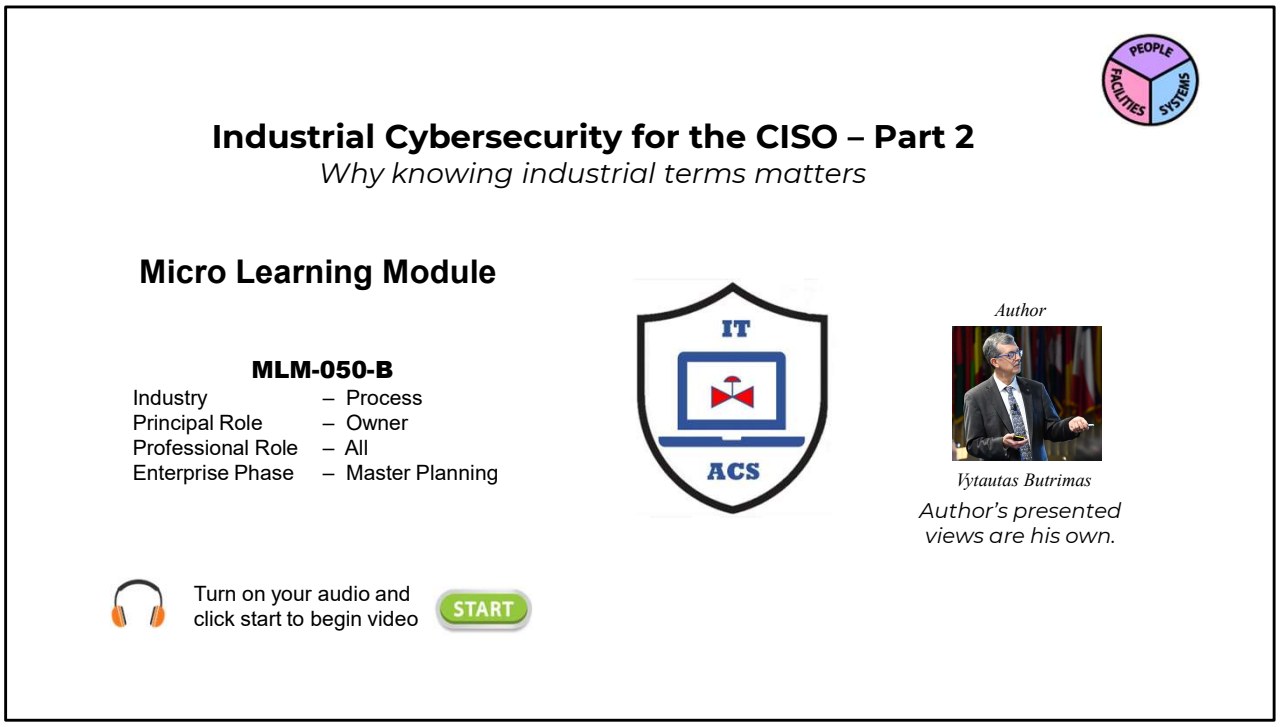


This module addresses what a Chief Information System/Security Officer (the CISO) needs to know to work with Automation and Control Systems (ACS). It will shed some light on the importance of defining what it is that needs to be protected in an industrial or manufacturing environment where the focus is more on protecting the physical process rather than the data or information used in the office or business part of the enterprise.

Click the NEXT button when you are ready to advance to the next slide.

Some Important Definitions

ACS/ICS – see MLM-014-A Definitions

Information Technology (IT)

Office-based (accounting, billing, etc.)

Focused on processing information

Creative Commons by V. Butrimas

Creative Commons by G.A.Rathwell & Adobe Firefly

Automation & Control Systems (ACS)

Monitoring / controlling a physical process

Human machine interface (HMI) interacts with industrial control system (ACS)

2

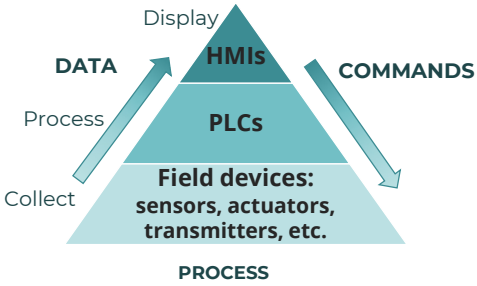
As CISOs, we need to understand what we are talking about if we are to communicate with our plant engineers and control room operators who may not have much time to stop and explain things to us. On the other hand, there are differing interpretations of what terms like Information Technology (IT), Automation & Control Systems (ACS), Industrial Control Systems (ICS) and Industrial Automation and Control System (ACS) mean. Of all these terms. you may find your engineers will understand you best if you use the latter two terms (ACS and ICS). I will focus on trying to explain IT, ACS and ICS. While ACS is similar to ICS, it is the term used in the ISA/IEC 62443 Standards, which some may not be familiar with. To get a further explanation of ACS and ICS I recommend looking at MLM-014-A that is specifically devoted to ACS Definitions.

For the purposes of this MLM, I refer to IT as what happens in your office, accounting, billing or the business administration part of your enterprise. The focus here is on the processing of information and trying to protect the confidentiality, integrity, and availability of the information that are vitally needed to administer the enterprise.
Automation & Control Systems(ACS) is the hardware and software used to monitor and control a physical process. The physical process is not found in your office near the meeting or server room but is at some other separate location (perhaps in a control room.) The state of these physical processes are visualized with the help of a Human Machine Interface (HMI). It is usually a Windows OS PC with a screen similar to what you are looking at right now or it might use some other OS. Essentially, it is showing what the intelligent electronic devices closely monitoring and controlling devices are telling us about the state of a physical process (such processes could be fuel being pumped through a pipeline or a turbine generating electricity.) The devices that closely monitor and control a physical process are part of an Industrial Control Systems (ICS).

Industrial Control Systems Act on the Process

Monitor and control physical processes...

..using the hardware and software closest to the physical process




Public Domain from WikiMedia


Creative Commons from WikiMedia


Creative Commons from WikiMedia


Creative Commons by V. Butrimas


Creative Commons by V. Butrimas

Industrial control systems (ICS) are mostly computer-based, used by infrastructures and industries to monitor and control sensitive processes and physical functions.

They collect sensor measurements and operational data from the field, process and display this information, and relay control commands to local or remote equipment.

They refer to the hardware and software closest to the actual physical process, such as RTUs, PLCs, actuators, drives, sensors, and field devices.

The photos are of:
- PLCs
- Gas leak detection
- Photo of turbine at large hydroelectric power plant
- Doppler sensors on a pipeline measuring rate of flow
- Actuator to start a boiler at a thermal plant for a municipality

Automated Control Systems (ACS) Versus Office IT

The laws of physics and chemistry operate here and can be used for wonderful benefits…

Creative Commons by Andy Beecroft

…or for inflicting great harm

Public Domain from US Government

4

The key thing to remember about Industrial Control System space as opposed to office IT space is that the laws of physics and chemistry operate here and can be used for wonderful benefits but unfortunately can accidentally (or through malicious intent) cause great harm.

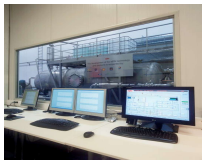
Chernobyl nuclear accident and disaster of 1986 is a good example of what can go wrong in the monitoring and control of a physical process. There was no malicious intention at play, but operators did not realize the potential dangers of their actions. In disabling some safety systems to allow a special test of the reactor control systems, a tragic incident resulted.

Industrial Control Systems safety depends on...

Industrial Control Systems (ICS) depend on people, automation and intelligent devices to keep operations safe and reliable

Basic Process Control Systems (BPCS)
- Keep the process running normally, reacts to small changes

Safety Instrumented Systems (SIS)
- Preset emergency actions to protect the facility and its people
- Brings things back to a safe state



Creative Commons
by G.A. Rathwell

Creative Commons
by V. Butrimas

Creative Commons
by G.A. Rathwell

Creative Commons
by David Dixon

5

Industrial Control Systems (ICS) rely on people, information and intelligent devices to keep operations safe and reliable.
The basic process control system (BPCS) is the main computer system of the operating process that receives information about the process (including pressure, temperature, flow, and level) and transmits signals to manipulate the positions of the control valves to ensure the system continues to operate under the desired operating conditions. It is a central processing unit and a computer that controls everything in the installation.
Safety Instrumented Systems (SIS) are independent safety systems that are pre-programmed to immediately react to a monitored physical process that strays beyond preset bounds. They are programmed to bring the physical process back to a safe state, thus avoiding a catastrophic event and allowing the operator to attend to the problem and make any repairs. When an SIS fails to do its job, we have unpleasant events like the Deep Water Horizon disaster where the SIS failed to perform its primary function of bringing the drilling operation back to a safe state.

How does IT differ from the ACS/ICS found in industrial environments?

In IT cybersecurity, the goal is to protect the data.

In ICS, the goal is to keep a physical process within pre-set bounds.

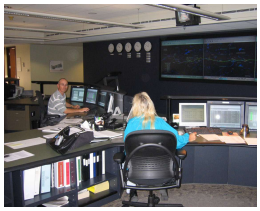
Safety is the main goal for operations in an industrial environment.

CIA
Confidentiality
Integrity
Availability
Password is: c124g5df8s*/pdq

Creative Commons
by V. Butrimas

≠

Safety - AIC
Availability
Integrity
Confidentiality
Password is: 1234



Creative Commons
by G.A. Rathwell

6

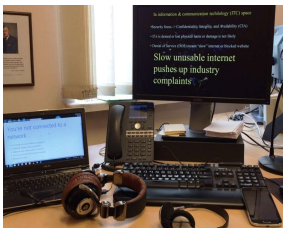
In IT cybersecurity, the goal is to protect the data. For an enterprise, this can be the billing and accounting information needed to manage the business transactions of a pipeline.
When you work in IT, you have passwords like the above because they need to be secure (confidentiality.) You also want to make sure the information is accurate, not corrupted (integrity). Getting to data when you need it is last in IT (availability.)
In ICS, the operation is to keep a physical process within pre-set bounds.
Safety is the main driver for operations in an industrial environment. Safety is a key feature of an industrial environment as opposed to the environment found in the office.
On the ACS side, you might have passwords which are 1234. And we can understand the reason for sharing passwords or having simple passwords; you need to have a password you can remember in an emergency to get into a piece of equipment or a system quickly to avoid a problem (availability is the most important.)

Consequences of Failure in IT Versus ACS

If the IT stops, the office stops:

Re-boot the PC, tell the admin, wait.

(You may go for a coffee.)



If ACS stops, the physical process will continue:

but it might do something unexpected (and you may need to call Fire & Rescue).

Creative Commons by G.A.Rathwell & Adobe Firefly

Public Domain From US Chemical Safety Board

The consequences of failure in IT and ACS systems are very different.
If the IT systems fail in an office, you stop working and wait for someone to get things back on-line again. You can go out for coffee in the meantime. The physical processes taking place on the ICS side should not be affected by an IT failure in the office, Examples include a computer being disconnected, a connection to a website being lost, the internet slowing down, or an email server malfunctioning. Hopefully, if there was no ransomware incident, things should go back to normal quickly and you can return to the work you were doing.

In an ICS environment, where the monitoring and control of a physical process is the main task, the consequences of failure can result in loss of life, damage to property or to the environment. If an ICS stops, the physical process will still go on, but it might do something unexpected. You might have to call fire and rescue. People could be injured, you could have a fire or have chemicals seeping into a river from your plant. A lot of time, effort, and resources may need to be expended to bring things back to normal.
The risk profile is completely different for these systems.

Even if plant equipment is not damaged, management may choose to stop production out of caution. This occurred in the Colonial Pipeline incident causing major economic losses that could have been avoided with clear separation of IT and ACS systems.

Key Messages

Understanding industrial cybersecurity terminology is vital in developing a cybersecurity program for the enterprise.

Before we can develop effective policies, we need to understand:

- What it is we are trying to protect
- The functions of equipment and Automation Systems that we wish to protect
- The security requirements of data and automation and Control Systems (ACS) that we wish to protect
- Potential threats and risks including IT risks that may impact ACS (and how to mitigate these).

Understanding industrial cybersecurity terminology is a vital step in developing a cybersecurity program for the enterprise.

We need to understand what it is we are trying to protect and their particular functions and security requirements before we can develop effective policies to protect them.

Knowledge of threats and risks that the owner wants to avoid should also be part of the process. For example, IT risks that may impact ACS (like ransomware) and measures to prevent this,

Further Information

- Related MLMs
  - MLM-014-A ACS Definitions
  - MLM-050-C Industrial Cybersecurity for the CISO, Part 3
  - MLM-001-A Principal Roles in ACS Cybersecurity
- References:
  - Butrimas, V., IT and ICS cybersecurity: a "Tale of Two Cities", https://scadamag.infracritical.com/index.php/2017/08/21/1984/
  - Industrial Cybersecurity Tips for CISOs, Tripwire, accessed 2021-07-01 https://www.tripwire.com/-/media/tripwiredotcom/files/feature/industrial_cybersecurity_tips_for_cisos.pdf

Please click here to rate this learning module.

Thank you for taking the time to interact with this MLM.
Select the Resources tab (at the top of the screen) to view and/or print this MLM, including the speaker notes. Some people like to review the slides and written narrative after listening to the micro learning module. Some like to print them and follow along as they are listening to the video. It's up to you.
The last link gathers feedback on ISA Workbench about this particular MLM.

Author – Vytautas Butrimas

Vytautas Butrimas has been working in defense and cyber security roles for over 30 years including:

- Vice-minister at the Ministry of Communications and Informatics, Republic of Lithuania responsible for Information Society programs.
- Defense Policy and Planning Director, Lithuanian Ministry of National Defense (MoND) responsible for preparing the first Military Defense Strategy.
- Deputy Director responsible for IT security at the Communications and Information System Service (CISS) responsible for preparing the first National Defense System Cybersecurity Strategy
- Chief Adviser for the MoND of Lithuania with a focus on cybersecurity policy, including the national task force that wrote the Lithuanian Law on Cybersecurity
- Member (Presidential appointee) of the National Communications Regulatory Service's Council (RTT-Council)
- Cybersecurity Subject Matter Expert for the NATO Energy Security Center of Excellence (NATO ENSECCOE) who performed a Cyber Risk Study of the ICS Used in the NATO Central Europe Pipeline System (CEPS)

Please click here to provide feedback on this MLM.