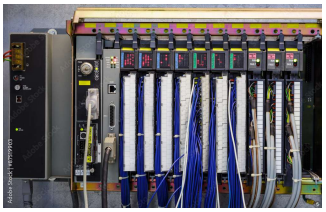
Cybersecure PLCs & RTUs - Principles & Definitions

© Adobe Stock



MLM-035-A

Industry	– Process
Principal Role	– Owner
Professional Role	– All
Enterprise Phase	– Master Planning

Turn on your audio and click start to begin video

START

This Micro-Learning Module (or MLM) discusses principles for the design and operation of PLCs and RTUs. It describes the components of a PLC, and the cybersecurity risks, and vulnerabilities it involves.

The intended audiences for this MLM are engineers and maintenance technicians, I T teams dealing with control systems, cyber defense consultants, systems integrators, and managers making decisions about eye-axe cyber security.

Overview of PLC and RTU Functions

- **Understanding PLCs and RTUs**
  - PLCs: involve many I/Os and complex plant processes
  - RTUs: simpler processes, fewer I/Os, but remote communications
- **Typical roles of the PLC and the RTU in an ACS**
  - Perform real-time processing required for each specific site
  - Integrate a reliable interface with connected sensors and actuators
  - Communicate with Peer devices and higher hierarchy controllers
  - Perform communication using special protocols as required
- **What is an ACS security model?**
  - For IT systems, we say "Never Trust-Always Verify" for each Session.
  - For a PLC and other ACS devices, we employ an adapted "Minimum Trust" security model.

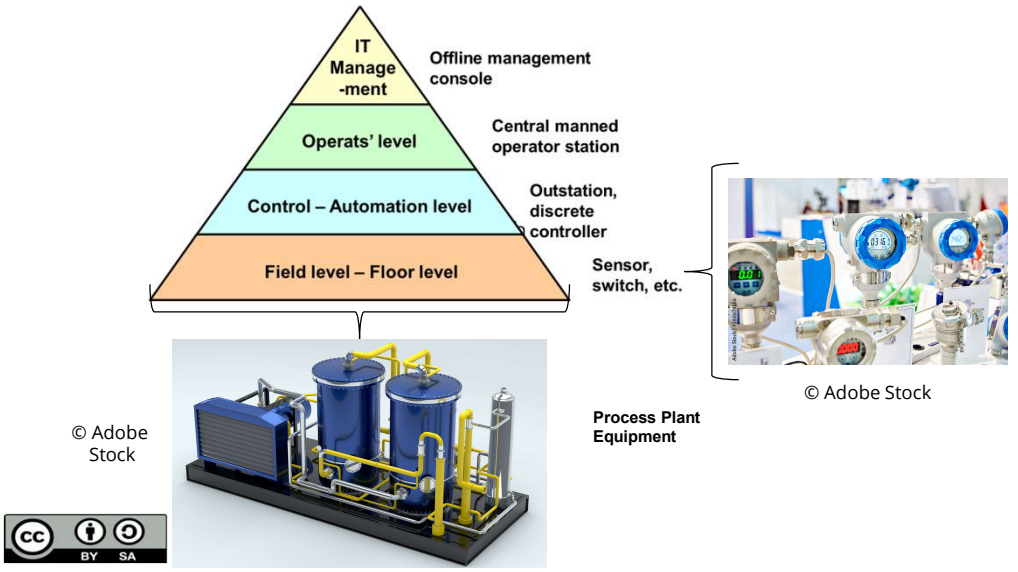
Let's start by defining the terms PLC and RTU. These are common devices used in industrial automation and control systems. This I A C S acronym may be pronounced as eye-ax.
The term PLC stands for Programmable Logic Controller, a device that is suitable for systems that must integrate many digital Input and output connections, such as industrial equipment controllers. PLCs are widely used in eye-axe that run complex processes, including high-speed communications.

The term RTU stands for Remote Terminal Unit. These are typically used for controlling simpler processes, with fewer Inputs and outputs, but strong remote communication capabilities, such as transportation pipelines that use Supervisory Control and Data Acquisition SCADA systems.
Both PLC's and RTU's provide data collection and control of real-time processes.

Typical roles of the PLC and the RTU in an eye-axe include the following:
- Perform real-time processing required for specific equipment,
- Provide reliable interfaces to connected sensors and actuators,
- Communicate with Peer devices and higher-level supervisory devices,
- Perform communication using specific protocols as required.

Let's briefly describe the "Minimum Trust" security model used with PLCs and other eye-axe devices.
- For I T systems, we often say, "Never Trust-Always Verify". This is called a "Zero Trust" model, and it involves verifying every transaction, with passwords and other means. It ensures that every request for information or change is valid before the transaction may proceed. Unfortunately, it also means that should validation fail, no action will occur. When dangerous equipment is involved, a bad password could result in a disaster, causing huge costs and even loss of life.
- Therefore, when we deal with a PLC or other eye-axe device, we use a "Minimum Trust model." This is part of a set of special design and programming practices designed to achieve the required level of operational safety and security to address the special risks associated with the control of hazardous plant equipment.

Major Components of an ACS Architecture



Here is an illustration of how an eye-axe system may be structured:
On the left side of this slide, you see a simplified version of a Purdue Enterprise Reference Architecture (or PERA model) showing the sensor, controller, and Operator levels that manage the real-time process.

a) On the top right side, you may see examples of sensors that convert parameters representing physical conditions such as temperature, pressure, etc., to electric analog signals. If smart sensors are used, data may be sent directly in digital format.

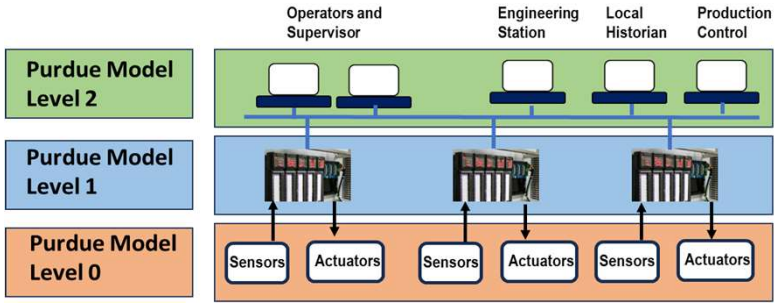
b) On the lower left, you see typical process control equipment, including equipment, pipes, physical property sensors, electric valves, pressure relief valves, etc.

c) This simplified model represents Purdue Level 0, Level 1, and Level 2.

d) At the top of the triangle, you see the I T zone including management levels. Depending on the type and size of the enterprise, the I T zone may include several levels.

ACS Cybersecurity Risks

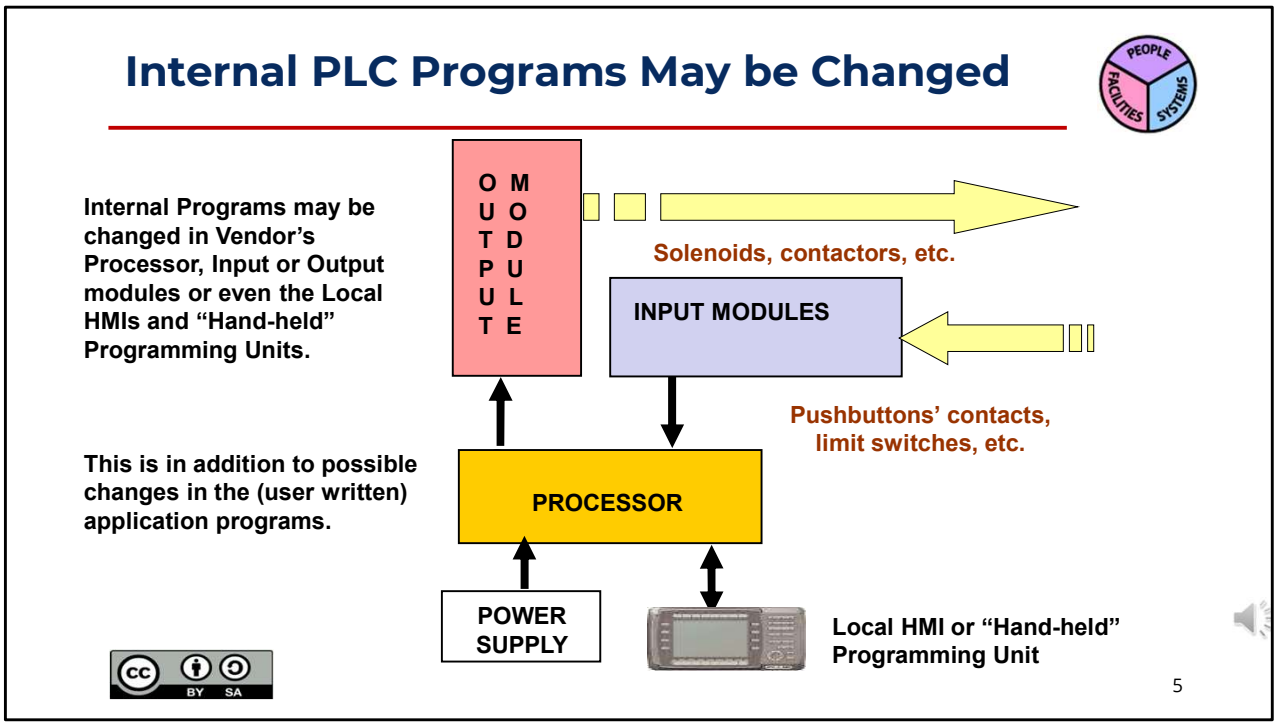
- **Any device may fail, so alerts are reported to the Operator at Level 2 of:**
  - Abnormal process values (alarms)
  - Loss of control
  - Communications failures
- **In recent incidents, attackers have caused failures of each of these ACS components.**



It must be assumed that any device, network or software component in an eye-axe can fail. Therefore, the PLC and every other device in the eye-axe should be programmed to (at least) inform the Operator (at PERA Level 2) of the failure. For example, when abnormal process values, loss of control, or communication are detected, the PLC should be programmed to, at the very least, alert the Process Operator.

However, in recent exploits such as the Stuxnet virus, attackers have even hidden information from the plant operator, causing them to fail to manually shut down the process before major equipment was destroyed.

Similarly, Engineering Stations have been used to modify measured data in the Operator's HMI or the Data Historian.



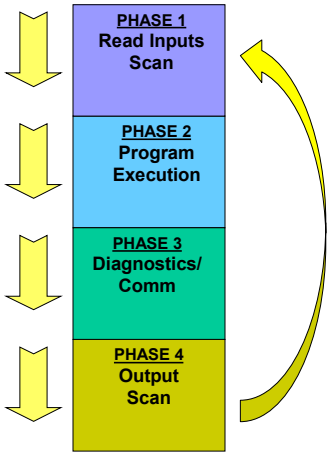
This block diagram illustrates the main modules associated with a PLC or RTU. Each module has its own internal programming that may be modified using the local HMI or a programming and maintenance terminal that plugs directly into the PLC or RTU, or by a remote computer.

Similarly, the application programs in the processor may be modified to change process operations or even change emergency shutdown logic.

It is therefore advisable to regularly inspect PLC programs and configuration to detect accidental errors or malicious changes.

PLC Run-Time Phases

- **The PLC operating sequence includes four-phases, which are repeated as follows:**
  - Read Inputs (On/Off and analog signals)
  - Execute PLC application program (e.g. Ladder Logic)
  - Diagnose processor and Communication devices
  - Scan Outputs (On/Off and analog signals)



On the top right side of the slide, you can see a typical PLC four-phase cycle:
Phase 1: Read the analog or status inputs delivered to the PLC. Following that, the PLC performs input validation and accepts the data only if it matches predefined criteria.
Phase 2: Execute the PLC program, considering the previous status, commands from the control center, and the analog and status inputs delivered to the PLC.
Phase 3: Diagnose the PLC hardware and software. If that cycle creates an unusual or risky condition, the PLC must switch to a fail-safe condition. It also accomplishes any communication tasks.
Phase 4: Output new values. Finally, the PLC sends outputs to adjust the process to suit new process conditions.

When the standard scan time of the PLC has passed, the program will restart.

This describes how the application program executes. The second MLM of this series provides tips on how to avoid programming errors that may be used by an attacker to gain control of the device.

Further Principles for PLC and RTU Design

- **Main Goals for Securing ACS**
  - For IT, we use cybersecurity practices and technologies for achieving CIA (Confidentiality-Integrity-Availability) goals.
  - For ACS we use special cybersecurity practices for achieving the required SAIC (Safety, Availability, Integrity, and Confidentiality) goals.

- **Cybersecurity Practices**
  - Cybersecurity is a precondition to Operating Safety and must be included in the ACS design.
  - Physical security for sensors, PLCs, communication appliances, the HMI, and Engineering Station, are a precondition for cyber-secure operations.

This MLM summarizes the main goals for securing eye-axe including:

- For I T, we use cyber security practices and technologies for achieving CIA (Confidentiality-Integrity-Availability) goals.
- However, for eye-axe, we must use special cybersecurity practices to achieve the defined S I A C (Safety-Integrity-Availability, Confidentiality) goals.

Cybersecurity Practices

- Achieving Cyber security for industrial operations is a critical part of maintaining Plant Operating Safety. Cybersecurity practices and guidelines must therefore be included in the eye-axe design.
- Physical security for sensors, PLCs, communication appliances, the HMI, and Engineering Station, is a precondition for achieving cyber-secure operations, since physical access may be used to defeat cyber security.

Key Messages

Establish corporate cybersecurity design and operating principles with reference to international, industry and regional standards. Examples include the following.

- Segregate operating zones, and networks according to an approved Architecture.
- Implement ACS Secure Design Principles, Procedures, and Policies:
  - in ACS zones to achieve the defined SAIC. and
  - in IT zones to achieve the defined CIA.
- PLC and RTU designers should use "Security by Design" principles from ISA 62443.
- Implement "minimum trust" security model for ACS including PLCs and RTUs.
- Harden ACS devices by disabling unused communication ports.
- Periodically validate PLC code to detect accidental or malicious changes.
- Monitor performance of PLCs and other ACS to detect attacks and errors.
- Control physical access to ACS devices and networks.
- Monitor Cyber Security Standards such as IEC/ISA 62443 and vulnerability advisories.

8

It is recommended that Enterprises establish corporate cybersecurity design and operating principles using a formal selection and approval process such as PERA. These principles should be established with reference to appropriate International standards such as I E C / I S A 62443, and I E C 27 thousand, as well as regional and industry standards such as Nist 800.

- Segregate operating zones and networks, according to an approved Enterprise Architecture.
- Implement eye-axe Secure Design Principles, Procedures, and Policies in eye-axe zones to achieve defined S A I C (Safety, Availability. Integrity, and Confidentiality) for PLCs, RTUs and other eye-axe devices and networks.
- Implement I T Secure Design Principles in I T zones to achieve defined CIA (Confidentiality, Integrity, and Availability).
- PLC and RTU designers should use "Security by Design" principles from I S A 62443.
- Implement principles of "minimum trust" for eye-axe including PLCs and RTUs, and "zero trust" for I T systems.
- Harden eye-axe devices by disabling unused communication ports and protocols.
- Periodically validate PLC code to detect accidental or malicious changes, for example, by comparing code and configurations to an approved "Golden Copy" that is stored in a secure location.
- Monitor performance of PLCs and other eye-axe, to detect unauthorized changes.
- Control physical access to eye-axe devices and networks.
- Monitor Cyber Security Standards such as I E C / I S A 62443 and

cybersecurity vulnerability websites like C I S A.

About the Author

Daniel Ehrenreich

Daniel has over 33 years of experience with control of industrial operations and integration of cyber security solutions.

He is a control engineering consultant, workshop lecturer, and an expert in cyber secured operation for ACS.

Daniel is contributing his knowledge and expertise to multiple ISA 62443 workgroups.

Since 2016, acting as the Chairman of the annual ICS-Cybersec Conference taking place in Israel

Please click here to provide feedback on this MLM.

Daniel Ehrenreich has over 32 years of experience with control of industrial operations and integration of cyber security solutions.

He is a control consultant, workshop lecturer, and expert at Secure Communications and Control Experts. Daniel is also contributing his expertise to multiple ISA 62443 workgroups and conducting podcast sessions for educating engineers worldwide. Since 2016 he has also served as Chairman of the annual ICS Cybersecurity Conference.

Please click this link to provide feedback to the author.