ASSET OWNER

Abstract

The purpose of this document is to define the minimal cybersecurity requirements that third-party vendors shall adhere to prior to connecting their equipment to the ASSET OWNER industrial control system network.

Cybersecurity vendor Policies

Vendor PLC Cybersecurity Integration Requirements

| Amendment History |
| --- |
| Revision No. | Date | Description of Amendments | Approver | Sections |
| 0 | MM/DD/YYYY | Issued for approval |  | All |
|  |  |  |  |  |
|  |  |  |  |  |

# Review Requirements

This document shall be reviewed on an annual basis in accordance with CORPORATE POLICY.

# Definitions

|  |  |
| --- | --- |
| Acronym | Definition |
| OT | Operational Technology |
| PLC | Programmable Logic Controller |
| HMI | Human Machine Interface |
| VFD | Variable Frequency Drive |
| FAT | Factory Acceptance Test |
| SAT | Site Acceptance Test |
| NTP | Network Time Protocol |

# Resources

|  |  |
| --- | --- |
| Resource | Description |
| Secure PLC Coding Practices: Top 20 List v1.0 | A global community developed set of guidelines for leading practices for secure PLC programming |
|  |  |
|  |  |

# Introduction

Figuring out where to start applying the Top 20 Practices can seem daunting. Keep in mind that this does not need to be an all or nothing approach and that you can really just start with incorporating the practices with some “quick wins”. This Specification sample document is focused on outlining requirements inspired by the Top 20 list for vendor control equipment (e.g., a new process unit is being added to the facility and a vendor skid package with a vendor template design and program). These requirements or the policy can be developed and provided to the vendor to improve the security & integration while beginning to adopt the practices.

# Intended Audience

* Control System Engineers
* OT Cybersecurity Personnel
* Control System Vendors

# Scope

All control equipment that will be connected to the SITE process control network shall abide by the requirements outlined in this document.

# Requirements

## General

* All PLC logic must be approved by the automation manager prior to bringing the controller online
* PLC, HMI, and VFD configurations shall be saved and provided to the ASSET OWNER upon completion of the FAT and SAT
* A control narrative shall exist for all control systems
* Where feasible, time sync the PLC and HMI clocks with the site NTP server
* The PLC shall be kept in RUN mode (e.g., RUN, REMOTE, PROGRAM)

## Hardware

* All PLCs, HMIs, and control network connected hardware must be approved by the automation and OT cybersecurity managers
* PLCs hardware shall support the ability to monitor the operating mode.

## Network Interfaces

* Ports and protocols on network interface modules shall be disabled when not required for the application
* Third-party connections (e.g. external network connections to third-party equipment not managed by ASSET OWNER) shall have a restricted data interface only allowing for pre-defined, operationally required read/write capabilities, and these connections shall not have the ability to access the PLC logic from the third-party network

## Programming

* All PLC logic must be approved by the automation manager prior to bringing the controller online
* PLC tag names shall follow the ASSET OWNER naming convention unless otherwise approved by the automation manager
* The vendor shall identify and provide a tag for monitoring the operating mode for the PLC
* Operational logic (e.g. totalizing or integrating) shall be handled in the PLC and not the HMI
* If timers and counters values are written to the PLC program, they shall be validated by the PLC for reasonableness and verify backward counts below zero
* Paired inputs/outputs shall alarm when states occur that are not physically feasible (e.g. valve open and close, motor start and stop)
* All "soft" operational analog inputs (e.g. setpoints) to the PLC that can be written to the PLC shall have clamps (i.e. acceptable inputs ranges) defined in the PLC to restrict the ability to write values to the PLC outside of the designed operational or safety values
* All externally accessible tags must be assigned to specific set of register blocks for specific functions (e.g. HMI read tags, HMI write tags, SCADA read tags, SCADA write tags, PLC-PLC communication tags)
* Input plausibility checks shall be implemented in the PLC to validate I/O and erroneous conditions shall be alerted upon
* Where practical, timers shall be used for monitoring expected operational processes (e.g. time to open or close a valve) and alerted upon when the operation is outside of the expected durations
* A safe state for PLC restarts (e.g., energize contacts, de-energize, keep previous state) shall be defined and implemented in the PLC
* Where feasible, the following PLC monitoring techniques shall be implemented and monitored from the HMI:
	+ Track and trend the PLC cycle time
	+ Track and trend the PLC restarts and uptime
	+ Track and trend PLC hard stop events from faults or shutdowns
	+ Track and trend PLC memory usage and alert for any large deviations from the trend

## Vendor Specific

### Allen-Bradley

* Where feasible, produce and consume tags shall be used for PLC-PLC communications (as opposed to message blocks)

# Approved Requirement Deviations

Any deviations from the requirements defined in this document shall not be implemented without prior approval from the ASSET OWNER automation and OT cybersecurity managers.

# Roles and Responsibilities

|  |  |
| --- | --- |
| Role | Responsibility |
| Automation Manager |  |
| OT Cybersecurity Manager |  |
|  |  |
|  |  |