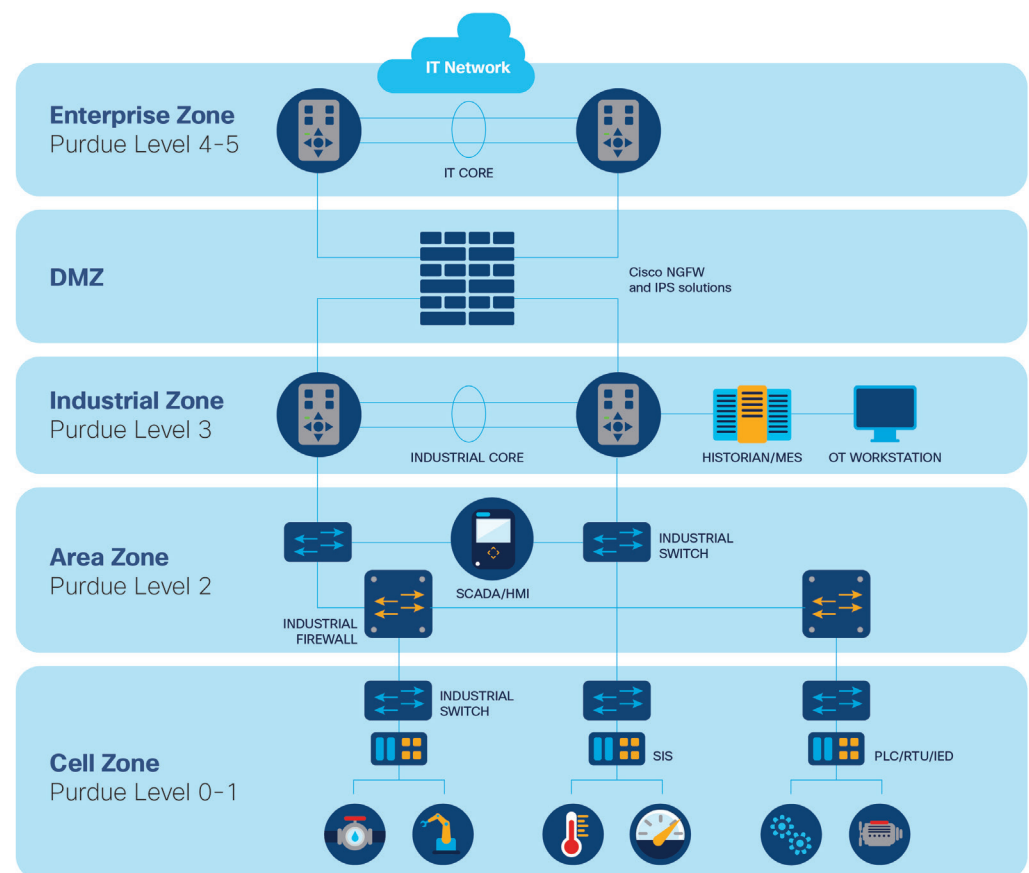
Industrial - Level 0 - Field: Sensors, actuators, motors

Industrial - Level 1 - Process: Automation devices, safety systems, controllers

Industrial - Level 2 - Supervision: SCADA stations, DCS operator station, engineering stations

Industrial - Level 3 - Manufacturing operations: MES, LIMS

IT - Level 4 and 5 - Business: Office, PC, messaging, intranet

It is often difficult to classify networks that would have been considered IT if looking only at their technical characteristics. In fact, since the 2000s, industrial systems have been integrating traditional IT components (Microsoft Windows, Ethernet, IETF, TCP/ IP, etc.) into their ICS networks, which makes the distinction even more challenging. However, there is a way to precisely define an industrial control network; **if at least 4 of the 5 characteristics below are met, it is an industrial control network:**

- It aims to pilot and supervise a physical process
- It is deployed in an environment requiring specific hardware resistance (up to 70° C, 12V or 24V DC power supply, dust resistance, IP levels between 20 and 80, etc.)
- It uses IEC standardized communication protocols or proprietary protocols from recognized manufacturers (see list of ICS device manufacturers below)
- It consists mainly of low-bandwidth "machine to machine" communications (10- to 100-Mbps local area networks, 512-kbps remote networks)
- The use of IT technologies (for example, HTTP IETF protocols) is reserved for management operations: web administration, SNMP, or ICMP monitoring. Conversely, there are no "user" communications (web surfing, messaging, etc.)

INDUSTRIAL CONTROL SYSTEMS VENDORS

ABB - Ansaldo - Bombardier - Beckhoff - Belden and its subsidiaries (Tofino, Hirshmann) - Emerson - General Electric - Honeywell - Moxa - Pilz - Schneider and its subsidiaries (Invensys, Foxboro, Telemecanique, Modicon) - Siemens - Yokogawa - Wago - and others

THE RISK LANDSCAPE

In the traditional IT world, the risk involves threats that would undermine the confidentiality, integrity, and availability of data and systems. The impact is mainly financial, such as the cases of extortion (Cryptolocker virus), bank fraud, or denial of service attacks distributed on web servers used by e-commerce sites.

Industrial control systems drive the physical world where operational technologies are used (called OT). The risk in ICS environments involves threats that would undermine the operational safety (physical security of goods and people, environmental impact) and the availability or even the physical integrity of the production tool. Theft of critical industrial data is also feared. The impacts are economic but also social; the civil and criminal liability of the leaders is also engaged.

SPECIFIC AND IDENTIFIED THREAT VECTORS

Unlike consumer-based networks, in which the main threat vectors involve the internet, in an ICS the fear is that malicious programs will be inserted **through USB keys** or by the lateral movement of malware to the stations that pilot the ICS.

Remote diagnostics and remote maintenance require remote access to networks and industrial control systems. Remote access is an even more serious threat vector because it interconnects networks of different criticalities and sometimes involves third parties.

Remote access workstations connect to the heart of critical industrial control systems to perform operations that can have a significant impact (such as updating software or downloading new firmware). They cannot simply be banned, **but they must be controlled by effective monitoring mechanisms.**

All of these threat vectors are, for the most part, specific to the industrial world. The security measures implemented in industrial control systems must take into account the operational reality that the OT staff need to continue to operate the facilities and work efficiently. They cannot simply ban all remote access or rely solely on access controls and organizational measures.

OT SYSTEMS ARE NOT DESIGNED TO FIGHT AGAINST MALICIOUS ACTIVITY

In addition, industrial control systems have never been designed to deal with cybersecurity threats. They are created with the objective of ensuring operational safety and the continuity of operations, and they often do not take into account the possibility that a motivated and malicious intruder could reach their digital interfaces.

This is why, so far, automation products have only a few cybersecurity functions. Moreover, in most cases, the cybersecurity functions are not activated by the industrial operators.

PROPRIETARY PROTOCOLS

Industrial systems are built on a set of protocols that allow the exchange of communications between the components on the networks. Some standards exist, such as MODBUS or PROFINET, but **the protocols for reprogramming or modifying the control systems are mostly proprietary and closed.** The majority of them (Siemens, Schneider, ABB, Rockwell Automation, etc.) have no plans to open their protocols, for legitimate intellectual property reasons.

Therefore, it is not feasible to apply IT techniques such as a protocol conformance check (syntax or semantic verification of compliance with a standard on all messages). This technique remains useful on those parts of the messages (protocol headers) that respect open standards (MODBUS for example), but it would be very difficult to apply on a closed protocol.

OPERATIONAL EVENTS TO QUALIFY

Moreover, from the point of view of the network, a "STOP" command sent to a programmable logic controller (PLC) is neither inherently malicious or legitimate. **It can be a maintenance operation, or it can be malware.** Under no circumstances should this command be treated as an "attack signature," as a classic intrusion detection system (IDS) using a blacklist-based design would do. The "STOP" command must therefore generate a security event, which must then be contextualized in a solution that centralizes the events and places them in their context and their history ("who does what, when/recurrences").

UNDERSTANDING ICS ATTACK TACTICS

To build an effective ICS cybersecurity strategy, it is crucial to identify the security events that are most likely to occur. This will let you focus on implementing the appropriate measures to protect the assets that are most likely to be targeted and improve the security of sensitive assets that an attacker could use to penetrate your ICS.

FEARED CYBERSECURITY EVENTS

In the field of industrial cybersecurity, a feared security event involves a cyberattack on an industrial information system that would cause significant harm to the company's operations, production tools, production output, or even its employees or customers. These events will have a material impact in the physical world. In some cases, they could lead to criminal cases targeting the company's leadership.

In the rest of the document, three events are described.
Each event is developed in three sections:

CATEGORIZATION	Goal, target, impact, and technical means of the attacker
DESCRIPTION	Motivations and processes of the attacker
PROCESS	Step-by-step attack scenario

CYBER KILL CHAIN

To codify the cyberattack scenarios and detail their different phases, we use the Cyber Kill Chain concept. This concept allows us to describe in detail the structure of a complex intrusion attempt, typical of new attacks.

The Cyber Kill Chain stages are: Recognition, Weaponization, Delivery, Operations, Installation, Command and Control, and Actions on Objectives. In the case of the dreaded events of this report and covered below, it is assumed that an attacker is already "connected" to the industrial control network. He successfully passed all of the steps in the attack chain until installation. It can be a malicious program that has been moved to an industrial station, or it can involve someone who has gained physical access.

Therefore, the following steps, which are considered to have already been successfully accomplished by the attacker, will not be detailed:

⚠️ Human and technical recognition of the target organization (social networks, public tenders, publications of the organization)

⚠️ Weaponization and delivery via malware (infected MS Office or PDF file, trapped video games, water hole website) sent by the web or by email

⚠️ Installation via a lateral displacement toward the point of interconnection with the industrial network or insertion in the industrial control network, more particularly in the control network of the process that contains the engineering stations

IDENTIFY YOUR WEAKNESSES

It is particularly important to understand how the attacker will hack into the industrial network of his target. There are many sensitive points of insertion to consider when designing a monitoring process. They are classified by likelihood:

1

Takeover of an industrial station
The attacker uses targeted IT propagation mechanisms (i.e., the malware communicates with the attacker's "command and control" server) to propagate the malware in the target network until it reaches a workstation in the industrial domain. The main targets are supervisory control and data acquisition (SCADA) and engineering stations because they contain important information about the process (set points, variables used in programming, etc.).

2

Spoofing authorized remote access for a third party
The attacker takes advantage of an authorized remote access for a third party, such as a subcontractor. It can be an ADSL or a VPN connection left open or used only for particular IP addresses. These remote accesses are often given access to the heart of the industrial facility, providing a "quality" entry point for the assailant.

3

Hijacking a wireless link
The attacker uses a public or proprietary weakness in the wireless links used (known attacks on WEP or WPA). In this way, he can connect to the industrial control network. He then has direct access to the heart of the system at engineering stations, SCADA stations, and PLCs.

4

Gaining access to the field network of the installation
The attacker has direct physical access to the facility's field network for his attack, for example, by having access to a computer cabinet along a distribution axis (a pipeline in a sewer or along a conduit). The field network gives direct access to the ICS equipment used to control the input/output modules. This is particularly important in the transportation sector.

5

Installing a foreign physical component to modify the network remotely
To take advantage of his physical access without being forced to be physically present in a compromising place, the attacker will install a remote-control module in the industrial network: for example, a miniaturized Raspberry Pi with a battery and a 4G modem allowing him remote control access.

Feared Event A: Intellectual property theft

CATEGORIZATION

- **Purpose of the attacker:** steal process or industrial data
- **Installation type:** manufacturing process (discrete), undistributed
- **Impact:** undermines data confidentiality
- **Technical means:** download of PLC programs of the installation

DESCRIPTION

Intellectual property theft constitutes an attack on an industrial control system intended to steal a process or industrial data of value. **The motivations of the attacker can be:**

- **Economic:** steal a manufacturing secret from a competitor to be able to duplicate its products or reverse design its manufacturing method.
- **Patriotic:** steal the plans of a sovereign product to replicate it, such as an airplane or a defense product (such as a frigate or submarine).

The ultimate goal of the attacker is to exfiltrate the desired data by escaping any detection so that the target does not implement countermeasures. It will not seek to act on the process itself, but only to undermine the confidentiality of the system.

The attack is placed in a long-term temporal context: the attacker will want to maintain access as long as possible, or at least until he has managed to extract all the sought-after data. If the attacker does not have direct physical access, he will need to maintain a "control" connection between his malware installed on the industrial control network and his command and control server.

PROCESS

1. Connection to PLCs: extraction of programs, extraction of variables
2. Exfiltration of PLC programs from engineering stations
3. Extraction of sensitive data from monitoring stations (programs, synoptics, setpoints, alarm threshold)
4. Extraction of information stored in a database (Historian)
5. Finally, once the data is acquired, it is necessary to extract it via the internet or removable media in the most discreet manner possible, which can be complicated if the data is bulky

Feared Event B: Industrial sabotage

CATEGORIZATION

- **Purpose of the attacker:** furtively modify an industrial process
- **Type of installation:** manufacturing process (discrete or continuous)
- **Impact:** undermines the integrity of the industrial process
- **Technical medium:** modification of the program of one or more controllers, decoy SCADA supervisions

DESCRIPTION

This scenario describes an attack on an industrial manufacturing system that results in sabotage. The motives of the attacker may be cyberterrorism, competitive positioning, or even an act of war between two nations.

The attacker seeks to act on the industrial process by escaping any detection - the exfiltration of data is not a goal. This scenario covers the persistent and undetectable modification of an industrial process so that it no longer functions in its nominal conditions and produces non-compliant parts. **To do this, the attacker will seek to:**

- Obtain the most detailed knowledge possible of the industrial process and its control system to be able to modify it. We are talking about architecture data (network plans, configurations, etc.) as well as purely industrial data such as pressure, temperature, rotational speeds, etc. The attacker must obtain the nominal values of this data and the associated alert thresholds so that they can be modified without anyone noticing it
- Once he has a detailed vision of the industrial process, he can modify the programs of some controllers to act on the industrial process. To prevent the change from being apparent, he must also potentially take control of SCADA stations to present false information or change the alarm thresholds

PROCESS

This scenario is a logical continuation of scenario A: it starts with the same attack steps. The difference lies in the additional steps, which make the scenario much more complex.

Once the attacker has exfiltrated the controller programs, he then modifies them and re-injects them in the controllers to act on the industrial process. He must make sure to make the changes discreetly, under the radar of potential supervision in place.

This is the plot of the Stuxnet attack, which was intended to change the spinning speed of centrifuges. But it is not confirmed whether the attack used program modification or the software alteration of operating system's low-level components (i.e., drivers).

Here the attacker chooses to directly modify the program installed on the controller (which is potentially visible), but one could also act directly on variable values or by modifying software that interacts with the industrial equipment (including, for example, supervision software).

Feared Event C: Denial of service on industrial installation

CATEGORIZATION

- **Purpose of the attacker:** provoke a production stop
- **Type of installation:** continuous distributed process (refinery, water, gas)
- **Impact:** undermines availability of the industrial process
- **Technical medium:** decommissioning of the controller

DESCRIPTION

This scenario is more directly oriented toward industrial denial of service. **The goal is to stop the production of a continuous process at an industrial plant** such as a refinery, a water treatment plant, or a gas distribution network.

The attacker will take control of part of the infrastructure to make it inoperative and possibly cause physical damage to the production tool to make restoring service very complicated. Stopping production of such a facility directly impacts all users who depend on it, which can have significant human consequences.

This type of installation is also often distributed. It is deployed over a fairly large area, which offers opportunities for an attacker to perform a physical takeover without going through the internet.

PROCESS

In this scenario, the attacker will use denial of service to remove from operation all or some of the controllers he can access. He can use several technical means, such as:

- **Network saturation denial of service:** the attacker generates so much traffic that the controller can no longer answer or perform its functions. This technique resembles the denial-of-service attack familiar in IT
- **Denial of service by reprogramming:** the attacker takes advantage of his direct access to the industrial network to install a non-functional program on the PLCs

MONITORING SYSTEM AND ANOMALY DETECTION

Industrial control networks are often geographically extended and made of many "small networks" with few components. To monitor it all without deploying a complex and costly infrastructure, the detection system is generally made of:

- Sensors close to the process that extract communication data between the devices
- A central server that gathers, stores, and analyzes the data collected by sensors
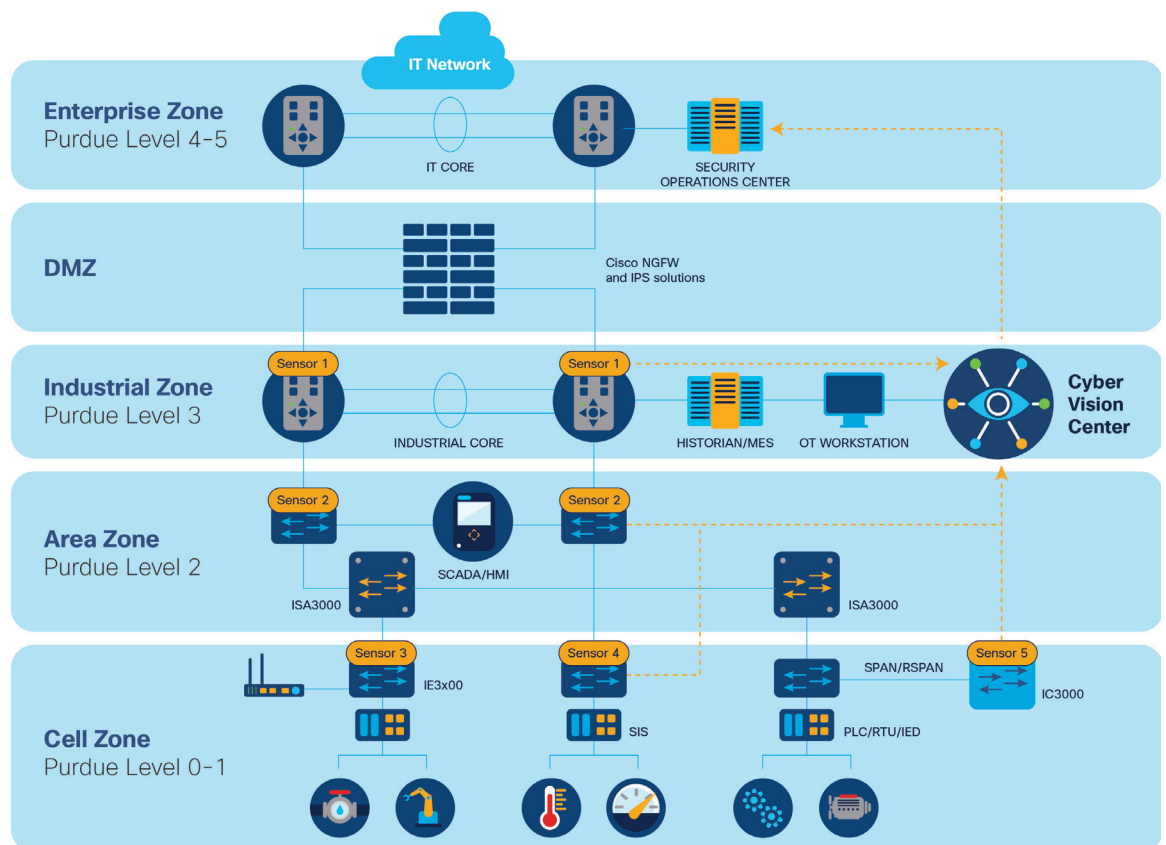
The placement of the sensors must make it possible to monitor the different interconnection points of the industrial system:

Sensor 1: Interconnection between the IT-based network and the OT network (Historian flow, Statistics, Driving)

Sensor 2: Process network between PLCs and Windows machines (supervision and control-command flow, SCADA station, engineering)

Sensor 3: Wireless interconnection or remote maintenance (DSL, LTE or MPLS router)

Sensor 4: Flow control between control systems and between control systems and safety systems

Sensor 5: Connection with the physically open field network.

In order to cover the risks mentioned above, the detection system analyzes the component properties, the control messages, and various markers:

- **Identification properties:** MAC address, protocol ID, TCP port, UDP port
- **Inventory properties:** Vendor name, PLC name, project name, project version, model name, firmware version, hardware version, hardware serial number, location / slot sub-module, product code, component role (SCADA, engineering)
- **Simple control of controllers/PLCs:** program downloads from/to PLC, stop/start commands, clock changes, firmware updates
- **Advanced controllers/PLC control:** monitor the content of PLC programs, program metadata (list of programming blocks, timestamp, size), authentication data (login and passwords), change of residual databases, memory erasure, change to maintenance mode, switch to diagnostic mode
- **Process control:** write and read commands, list of variables/registers
- **Indicators of compromise (IOCs):** DNS queries made by industrial stations, or by HTTP or FTP metadata; these IoCs can point to the activities of a command and control server communicating with malware installed on industrial stations

It is important to understand that the so-called "simple control of controller" commands offer multiple possibilities to attackers. From the point of view of detection, it is necessary to know how to detect these commands on the network.

To extract the information needed to monitor industrial system cybersecurity, the platform needs to decode application flows collected on the industrial network. **These flows can use several types of network protocols:**

- Open protocols whose specifications are known and available. These protocols have been standardized by international organizations
- Proprietary extensions in open protocols. These extensions use an open data area and incorporate proprietary, undocumented data structures
- Proprietary protocols whose specifications are not public

Unfortunately, the protocols used to modify control systems (change of program or parameters) are proprietary.

INDUSTRIAL CYBERSECURITY:
Monitoring & Anomaly Detection

KICK-START YOUR INDUSTRIAL CYBERSECURITY PROJECT

Whether you need a precise view of your industrial asset inventory to start segmenting your network, or live monitoring of ICS application flows to detect intrusions and abnormal behaviors, Cisco® Cyber Vision can help you define your path forward and extend your cybersecurity policies to the operational technology domain.

Cisco Cyber Vision has been specifically designed for industrial organizations to gain full visibility into their industrial networks, so they can ensure process integrity, build secure infrastructures, drive regulatory compliance, and enforce security policies to control risks.

Combining a unique edge monitoring architecture and deep integration with Cisco's leading security portfolio, Cisco Cyber Vision can be easily deployed at scale so you can ensure the continuity, resilience, and safety of your industrial operations.

www.outcomex.com.au

sales@outcomex.com.au   1300 875 469

CISCO Partner
Gold Integrator