INL/RPT-22-66453-Revision-0



# Prioritizing ICS Beachhead Systems for Cyber Vulnerability Testing

March 2022

Daniel Paul Keys, Virginia L Wright, Samuel Douglas Chanoski, Sarah G Freeman, Cherylene Caddy

Changing the World's Energy Future

Idaho National Laboratory

*INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC*

INL/RPT-22-66453-Revision-0

# Prioritizing ICS Beachhead Systems for Cyber Vulnerability Testing

**Daniel Paul Keys, Virginia L Wright, Samuel Douglas Chanoski, Sarah G Freeman, Cherylene Caddy**

**March 2022**

**Idaho National Laboratory**
**Idaho Falls, Idaho 83415**

**http://www.inl.gov**

**Prepared for the**
**U.S. Department of Energy**
**Under DOE Idaho Operations Office**
**Contract DE-AC07-05ID14517**

# Prioritizing ICS Beachhead Systems for Cyber Vulnerability Testing

March 1, 2022

CyTRICS™ Cyber Testing for Resilient Industrial Control Systems

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

# 1. Executive Summary

Cyber Testing for Resilient Industrial Control Systems™ (CyTRICS™) is the Department of Energy's (DOE's) program for cybersecurity vulnerability testing, digital subcomponent enumeration, and forensic assessment. CyTRICS leverages best-in-class test facilities and analytic capabilities at six DOE National Laboratories and strategic partnerships with key stakeholders including technology developers, manufacturers, asset owners and operators, and interagency partners.

During the program's development, CyTRICS established a unique methodology for prioritizing digital components within operational technology (OT)[a] and industrial control systems (ICS) in the Energy Sector Industrial Base (ESIB) for cyber vulnerability testing. The CyTRICS Prioritization Process leverages multiple characteristics of systems, components, and their contextual deployment to calculate a quantification of individual digital components for CyTRICS testing. The initial version of the CyTRICS Prioritization Process was premised largely upon the impact which could result to an industrial control system if the digital component under testing was compromised, either through malicious means, faulty engineering, or other modes.

The worldwide compromise of the SolarWinds Orion platform, first reported in December 2020, [1] through malicious interference with the digital patching cycle was a watershed event in cyber supply chain security. The SolarWinds compromised demonstrated the strategic importance of certain types of ubiquitous software, and the ability to generate widespread cybersecurity effects. To address this challenge and as a part of the Department of Energy's response to the SolarWinds compromise, DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) directed the National Laboratories to evolve the CyTRICS Prioritization Process methodology to encompass additional factors related to the strategic importance of digital components. CESER directed CyTRICS researchers to identify, characterize, and append strategic factors to the CyTRICS Prioritization Process to provide additional weight to these characteristics. National Laboratory expert researchers identified functionality, distribution, and platform characteristics for digital components in ICS and OT that they assessed would be likely targeted in strategic initial-access cyber attack. CyTRICS has termed these factors "ICS Beachhead Systems," leveraging a definition first advanced by Schneider Electric,[2] which is intended as a blanket term to encompass digital components, products, and systems in OT.

This paper describes the ICS Beachhead Systems identified and the rationale for inclusion. As a next step in the research and refinement process, the National Laboratories will validate this initial set of characteristics against digital components evaluated by the CyTRICS program and current implementation of the CyTRICS Prioritization Process. After validation, CyTRICS researchers will then develop a scoring methodology to generate a quantitative score to assess the degree to which a digital component is characterized as an ICS Beachhead System. Finally, the National Laboratories will append this scoring to the existing CyTRICS Prioritization Process algorithm.

[a] Operational technology (OT) encompasses a broad range of programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems. (https://csrc.nist.gov/Projects/operational-technology-security)

# 2. Acknowledgments

The Idaho National Laboratory and U.S. Department of Energy (DOE) acknowledges all stakeholders who participate in the CyTRICS program and who contributed input used in the development of this report.

**Authors**

Daniel Paul Keys, Control Systems Cybersecurity Analyst, Idaho National Laboratory,

Samuel Chanoski, Technical Relationship Manager, Idaho National Laboratory,

Sarah Freeman, Senior Intelligence Analyst, Idaho National Laboratory,

Virginia Wright, Energy Cyber Portfolio Manager, Idaho National Laboratory,

Cherylene Caddy, Senior Advisor for Cybersecurity, Office of Cybersecurity, Energy Security, and Emergency Response, U.S. Department of Energy,

**Contributors**

Jeff Mitchell, Program Manager, Idaho National Laboratory,

Megan Samford, Chief Product Security Officer (CPSO) for Energy Management, Schneider Electric,

**Reviewers**

Jessica Smith, Senior Cybersecurity Research Scientist, Pacific Northwest National Laboratory,

Robert Hanson, Deputy Associate Program Leader for Defense Infrastructure, Lawrence Livermore National Laboratory,

Adam Hahn, Principal Critical Infrastructure Security Engineer, MITRE Corporation,

Marie Collins, Manager, Mobile & Cyber-Physical Systems Technology, MITRE Corporation,

Deb Bodeau, Senior Principal Security Engineer, MITRE Corporation,

Kevin Reifsteck, Director for Critical Infrastructure Protection and the Azure Critical Infrastructure solutions and Defender for IoT teams at Microsoft Corporation.

# 3. Table of Contents

# 4. Acronyms

AD FS: Active Directory Federation Services

AD: Active Directory

AI: Artificial Intelligence

AMI: Advanced Metering Infrastructure

AR: Augmented Reality

AWS: Amazon Web Services

BESS: Battery Energy Storage Systems

C2: Command & Control

CESER: DOE's Office of Cybersecurity, Energy Security, and Emergency Response

CISA: Cybersecurity and Infrastructure Security Agency

CSP: Cloud Service Provider

CyTRICS: Cyber Testing for Resilient Industrial Control Systems™

DaaS: Desktop as a Service

DCS: Distributed Control System

DER: Distributed Energy Resource

DER: Distributed Energy Resource Management

DIB: Defense Industrial Base

DOE: Department of Energy

DRaaS: Disaster Recovery as a Service

DRMS: Demand Response Management System

EMaaS: Energy Management as a Service

EV: Electric Vehicle

GCP: Google Cloud Platform

HMI: Human Machine Interface

HTTP: Hypertext Transfer Protocol

I/O: Input/Output

IaaS: Infrastructure as a Service

ICS: Industrial Control System

IED: Intelligent Electronic Device

IIoT: Industrial Internet of Things

IoT: Internet of Things

IT: Information Technology

LDAP: Lightweight Directory Access Protocol

LRU: Line Replaceable Unit

LSE: Load Serving Entities

M&A: Merger and Acquisitions

MDM: Meter Data Management

MSP: Managed Service Provider

NERC CIP: North American Electric Reliability Corporation Critical Infrastructure Protection

NERC: North American Electric Reliability Corporation

OEM: Original Equipment Manufacturers

OMS: Outage Management System

OPC UA: Open Protocol Consortium Unified Architecture

OPC: Open Protocol Consortium

OS: Operating System

OT: Operational Technology

PaaS: Platform as a Service

PdM: Predictive Maintenance

PLC: Primary Logic Controller

RTU: Remote Terminal Unit

SaaS: Software as a Service

SAM: Secure Access Manager

SAML: Security Assertion Markup Language

SBOM: Software Bill of Materials

SCADA: Supervisory Control and Data Acquisition

SME: Subject Matter Expert

SSO: Single Sign On

SVR: Foreign Intelligence Service of the Russian Federation

TCP: Transmission Control Protocol

VPN: Virtual Private Network

VR: Virtual Reality

XaaS: Anything-as-a-Service

# 5. Background of Cyber Testing for Resilient Control Systems (CyTRICS) Program

Cyber Testing for Resilient Industrial Control Systems (CyTRICS) is the Department of Energy's (DOE) program for cybersecurity vulnerability testing, digital subcomponent enumeration, and forensic assessment. First developed and piloted in 2018, CyTRICS enhances the cyber resilience of highly critical equipment in the Energy Sector Industrial Base (ESIB) by partnering with stakeholders to identify high priority operational technology (OT) components, perform expert testing, share information about vulnerabilities in the supply chain, and inform improvements in component design and manufacturing. The overall goal of the CyTRICS program is to identify critical cyber vulnerabilities prior to exploitation and reduce the cycle time to mitigation. The program leverages best-in-class test facilities and analytic capabilities across six DOE National Laboratories, as well as strategic partnerships with technology developers, manufacturers, asset owners and operators, and interagency partners. CyTRICS is led by the DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER).

CyTRICS was born out of increasing examples of cyber supply chain compromises and the growing concern adversaries could exploit weakness in digital supply chains, possibly triggering catastrophic effects on energy infrastructure and beyond. To address these concerns, the program identifies common mode vulnerabilities in high-impact hardware, software, and firmware and responsibly discloses them to manufacturers, who can develop mitigations before adversaries can exploit them. The CyTRICS program employs several unique and innovative processes: a quantitative methodology for prioritizing OT components, a standardized testing process that produces results (*e.g.*, taxonomies, ontologies, software and hardware bills of materials, and findings) in standard formats, a central repository to house testing results that supports cross-component analyses and reporting, and formal partnership agreements with manufacturers and asset owners to foster deep engagement and cooperation.

The mission of CyTRICS is to support DOE's strategy to shift left to anticipate, confront, and thwart multiple, ever-changing cybersecurity threats and vulnerabilities. The CyTRICS perspective is that the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is and to the consequences we would suffer if that trust were misplaced.[3]

# 6. Identifying Characteristics for Beachhead Products

The SolarWinds cyber supply chain compromise illustrated a sophisticated adversary's capability to obtain large-scale, strategic access to central computing infrastructure through a commonly used system. Based on research and analysis of the SolarWinds attack, CyTRICS analysts and subject matter experts (SMEs) formed the following questions to identify characteristics of OT products used within the ESIB which would make these components likely targets of a similar strategic access attack:

- Are components or products used in OT potential targets for strategic access campaigns?
- What characteristics make products most valuable to adversaries?
- Is CyTRICS already measuring these characteristics?
- How can CyTRICS augment testing prioritization to ensure CyTRICS assesses these products for vulnerabilities?

## 6.1 SolarWinds Overview

In September 2019, an advanced persistent threat (APT) actor (formally identified as APT 29 and Russia by the U.S. Government [4]) initiated an attack against SolarWinds, a managed service provider (MSP) based in the United States.[5] The attack, attributed to the Russian Foreign Intelligence Service (SVR),[6] was one of the largest global cyber supply chain attacks to date, affecting dozens of organizations in the United States, including U.S. government agencies.[7]

During the course of the attack, APT 29 compromised then deployed malware into the SolarWinds Orion build process. As SolarWinds Orion users downloaded and installed system updates, their systems were infected with SUNBURST malware, providing a vector for conducting further attacks. For example, attackers leveraged SUNBURST-provided access to steal Active Directory Federation Services (AD FS) token-signing certificates and forge user tokens (aka, Golden Security Assertion Markup Language (SAML)), the first known instance of the Golden SAML attack technique being used "in the wild."[8] Table 1 SolarWinds Attack Overview, details the SolarWinds attack and additional malware discovered throughout the course of subsequent investigations.

| Attacker Tool | Alternate Name(s) | Description/Activity |
|---|---|---|
| **SUNSPOT** (CrowdStrike) | None | SUNSPOT malware was used to insert a SUNBURST backdoor malware into SolarWinds Orion build process via msbuild.exe.[9] |
| **SUNBURST** (Kaspersky, Symantec) | Solorigate (Microsoft) | Once SolarWinds Orion updates were installed on customer networks, the .Net-based SUNBURST backdoor malware activates and sends information back to UNC2452 command and control (C2) servers.[10] |
| **RAINDROP** (Symantec)<br>**TEARDROP** (Symantec) | None | If determined to be a worthy target, UNC2452 installs the RAINDROP[11] memory dropper or TEARDROP memory dropper[12, 13] on target systems. UNC2452 may also instruct SUNBURST to delete itself from networks it deems insignificant or high risk. |
| **Cobalt Strike Beacon** | None | Both TEARDROP and RAINDROP are loaders designed to decrypt and execute an embedded payload (Cobalt Strike Beacon Implant (v4)) on the target system.[14, 15] The payload gives a remote operator C2 capabilities over a victim system via an encrypted network tunnel and the ability to rapidly exfiltrate data, log keystrokes, take screenshots, and deploy additional payloads. |
| **Sunshuttle** (malware family)<br>• **GoldMax** (Microsoft)<br>• **GoldFinger** (Microsoft)<br>• **Sibot** (Microsoft) | None | SUNSHUTTLE represents a family of malware (GoldMax, GoldFinger, and Sibot) found on systems compromised by SUNBURST.[16, 17, 18]<br>GoldMax, C2 backdoor designed to look like a system management software scheduled task,<br>GoldFinger, a HTTP trace tool,<br>Sibot achieves persistence on an infected machine, then downloads and executes a payload from a C2 server. |

**Table 1 SolarWinds Attack Overview**

Industry and cybersecurity organizations continue to identify organizations impacted by the SolarWinds Orion attack.[19] Furthermore, additional strategic access cyber supply chain attacks have been discovered since the SolarWinds Orion attack,[20] highlighting the importance of using strategic factors to prioritize energy sector OT products for cyber vulnerability testing.

## 6.2 Impact-Centric Models and Strategic Access Attacks

In 2015, Michael Assante and Robert M. Lee introduced the ICS Cyber Kill Chain in the wake of the Havex campaign.[21] Building on Lockheed Martin's Cyber Kill Chain, Assante and Lee sought to differentiate ICS-focused attacks from those targeting traditional IT systems. They argued that the creation of custom ICS attacks required significant understanding of not only the hardware and software used in an OT environment, but of the process physics. Due to these knowledge requirements, ICS attacks are comprised of two distinct stages: 1) cyber intrusion, preparation, and execution, and 2) ICS attack development and execution. Collectively, these two phases provide a model for how to frame ICS-focused cyber-attacks.

MITRE provides a similar model in its ATT&CK for ICS, a knowledge base which describes adversary actions during an ICS cyber-attack. ATT&CK for ICS focuses on the specific attack techniques used for each step of an attack.[b] Both SANS and MITRE, informed by historical attack and threat actor information, address the adversary's decision-making processes for conducting access campaigns. Both works assume the goal of an adversary ICS attack is to create a measurable impact on the targeted architecture.

The research in this paper, however, differs from SANS and MITRE in that it focuses on the identification of strategic ***access*** targets, rather than the identification of targets based on impact. Although some access campaigns are conducted with specific end-targets and impacts in mind, others are conducted because of the potential broad value for future and not-yet-defined cyber operations. This paper seeks to define characteristics of the products which ICS attackers are most likely to focus on to achieve strategic access goals.

The SolarWinds Orion product represented a strategic target, in part because of its prevalence throughout the U.S. and globally, with nearly 300,000 customers as of December 2020, and rated number one in Network Management Software market share.[22]

[b] MITRE's ATT&CK for ICS defines techniques listed under 12 tactics: Initial Access, Execution, Persistence, Evasion, Discovery, Lateral Movement, Collection, Command and Control, Inhibit Response Function, Impair Process Control, and Impact.

# 7. ICS Beachhead Product Characteristics

## 7.1 Introduction

This paper identifies characteristics associated with OT product functionality, distribution, and platform determined by the CyTRICS research team to be principal factors for indicating the value of the product in a strategic access campaign. Although CyTRICS recognizes the prevalence of IT networks and products as initial entry points to OT networks, the present research effort focuses on products manufactured for the OT market. IT products may be considered in the context of the same characteristic set where they are also used in OT networks.

In the development of this paper, CyTRICS researchers consulted with OT vendors, such as Schneider Electric, to obtain feedback on initial assumptions. Schneider Electric recommended CyTRICS consider the term “Beachhead Product” for inclusion and offered Human Machine Interfaces (HMIs) as an example of a Beachhead Product.[23] The term “beachhead” refers to a common military strategy of winning a small border area that becomes a stronghold, and from which forces can advance to the rest of a territory. The small border area is referred to as a “beachhead."[24] A beachhead system or device enables execution of tactics, techniques, and procedures (TTPs) in support of access, persistence, and lateral movement. CyTRICS researchers further considered the idea of “Beachhead Product” and determined “Beachhead System” to be the optimal descriptive label for systems associated with characteristics the team had already identified, resulting in this paper being titled “Prioritizing ICS Beachhead Systems for Cyber Vulnerability Testing.”

The final list of characteristics shown in
Figure 1 Beachhead System Characteristics, was sorted into two categories: Product Functionality and Product Platform & Distribution.

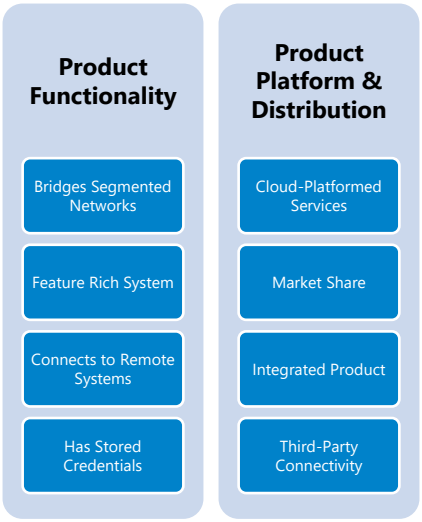


**Figure 1 Beachhead System Characteristics**

Definitions for each characteristic; rationale for consideration; and how the characteristic might be leveraged to gain initial access, maintain persistence, and perform lateral movement to achieve attack

campaign objectives are provided in their respective sections. Where relevant to the SolarWinds Orion attack campaign, additional descriptions of adversary exploitation techniques are provided.

The characteristic set was developed to evaluate systems used in the U.S. Energy Sector Industrial Base and their applicability to energy subsectors such as Electric, Oil & Natural Gas, and Renewable Energy.

In each characteristic description, an example product is analyzed. These examples are provided for illustrative purposes only; no assessment of vulnerability or compromise is intended or implied.

As a next step in the research process, National Lab experts will use evaluation methods recommended in this paper to assess systems based on how each system aligns with the identified Beachhead System characteristics. Systems will be assessed based on default configuration, features, and connectivity provided by the vendor or original equipment manufacturers (OEMs), without regard to how they are configured in any specific installation environment. Results will be documented in a report, like the example located in the "Sample System Analysis Report."

## 7.2 Product Functionality Characteristics

### 7.2.1 Bridges Segmented Networks

#### *7.2.1.1 Definition and Rationale*

The **Bridges Segmented Networks** characteristic identifies hardware and software systems designed to move data across otherwise separate security zones and networks. Examples of products with this capability include firewalls, security applications, virtual private networks (VPNs), HMIs, historians, Advanced Metering Infrastructure (AMI), Outage Management System (OMS), and ticketing systems. Systems which support external, remote access to virtual machines or management consoles also may bridge segmented networks.

Systems bridging segmented networks are valuable targets for an initial-access attack because they offer attackers a pathway into an otherwise segmented network, potentially providing access to devices and services across that network. Furthermore, this characteristic is useful for gaining access to otherwise protected ICS networks and systems useful for furthering adversary campaign goals and operational objectives. This characteristic is also reflected in the Mandiant "Funnel of Opportunity"[25] where systems which bridge segmented networks are viewed as "intermediary systems" used as steppingstones by attackers to reach intended OT targets.

Ivanti Pulse Connect Secure VPN is an example of a system which **Bridges Segmented Networks.** Ivanti Pulse Connect Secure is a software product used in OT networks to enable secure access for remote administrators. On April 20, 2021, Mandiant reported critical vulnerabilities in the Ivanti Pulse Connect Secure VPN product. [26] Attackers had exploited Ivanti Pulse Connect Secure VPN devices to gain access to Defense Industrial Base (DIB), government, green energy manufacturing, utilities, and financial networks in the United States and Europe where they bypassed single and multifactor authentication, persisted across upgrades, and maintained access through webshells. As of May 27, 2021, Mandiant noted 16 malware families associated with these attacks, now suspected to be espionage activity conducted by Chinese affiliated UNC2630 and UNC2717 APT groups.[27]

#### *7.2.1.2 Evaluation Method*

Systems with the **Bridges Segmented Networks** characteristic may list features such as support for secure data transfer, remote device status reporting, or the ability to store or cache network or remote device credentials allowing access to devices across the network. This characteristic may apply to devices located inside the ICS network perimeter, external devices residing on the ICS network edge, cloud devices, virtual appliances, or devices located at vendor sites for monitoring or maintenance. The CyTRICS research team's assessment is based on system feature sets (as designed) instead of how the system is deployed in any particular asset owner environment. News releases, marketing material, product manuals, data sheets, architecture diagrams, and product security hardening guides can be used to evaluate systems for this characteristic and identify indicators a system is designed to move data between security zones and networks.

#### *7.2.1.3 Product Example*

**Waterfall Unidirectional Security Gateway WF-500**

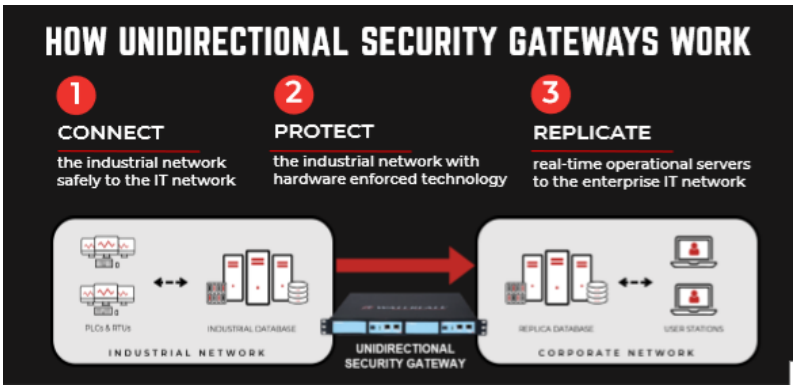


**Figure 2: How Unidirectional Security Gateways Work[28]**

Waterfall Unidirectional Security Gateway WF-500 systems enable IT/OT integration, control, and real-time industrial network monitoring.[29, 30, 31] Gateways replace firewalls in industrial network environments, providing protection from attacks originating on external networks. Unidirectional Security Gateways enable vendor monitoring, industrial cloud services, and visibility into operations for modern enterprises and customers by replicating servers, emulating industrial systems, and translating industrial data to cloud formats. The WF-500 modular hardware architecture is sold with a variety of modules to support customer operations and desired security posture. This includes a "Secure Bypass" mode where network connectivity across the WF-500 can be established in the event of a plant emergency.

### 7.2.2 Feature Rich System

#### *7.2.2.1 Definition and Rationale*

Systems designed for OT can contain a broad range of features and functionality designed to provide utility across a wide range of asset owner environments and uses. Trending IT and OT convergence also has introduced IT features into the OT environment. **Feature Rich System** is a contrast to systems built for single or limited purposes. Some examples of new system features introduced into the energy market, especially distribution include:

- IP-based Local Area Network (LAN) and Wide Area Network (WAN) networks;
- Integrated enterprise resource systems;
- Adoption of geospatial technologies;
- Virtualization;
- Implementations of OT systems onto cloud-based platforms; and
- Mobile technologies.[32]

IT systems repurposed for OT also may contain features which are well known across industry. The volume, variety, and complexity of features found on some repurposed IT systems could provide a platform for initial access, persistence and the flexibility needed by an adversary to advance attack campaign objectives.

#### *7.2.2.2 Evaluation Method*

**Feature Rich Systems** are systems designed to do many things across a wide variety of use cases and industries. This contrasts with systems designed for a single, specific use. Indicators may be a large number of communication options, services, interfaces, and protocols, web services, enhanced monitoring capabilities, databases, automation. Documentation also may note the system can be used across a wide range of deployment environments and uses. Indicators of the Feature Rich System characteristic may be found in marketing material, product manuals, data sheets, and news releases.

#### *7.2.2.3 Product Example*

**Schneider Electric EcoStruxure Foxboro Evo DCS**

**Figure 3: EcoStruxure Foxboro Evo DCS[33]**

EcoStruxure Foxboro DCS is an open, interoperable, IoT-enabled system architecture.[34] It includes the following features and subcomponents:

- An extensive suite of maintenance and provisioning tools, i.e., Maintenance Response Center for alerting, Predictive Maintenance tools, and Field Device Manager to help integrators and asset owners commission, configure, maintain, and diagnose devices;
- Provides functionality to remotely access maintenance software (Engineer Anywhere), review procedures, and generate reports leveraging cloud-based technology and mobile devices;
- Control Editor engineering software and configuration tool supports virtualization and remote engineering capabilities;
- Supports OEM based remoted monitoring and maintenance;
- Alarm Shelving Utility (ASU) suppresses less critical alarms and reduces nuisance alarms;

- System Auditor provides support for system configuration, alarm management, operator action analysis and document management;
- Supports tag selection and PLC tag data storing via a Unity Pro PLC configuration interface;
- Foxboro Evo DCS supports virtualization and allows remote engineers (from anywhere in the world) to maintain and troubleshoot the system and perform maintenance. Automatic replication, live migration, load shifting, and centralized management are supported;
- Supports OEM and third-party device vendor Field Device Tool (FDT) and Enhanced Electronic Device Description Language (EDDL) connectivity, allowing vendors to program device configuration and maintenance;
- Capability to failover to a redundant historian server;
- Integration with a broad variety of engineering and productivity tools such as:
    - SimSci Process Automation
    - Avantis enterprise asset performance management
    - Wonderware operations management
    - Wonderware workforce enablement
- Redundant fiber ethernet connections to the plant control network;
- A simulated control processor (SCP), a virtual simulation for Foxboro CP270 and CP280 control processors combined with DYNSIM dynamic modeling capability supporting system design, analysis, troubleshooting and reduces time to commission and startup Foxboro Evo systems. Directly links to other control software including Triconex, Rockwell, Emerson, Siemens, GE and Yokogawa;
- A control network scalable from one to several thousand station connections at data speeds up to 1GBps. Also supports wireless and the ability to integrate nodebus-based systems into Foxboro Evo;
- A Control Network Interface (CNI) which supports interconnection (or segmentation) of multiple Foxboro Evo systems, allowing them to be managed “as one system.” CNI segmentation supports the ability to perform target upgrades and the ability to isolate systems to reduce cyber vulnerability;
- Foxboro Evo DCS supports integration with McAfee ePolicy Orchestrator (ePO), virus scanning, host intrusion detection (HIDS), data loss prevention (DLP), active directory (AD), whitelisting, and a hardened OS;
- Easy integration using FOUNDATION fieldbus, Fieldbus Foundation CIF, HART, PROFIBUS, DeviceNet, Modbus, FoxCom and more. The open field device manager (FDM) with FDT allows Foxboro Evo to connect to any device from any vendor;
- Migration I/O modules reuse existing termination assemblies, cabinets, power supplies, and I/O racks to ease migration to a Foxboro Evo DCS process automation solution.

## 7.2.3 Connects to Remote Systems

### *7.2.3.1 Definition and Rationale*

Systems with the ability to access, control, modify, or manage configuration and/or programming on separate, connected systems fit the **Connects to Remote Systems** characteristic. How these systems authenticate to remote systems is irrelevant; what matters is the connectivity these systems have to remote systems. These systems are extensively used by engineers in the energy sector, and specifically the electric utility market, to manage and monitor OT networks, systems, devices, and sensors. An

example could be a Remote Terminal Unit (RTU), which interfaces objects in the physical world (substation) to a distributed control system (DCS) or SCADA system.[35] Systems with the **Connects to Remote Systems** characteristic can provide a strategic platform for reconnaissance, lateral movement, and advancement of adversary campaign goals and objectives.

#### *7.2.3.2 Evaluation Method*

Indicators of the **Connects to Remote Systems** characteristic would be diagrams indicating network connectivity, instructions for storing remote system configuration or authentication data, automated device discovery, ingest of remote device tags or setpoints, or web server integration. These indicators may be found in product manuals, architectural diagrams, marketing material, and data sheets.

#### *7.2.3.3 Product Example*

**Hitachi ABB RTU560**

**Figure 4: Hitachi RTU560[36]**

The RTU560 connects to a range of Intelligent Electronic Devices (IEDs), parallel Inputs/Outputs (I/Os), and serial connected devices which communicate via IEC 68150. This real-time sensor and machine data can then be transmitted to a central SCADA system and leveraged to manage and protect primary equipment from overloading the grid.[37] The RTU560 supports multigenerational infrastructures, primary substation and transmission substation automation, and transformer automation and control.[38]

### 7.2.4 Has Stored Credentials

#### *7.2.4.1 Definition and Rationale*

Systems which store credentials for authenticated access to OT devices exhibit the **Has Stored Credentials** characteristic. These systems are often leveraged for asset condition monitoring, event response and investigation, asset owner and vendor maintenance, and utilized by engineering staff to access OT networks to perform technical tasks.[39] Systems with stored credentials have gained prevalence in the U.S. energy sector largely due to NERC-CIP regulatory guidance, reflecting security best practices in environments where systems cannot authenticate using user-based authentication services like Lightweight Directory Access Protocol (LDAP) or Active Directory (AD). These systems rarely contain business data.

Systems with the **Has Stored Credentials** characteristic are strategic because they hold credentials which can be used to conduct network and device reconnaissance and laterally move across OT networks.

#### *7.2.4.2 Evaluation Method*

Indicators of systems with the **Has Stored Credentials** characteristic may be:

- Mention of secure password management to remote site locations;
- Mention of a "Secure/d Access or Secure Access Manager" for access to OT networks and devices;
- LDAP, Active Directory, SecurID or other authentication methods for user authentication;
- Stored credential database(s);
- Support for NERC CIP-007 compliance, i.e., having a method(s) to enforce authentication of interactive user access, where technically feasible;[40] and
- Use cases and network architecture drawings indicating how engineering and technical staff can use the product to authenticate (locally or remotely) to obtain access to the OT network and perform technical tasks.

These indicators may be found in marketing material, product manuals, and located on manufacturer websites.

#### *7.2.4.3 Product Example*

**Siemens RUGGEDCOM CROSSBOW**

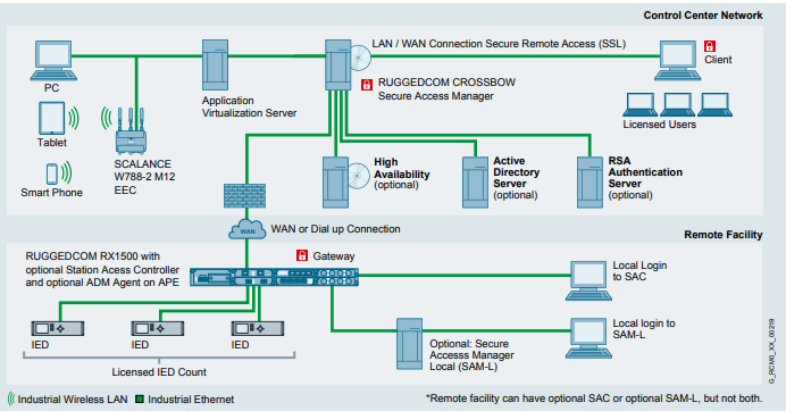


**Figure 5: RUGGEDCOM CROSSBOW system configuration[41]**

Siemens RUGGEDCOM CROSSBOW provides remote users secure Single Sign On (SSO) access to field devices. After logging into the Secure Access Manager (SAM), users are presented with a controlled, role-based view of the OT network directory structure including regions, facility sites, end devices, and applications. Once connected, a user can maintain, configure, and retrieve information from the end device.[42]

# 8. Product Platform & Distribution Characteristics

## 8.1.1 Cloud-Platformed Services

#### *8.1.1.1 Definition and Rationale*

This characteristic identifies systems and services which can be deployed onto a public, private, or hybrid cloud platforms, including "Edge-to-Cloud." **Cloud-Platformed Services** have the potential to provide adversaries a toehold onto a platform with a variety of entry and exit points useful for achieving attack campaign objectives.

Cloud Service Providers (CSPs) widely market public and hybrid cloud-platformed solutions for the OT market. For example, Amazon Web Services (AWS) Power and Utilities promote cloud-based distributed energy resource (DER) tools for the utilities industry.[43] Vendors such as Rockwell Automation, Schneider Electric, ABB, GE, and Emerson have built cloud platforms for aggregating and analyzing operational data. Machine vendors are beginning to offer enhanced support and services which depend on connected equipment, which include predictive maintenance, planned downtime, and data-drive failure analysis.[44] The primary driver for cloud migration appears to be an ability to easily manage data from devices such as smart meters, Internet of Things (IoT) devices, customer home energy systems (smart thermostats, EV chargers, batteries, etc.), and network sensors. Utilities anticipate the systems most likely to be migrated to cloud platforms include meter data management (MDM), advanced metering infrastructure (AMI), distributed energy resource management systems (DERMs), and demand response management systems (DRMS).[45]

#### *8.1.1.2 Evaluation Method*

Systems with the **Cloud-Platformed Services** characteristic are often associated with AWS, GCP, IBM Cloud, Microsoft Azure, or other vendor cloud platforms. Indicators may be found in in vendor news releases, product brochures, product documentation, and manufacturer websites.[46, 47, 48] Mention of vendor-managed services, or solutions installed onto internet accessible vendor servers could indicate presence of the **Cloud-Platformed Services** characteristic and may merit further investigation.

#### *8.1.1.3 Product Example*

**Emerson Plantweb Optics Analytics**


**Figure 6: Emerson Plantweb Optics Analytics[49]**

Emerson Plantweb Optics Analytics provides system owners an Emerson-managed service (servers, software, system security, updates, and IT support) on the Microsoft Azure cloud platform.[50]

### 8.1.2 Market Share

#### *8.1.2.1 Definition and Rationale*

The **Market Share** characteristic measures the percentage of the U.S. Energy Sector market accounted for by a specific OEM or vendor product or service. CyTRICS leverages contracts with multiple market intelligence data providers to obtain data for evaluating this characteristic.

**Market Share** offers an indicator of the extent a potentially vulnerable vendor system could be deployed in U.S. energy infrastructure. It is inexact, as deployed systems may be at many differing version and patch levels, but it does establish an indicator of the prevalence of system deployment. The greater the **Market Share**, the higher the potential a developed attack may be reusable for another entity or system, and thus, the greater potential value it may have for adversary development prioritization. The SolarWinds Orion and Kaseya's VSA supply chain attacks occurring in 2020 and 2021, respectively, illustrate how the **Market Share** characteristic could be used by an adversary when planning an attack campaign. In both campaigns, market share contributed to the volume of systems attackers were able to exploit and leverage as platforms for conducting further attacks. **Market Share** also could be used as an indicator of install-base given unavailability of comprehensive, accurate install-base data. For example, International Data Corporation (IDC) ranked SolarWinds No. 1 in Network Management Software market share for the third year in a row in 2020.[51] This metric indicates probability that SolarWinds has a large install-base as realized in the 2020-2021 attack against SolarWinds Orion.

The **Market Share** characteristic may not reflect market share for systems integrated into other vendor products. The Integrated Product characteristic allows consideration for systems which are sold in a standalone capacity as well as those sold as components integrated into larger products, providing an additional market share consideration.

#### *8.1.2.2 Evaluation Method*

**Market Share** can be evaluated using commercial market data procured from either a specific commercial vendor or a recognized source. For this paper, CyTRICS analysts and SMEs will leverage commercial market data initially procured for the CyTRICS program. This data, produced through CyTRICS contracts with multiple market data providers, provides general market share data by country, market (for this project, the U.S. Energy Sector), vendor, and in some instances, system class and model.

#### *8.1.2.3 Product Example*

**GE Multilin Protective Relays**


**Figure 7: GE Multilin 750/760 Feeder Protection System**[52]

Based on available market research data from Newton Evans, "Overall, the GE share of protective relays in the U.S. is about 15-18% comprised of both its Multilin relays and its MiCOM P40 Agile line. GE maintains a 12-15% share of protective relay sales in each of five international regions. This has held steady for a number of years."[53] SEL products currently hold the largest percentage of protective relay market share in the U.S. with 52% in 2017, followed by GE which is the second most popular at 17%, then ABB with 15%.[54]

## 8.1.3 Integrated Product

### *8.1.3.1 Definition and Rationale*

The **Integrated Product** characteristic allows identification of products which are distributed both in a stand-alone model as an independent product, and as subcomponents within separate products, often manufactured by another vendor and designed and marketed for a wholly different purpose. These integrated products provide well-known industry-accepted sources of functionality within large, complex systems. **Integrated Products** can be invisible to asset owners who may not be aware of third-party product vulnerabilities. Vendors incorporating these integrated products may need to align their system's patch and release cycle with the patch and release cycle for the product integrated within. Figure 8 Standalone vs. Integrated Product shows how a product can be sold and used as both a standalone product and as an **Integrated Product** within a larger OEM product. Integrated products may be especially attractive to an attacker due to the prevalence of their inclusion within a wide range of OEM products.

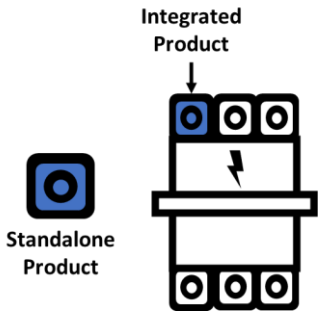


**Figure 8 Standalone vs. Integrated Product[55]**

This characteristic also provides an indicator that market share numbers may not reflect the totality of the product's deployment through integration.

#### *8.1.3.2 Evaluation Method*

Indication of integrated products can be found in vendor websites and marketing materials described as features which add functionality and enable use across a range of deployment options. Third-party **Integrated Product** names are often noted and may refer readers back to product websites and manuals for additional information. Details may become less prevalent in vendor documentation as the time since integration increases, leading to **Integrated Product** "invisibility." Lack of detail may require evaluators to research several generations of product documentation to identify integrated third-party products which have become "invisible" over time. Integrated products may also be identified as "options" or "add-ons" available for installation via software download. For example, Rockwell Automation FactoryTalk Linx Gateway provides a Classic OPC DA[56] and OPC UA[57] server interface to deliver information collected by FactoryTalk Linx from Logix5000 and other Allen-Bradley controllers to external OPC clients, permitting third-party software to coexist with FactoryTalk software.[58] Marketing materials and software bills of materials (SBOMs), where available, also may indicate existence of integrated products.

#### *8.1.3.3 Product Example*

**OSISoft PI**


**Figure 9: OSIsoft PI Reference System Architecture[59]**

OSIsoft OCS allows equipment vendors to embed PI System edge technology in their offerings.[60] OSIsoft Marketplace lists twenty-five solutions powered by the PI System. Some examples of vendors with solutions powered by the PI System are Siemens, Rockwell Automation, and Emerson. Furthermore, OSIsoft lists eighty-six applications for the PI System, such as Smart Building Application, Hospital of the Future App, Data Diodes, Edge Gateways, Intelligent Plant Controllers, and more.[61]

## 8.1.4 Third-Party Connectivity

### *8.1.4.1 Definition and Rationale*

The **Third-Party Connectivity** characteristic addresses systems with enduring connectivity to vendors, OEMs, or business partners. This connectivity is typically associated with system monitoring, data analytics, platform administration, and predictive maintenance conducted by the third party on behalf of the asset owner. Asset owners may purchase and install systems without being aware of the extent or degree of persistent third-party connectivity. For example, several high-profile companies (and customers whose personal data was exposed) were impacted by the Accellion file transfer (FTA) tool breach. Accellion FTA was used by third-party vendors, so the breach not only impacted the services it provided its customers, but also the customers of its customers.[62] Another example is threat monitoring software, often used on IT networks, which might be installed on Engineering Workstations or endpoints running industrial automation suites. This software often reports endpoint data back to the product vendor to facilitate "up-to-the-second" threat protection, as indicated in a recent Trend Micro report on Threats Affecting ICS Endpoints.[63] Products with **Cloud-Platformed Services** characteristics could also require **Third-Party Connectivity** for product maintenance and monitoring purposes.

If compromised, vendor, OEM, or business partner systems can provide attackers strategic, initial access useful for conducting reconnaissance on connected customer systems and networks. Connectivity also provides attackers access to multiple customer endpoints to exploit for further attacks on OT networks and devices. In the SolarWinds Orion attack, after exploiting Orion, adversaries pivoted to Microsoft Office 365 /Azure and collected local instance keys. These keys allowed adversaries to successfully target and penetrate other organizations within the same trusted cloud deployment.[64]

### *8.1.4.2 Evaluation Method*

Product datasheets, vendor manuals, and websites will provide indicators of enduring vendor connectivity. For example, GE Energy's MarkVIe UCSC product data sheet indicates vendor connectivity by stating, "It augments real-time deterministic control with embedded Field Agent technology, delivering near-real-time advice through market analysis, fleet and enterprise data, or asset/process knowledge to optimize the outcomes that today's businesses require." [65] As noted in the definition for this characteristic, Trend Micro indicates vendor connectivity in the Disclosure paragraph of its referenced report stating, "Users can opt out of data collection by disabling the Certified Safe Software Service, Smart Scan, and Behavior Monitoring features from the product administration console. However, this will disable the benefit of having up-to-the-second threat protection afforded by the Smart Protection Network."[66] Indicators of **Third-Party Connectivity** also may be found in system architecture drawings.[69]

### *8.1.4.3 Product Example*

**GE Predix Edge**

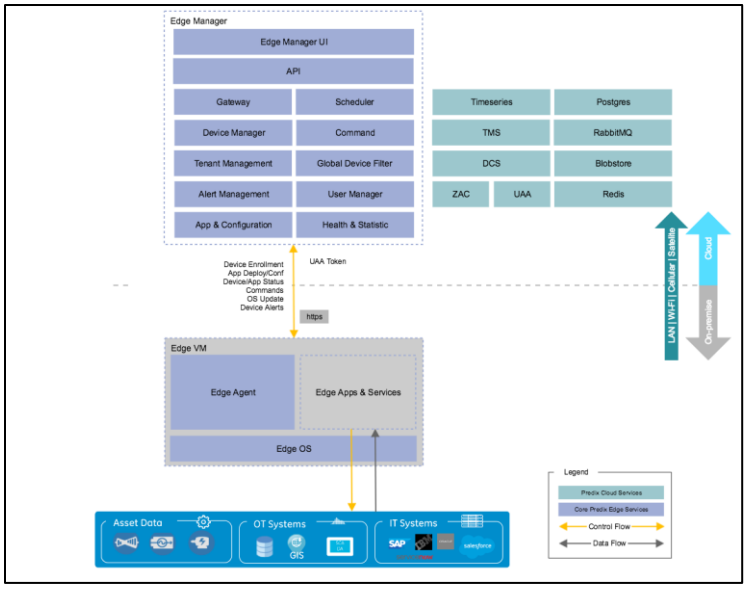


**Figure 10: GE Predix Edge Manager Architecture[67]**

GE's Predix Edge is an Edge-to-Cloud Industrial Internet of Things (IIoT) platform as a service (PaaS) used to collect data from IT/OT assets and sources, apply analytics, leverage container apps, forward data to the Predix Cloud, configure and manage edge devices, and use either integrated software or embedded deployment. Predix Edge Manager is a cloud-based application to help enroll and manage Edge and Edge-connected devices, manage Edge applications and analytics, and control all Edge operations. Leveraging controller APIs, Predix Edge also can issue direct control commands to industrial equipment.[68]

While cloud platforms can be private, public cloud platforms (such as Microsoft Azure used by GE for Predix) are often managed by second or third-parties who maintain enduring connectivity to hardware and containers for platform monitoring and management purposes.

# 9. Sample System Analysis Report

**System Analysis Report**

**OSIsoft PI System (2018 SP3)**

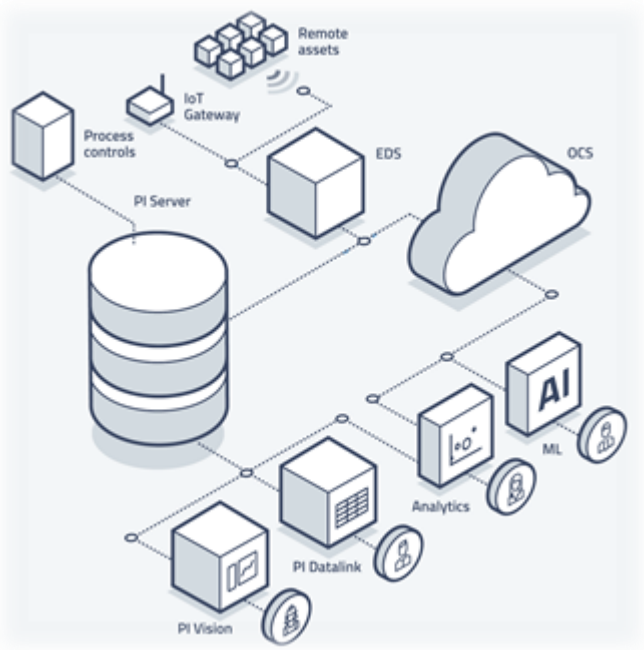


Figure 11: Reference Architecture: How the PI System Works[69]

**Product Overview**

The **OSIsoft PI System** serves the historian market as a data management, analytics, and visualization solution used to gather, store, and contextualize diverse datasets. Contextualized datasets are used by engineers, asset owners, and business partners to monitor asset health and process productivity. Data is also used to conduct analytics used for decision making and perform predictive analytics useful for reducing cost, cultivating quality, improving health & safety, and minimizing system downtime. Furthermore, the OSIsoft PI System is integrated into several OEM platforms and used across the following industries:

- Chemical
- Discrete manufacturing
- Facilities & infrastructure
- Food & beverage
- Forestry
- Mining, metals & materials
- Oil & gas
- Pharmaceutical and life sciences
- Power generation
- Transmission & distribution
- Transportation, and

- Water

**Assessment**

**OSIsoft PI System** meets seven out of eight ICS Beachhead System characteristics. It is designed to obtain data from OT assets located across security zones and, while use of Windows authentication is recommended, stores PI credentials locally using dated encryption. PI is a complex, feature rich system having the ability to interface with hundreds of vendor systems, assets, and sensors. It is very versatile, allowing developers to build interfaces to new devices leveraging OSIsoft Message Format (OMF). The system can be run on local asset owner infrastructure or in the cloud. It can also be virtualized. If the cloud option is used, the vendor offers a "managed service" option, and third-party vendors can leverage cloud access to provide a variety of services.

**OSIsoft PI System** is widely integrated into a number of OEM products, twenty-five listed on OSIsoft's website. Furthermore, the **OSIsoft PI System** currently holds 45-55% of Electric Utility historian market share and 40-55% of Oil/Gas historian market share.

| Characteristic | Assessment |
|---|---|
| **Bridges Segmented Networks** | • OSIsoft PI System uses PI interfaces to connect data sources across the Process Control Network (PCN), firewalls, and Demilitarized Zones (DMZs) where PI System servers are located.[2]<br>• PI Adapters access data on remote assets and secondary networks such as IIoT gateways and sensor enabled equipment and route it through the PCN to edge applications, PI Server, OSIsoft Cloud Services (OCS), or cloud-hosted platform-as-a-service (PaaS) databases.[3] |
| **Feature Rich System** | • OSIsoft PI System provides a variety of features, to include interfaces, connectors, and adapters to hundreds of vendor systems, assets, sensors, IoT devices, legacy systems, and remote assets. It offers multiple system deployment options, such as OSIsoft's cloud-hosted database PaaS.<br>• PI Integrators leverage artificial intelligence and machine learning to analyze, cleanse, and automate transformation of complex datasets with outliers and uneven data points into useful data.[5] Curated data is used to enhance insight and visibility into OSIsoft PI System status and performance. Data analytic features allow customization of expressions based on performance equation syntax, rolling up attributes for aggregation, generation of event frames based on user-defined triggering conditions and statistical quality control (SQC) analysis.[2] |

| | |
|---|---|
| **Connects to Remote Systems** | • Although OSIsoft PI System does connect to remote systems, there are no indicators the system has the ability to control remote systems. |
| **Has Stored Credentials** | • Passwords for remote devices, if required, are used by PI connectors to access data sources. They are stored in data source configuration files located on the connector and PI Data Collection Manager hosts.[9] |
| **Cloud-Platformed Services** | • OSIsoft PI System offers a PI Cloud deployment option, OSIsoft Cloud Services (OCS) built on Microsoft Azure.[4, 6] |
| **Market Share** | • According to INL procured market data, OSIsoft PI System holds 45-55% of Electric Utility historian market share and 40-55% of Oil/Gas historian market share. Major competitors include ABB Enterprise Historian, S-E AVEVA/eDNA, Siemens Simatic Process Historian, GE Proficy Historian, OSII Chronus, AVEVA Historian, ABB Production Data Historian, Emerson Delta V Historian, and Rockwell FactoryTalk.[8] |
| **Integrated Product** | • OSIsoft OCS allows equipment vendors to embed PI System edge technology in their offerings.[6]<br>• OSIsoft Marketplace lists twenty-five solutions powered by the PI System. Some examples of vendors are Siemens, Rockwell Automation, and Emerson. Furthermore, OSIsoft lists eighty-six applications for the PI System such as Smart Building Application, Hospital of the Future App, Data Diodes, Edge Gateways, Intelligent Plant Controllers, and more. [7] |
| **Third-Party Connectivity** | • OSIsoft PI System offers customers a "managed service" option for OCS software maintenance and updates.[4] Users can share operational data with trusted partners or vendors. IT and Business Intelligence (BI) groups can use, and share formatted and contextualized OT data across enterprise applications and cloud providers, such as Microsoft Azure, Amazon Web Services, and Google Cloud Platform.[6] Fifteen Managed Service offerings are listed on the OSIsoft Marketplace.[7] |
| **Analyst Notes:**<br>• OSIsoft PI System is delivered with a myriad of features. While this report highlights a few features around connectivity, interoperability, analytics, and customization, CyTRICS SMEs recommend more definition on what does or does not constitute a feature. CyTRICS anticipates more definition will be obtained with development of a scoring method for the Feature Rich | |

| |
|---|
| System characteristic. |
| **References:**<br>[2] [(U) PDF \| OSIsoft \| PI Server 2018 SP3 User Guide \| https://docs.osisoft.com/bundle/pi-server/page/pi-server.html \| Date of Publication: May 3, 2021 \| Date of Access: August 26, 2021]<br>[3][(U) Website \| OSIsoft \| Pi Core – Collection \| https://www.osisoft.com/pi-system/pi-core/collection \| Date of Access: August 26, 2021]<br>[4][(U) Website \| OSIsoft \| PI Cloud \| https://www.osisoft.com/pi-system/pi-cloud \| Date of Access: September 7, 2021]<br>[5] [(U) Website \| OSIsoft \| PI Core Integration \| https://www.osisoft.com/pi-system/pi-core/integration \| Date of Access: September 7, 2021]<br>[6] [(U) PDF \| OSIsoft \| Product Brief \| https://www.osisoft.com/-/media/Files/OCSusecase_ProductBrief__lt_en.ashx \| Date of Access: September 7, 2021]<br>[7] [(U) Website \| OSIsoft \| Marketplace \| https://resources.osisoft.com/marketplace \| Date of Access: September 7, 2021]<br>[8][(U) PDF \| Newton-Evans \| OSIsoft PI System Profile \| INL Purchased Data \| Date of Access: September 7, 2021]<br>[9] [(U) Website \| OSIsoft \| PI Connector Administration 2.2 \| https://livelibrary.osisoft.com/LiveLibrary/content/en/con-admin-v3/GUID-F7F471A2-C661-4D8B-9BE1-F35012B65B58 \| Date of Access: September 20, 2021] |

# 10. Alternative Characteristics Considered

# 11. Deprecated Characteristics

During research for this project, characteristics were evaluated against an array of criteria to eliminate duplication and ensure accurate assessment by evaluators to provide qualitative results. CyTRICS analysts and researchers collaborated to define each characteristic, note rationale for inclusion, and determine evaluation criteria. Analysts found several proposed characteristics were variations of the same concept. Others could not be defined or evaluated due to the lack of market and vendor data. In each case, the proposed characteristics were deprecated from consideration in this paper. Furthermore, some characteristics were deprecated because they could only be evaluated based on an installed, configured instance of a product and not as part of the overall product capability set. Other characteristics were deprecated after analysis determined adversaries would not consider them useful for a strategic, initial-access attack or strategic access campaign. Additional characteristics may be deprecated as evaluators gain experience using characteristics in this paper to evaluate products. A list of deprecated characteristics is provided below and further detailed in Appendix A.

**Product Functionality**

- Dated Code Base
- High Urgency Updates
- "Hard Coded" Weaknesses, Weak by Default, Default Accounts
- Local Logging, Susceptible to Obfuscation
- Products for Operational Process, Process-centric Products

**Product Platform & Distribution**

- Brand Comfort and Familiarity, Trusted Product
- Significant Reach or Revenue for Entity Size, High Revenue for Entity Size
- Market Ubiquity
- Dominant Tool for Function
- Market Desirability, Best in Class Product

- "Invisible Devices," Install and Forget
- Open Default Configuration
- Indirect Distribution/Support Channels, Sold through Distribution Channels (not OEM)
- Legal, Safety, or Regulatory Requirement
- Vendor on Premise
- Virtualization

# 12. Potential Future Strategic Research Areas

As CyTRICS analysts and researchers considered characteristics for inclusion in this paper, several characteristics and systems of interest were identified as prevalent in IT and repurposed for use in ICS environments. Others were associated with emerging technologies and methodologies expected to gain adoption by asset owners with the promise of providing enhanced data analytics, predictive maintenance, and increased security. While these characteristics and systems are gaining a foothold in the OT market, insufficient data exists to support effective evaluation and, in some instances, overcome regulatory hurdles prior to widespread adoption within the OT market. Though these potential characteristics were not considered for this paper, they are being documented for future research due to CyTRICS program expectations they will gain adoption in OT and adversaries may begin to find them useful for conducting strategic, initial-access attacks or attack campaigns. A list of potential future, strategic research areas is detailed in Appendix B.

**Potential Future Characteristics**

- Anything-as-a-Service (XaaS).

**Potential Future Systems of Interest**

- Predictive Maintenance (PdM);
- Digital Twin Technology;
- Peripheral (VR) Enabled, Augmented Reality (AR) Enabled Maintenance;
- Industrial Internet of Things (IIoT) Middleware and Interoperability Platforms.

# 13. Next Steps

# 14. Characteristic Evaluation

Concepts and methodology in this paper will be evaluated and validated on systems identified by the CyTRICS program, providing a sampling of a variety of systems used in the U.S. ESIB to allow for the validation of the identified characteristics. Each system will be evaluated against the full set of characteristics with findings documented in a System Analysis Report. CyTRICS analysts and researchers will revise Beachhead System characteristics based on findings from the validation effort.

# 15. Scoring Methodology

Once Beachhead System characteristics are validated and updated, the CyTRICS program will develop a formal scoring methodology which is both defensible and useful for the CyTRICS Prioritization Process. The findings and an updated scoring methodology will be documented in updates to this paper.

# 16. Appendix A – Deprecated Characteristics

**Deprecated Characteristics Within Product Functionality**

**Dated Code Base –** this characteristic was initially considered for systems designed using insecure or outdated coding practices. It was assumed software with dated code base might also be unsupported, contain known vulnerabilities, and asset owners would most likely not be aware of systems containing a dated code base. This characteristic was deprecated during validation because CyTRICS found it difficult to locate information on dated code base (software packages, libraries, etc.) found within evaluated systems.

**High Urgency Updates -** CyTRICS determined products with this characteristic would be attractive to adversaries because asset owners would install, patch, and update these systems with limited testing. Products fitting this characteristic might be considered a single point of failure or non-redundant component, leading to a sense of urgency when patching. This characteristic was associated with the SolarWinds Orion attack as customers who trusted the SolarWinds Orion product were informed of available updates and updated their systems without testing or questioning software update integrity. This characteristic was initially identified as Trusted Updates. CyTRICS concluded this characteristic is more likely found in IT rather than OT environments and ICS asset owners are more likely to push back against high urgency system updates due to safety considerations and regulatory testing requirements.

**"Hard Coded" Weaknesses, Weak by Default, Default Accounts -** these characteristics are associated with products considered insecure by design and valuable to adversaries for strategic, initial-access attacks. CyTRICS assumed some products are sold with weak or predictable encryption algorithms, default accounts, open configurations, and enabled services with vendors expecting asset owners will harden products prior to their being placed into operations. It was determined legacy OT products hold default weaknesses, but also are considered to be immature adversary targets which offer little strategic value to an attacker. These characteristics were deprecated because they are often found at lower levels of the Purdue model[c] with limited connectivity, offering minimal value to adversaries interested in obtaining initial access.

**Local Logging, Susceptible to Obfuscation -** these characteristics were considered for legacy OT devices which support limited local logging and may lack the ability to send logs to external servers or services, such as Splunk. Logs on these devices are often overwritten on a scheduled basis or when log size meets maximum thresholds. CyTRICS assumed adversaries with access to a legacy device might obfuscate logs to hide malicious activity. CyTRICS research efforts resulted in the conclusion adversaries with access to devices often located further down the ICS Kill Chain would be less interested in log obfuscation and more interested in modifying or impacting processes the device controls or using the device to pivot to other devices in the OT network. It was determined these devices would be rarely targeted for strategic, initial access.

[c] The Purdue model, or Purdue Reference Model was developed as a reference model useful for defining how facilities, people, control, and information systems interact. Legacy OT products, such as PLCs or HMIs, are often found on Local Supervisory level (Level 2) or Local Controllers (Level 1).

**Products for Operational Process, Process-centric Products -** CyTRICS considered Products for Operational Process, or Process-centric Products as characteristics based on the assumption systems close to operational processes might be considered an attractive target to attackers. CyTRICS found these systems are often IT systems repurposed for managing OT network access. When used on OT networks, they also may be installed, configured, and managed by OT engineering staff less familiar with the system and its use compared to IT staff responsible for network security. These characteristics were deprecated because CyTRICS determined they were implementation dependent and difficult to evaluate.

**"Invisible" Devices, Install and Forget** - CyTRICS identified "Invisible" Devices, or Install and Forget as characteristics for evaluation because systems fitting these characteristics are often single purpose, require little to no configuration, and are frequently installed or replaced with little thought or consideration to monitoring or security hardening. These systems require minimal interaction and are often considered in the same category as network cabling, peripherals, and Line Replaceable Units (LRUs). Examples include media converters, multiplexers (such as GE JungleMUX), and data diodes. CyTRICS concluded an adversary might attack these systems because they are often located on an OT network, yet rarely monitored or considered when preparing for or responding to an attack. These characteristics were deprecated because researchers found products fitting the characteristic difficult to define, requiring further research.

**Open Default Configuration -** CyTRICS identified this characteristic because it was assumed some systems are sold with default configurations, accounts, and enabled services which are recorded in vendor documentation and available to the public. These systems are often sold with an open configuration to ease installation and deployment with the expectation asset owners will security harden the systems prior to live operation. It was determined an adversary with knowledge of default device accounts, configuration, and services might exploit a lack of security hardening to establish a foothold on systems. However, this characteristic was deprecated when CyTRICS determined adversaries rarely consider default configuration for initial access when selecting an attack target.

**Deprecated Characteristics Within Product Platform and Distribution**

**Brand Comfort and Familiarity; Trusted Product -** CyTRICS hypothesized system patches and updates from trusted vendors were more likely to be installed by asset owners without testing for any security issues. This characteristic was considered to have led to the success of the SolarWinds Orion attack. It was concluded the more trusted a system is, the more likely it is to be targeted by an adversary. CyTRICS found these characteristics opinion driven and difficult to measure given a lack of pertinent, available data, leading to their deprecation.

**Significant Reach or Revenue for Entity Size; High Revenue for Entity Size -** both Significant Reach or Revenue for Entity Size and High Revenue for Entity Size were initially considered as characteristics because industry data indicated companies with a small staff and large revenue stream might have limited staff resources for system security monitoring and incident response. CyTRICS research found applicable vendor, system, and market share data difficult to locate and often skewed by industry merger and acquisition (M&A) activity. It was also determined

company revenue data often reflects revenue from a wide range of products and support contracts instead of specific products. For these reasons, CyTRICS opted to deprecate these characteristics in favor of Market Share and future research.

**Market Ubiquity –** this characteristic was considered by CyTRICS because it was assumed a sole product on the market for any given function would make it an attractive target to adversaries. CyTRICS determined evaluation data for "sole products for a given function" was difficult to locate, any evaluation was subjective, and therefore, difficult to defend. In cases where a system was determined to hold the market ubiquity characteristic, CyTRICS determined it would also be captured in Market Share.

**Dominant Tool for Function –** this characteristic reflects a software or hardware product which might be considered a key, or dominant tool of choice to perform a function within a particular market sector; subverting such a tool could provide an adversary with a wide range of targets across many asset owner organizations. SolarWinds Orion could be considered such a product. CyTRICS found this characteristic difficult to assess because a particular product might be considered a key or dominant tool for a particular submarket, but not for another. Although data was available for evaluating this characteristic, submarket data indicating "product dominance" was difficult to locate and lacked detail when found.

**Market Desirability, Best-in-Class Product -** CyTRICS determined the rationale and evaluation method for these characteristics, particularly Best-in-Class, to be subjective. They were considered duplicative and deprecated due to similarities with other factors such as Trusted Product, Dominant Tool for Function, and Market Share.

**Indirect Distribution/ Support Channel, Sold Through Distribution Channels (Not OEM) -** these characteristics were considered because some products are developed, sold, and maintained by third parties, such as an integrator, instead of the OEM. Delayed product security patching or updates could result in vulnerabilities an adversary might exploit. It was determined security responsibilities, such as vulnerability reporting and remediation may be split between third parties and the OEM, driving the potential for inefficiency and delay in the detection and remediation of security events. CyTRICS found these characteristics difficult to evaluate given the lack of data and deprecated them in favor of other characteristics.

**Legal, Safety or Regulatory Requirement -** CyTRICS identified this characteristic to address system updates which may be "directed" or "strongly recommended" based on external legal, safety or regulatory requirements. It was concluded requirements vary widely based on environment (*e.g.*, nuclear vs. hydro), which may conflict with each other. This characteristic was deprecated because it was determined to be based on environment as opposed to how a product is designed.

**Vendor on Premise -** this characteristic was identified because some asset owners allow onsite vendors and integrators for system maintenance and support. Researchers considered onsite vendors may not be held to the same rigor as asset owner staff, resulting in increased insider threat risk. CyTRICS determined this characteristic to be environmentally driven rather than based on how a product is designed, leading to this characteristic being deprecated.

**Virtualization –** virtualization was identified as a characteristic because vulnerabilities in hypervisors and virtual machines could be exploited to provide adversaries a platform from which to conduct attack campaigns. During CyTRICS discussion, it was determined the attributes of virtualization were already being captured by Bridges Segmented Networks, Has Stored Credentials and Third-Party Connectivity characteristics.

# 17. Appendix B – Potential Future Strategic Research Areas

## Potential Future Characteristics

**Anything-as-a-Service (XaaS) -** XaaS is a new concept gaining ground in IT—and increasingly, OT—due to the growing IIoT market. It encompasses Platform as a Service (PaaS), Software as a Service (SaaS), Infrastructure as a Service (IaaS), Desktop as a Service (DaaS), and Disaster Recovery as a Service (DRaaS). These services are being tailored for OT environments and vendors are building systems which leverage XaaS—Energy Management as a Service (EMaaS) in the electric utility sector, for instance. Technology which could eventually leverage XaaS include smart meters, Advanced Metering Infrastructure (AMI), Micro Grids, Distributed Generation, Load Aggregation, Demand Response, Electric Vehicles (EVs) and their smart chargers, and Battery Energy Storage Systems (BESS). Some generation asset owners/operators (typically wind) and Municipality/Load Serving Entities (LSE) are already using XaaS solutions instead of traditional computing assets and control rooms.[70]

While CyTRICS didn't include XaaS in this paper, XaaS warrants further research and may be included in future papers.

## Potential Future Systems of Interest

**Predictive Maintenance (PdM) -** PdM leverages operational data obtained from devices located throughout an OT network (down to the sensor level) to perform real-time data analytics and predict issues with equipment maintenance, failures, and process deviations. It also promises to reduce unplanned downtime, resulting in significant cost savings and increase industrial process efficiency. Furthermore, PdM solutions provide asset owners a real-time monitoring capability and detailed insight into their industrial assets. PdM is already gaining adoption within some industrial markets, such as the Packaging and Processing industry whereas of February 2021, it has been implemented by 23%, piloted by 22%, and is currently being evaluated by 29% of surveyed organizations.[71]

So, how does PdM technology work? OT systems, some leveraging smart (wireless enabled) sensors provide operational data to artificial intelligence (AI) based analytical engines. GE Predix, also known as Predix Edge, is an example of a cloud platform-based solution.[72] Other manufacturers building PdM solutions include Siemens, ABB, Schneider Electric, and Rockwell Automation.[73, 74, 75, 76] PdM solutions leverage machine learning to perform the following tasks:

- Establish asset baseline patterns;
- Compare real-time behavior to baselines;
- Alerts users of abnormal behavior, and
- Take remedial action based on recommendations.[77]

CyTRICS determined more research relating to PdM is required to gather a complete understanding of how it might be exploited by an adversary to conduct a strategic, initial-access attack.

**Digital Twin Technology -** Use of digital twins in inspection, operations, and maintenance was highlighted as a topic of interest in a recent poll of Energy sector professionals conducted by Energy Central in June 2021.[78] Digital twins, digital mockups of asset owner systems, are built using data

obtained by **PdM** platforms, such as GE Predix.[79] They are used by **PdM** solutions to establish a known good asset baseline for reflecting past conditions, current conditions, and to predict future conditions. **Digital Twin Technology** also can be used for safe testing of updates, system changes, and maintenance procedures. While this characteristic was considered for this paper, the decision was made to conduct further research and potentially include it a future paper.

**Peripheral Virtual Reality (VR) Enabled, Augmented Reality (AR) Enabled Maintenance -** VR and AR enabled maintenance provides the capability to obtain remote troubleshooting and virtual support on mobile devices and VR headsets, reducing maintenance callouts and system downtime. GE, Schneider Electric, ABB, and Rockwell Automation are vendors currently researching or selling VR and AR enabled maintenance solutions.[80, 81, 82, 83]

**Industrial Internet of Things (IIoT) Middleware and Interoperability Platforms -** Industrial system interoperability is becoming increasingly complex with the advent of new platforms, solutions, technologies, and protocols. Solutions which simplify interoperability are crucial for ensuring real-time system operations and management. Examples such as OPC Foundation's OPC Unified Architecture (UA), or RTI's Data Distribution Service are designed to move data between devices and hardware in the case of UA or across multi-node applications within a software data flow (RTI). Such systems could provide a rich attack surface of connected systems or data streams for an adversary.

Claroty released a report in February 2021 titled "Exploring the OPC Attack Surface" where it provided an overview of platform vulnerabilities.[84]

# 18. References

[1] [(U) News Release | SolarWinds OrangeMatter | An Investigative Update of the Cyberattack | https://orangematter.solarwinds.com/2021/05/07/an-investigative-update-of-the-cyberattack/ | Date of Publication: May 7, 2021 | Date of Access: August 19, 2021]
[2] [(U) Blog | Scyth.io | Beachhead Access in Industrial Control Systems | https://www.scythe.io/library/beachhead-access-in-industrial-control-systems | Date of Publication: July 19, 2021 | Date of Access: October 20, 2021]
[3] [(U) Executive Order | United States, Executive Office of the President | Executive Order 14028: Improving the Nation's Cybersecurity | Date of Publication: May 12, 2021 | Date of Access: July 21, 2021]
[4] [(U) Press Release | The White House |FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government | https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/ | Date of Publication: April 15, 2021]
[5] [(U) Website | MITRE | APT29 | https://attack.mitre.org/groups/G0016/ | Date of Access: July 12, 2021
[6] [(U) PDF | CISA | Fact Sheet: Russian SVR Activities Related to SolarWinds Compromise | https://us-cert.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Russian_SVR_Activities_Related_to_SolarWinds_Compromise_508C.pdf | Date of Publication: May 7, 2021 | Date of Access: July 14, 2021]
[7] [(U) News Article | WSJ | Suspected Russian Hack Extends Far Beyond SolarWinds Software, Investigators Say | https://www.wsj.com/articles/suspected-russian-hack-extends-far-beyond-solarwinds-software-investigators-say-11611921601?mod=djemalertNEWS | Date of Publication: January 29, 2021 | Date of Access: July 14, 2021]
[8] [(U) Blog | CYBERARK | Golden SAML Revisited: The Solarigate Connection | https://www.cyberark.com/resources/threat-research-blog/golden-saml-revisited-the-solorigate-connection | Date of Publication: December 29, 2020 | Date of Access: Date of Access: June 2, 2021]
[9] [(U) Website | Crowdstrike | https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/ | SUNSPOT: An Implant in the Build Process | Date of Publication: January 11, 2021 | Date of Access: June 2, 2021]
[10] [(U) Website | SolarWinds | https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/ | New Findings From Our Investigation of SUNBURST | Date of Publication: January 11, 2021 | Date of Access: June 2, 2021]
[11] [(U) Website | ZDNet | Third malware strain discovered in SolarWinds supply chain attack | https://www.zdnet.com/article/third-malware-strain-discovered-in-solarwinds-supply-chain-attack/ | Date of Publication: January 12, 2021 | Date of Access: June 2, 2021]
[12] [(U) Website | ZDNet | Fourth malware strain discovered in SolarWinds incident | https://www.zdnet.com/article/fourth-malware-strain-discovered-in-solarwinds-incident/ | Date of Publication: January 19, 2021 Date of Access: June 2, 2021]
[13] [(U) Website | CISA | Malware Analysis Report (AR21-039B) MAR-10320115-1.v1 – TEARDROP | https://us-cert.cisa.gov/ncas/analysis-reports/ar21-039b | Date of Publication: February 8, 2021 | Date of Access: June 2, 2021]
[14] [(U) Website | Symantec | Raindrop: New Malware Discovered in SolarWinds Investigation | Date of Publication: January 18, 2021 | https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-raindrop-malware | Date of Access: June 2, 2021]
[15] [(U) Website | FireEye | Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor | https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html | Date of Publication: December 13, 2020 | Date of Access: June 2, 2021]
[16] [(U) | Website | FireEye | New SUNSHUTTLE Second-Stage Backdoor Uncovered Targeting U.S.-Based Entity; Possible Connection to UNC2452 | https://www.fireeye.com/blog/threat-research/2021/03/sunshuttle-second-stage-backdoor-targeting-us-based-entity.html | Date of Publication: March 4, 2021 | Date of Access: June 2, 2021]

[17] [(U) Website | Security Affairs | Sunshuttle, the fourth malware allegedly linked to SolarWinds hack | Date of Publication: March 4, 2021 | https://securityaffairs.co/wordpress/115291/malware/sunshuttle-backdoor-solarwinds-hack.html | Date of Access: June 2, 2021]
[18] [(U) Website | Microsoft | GoldMax, GoldFinder, and Sibot: Analyzing NOBELIUM's layered persistence | Date of Publication: March 4, 2021 | https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/ | Date of Access: June 2, 2021]
[19] [(U) Blog | Microsoft | New Nobelium activity | https://msrc-blog.microsoft.com/2021/06/25/new-nobelium-activity/ | Date of Publication: June 25, 2021 | Date of Access: July 13, 2021]
[20] [(U) Advisory | Kaseya | Kaseya Important Notices | https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689 | Date of Publication: July 12, 2021 | Date of Access: July 13, 2021]
[21] [(U) White paper | Michael Assante and Robert M. Lee | SANS | The Industrial Control System Cyber Kill Chain | https://sansorg.egnyte.com/dl/HHa9fCekmc/? | Date of Publication: October 2015 | Date of Access: July 26, 2021]
[22] [(U) Article | SolarWinds IT Operations Management Market Share Leadership Recognized by Top Industry Research | https://www.businesswire.com/news/home/20211208005064/en/SolarWinds-IT-Operations-Management-Market-Share-Leadership-Recognized-by-Top-Industry-Research | Date of Publication: December 8, 2021]
[23] [(U) Opinion Article | Scythe | Beachhead Access in Industrial Control Systems | https://www.scythe.io/library/beachhead-access-in-industrial-control-systems | Date of Publication: July 19, 2021 | Date of Access: July 20, 2021]
[24] [(U) Website | Corporate Finance Group | Beachhead Strategy | https://corporatefinanceinstitute.com/resources/knowledge/strategy/beachhead-strategy/ | Date of Access: July 26,2021]
[25] [(U) Research | Mandiant | The FireEye Approach to Operational Technology Security | https://www.mandiant.com/resources/fireeye-approach-to-operational-technology-security | Date of Publication: December 11, 2019 | Date of Access: October 20, 2021]
[26] [(U) Website | FireEye | | Check Your Pulse: Suspected APT Actors Leverage Authentication Bypass Techniques and Pulse Secure Zero-Day | https://www.fireeye.com/blog/threat-research/2021/04/suspected-apt-actors-leverage-bypass-techniques-pulse-secure-zero-day.html | Date of Publication: April 20, 2021 | Date of Access: May 19, 2021]
[27] [(U) Website | FireEye | Re-Checking Your Pulse: Updates on Chinese APT Actors Compromising Pulse Secure VPN Devices | https://www.fireeye.com/blog/threat-research/2021/05/updates-on-chinese-apt-compromising-pulse-secure-vpn-devices.html | Date of Publication: May 27, 2021 | Date of Access: June 21, 2021]
[28] [(U) Image from Brochure | Waterfall Security | Unidirectional Security Gateway WF-500 Product Brochure | https://waterfall-security.com/wp-content/uploads/Unidirectional_Security_Gateway_WF500_Brochure.pdf | Date of Access: Mar 7, 2022]
[29] [(U) Website | Waterfall Security | Unidirectional Security Gateways | https://waterfall-security.com/unidirectional-security-gateways/ | Date of Access: Mar 5, 2021]
[30] [(U) Marketing Brochure | Waterfall Security | WF-500 Hardware Data Sheet | https://waterfall-security.com/wp-content/uploads/WF-500-Data-Sheet.pdf | Last Modified: April 15, 2021 | Date of Access: May 20, 2021]
[31] [(U) Marketing Brochure | Waterfall Security | Waterfall's WF-500 Modular Architecture | https://www.waterfall-security.com/wp-content/uploads/2014/09/Waterfalls-WF-500-Modular-Architecture_914.pdf | Last Modified: April 15, 2021 | Date of Access: May 20, 2021]
[32] [(U) Article | T&D World | Grid Innovations - IT/OT convergence | https://www.tdworld.com/grid-innovations/article/20963808/itot-convergence | Date of Publication: Jan 1, 2014 | Date of Access: June 28, 2021]
[33] [(U) Image | Schneider Electric | Foxboro Evo process automation system | https://www.se.com/ca/en/assets/v2/680/media/70852/900/fcp280-IC-490x280.jpg | Date of Access: March 14, 2022]
[34] [(U) PDF | Schneider Electric | Next-Generation EcoStruxure Foxboro Control Software Future-Proofs Industrial Operations | https://download.schneider-electric.com/files?p_enDocType=Software+-

+Release+Notes&p_File_Name=Press+Release_EcoStruxure+Foxboro+DCS+Control+Software+7.1_8.7.18.pdf&p_Doc_Ref=FoxboroDCS_press070818 | Date of Access: June 14, 2021]

[35] [(U) Website | Techopedia | Remote Terminal Unit (RTU) | https://www.techopedia.com/definition/1033/remote-terminal-unit-rtu | Date of Access: July 21, 2021]

[36] [(U) Image | Hitachi Energy | RTU560 product line | https://dynamic-assets.hitachienergy.com/is/image/hitachiabbpowergrids/rtu560_filled_with_560cmr02-w400-1?wid=400&hei=239&fmt=webp-alpha&fit=crop%2C1 | Date of Access: July 21, 2021]

[37] [(U) Website | Hitachi Energy | RTU560 product line | https://www.hitachienergy.com/offering/product-and-system/substation-automation-protection-and-control/products/remote-terminal-units/rtu560-product-line | Date of Access: July 21, 2021]

[38] [(U) Marketing | Hitachi ABB | RTU560 product line flyer | Date of Access: Jun 14, 2021]

[39] [(U) Brochure | Siemens | RuggedCom Crossbow Secure Access Management Solution | https://cache.industry.siemens.com/dl/files/380/109766380/att_981040/v1/sie_crossbow_en.pdf | Date of Publication: | Date of Access: July 6, 2021]

[40] [(U) Standard | NERC | NERC CIP-007-06 Part 5.1 | https://www.nerc.com | Date of Publication: July 1, 2016 | Date of Access: July 6, 2021}

[41] [(U) Image | Siemens | RUGGEDCOM CROSSBOW | https://assets.new.siemens.com/siemens/assets/api/uuid:bb4f8814-d4d0-492b-ad9f-0baa55c95d1f/width:750/quality:high/ruggedcom-crossbow-system-configuration.png | Date of Access: April 7, 2021]

[42] [(U) Brochure | Siemens | Siemens RUGGEDCOM CROSSBOW Starter Edition | https://support.industry.siemens.com/cs/attachments/109766264/crossbow_starter_edition_en.pdf | Date of Access: Apr. 7, 2021]

[43] [(U) Website | Amazon Web Services | Operational Technology (OT) Transformation in Power & Utilities | https://aws.amazon.com/power-and-utilities/ot-transformation/ | Date of Access: July 7, 2021]

[44] [(U) White Paper | OWL Cyber Defense | A New Paradigm: OT Security and Data in the Cloud | https://go.owlcyberdefense.com/a-new-paradigm-OT-security-data-cloud | Date of Access: July 7, 2021]

[45] [(U) Article | Smart Energy | Cloudy skies ahead for utilities | https://www.smart-energy.com/industry-sectors/data_analytics/cloudy-skies-ahead-for-utilities-cloud-technologies/ | Date of Publication: April 3, 2020 | Date of Access: July 8, 2021

[46] [(U) News Release | Rockwell Automation | Softing tManager | https://www.rockwellautomation.com/en-us/company/events/in-person-events/automation-fair/new-products-and-solutions-showcase-at-automation-fair-at-home/softing-new-product-and-solution-at-automation-fair-at-home.html | Date of Access: July 8, 2021]

[47] [(U) Product Brochure | GE Grid Solutions | Advanced Automation Applications | https://www.gegridsolutions.com/products/brochures/advanced-automation-applications-en-202001-33142.pdf | Date of Publication: 2020 | Date of Access: July 8, 2021]

[48] [(U) Website | Hitachi ABB | Cloud Services | https://www.hitachiabb-powergrids.com/us/en/offering/solutions/asset-and-work-management/services/cloud-services | Date of Access: July 8, 2021]

[49] [(U) Image | Emerson | Plantweb Optics Analytics | https://www.emerson.com/resource/image/5991302/landscape_ratio2x1/1180/590/5d1baf6aff1a48d25d9018bd0ca598e8/Jf/c067.jpg | Date of Access: April 7, 2021

[50] [(U) Website | Emerson | Plantweb Optics Analytics Cloud Hosted Solution | https://www.emerson.com/en-us/automation/asset-management/asset-monitoring/health-monitoring/plantweboptics/plantweb-optics-analytics | Date of Access: Apr 7, 2021]

[51] [(U) News Release | SolarWinds | SolarWinds Recognized by Industry Analysts for IT Operations Management Market Share Leadership | https://investors.solarwinds.com/news/news-details/2020/SolarWinds-Recognized-by-Industry-Analysts-for-IT-Operations-Management-Market-Share-Leadership/default.aspx | Date of Publication: October 20, 2020 | Date of Access: July 8, 2020]

[52] [(U) Image from Brochure | GE Grid Solutions | Multilin 750/760 | https://www.gegridsolutions.com/products/brochures/750760_gea31955.pdf | Date of Publication: Mar 30, 2016 | Date of Access: Mar 7, 2022]
[53] [(U) Report | Newton Evans | Excerpts from The World Market Study of Protective Relays in Electric Utilities: 2019-2022 | January 2021]
[54] [(U) Report | Newton Evans | Excerpt from MiCOM Relays - U.S. Market Share Assessment2017 Data –Feeder Protection Relays | January 2021]
[55] [(U) Diagram | Sara Freeman, Idaho National Laboratory | Standalone vs. Integrated Product]
[56] [(U) Website | OPC Foundation | Classic Data Access (DA) Specifications | https://opcfoundation.org/developer-tools/specifications-classic/data-access/ | Date of Access: July 27, 2021]
[57] [(U) Website | OPC Foundation | Unified Architecture | https://opcfoundation.org/about/opc-technologies/opc-ua/ | Date of Access: July 27, 2021]
[58] [(U) Website | Rockwell Automation | FactoryTalk Linx Gateway Product Description | https://commerce.rockwellautomation.com/rockwell/en/EUR/p/9355C-FTLNXGW/bundleBrand#productDescription | Date of Access: July 27, 2021]
[59] [(U) Image | OSIsoft | Pi System | https://www.osisoft.com/-/jssmedia/osisoft-sitecore/data/media/img/data_anim_3-md.ashx?h=1200&iar=0&w=1200&hash=3A8D6ED65F0AFCD4890B49EC9E737EA6 | Date of Access: March 14, 2022]
[60] [(U) PDF | OSIsoft | Product Brief | https://www.osisoft.com/-/media/Files/OCSusecase_ProductBrief__lt_en.ashx | Date of Access: September 7, 2021]
[61] [(U) Website | OSIsoft | Marketplace | https://resources.osisoft.com/marketplace | Date of Access: September 7, 2021]
[62] [(U) News Article | Security Affairs | Morgan Stanley discloses data breach after the hack of a third-party vendor | https://securityaffairs.co/wordpress/119865/data-breach/morgan-stanley-data-breach.html | Date of Publication: July 8, 2021 | Date of Access: August 3, 2021]
[63] [(U) Report | Trend Micro | 2020 Report on Threats Affecting ICS Endpoints | https://documents.trendmicro.com/assets/white_papers/wp-2020-report-on-threats-affecting-critical-industrial-endpoints.pdf | Date of Access: July 9, 2021]
[64] [(U) Blog | Malwarebytes Labs | Malwarebytes targeted by Nation State Actor implicated in SolarWinds breach. Evidence suggests abuse of privileged access to Microsoft Office 365 and Azure environments | https://blog.malwarebytes.com/malwarebytes-news/2021/01/malwarebytes-targeted-by-nation-state-actor-implicated-in-solarwinds-breach-evidence-suggests-abuse-of-privileged-access-to-microsoft-office-365-and-azure-environments/ | Date of Access: Mar 5, 2021]
[65] [(U) PDF | GE Digital | MarkVIe UCSC product data sheet | https://www.ge.com/content/dam/gepower-pgdp/global/en_US/documents/automation/gfa-2120b_mark-vie-ucsc-ds.pdf
[66] [(U) Report | Trend Micro | 2020 Report on Threats Affecting ICS Endpoints | https://documents.trendmicro.com/assets/white_papers/wp-2020-report-on-threats-affecting-critical-industrial-endpoints.pdf | Date of Access: July 9, 2021]
[67] [(U) Image | GE Digital | Predix Edge Manager Architecture | https://www.ge.com/digital/documentation/edge-software/Edge%20Manager.png | Date of Access: March 14, 2022]
[68] [(U) Data Sheet | GE Digital | Predix Edge from GE Digital | https://www.ge.com/digital/sites/default/files/download_assets/predix-edge-from-ge-digital-datasheet.pdf | Date of Access: June 14, 2021]
[69] [(U) Image | OSIsoft | Pi System | https://www.osisoft.com/-/jssmedia/osisoft-sitecore/data/media/img/data_anim_3-md.ashx?h=1200&iar=0&w=1200&hash=3A8D6ED65F0AFCD4890B49EC9E737EA6 | Date of Access: March 14, 2022]

[70] [(U) Website | CIO Review | EMaaS – The Convergence of Cloud and Critical Infrastructure | https://www.cioreview.com/cioviewpoint/emaas-the-convergence-of-the-cloud-and-critical-infrastructure-nid-15424-cid-89.html | Date of Access: July 20, 2021]
[71] [(U) Article | Automation World | Predictive Maintenance 1010 | https://www.automationworld.com/home/article/21295786/predictive-maintenance-101 | Date of Publication: February 25, 2021 | Date of Access: July 22, 2021]
[72] [(U) Website | GE | GE Predix | https://www.ge.com/digital/iiot-platform | Date of Access: July 22, 2021]
[73] [(U) Website | Siemens | Predictive maintenance – thanks to artificial intelligence | https://new.siemens.com/global/en/products/services/digital-enterprise-services/analytics-artificial-intelligence-services/predictive-services.html | Date of Access: July 22, 2021]
[74] [(U) News Release | ABB | ABB to launch predictive maintenance solution that helps customers minimize environmental impact and increase safety | https://new.abb.com/news/detail/57517/abb-to-launch-predictive-maintenance-solution-that-helps-customers-minimize-environmental-impact-and-increase-safety | Date of Access: July 22, 2021]
[75] [(U) Website | Schneider Electric | Predictive Maintenance Solutions | https://www.se.com/us/en/product-range/64263-predictive-maintenance-solutions/#overview | Date of Access: July 22, 2021]
[76] [(U) Website | Rockwell Automation | FactoryTalk Analytics | https://www.rockwellautomation.com/en-us/products/software/factorytalk/innovationsuite/analytics.html | Date of Access: July 22, 2021]
[77] [(U) Website | IIoT-World | How to Minimize Asset Failure with Predictive Maintenance | https://www.iiot-world.com/industrial-iot/connected-industry/how-to-minimize-asset-failure-with-predictive-maintenance/ | Date of Publication: July 24, 2020 | Date of Access: July 22, 2021]
[78] [(U) News Article | Energy Central | Topics YOU Want Energy Central to Focus On: Poll Results | https://energycentral.com/o/energy-central/topics-you-want-energy-central-focus-poll-results | Date of Publication: June 22, 2021 | Date of Access: July 22, 2021]
[79] [(U) Website | GE | Digital Twin | https://www.ge.com/digital/applications/digital-twin | Date of Access: July 22, 2021]
[80] [(U) Website | GE | Project Augmented Reality | https://www.ge.com/research/project/augmented-reality | Date of Access: July 22, 2021]
[81] [(U) Website | Schneider Electric | EcoStruxure Augmented Operator Advisor | https://www.se.com/us/en/work/services/field-services/industrial-automation/performance-optimization-services/ecostruxure-augmented-operator-advisor.jsp | Date of Access: July 22,2021]
[82] [(U) Website | ABB | ABB Ability Augmented Field Procedures | https://new.abb.com/cpm/industry-software/collaborative-operations/abb-ability-augmented-field-procedures | Date of Access: July 22, 2021]
[83] [(U) Website | Rockwell Automation | Augmented Reality | https://www.rockwellautomation.com/en-us/products/software/factorytalk/innovationsuite/augmented-reality.html | Date of Access: July 22, 2021]
[84] [(U) PDF | Claroty | Exploring the OPC Attack Surface | https://www.claroty.com/wp-content/uploads/2021/02/FINAL_Claroty_OPC_Research_Paper.pdf | Date of Access: July 22, 2021]