OPERATIONAL TECHNOLOGY SECURITY: MONITORING AND LOGGING

EDITOR(S):

Ikechukwu Mezu, Meta

Eehern Wong, Google

Megan Diefenbach, Meta

Randy Armstrong, OPC Foundation

Todd Leblanc, Schneider Electric

Matthew Clapham, Individual

Table of Contents

Introduction

The Operational Technology (OT) used to run Data Centers, including Industrial Control Systems (ICS) that support building operations, is frequently designed with safety and availability as the focus rather than to mitigate security risks or vulnerabilities. This has presented a unique security challenge across multiple industries from Manufacturing to Data Centers. While IT equipment is designed to be replaced in 3-5 years, OT equipment is designed with long lifespans that typically exceed that of traditional IT systems. As a result, this equipment is often lagging in security features such as: modern communication, authentication, and authorization mechanisms we would expect in critical equipment attached to a network.

The lack of security features has led to a need to build out a set of best practices when it comes to monitoring and logging capabilities of OT systems. In the IT environment, logging and monitoring of networks, users, and devices is critical for a variety of reasons. Some of this information is needed operationally. Other times, the logging and monitoring of networks, users, and devices may be driven for security reasons, and most notably in the last 5 to 10 years it's been driven by analytics to increase efficiency. These same needs are also important in the OT environment.

The purpose of this document is to build out guidelines that increase the ability of Data Center designers and operators to monitor the security health of ICS devices that provide electrical monitoring and mechanical cooling using operational data to derive security related insights for resilient operations.

Out of Scope:

- This document will not focus on how data is captured, i.e. communication protocols.
- Vulnerability Management
- Incident Management
- Asset Management

1 Background

IT vs OT Systems

When most think of cybersecurity they think of information technology, or IT. These systems support traditional workloads such as email, software applications, etc. Security in this environment is really predicated on the traditional CIA triad of confidentiality, integrity, and availability.

For operational technology, or OT systems, the focus is on availability and safety because the consequences in these environments impact human health and safety as opposed to IT service

availability. OT environments consist of systems that monitor, measure, and maintain control of our critical infrastructure such as, our power grids, manufacturing plants, and even our buildings/homes. Central to the availability aspects of these devices is their robustness; their ability to operate reliably, maintain fault tolerance, and recover from failures in harsh conditions. These systems must achieve this with the expectation that they will run for decades.

How IT & OT support Data Center Activities

Why monitoring is critical to DC Operations

The Data Center (DC) sits at the intersection of network, compute, and storage, with a myriad of critical parts run by an ever-expanding suite of industrial control systems that bridge the physical and digital world. Threat vectors are increasing, and operational technologies are frequently designed with safety and availability as the focus rather than mitigation of security risks, leaving them open to malicious activity.

Operational & Security Perspective

Unlike traditional IT environments, when it comes to Industrial Control and Building Management Systems, the largest risk to the environment is not through loss of information, it is instead loss of overall availability of services. As a result, operational metrics can directly help influence security detection and monitoring systems.

Purdue Model

The Purdue Enterprise Reference Architecture is a model created by Purdue University Consortium for computer integrated manufacturing to define the different levels of systems and their functions that are used in ICS systems and how best to secure them from a logical standpoint. Akin to the conceptual framework used in networking systems (OSI Model), the 6 layers identified in the Purdue Model when implemented can mitigate cyber risk prevailing in OT environments.

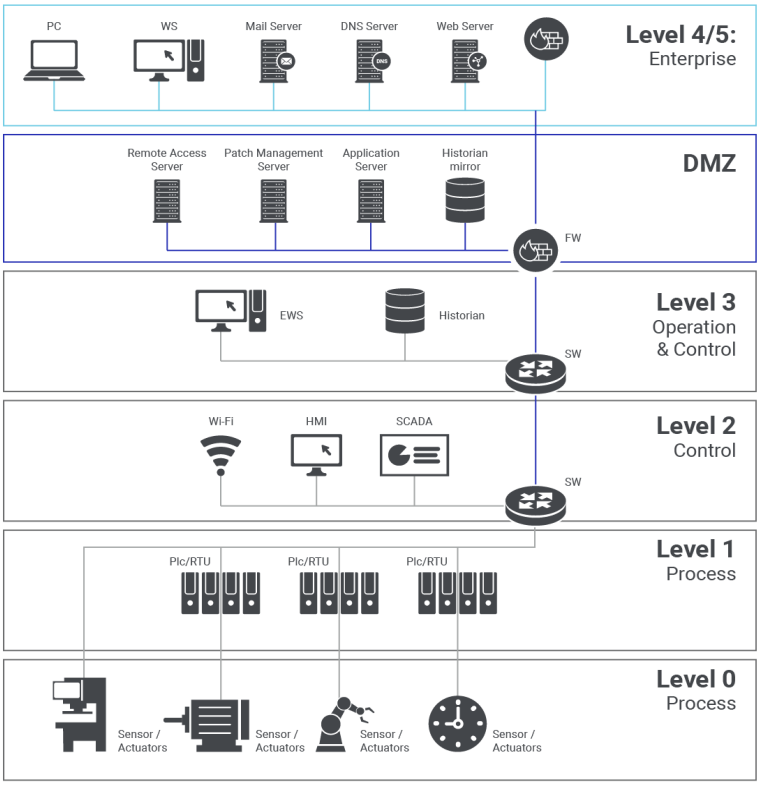

Figure 1. Purdue Enterprise Reference Architecture

Level 4/5 – Enterprise

Level 4/5 is known as the enterprise layer and are home to systems that you would find in a traditional IT network such as email, Enterprise Resource Planning (ERP) capabilities, and other business specific applications and systems. At this layer, confidentiality and the integrity of information are of primary concern from a security perspective.

Level 3.5 – Demilitarized zone (DMZ)

To reduce the attack surface of the OT network a DMZ is employed to segment devices and services between the two zones. Connections and services terminating in this level are reviewed, validated, and qualified before connecting to the ICS network. Terminal services for remote access into the ICS network for vendor/external support generally live in this network zone where remote user access is authenticated and only required resources are accessible to them in the ICS environment. Operating System and firmware patches obtained externally may also terminate in this zone and be allowed into the ICS environment after validation.

Level 3 – Facilities/Process Control Network

Level 3 in the Purdue Model is home to supporting infrastructure for the ICS environment. These systems include but are not limited to Active Directory services, historians for controls data acquisition, and backhaul network infrastructure for the data center.

Level 2 – Supervisory Control (real-time monitoring & operations supervision & control)

In this zone programmatic changes to programmable logic controllers (PLCs) and other OT devices involved in supervisory control are managed here. This could include but is not limited to engineering workstations (EWS) and operator workstations/human machine interfaces (HMI). At a system level, the Building Management System (BMS), Electrical Power Management System (EPMS), and Safety Information Systems (SIS) would be found at this level.

Level 1/0 – Intelligent Devices & Physical Processes (PLCs, Controllers, RTUs, Sensors, Actuators)

Sensors and instrumentation that control the physical processes at the data center are found on this level. For this paper, Level 1 assets are those that are on a shared network with other assets, while Level 0 assets are those downstream of Level 1 assets (e.g. direct I/O & simple sensor networks such as HART).

Typical OT systems used in Data Centers

Several examples of mechanical, electrical, and other building support systems as described below. These are common to the Data Centers space and can be used to help identify relevant assets to evaluate. Additionally, an example Data Center single line diagram is shown in Appendix A with more detailed information on how some of these assets are interconnected.

Mechanical Systems: Brief overview

The cooling stack and associated water storage and treatment systems are examples of mechanical infrastructure used in Data Centers. Within the cooling stack may be found cooling towers and chillers, process chilled water (PCW) pumps, air handling units (AHUs), coolant distribution units (CDUs), and rooftop units (RTUs). Other liquid/liquid, liquid/air, air/air heat exchangers may also be used in various designs to transport power away from IT payloads.

Most of these systems are often on the facilities network, as they consist of a mixture of PLCs and embedded controllers from a diverse set of vendors and integrators, and often need to be commissioned prior to IT equipment being commissioned.

Electrical Systems: Brief Overview

Power distribution and monitoring systems are examples of electrical infrastructure used in Data Centers. Within the electrical stack we have substations, any transformer stages, any power distribution centers, any backup power or power generation sources, and any power protection networks. Other power components that are part of a Data Center's power hierarchy would also be in scope.

Like the mechanical systems, the electrical systems arrive at various times from different vendors and integrators, and need to be commissioned prior to IT arrival. With much faster system time constants than mechanical systems, power protection is an important aspect of human and equipment safety and is often much more robust than on mechanical systems.

Other Building Support Systems (Life Safety, Access Control etc.): Brief Overview

Other building support systems would include Life Safety and Building Access controls. Depending on unique needs and requirements, different data centers may have different systems not specifically called out here. This document provides high level guidelines that can be integrated into any system that supports operational needs.

Examples: Fire panels, smoke detectors, leak detection, fuel spill detection, fire smoke dampers

2 Defining Critical Assets

Moving with speed is critical for Data Center Designers and Operators as they continue to expand their data center footprint to meet the capacity needs for their users and products/services. To meet these goals and address the cybersecurity challenges required to secure the capacity for these services, a risk management strategy that addresses how to assess, respond to, and monitor risk in making both investment and operational decisions is paramount. Central to this strategy is identifying the critical assets/systems required for data center operations.

This exercise is an effort to identify and prioritize cyber risk from a component and system level to determine the extent to which circumstances or events could adversely impact data center operations and the likelihood that such circumstances or events will occur.

System Classification

An understanding of the functional systems and components of ICS supporting DC operations requires not only critical security readiness, but operational resiliency as well. Classifying systems in this manner provides for a playbook for aligning security controls to common objectives for DC environments and prioritizing cyber risk management activities. From a classification standpoint, systems and components lower in the Purdue Model (0-2) have the greatest impact on human safety and operational availability/resilience.

Identify the asset's function within the system hierarchy

The Purdue Model may be utilized to determine where the asset sits relative to other system assets. Moving up the levels in the Purdue Model, will require more security relevant features.

Actual installations may not follow the Purdue Model hierarchy as IoT centric architectures that are more mesh in structure take hold, and in those scenarios an alternative hierarchical classification may be more appropriate.

Identify the control system's functional objectives

Depending on the functional objective of a control system, information from that system may be handled with different priorities. Most applications can be classified using several of the following:

- Environmental Safety
- Human Safety
- Sensitive Information
- IT payload operation and availability
- Physical Security

Safety will typically be prioritized the highest, followed by security. For additional examples for what assets may be classified under these functional objectives, please refer to Appendix C.

Domain Classification

For IT operations, given that datacenter operation is highly dependent on the physical and logical domain sizes of the control system's influence, it is also convenient to expand asset subclassification to the following:

- Damage / outage of entire region
- Damage / outage of entire zone
- Damage / outage of entire facility
- Damage / outage of entire cluster
- Damage / outage of entire row
- Damage / outage of rack
- Damage / outage of machine
- Suboptimal operation of above

Each Data Center Designers and Operators may have a distinct architecture and need to apply a different cost function associated with the above domains, yet the priority likely remains the same. The impact of damage and outages are typically straightforward to calculate and prioritize given the availability requirements of the architecture, while suboptimal performance may be more difficult to prioritize among outages.

3 Event and Monitoring Requirements

Devices that monitor, protect and control equipment in a data center may be in operation for decades. As cybersecurity attacks evolve, these devices need to provide information that supports the investigation and resolution of security incidents.

The following tables describe the types of information these systems need to provide and how these can help to improve our ability to monitor their security health and provide data to drive analytics. These tables have been organized into 3 areas, and should be used for initial guidance rather than as a comprehensive set of recommendations:

1. Security Relevant Features - Capabilities that assets may provide to assist with security
2. Configuration Data - Data that assets should provide to assist with investigations
3. Data Quality / Operational Data - Data not directly related to security, which may assist with detection of an operational anomaly caused by a security event

All features and data described may not be required for all assets and should instead be evaluated through Risk Assessment.

Component Categories

Table 1. Security Relevant Features

Security Features	Purpose	Notes
Authentication (unique ID) and authorization (ACL)	Unique identifier for access logs, and restricted access to resources	Not all devices/protocols have authentication • Modbus device, for example, will reply to any request
Certificates, encryption keys	Trusted users	TLS certificates as an example. • Have they expired, when do they expire? • When do they need to be renewed? • Log a message / warning when these are about to expire?
Heartbeat	Signal uninterrupted asset identity	Capture loss of connectivity to client. • Signal if unresponsive to a heartbeat message
Default credentials alerts	Provide mechanism to detect if default credentials have been changed	Credential management: • Passwords are not preferred. • A device that will not do anything until default passwords or trust lists are changed.
Logs	Provide history of access and actions on assets	Separate dedicated log for security events. • Access logs • Maintenance logs (Changes to system or user configuration) • Centrally managed security log (protections to detect alterations)

Security Features	Purpose	Notes
Secure communication protocols	Mitigate man-in-the-middle vulnerabilities	On startup, device may report protocols it is configured to use, and which ones are enabled/disabled Let's remove this as a requirement but fit it into the startup category (which still needs to be created) On startup it would be useful if the device reported the protocols it is configured to use

Table 2. Configuration Data

Any configuration change in general should generate risk signal

Configuration Item	Purpose	Notes
Acceptable system parameters (valid range)	Create a baseline of system wide parameters once configured. Detect changes to this baseline.	The change of system parameters could be a security event. • Baseline configurations should likely be stored upstream of assets through an asset or configuration management system. • Include settings at the control system level and device level.
Firmware Control	Verification (ie, signed) that the firmware is of the correct version. Device specific.	Facilitate firmware management • Provide mechanism to know if new firmware is available • Verify firmware version • Ideally update devices in place without taking triggering an outage

Configuration Item	Purpose	Notes
Network links (source & destination IPs, ports, and protocols)	Network monitoring	Identification of resources to communicate with. • Mapping of source and destination identifiers, and inclusion in logs • A change could be a security event.
Device Identifier (Mac & IP address)	Network identity	Name, Type, IP and MAC Address, serial number, certificate, category • Example: “I am a HVAC controller or power meter”
Device classification	Verify the correct asset (or asset class) is physically/logically connected to the correct location.	Similar to Device Identifier. • Assist with detection of unauthorized assets connected to various locations within the system hierarchy
Session state	Track connection details	Provides a mechanism to know whether a device is still alive (or disconnected, reconnected, or replaced)
Sensor/device units (Temperature, Voltage)	Units associated with a measurement and often a scaling factor as well	Useful to know if a unit of measurement or scaling factor ever changes. Difference between process level configuration and system level configuration a challenge.
Application in controller	Programming for specific applications.	Like firmware control. Track application version to help triage for known security alerts.

Configuration Item	Purpose	Notes
	Potentially monitoring for changes in code.	
Documentation that describes all possible security events for a given device	List of possible events and what each one means. Like an error code lookup	Potential risk to expose these in documentation

Table 3. Data Quality / Operational Data

Item	Purpose	Notes
Sensor/device valid range (Temperature, Voltage, network traffic)	Provides ability to detect operational anomaly, as a potential signal of an attack	Operational anomalies would be used as a proxy for a potential security event.
Sensor/device functional range (Temperature, Voltage, network traffic)	Provides ability to detect operational anomaly, as a potential signal of an attack	Like a valid range, except with additional customer context to restrict the operational range within the asset's function. For example, a temperature sensor may have a valid range from 0-255C, but a functional range of 15-65C.
Exceeded thresholds/parameters	Alert/Alarm on user defined conditions for a given parameter	Built in alert/alarms tied with an asset's functional range contains the complexity of thresholding to within the asset.

Item	Purpose	Notes
System/application alerts	Flag different conditions of the system/application with different priorities.	System/application alerts may combine knowledge from various sensors across multiple assets to flag system conditions.

4 Risk Assessment

Risk Assessment Matrix

To evaluate risks associated with an asset and whether it requires mitigation, it is proposed that using a risk assessment matrix (RAM) of the format below:

Severity Rating	Assets	Increasing probability			
		Rare occurrence	Low occurrence	Common occurrence	Regular occurrence
0	Zero damage	Mitigation optional	Mitigation optional	Mitigation optional	Mitigation optional
1	Slight damage	Mitigation preferred	Mitigation preferred	Mitigation preferred	Mitigation preferred
2	Minor damage	Mitigation preferred	Mitigation preferred	Mitigation required	Mitigation required
3	Local damage	Mitigation required	Mitigation required	Mitigation required	Mitigation required
4	Major damage	Mitigation required	Mitigation required	Mitigation required	Mitigation required
5	Extensive damage	Mitigation required	Mitigation required	Mitigation required	Mitigation required

This paper chooses to focus on evaluating assets, rather than additional dimensions that are also common with other RAMs. Also, this paper chooses to evaluate them with a security context to help focus the exercise on mitigating the impact of risks associated with attacks or compromises.

The RAM can be used from the point of view of either a system integrator or a vendor.

For the **vendor**, it is important to evaluate the impact of losing that asset in all possible configurations:

- Forget all the redundancy and all the other systems
- Look at worst case scenario on how that asset may be used in a customer system
- Evaluate the occurrence based on customer data on similar use cases

For the **system integrator**, it is important to evaluate the impact of losing that asset:

- Evaluate the availability of the asset first without any redundancy, and then based on the redundancy in the existing topology.
- Look at worst case scenario on how that asset is used within the system
- Evaluate the occurrence based on industry data or existing fleet data

Once the severity and occurrence of the asset is evaluated, the RAM will provide a recommendation on how to mitigate the asset through the implementation of monitoring and logging features.

Mitigation Techniques

For assets that are deemed moderate to high risk, the mitigation techniques in this section can be used. The classification techniques described in the previous sections can now be leveraged to determine what subset of risk signals to focus on.

First, the asset can be evaluated based on its positioning in the Purdue Model. The recommended response is listed in the table below:

Category	Component	L0	L1	L2	L3
Security Relevant Feature	Authentication (unique ID) and authorization (ACL)	Optional	Preferred	Required	Required
Security Relevant Feature	Certificates, encryption keys	Optional	Preferred	Required	Required
Security Relevant Feature	Heartbeat	Optional	Preferred	Required	Required
Security Relevant Feature	Default credentials alerts	Optional	Preferred	Required	Required
Security Relevant Feature	Logs	Optional	Preferred	Required	Required

Category	Component	L0	L1	L2	L3
Security Relevant Features	Secure communication protocols	Optional	Required	Required	Required
Configuration Data	Acceptable system parameters (valid range)	Optional	Required	Required	Required
Configuration Data	Firmware Control	Optional	Required	Required	Required
Configuration Data	Network links (source & destination IPs, ports, and protocols)	Optional	Required	Required	Required
Configuration Data	Device Identifier (Mac & IP address)	Optional	Required	Required	Required
Configuration Data	Device classification	Optional	Required	Required	Required
Configuration Data	Session state	Optional	Required	Required	Required
Configuration Data	Sensor/device units (Temperature, Voltage)	Optional	Required	Required	Required
Configuration Data	Application in controller	Optional	Required	Required	Required
Configuration Data	Documentation that describes all possible security events for a given device	Optional	Required	Required	Required
Data Quality / Operational Data	Sensor/device valid range (Temperature, Voltage, network traffic)	Optional	Required	Preferred	Required
Data Quality / Operational Data	Sensor/device functional range (Temperature, Voltage, network traffic)	Optional	Required	Preferred	Required
Data Quality / Operational Data	Exceeded thresholds/parameters	Optional	Required	Preferred	Required
Data Quality / Operational Data	System/application alerts	Optional	Required	Preferred	Required

Next, evaluate the asset in the domain size that it serves:

Category	Component	Damage / outage of entire region	Damage / outage of entire zone	Damage / outage of entire facility	Damage / outage of entire cluster	Damage / outage of entire row	Damage / outage of rack	Damage / outage of machine	Suboptimal operation of above
Security Relevant Feature	Authentication (unique ID) and authorization (ACL)	Required	Required	Required	Preferred	Preferred	Optional	Optional	Optional
Security Relevant Feature	Certificates, encryption keys	Required	Required	Required	Preferred	Preferred	Optional	Optional	Optional
Security Relevant Feature	Heartbeat	Required	Required	Required	Preferred	Preferred	Optional	Optional	Optional
Security Relevant Feature	Default credentials alerts	Required	Required	Required	Preferred	Preferred	Optional	Optional	Optional
Security Relevant Feature	Logs	Required	Required	Required	Preferred	Preferred	Optional	Optional	Optional
Security Relevant Features	Secure communication protocols	Required	Required	Required	Preferred	Preferred	Optional	Optional	Optional
Configuration Data	Acceptable system parameters (valid range)	Required	Required	Required	Preferred	Preferred	Optional	Optional	Optional
Configuration Data	Firmware Control	Required	Required	Required	Preferred	Preferred	Optional	Optional	Optional
Configuration Data	Network links (source & destination IPs, ports, and protocols)	Required	Required	Required	Preferred	Preferred	Optional	Optional	Optional
Configuration Data	Device Identifier (Mac & IP address)	Required	Required	Required	Preferred	Preferred	Optional	Optional	Optional
Configuration Data	Device classification	Required	Required	Required	Preferred	Preferred	Optional	Optional	Optional

Category	Component	Damage / outage of entire region	Damage / outage of entire zone	Damage / outage of entire facility	Damage / outage of entire cluster	Damage / outage of entire row	Damage / outage of rack	Damage / outage of machine	Suboptimal operation of above
Configuration Data	Session state	Required	Required	Required	Preferred	Preferred	Optional	Optional	Optional
Configuration Data	Sensor/device units (Temperature, Voltage)	Required	Required	Required	Preferred	Preferred	Optional	Optional	Optional
Configuration Data	Application in controller	Required	Required	Required	Preferred	Preferred	Optional	Optional	Optional
Configuration Data	Documentation that describes all possible security events for a given device	Required	Required	Required	Preferred	Preferred	Optional	Optional	Optional
Data Quality / Operational Data	Sensor/device valid range (Temperature, Voltage, network traffic)	Required	Required	Required	Preferred	Preferred	Optional	Optional	Optional
Data Quality / Operational Data	Sensor/device functional range (Temperature, Voltage, network traffic)	Required	Required	Required	Preferred	Preferred	Optional	Optional	Optional
Data Quality / Operational Data	Exceeded thresholds/parameters	Required	Required	Required	Preferred	Preferred	Optional	Optional	Optional
Data Quality / Operational Data	System/application alerts	Required	Required	Required	Preferred	Preferred	Optional	Optional	Optional

Finally, evaluate the asset's functional objectives:

Category	Component	Environmental Safety	Human Safety	Sensitive Information	IT payload operation and availability	Physical Security
Security Relevant Feature	Authentication (unique ID) and authorization (ACL)	Preferred	Required	Required	Preferred	Preferred
Security Relevant Feature	Certificates, encryption keys	Preferred	Required	Required	Preferred	Preferred
Security Relevant Feature	Heartbeat	Preferred	Required	Required	Preferred	Preferred
Security Relevant Feature	Default credentials alerts	Preferred	Required	Required	Preferred	Preferred
Security Relevant Feature	Logs	Preferred	Required	Required	Preferred	Preferred
Security Relevant Features	Secure communication protocols	Required	Required	Required	Required	Required
Configuration Data	Acceptable system parameters (valid range)	Preferred	Preferred	Preferred	Preferred	Preferred
Configuration Data	Firmware Control	Preferred	Preferred	Preferred	Preferred	Preferred
Configuration Data	Network links (source & destination IPs, ports, and protocols)	Required	Required	Required	Required	Required
Configuration Data	Device Identifier (Mac & IP address)	Required	Required	Required	Required	Required
Configuration Data	Device classification	Optional	Optional	Optional	Optional	Optional
Configuration Data	Session state	Optional	Optional	Optional	Optional	Optional
Configuration Data	Sensor/device units (Temperature, Voltage)	Preferred	Preferred	Preferred	Preferred	Preferred

Category	Component	Environmental Safety	Human Safety	Sensitive Information	IT payload operation and availability	Physical Security
Configuration Data	Application in controller	Optional	Preferred	Preferred	Optional	Optional
Configuration Data	Documentation that describes all possible security events for a given device	Optional	Optional	Optional	Optional	Optional
Data Quality / Operational Data	Sensor/device valid range (Temperature, Voltage, network traffic)	Optional	Preferred	Preferred	Preferred	Optional
Data Quality / Operational Data	Sensor/device functional range (Temperature, Voltage, network traffic)	Optional	Optional	Optional	Optional	Optional
Data Quality / Operational Data	Exceeded thresholds/parameters	Optional	Preferred	Optional	Preferred	Optional
Data Quality / Operational Data	System/application alerts	Preferred	Preferred	Preferred	Preferred	Preferred

Examples

Door Controller

Assuming a door controller asset is evaluated to be a high-risk asset, run it through each of the classification topics above, and come up with a resultant recommendation based on the highest level of guidance. Note below that most signals are preferred or required:

Group	Security Signals	Door controller			
		L1	Suboptimal operation of above	Environmental Safety	**Recommendation**
Security Relevant Feature	Authentication (unique ID) and authorization (ACL)	Preferred	Optional	Preferred	**Preferred**
Security Relevant Feature	Certificates, encryption keys	Preferred	Optional	Preferred	**Preferred**
Security Relevant Feature	Heartbeat	Preferred	Optional	Preferred	**Preferred**
Security Relevant Feature	Default credentials alerts	Preferred	Optional	Preferred	**Preferred**
Security Relevant Feature	Logs	Preferred	Optional	Preferred	**Preferred**
Security Relevant Features	Secure communication protocols	Required	Optional	Required	**Required**
Configuration Data	Acceptable system parameters (valid range)	Required	Optional	Preferred	**Required**
Configuration Data	Firmware Control	Required	Optional	Preferred	**Required**
Configuration Data	Network links (source & destination IPs, ports, and protocols)	Required	Optional	Required	**Required**
Configuration Data	Device Identifier (Mac & IP address)	Required	Optional	Required	**Required**
Configuration Data	Device classification	Required	Optional	Optional	**Required**
Configuration Data	Session state	Required	Optional	Optional	**Required**
Configuration Data	Sensor/device units (Temperature, Voltage)	Required	Optional	Preferred	**Required**

Group	Security Signals	Door controller			
		L1	Suboptimal operation of above	Environmental Safety	**Recommendation**
Configuration Data	Application in controller	Required	Optional	Optional	**Required**
Configuration Data	Documentation that describes all possible security events for a given device	Required	Optional	Optional	**Required**
Data Quality / Operational Data	Sensor/device valid range (Temperature, Voltage, network traffic)	Required	Optional	Optional	**Required**
Data Quality / Operational Data	Sensor/device functional range (Temperature, Voltage, network traffic)	Required	Optional	Optional	**Required**
Data Quality / Operational Data	Exceeded thresholds/parameters	Required	Optional	Optional	**Required**
Data Quality / Operational Data	System/application alerts	Required	Optional	Preferred	**Required**

5 Glossary

Alarm: Notification which can be visual or audible signifying a change in state of a system and/or device that requires immediate attention.

Event: An event is a generic term referring to any point of interest. Events are typically generated from systems and/or devices.

Industrial Control System (ICS): This is a broad classification of automation systems and their associated instrumentation used to provide command and control functions for processes in industrial/manufacturing environments.

Supervisory Control and Data Acquisition (SCADA): SCADA refers to the culmination of systems and networks that communicate with industrial control systems to provide supervisory functions to an operator. Like ICS, SCADA systems typically span a large geographic area.

Building Management Systems (BMS): A type of ICS that controls various electrical and mechanical functions within a building such as lighting, HVAC, and power systems.

Electrical Power Management System: A type of ICS that provides information on power quality and other vital metrics to optimize the use of energy and electrical consumption.

6 References

1. National Institute of Standards and Technology. “FIPS 199, Standards for Security Categorization of Federal Information and Information Systems.” *NIST Technical Series Publications*, February 2004, https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf. Accessed 22 December 2021.
2. Skarvelis, Nick. “BMS vs. EPMS | Discover the Right Solution for Your Facility - APT, Inc.” *Applied Power Technologies, Inc.*, 15 July 2021, https://www.apt4power.com/2021/07/15/bms-vs-epms-discover-the-right-solution-for-your-facility/. Accessed 22 June 2022.
3. Zscaler Inc. “What Is the Purdue Model for ICS Security?” *Zscaler*, https://www.zscaler.com/resources/security-terms-glossary/what-is-purdue-model-ics-security. Accessed 22 January 2022.

7 License

Creative Commons

OCP encourages participants to share their proposals, specifications, and designs with the community. This is to promote openness and encourage continuous and open feedback. It is important to remember that by providing feedback for any such documents, whether in written or verbal form, that the contributor or the contributor's organization grants OCP and its members irrevocable right to use this feedback for any purpose without any further obligation.

It is acknowledged that any such documentation and any ancillary materials that are provided to OCP in connection with this document, including without limitation any white papers, articles, photographs, studies, diagrams, contact information (together, “Materials”) are made available under the Creative Commons Attribution-ShareAlike 4.0 International License found here: https://creativecommons.org/licenses/by-sa/4.0/, or any later version, and without limiting the foregoing, OCP may make the Materials available under such terms.

As a contributor to this document, all members represent that they have the authority to grant the rights and licenses herein. They further represent and warrant that the Materials do not and will not violate the copyrights or misappropriate the trade secret rights of any third party, including without limitation rights in intellectual property. The contributor(s) also represent that, to the extent the Materials include materials protected by copyright or trade secret rights that are owned or created by any third-party, they have obtained permission for its use consistent with the foregoing. They will provide OCP evidence of such permission upon OCP’s request. This document and any "Materials" are published on the respective project's wiki page and are open to the public in accordance with OCP's Bylaws and IP Policy. This can be found at http://www.opencompute.org/participate/legal-documents/. If you have any questions, please contact OCP.

Footer:

8 About Open Compute Foundation

At the core of the Open Compute Project (OCP) is its Community of hyperscale data center operators, joined by telecom and colocation providers and enterprise IT users, working with vendors to develop open innovations that, when embedded in products are deployed from the cloud to the edge. The OCP Foundation is responsible for fostering and serving the OCP Community to meet the market and shape the future, taking hyperscale led innovations to everyone. Meeting the market is accomplished through open designs and best practices, and with data center facility and IT equipment embedding OCP Community-developed innovations for efficiency, at-scale operations and sustainability. Shaping the future includes investing in strategic initiatives that prepare the IT ecosystem for major changes, such as AI & ML, optics, advanced cooling techniques, and composable silicon. Learn more at www.opencompute.org.

9 Appendix

Appendix A: Example datacenter BMS/EPMS Architectures

To help identify the typical types of devices found in data centers we have created example BMS and EPMS architectures:

Use the different types of devices from these architectures to help evaluate the risk associated with losing each asset. Eventually, define the types of data these devices could provide to mitigate the identified risks.

Appendix B: Example risk matrix factors and references

As a means of categorizing the level of risk associated with losing an asset in a data center, below are evaluations of a few examples of risk matrices available today:

1) How modernizing control systems can reduce business risk and deliver profit improvement - Schneider Electric Blog

Appendix C: Additional Example Assets

Associated risks can be used to determine the severity rating in the risk assessment matrix. System classification, functional objections, and domain sizes can then be used to evaluate what mitigation techniques should be applied.

Air Handling Unit (Controller)

Associated Risks	**Damage to various workloads supporting DC operations** **Environmental health safety concerns**
System Classification	Purdue Level - 1
Control System Functional Objectives	IT payload operation and availability Environmental Safety
Domain size	Damage / outage of entire cluster

Air Handling Unit (VFD)

Associated Risks	**Damage to various workloads supporting DC operations** **Environmental health safety concerns**
System Classification	Purdue Level - 0
Control System Functional Objectives	IT payload operation and availability
Domain size	Damage / outage of entire cluster

Power Supply (UPS)

Associated Risks	**Damage to various workloads supporting DC operations** **Environmental health safety concerns**
System Classification	Purdue Level - 1
Control System Functional Objectives	IT payload operation and availability
Domain size	Damage / outage of entire cluster