FORTINET

WHITE PAPER

Securing OT in the Face of IIoT and 5G

Table of Contents

Introduction

Until recently, most operational technology (OT) processes ran on isolated networks with specific protocols. This tended to make security a simple matter of physical protection. The separation of the OT network from everything else—the so-called air gap—made it easy to ignore the major cybersecurity headaches being faced in data centers and business networks.

Over the last decade, OT protocols have increasingly been encapsulated into internet-based routable protocols (e.g., Transmission Control Protocol [TCP]/Internet Protocol [IP]). Industrial networks are now converging with the IT network as well. To use Purdue model terminology, while the physical process, operations, and control zones are still segregated from the business and logistics zone, as the traditional air gap is vanishing. A demilitarized zone with a network firewall is put in place to keep them apart. However, an ever-increasing amount of information now needs to pass between these zones. As ingress and egress data flows to OT systems increase, threat exposure also increases.

In parallel to these developments, there have been other technological shifts such as miniaturization of sensors and controls as well as applied artificial intelligence (AI) to help make sense of huge amounts of data supplied by OT systems. Perhaps most significant from the standpoint of security is wireless connectivity, which can allow direct connection to the internet, bypassing traditional OT network connections. Many industrial tools and devices now have built-in wireless connectivity, allowing process data and telemetry to be directly uploaded to business information systems or to supply maintenance data directly to the manufacturer of the system. This connectivity of many different types of devices via the internet is known as the Internet of Things (IoT). When IoT devices run within the perimeter of an OT environment, they are usually referred to as the Industrial Internet of Things (IIoT).

Regardless of the technological similarities and differences between IoT and IIoT, both infrastructures must be protected from cyber risks and should have minimum baseline security implementations following industry standards and best practices. This paper will investigate the implications of IIoT, including Wi-Fi and 5G, and other trends for the protection of production infrastructures. After illustrating several typical use cases of IIoT wireless connectivity, this paper will define an appropriate technology architecture for securing these devices. This architecture provides a foundation for making specific recommendations for the strategies and tactics necessary to ensure appropriate cybersecurity in a modern OT infrastructure with hybrid wired and wireless interconnections. Further, the paper will also illustrate these tactics with examples from the Fortinet portfolio of products.

IIoT, wireless, 5G, and other trends have implications for OT environments that are frequently built on the Purdue Enterprise Reference Architecture (PERA). This model describes a hierarchical set of levels for applications and controls. Levels 0, 1, and 2 (the *process control zone*) define physical processes, sensors, actuators, and related instrumentation as well as the systems that supervise these implementations. Level 3 (the *operations and control zone*) describes overall manufacturing operations across multiple processes. Together, these levels comprise an OT environment. Levels 4 and 5 are collectively known as the *business zone*, comprised of enterprise IT systems and applications. First conceived in the early 1990s, the original Purdue model did not anticipate IIoT, wireless, or cloud connectivity. With the general rollout of 5G technology, this process of bypassing the traditional Purdue levels will only accelerate.

This paper will discuss the impact of IIoT and 5G on security for a modern OT environment. It will also review the architectural considerations for providing secure connectivity in the enterprise and demonstrate how modern techniques can support both the security and flexibility required in today's enterprise.

IIoT and Wireless Deployment Use Cases

The security risks inherent to IIoT devices are associated with their direct or indirect internet connections. Before examining the risks involved with IIoT and wireless devices within an OT secured perimeter, the primary use cases for IIoT and the associated information flows should first be examined. An OT deployment may include a mix of the following three main use cases.

IIoT and/or Wireless: Outbound Only Communication

This use case consists of a smart sensor connected to a digital asset and sending data to a remote monitoring center (mostly third party) to perform Asset Performance Management, condition-based maintenance, etc. This case is the lowest risk because the information flow is one-way outbound from the sensor. Regardless of the connection—direct to a destination outside the secured OT perimeter or to a gateway within it—the sensor does not receive commands or instructions. A bad actor can therefore intercept the information, and potentially hide it from the HMI, but cannot influence the sensor directly.

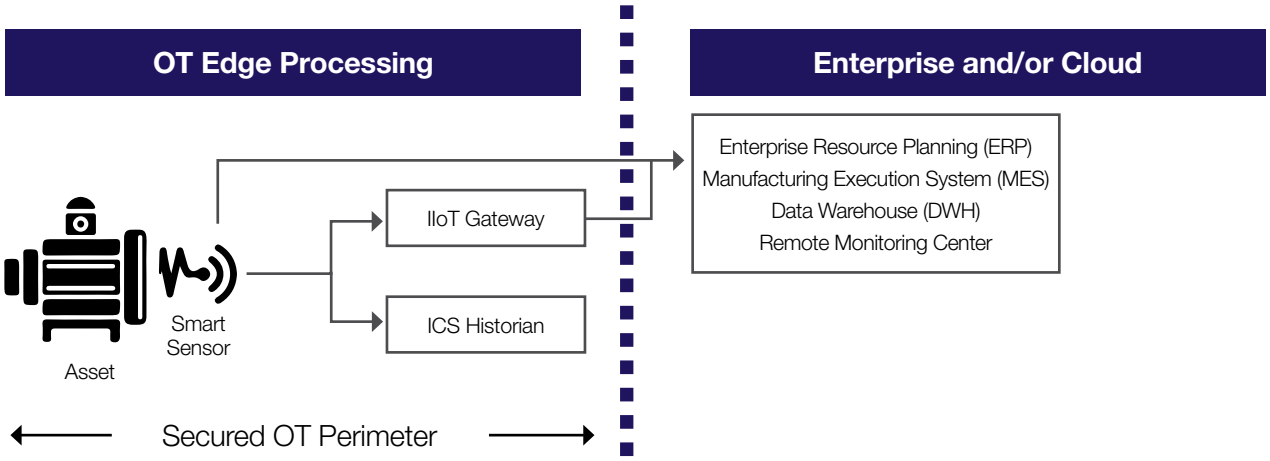


Figure 1: Outbound (egress) only communication.

IIoT and/or Wireless: Outbound and Inbound Communication

This use case provides for the outbound flow above and adds an inbound flow into the sensor to query it (e.g., for status). Queries and commands requesting analytics information can be sent from the enterprise or cloud IT environment, or potentially from the IIoT device manufacturer to gather data or access information for troubleshooting. Because of the two-way nature of the flows, this use case involves greater risk than the outbound-only case.

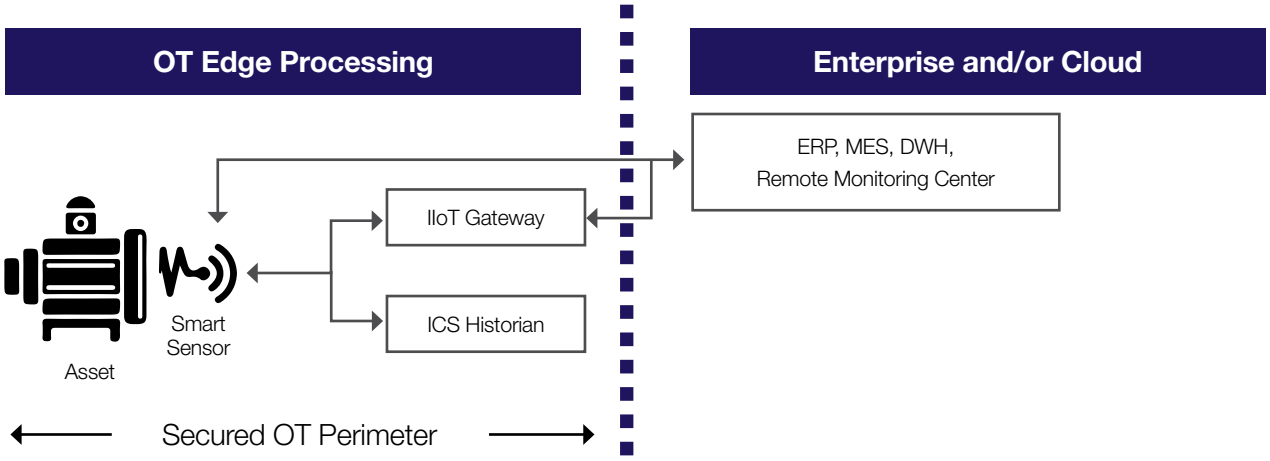


Figure 2: Outbound (egress) and inbound (ingress) communication.

IIoT and/or Wireless: Remote Access, Maintenance, and Diagnostics

This use case represents the highest risk because it does not just involve sensors (which are limited to providing information) but also actuators that make modifications in the production environment. As with sensors in the previous use cases, there is two-way communication between the enterprise or cloud IT systems and actuators. They may then respond to commands and take subsequent

actions. For example, an actuator could be sent commands to change a state, modify the speed of a process, or alter a flow. This use case may also describe the remote control of processes involving IIoT devices or even of a full plant. While it is clearly useful to be able to run processes remotely, it is crucial to recognize the security threats that these capabilities pose and protect against any threat exposures.

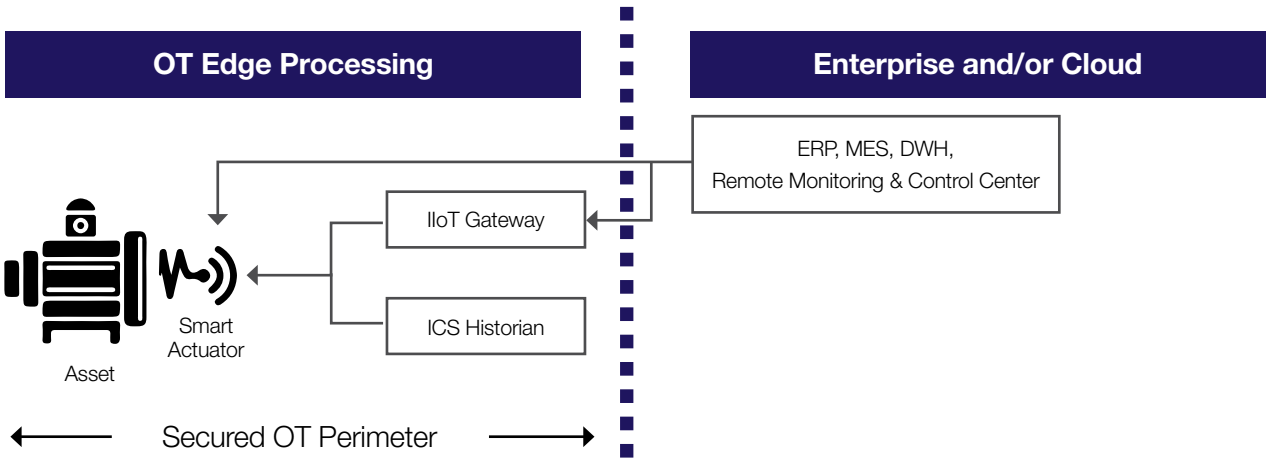


Figure 3: Remote access, maintenance, and diagnostics.

IIoT in the Production Control Structure

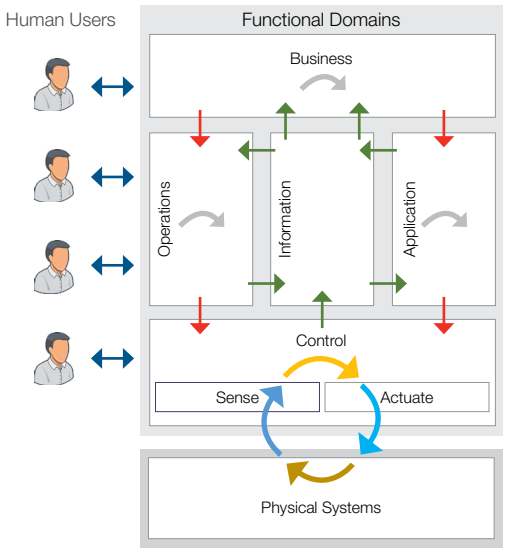
A production system is far more complicated than the single-asset use cases described above. It involves a complex interaction of OT devices, with flows of information moving along conduits between zones of the Purdue model. With the addition of numerous IIoT devices, the environment becomes even more difficult to manage. In order to secure the IIoT environment, it is essential to start with an understanding of how it should be organized.

IIoT Functional Domains

In order to understand the business and technology aspects of the IIoT ecosystem, a comprehensive reference architecture is necessary. The Industrial Internet Consortium (IIC) is an open membership organization managed by Object Management Group (OMG). The IIC was formed to accelerate the development, adoption, and widespread use of the industrial internet—a subset of the IIoT where the Industrial Revolution meets the Internet Revolution. While not a standards organization, members of the IIC catalyze and coordinate the priorities and enabling technologies of the industrial internet. In collaboration with industry experts, including National Institute of Standards and Technology (NIST), MITRE Corporation, IBM, and General Electric (GE), IIC has developed a comprehensive reference architecture guide for IIoT—*The Industrial Internet of Things Volume G1: Reference Architecture Guide* (IIRA).[1] Figure 4 is taken from the recent publication of IIRA guide v1.9. It shows an IIoT ecosystem divided into five functional domains:

- Control domain
- Operations domain
- Information domain
- Application domain
- Business domain

The control domain mainly deals with the industrial or machine aspects (i.e., physical systems), such as control, sense, and actuation



Green Arrows: Data/Information Flows, Grey Arrows: Decision Flows, Red Arrows: Command/Request Flows

Figure 4: IIoT ecosystem functional domains.

technologies. For example, industrial automation and control systems (IACS/ICS) reside within this domain. The combined control and operations domains can be considered as part of the OT side of the business, and the remaining domains as being on the IT side.

IIoT Technology Architecture

The IIRA guide further suggests the IIoT system architecture. This technology architecture uses a three-tier structure, as shown in Figure 5:

- The **edge tier**, which deals with OT
- The **platform tier**, which deals with OT and IT integration
- The **enterprise tier**, which deals with IT

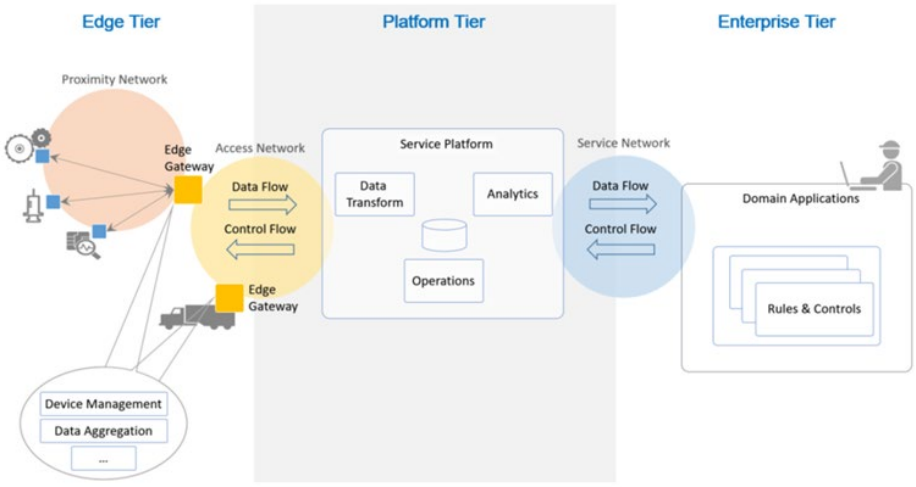


Figure 5: Three-tier IIoT system architecture.

Further, the IIRA maps the five functional domains to the three-tier technology architecture with an overlay of three networks—the **proximity network**, the **access network**, and the **service network**—which enable communication and connectivity across each domain and technology tiers. This mapping is illustrated in Figure 6 below. Communication networks can be based on either wired or wireless technologies. This may include local Ethernet or Bluetooth/Zigbee (in the case of the proximity network) or wide-area network (WAN) broadband, multiprotocol label switching (MPLS), or 5G technology (in the case of the access and/or service network).

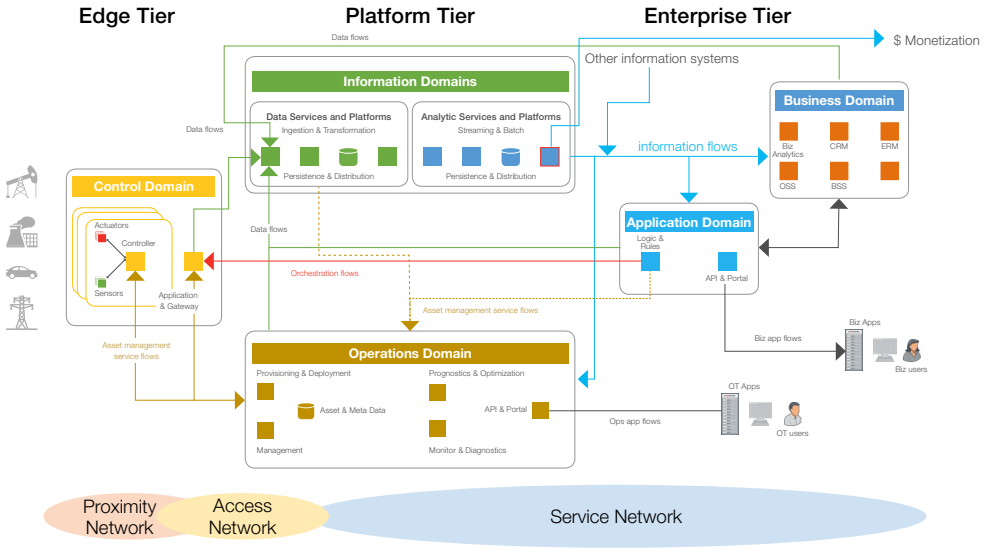


Figure 6: IIoT functional domains mapped to the three-tier technology architecture.

IIoT Security Architecture

Development of a detailed security architecture is key in any security implementation process. A security architecture not only guides the implementation of technologies and solutions but also assists in the evaluation of whether security technologies and solutions fulfill the specific security objectives and requirements applicable for various parts of the architecture.

The standard that guides the deployment for security in OT is ISA/IEC 62443.[2] Based on its architectural guidance for utilization of the PERA, Figure 7 below illustrates a mapping of the IIoT functional domains, technology tiers, and security requirements to the Purdue model. The figure also shows various communication networks used within the IIoT ecosystem.

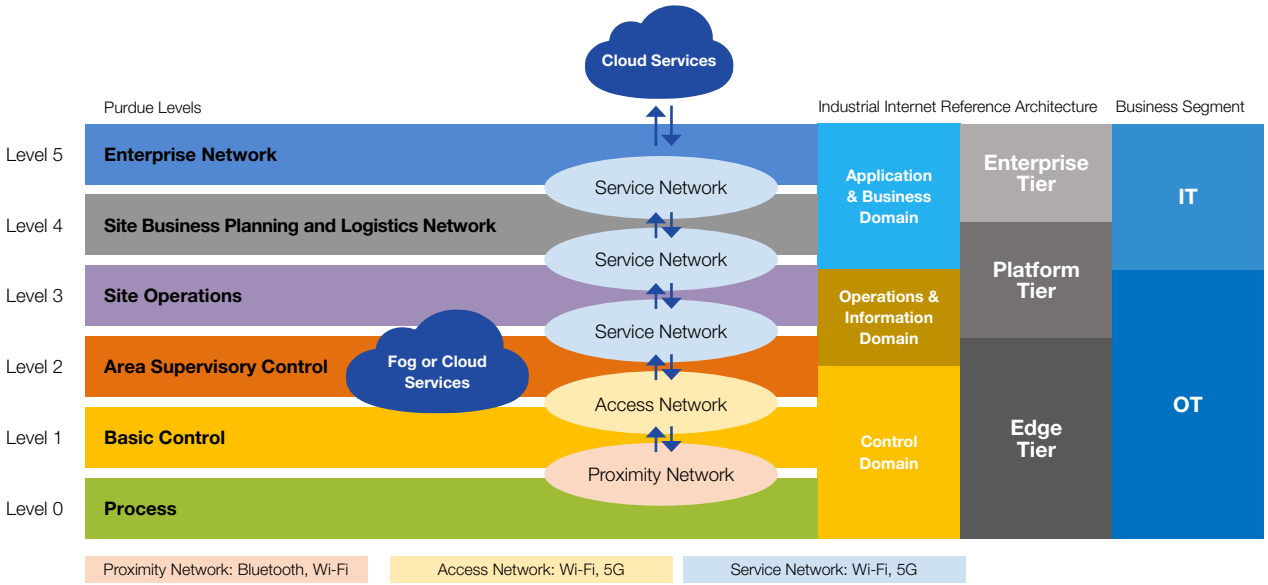


Figure 7: IIoT functional domains, technology tiers, and security requirements mapped to Purdue levels.

As highlighted in Figure 7, there may be various communication networks in the IIoT ecosystem providing communication channels between different levels; these communication channels need to be protected and secured. The service network typically relies on privately owned, dedicated communication networks or leased private networks—also known as mobile private networks (MPNs) or private access point names (APNs) that include cellular networks (e.g., 4G/LTE, 5G). All of these networks' entry and exit points need to be proactively monitored and secured.

The edge tier (comprised of Levels 0, 1, and 2) typically runs multi-access edge computing (MEC)-based technologies that provide compute, storage, and analytical functionality within the IIoT ecosystem. The MEC platform talks to the sensors, controllers, and machines (the "things" of the IIoT) located within Level 1. It then connects these "things" to the platform and enterprise tiers. The MEC platform usually runs virtualized operating systems, software applications, and tools. All of these MEC-based implementations should be secured and protected with the necessary security measures described below.

Fortinet Solutions for Securing the IIoT

Securing IIoT environments involves applying many of the same cybersecurity strategies used in IT to IIoT architectures and use cases. However, there are clear specificities to OT environments and IIoT in particular that must be taken into consideration. Using the ISA/IEC 62443 standard for security in OT as a base, and additional references to the NIST Cybersecurity Framework (CSF),[3] the following list represents security objectives for securing the connected IIoT infrastructure.

1. Asset Management
2. Application Visibility and Control
3. Intrusion Detection and Prevention
4. Network Access Control (NAC)
5. Network Segmentation and Microsegmentation
6. Signaling Protection
7. IoT Platform Protection
8. Logging and Monitoring

This section will describe each security objective and provide an overview of the associated Fortinet solution. Fortinet maps its solutions to the security requirements of the organization, not to a specific architecture. The objective is to enable security with whatever architectural choice is made by the asset owner.

Asset Management

Asset management is applicable to all levels of the Purdue model. However, in the context of network-connected assets, it applies to the assets in Levels 1 to 5 that have the capability to be probed and identified over the network. Asset management is a broad subject and there are industry standards and best practices available that can be applied to devise both an asset management strategy as well as implementation (e.g., ISO 55001:2014 or NIST SP 1800-5).

In terms of asset management within the IIoT ecosystem, several solutions within the Fortinet Security Fabric AI Fortinet Security Fabric can help—including FortiGate next-generation firewalls (NGFWs) and FortiNAC network access control, in combination with the FortiAnalyzer central log management and analysis platform.

Fortinet has an extensive partner network known as the Open Fabric Ecosystem, where solution vendors from across the industry can leverage Fortinet Security Fabric application programming interfaces (APIs) for two-way integration. Security Fabric API integration enables the partner solution to be "Fabric-Ready" and offer solution-specific capabilities.[4] The Fabric-Ready partner portfolio includes many well-known ICS/OT specific asset management solutions that can be integrated seamlessly with Fortinet solutions such as FortiGate and FortiSIEM security information and event management system to offer holistic visibility of assets and to assist with asset management. This allows any asset identification information collected by a third-party solution to be shared with and integrated across the Fortinet Security Fabric platform.

Industrial sensors and actuators are numerous, distributed, and well-hidden. This makes it all the more important to employ systems capable of automatically building an inventory and tracking the real-time status of these devices, gathering metrics such as:

- Device type, hardware version, software version (where available)
- Location
- Network traffic patterns (protocols, packet/byte counts, number of sessions)
- Addressing information and credentials
- Threat level

Due to the specialized nature of components in an OT environment, a number of vendors have developed tools focused on finding and identifying them in various environments. Open APIs enable Fortinet solutions to interoperate with well-known asset visibility and network intrusion detection system (NIDS) solutions from various vendors.

Application Visibility and Control

Identifying devices is only one part of asset visibility. Protocols and application types also have to be controlled. The FortiGate Application Control feature can monitor or limit which protocols can be used by the device as well as the applications with which it can communicate. Use of any unauthorized communication protocol or its functions can generate an alert and optionally be blocked. Application and protocol definitions include more than 4,000 rules in 24 categories. All commonly used IoT protocols (such as MQTT, AMQP, HTTP, and CoAP) are covered, and transport layer security (TLS) inspection can be performed with appropriate configuration. A wide range of industrial protocols are available for hybrid IIoT solutions.

FortiAnalyzer provides a high-level security operations center (SOC) view of gathered information, with the ability to drill down to specific events. Reports can be generated on a regular basis to provide ongoing visibility for assets and communication networks. FortiAnalyzer also incorporates a sophisticated event management tool that can take actions based on log events from registered security components. FortiSIEM can be used for more advanced correlation, customization, and out-of-the-box integration with a wide range of third-party products.

Intrusion Detection and Prevention

IIoT devices are prime candidates for attack, mainly because of their ability to “short circuit” multiple layers of the Purdue model and provide access from the outside world directly to devices at the lowest layers. Generally, these devices will have limited connectivity and communicate with a small number of destinations (such as an IoT platform and maybe application servers providing other services, such as firmware upgrades or data storage). This means that in a well-designed network, the possibility of launching an attack from a compromised device is limited. But it should always be assumed that the IoT platform or application servers may become compromised, allowing the launch of an attack from inside the local OT network.

Most IIoT devices have limited functionality. Although this reduces the probability of vulnerabilities, it introduces a different problem. IIoT functionalities are often custom developed, which may introduce bugs that would not have appeared in general-purpose components that are typically field-hardened. Furthermore, the full breadth and diversity of devices that may be labeled IIoT or IoT must also be considered. An agricultural soil monitor functions in an environment that is very different from that of an autonomous vehicle. No matter what the device, exploits must be expected and protection put in place.

IoT platforms may have vulnerabilities just like any other software. In most cases, they will consist of coding bugs that allow buffer overflows or other memory corruptions. In addition, most IoT platform signaling happens via some kind of API—so typical API attacks should also be considered. Finally, data received by the platform will often result in a read or write to a database. Therefore, SQL attacks must also be covered.

Like any service platform, care must be taken to expose only the minimum, and not to leave unused services running (which is often the default case). For example, Server Message Block (SMB) services are often enabled by default and are also a common vector for attack. Open ports should be checked and any unnecessary services should be disabled or removed from the system.

When communications are protected end to end with TLS, there should be at least one security device that is decrypting the traffic to ensure that the protected traffic is as expected. If this is not the case, a compromised IoT device could use the encrypted connection to hide malicious traffic from the operator. If the security device is co-located with the IoT platform, then it may offload the TLS

processing and send decrypted traffic directly to the platform. Otherwise, it should reencrypt the traffic to ensure that eavesdropping is not possible.

Intrusion prevention

To deal with many of these types of attack, the FortiGate intrusion prevention system (IPS) is designed to detect and block a wide range of attacks against IIoT and IoT:

- **Exploits:** This includes any attack on a vulnerability, and will typically be used either to cause a denial of service (DoS) (by causing crashes or extra work within software) or local code execution, which will often result in a second-stage attack (such as transferring a malicious executable).
- **Reconnaissance:** Scanning attacks, which include looking for open TCP or User Datagram Protocol (UDP) ports, and looking for known software or protocol versions. Usually the goal of reconnaissance attacks is to identify vulnerable or high-value targets.
- **Fuzzing attacks:** This is another method for finding vulnerabilities. It is usually done locally in a controlled environment but can be used as a blunt-instrument attack on a live network. Examples include deliberate protocol anomalies, the use of extremely long fields, or using an invalid/unusual date. All of these techniques are designed to trigger programming errors. The goal is to find vulnerabilities or simply to cause disruption.

All of these attack types (and more) are identified and blocked by the FortiGate IPS function, which contains more than 30,000 rules, including an optional industrial security service package for ICS/OT. Rule packages are automatically updated on a daily basis by **FortiGuard Labs** (the research and analysis arm of Fortinet) to ensure that protection is constantly up to date.

Virtual patching

Whenever vulnerabilities are uncovered in IIoT devices, controllers, or infrastructure components, the most effective solution is to patch the affected device with a vendor-supplied firmware update. However, this is not always possible. Security updates may no longer be available for legacy devices. Even if they are, installing updates presents a risk, and in most cases, a period of testing will be performed before a new release is put into production. In some cases, devices may not even support firmware updates.

Fortinet's virtual patching (also known as vulnerability shielding) between patching and capabilities provides a solution for these sorts of problems. By using an upstream intrusion prevention device (e.g., a FortiGate NGFW), exploits can be detected and blocked before they reach the vulnerable target. This can provide temporary protection until a definitive patch is installed, or permanent protection for cases where patching is not an option.

Breach detection

Whether for IT or OT, the general goal of cybersecurity should be to stop attacks before they are able to compromise a device. However, when an attack does get through defenses, IIoT security solutions must be able to detect signs of the infection and act quickly.

There are a number of threat possibilities if an attacker successfully gains control of a device. The attack may simply disable the device. This is generally the easiest type of attack, since it does not require any malicious firmware (bot) to be installed. Attacks like this may also be monetized using a ransom model, where a payment must be made to prevent the attack. In some cases, a device may be permanently destroyed by an attacker. An example of this could be to substantially increase battery usage to the point of exhaustion in a deployment where the battery is intended to last the lifetime of the device.

A more common approach (and one that gives maximum flexibility to the attacker) is a botnet. The effectiveness of IoT botnets was shown in 2017 with Mirai, where hundreds of thousands of IoT devices (mainly cameras and DVRs) were used to stage the largest ever known distributed denial-of-service (DDoS) attack.[5] Botnets can exploit IIoT devices in the same way.

Using FortiOS botnet protection, any botnet activity—whether detected by destination address, domain, or protocol—can generate an alert and be blocked. FortiGuard Labs maintains a list of all known botnet destination address and port combinations, which is frequently updated across all FortiOS devices. All outgoing sessions are checked against this list. Additionally, connections to other known bad destinations as detected by the FortiGuard Indicators of Compromise (IOC) Service can generate a compromise alert. Botnets that use fast-flux domains (where a domain continually changes its IP address mapping) can be checked against the domain itself by intercepting and checking the DNS request. Finally, even if the destination address and domain are unknown, many botnets can be detected by their command-and-control protocols. By using these three methods in parallel, Fortinet ensures the best chance of detecting botnet-infected devices.

Network Access Control (NAC)

NAC is applicable for all communication network boundaries. However, the way it is deployed will differ depending on the type of communication network (e.g., Layer 2 vs. Layer 3). The simplest form of NAC can be achieved by enabling the 802.1X network authentication protocol on supported IIoT assets. Fortinet technologies—such as the combination of FortiGate, FortiNAC, and FortiAuthenticator solutions—can simplify NAC implementation with integrated authentication and authorization capabilities. In the case of wireless networks, a FortiAP secure wireless access point can be integrated with FortiGate for wireless device control. Additionally, FortiSwitch solutions can be implemented within the access network to offer granular access control for IIoT controllers.

Typically, third-party remote access is common within IIoT networks for routine or ad hoc maintenance and troubleshooting purposes. This may include remote configuration of assets or remote factory/site acceptance tests (FAT/SAT). NAC capabilities can apply pre-admission or post-admission network policies to such third-party connection requests. Remote access can be supplemented with multi-factor authentication (MFA) via FortiToken solution integration.

Network Segmentation and Microsegmentation

Segmentation and microsegmentation provide the key methods for segmenting industrial networks into physical or virtual secure segments (zones). Typically, segmentation is performed between the local area networks (LANs) or wide-area networks (WANs). This is sometimes referred to as north-south communication. Microsegmentation is performed within the LANs, and is used to control east-west communication. As for the industrial networks, network segments may include various industrial LANs or WANs and network microsegments may include various industrial controllers and hosts such as RTUs, HMIs, etc.

Traditionally, network segmentation has been utilized within industrial networks for separating assets, making it harder for attackers to gain access to large numbers of devices, and preventing a cyberattack from spreading across the entire network. Other advantages of such splitting are in improving security enforcement and control as well as improving network visibility. In general, this applies to all network boundaries and within each Purdue level. As stated earlier, segmentation can be physical or logical, depending on the protection level desired for the assets within each level. The assets must be grouped (or "zoned" in Purdue terminology) and segmented from other assets. Special segments (zones) known as "conduits" need to be implemented between the zones and network boundaries or where the zones converge. This allows implementation of various security controls—including monitoring and filtering of network communication or information exchange.

Network segmentation is typically implemented by way of network switches and virtual LANs (VLANs). A network router or firewall is utilized for allowing communication between different VLANs also known as inter-VLAN communication. At the network switch level, VLANs provide a good mechanism for virtually splitting the LANs and grouping the network assets into virtual zones. However, it is not effective in terms of inspecting the network traffic and making decisions should a malicious communication (payload) traverse the communication channel. Introduction of an NGFW with built-in next-generation intrusion prevention (NGIPS) functionality for inter-VLAN communication can solve the problem of inspecting network traffic between the VLANs and can be effective in implementing decision-based security policies for VLAN communication. However, this still leaves one gap: communication within the VLAN between hosts, also known as intra-VLAN communication. The intra-VLAN communication will not be inspected by the NGFW unless this traffic is specifically routed to the NGFW for inspection. This is known as microsegmentation.

Microsegmentation within industrial networks carries network segmentation to its logical conclusion by further dividing each industrial VLAN or LAN into distinct security segments down to the individual asset level, then defining security controls and delivering services for each unique microsegment. Today's industrial IoT environments utilize internet-enabled, open-standard, and complex communication protocols that often carry sensitive information for production control environments. Due to its openness and complexity, the information carried over these protocols can be manipulated to cause disruption in the environment, opening the door to cyberattacks.

An NGFW with built-in NGIPS that understands industrial protocols and communication can prove very effective for microsegmentation. It allows communication to and from an asset to be evaluated based on security policies, inspecting IIoT protocols and communication at the ingress and egress points for the assets.

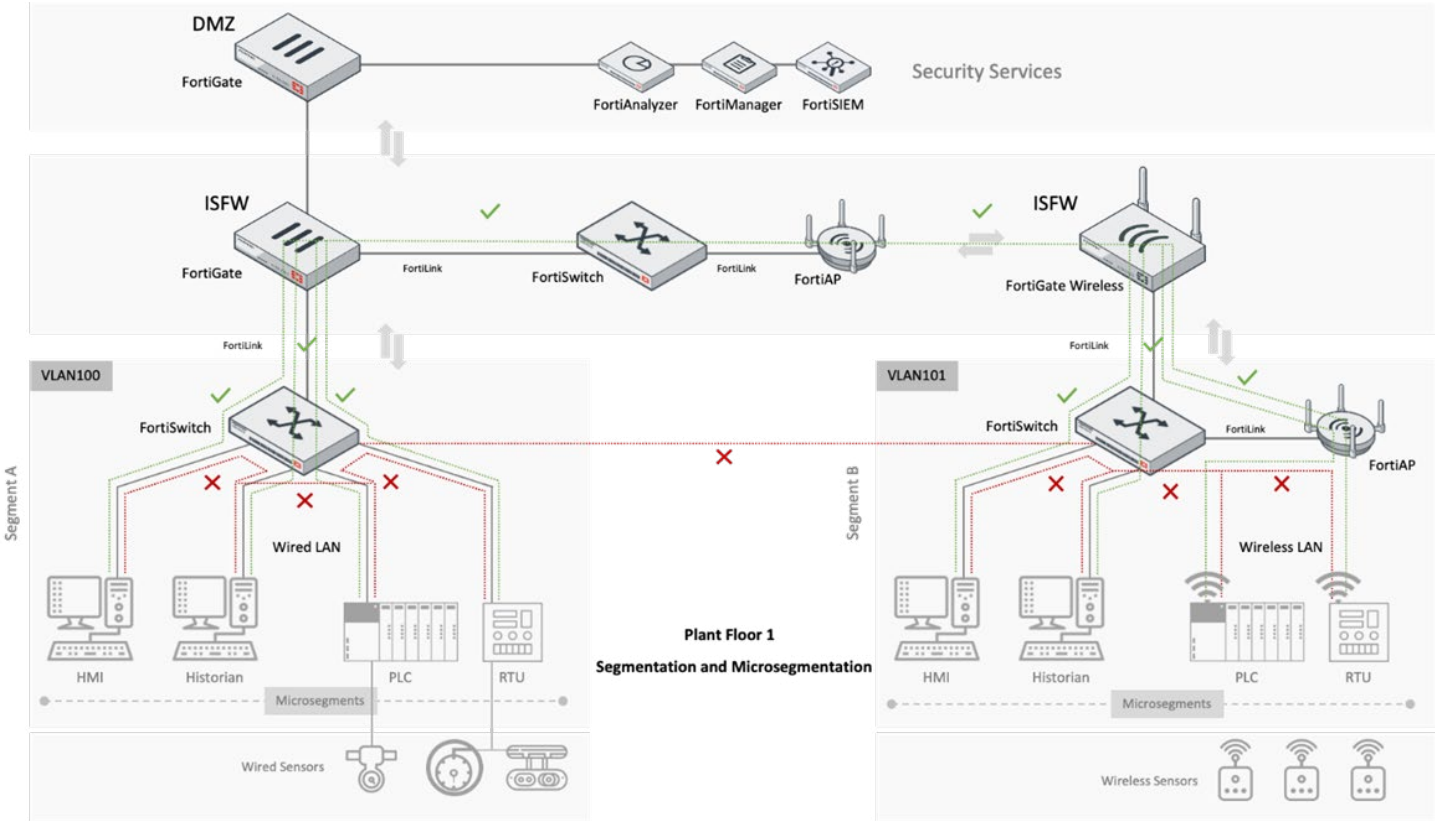


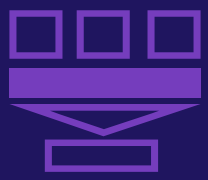
Figure 8: Segmentation and microsegmentation in wired and wireless industrial networks.

For example, Figure 8 illustrates an industrial environment consisting of many production LANs. Within each production LAN there are several VLANs, each with multiple hosts (RTUs, HMIs, etc). The LANs communicate over a wired network using FortiSwitch or wireless connections using FortiAP. FortiGate NGFW is used as an internal segmentation firewall (ISFW) for segmenting the LANs into Segments A and B, and performing inter-VLAN routing, visibility, and inspection for all the network communication between the two network segments.

Further, each VLAN (VLAN 100 and 101) is microsegmented using the same ISFW, isolating each host within its own segment. The FortiGate NGFW runs built-in NGIPS with deep packet inspection (DPI) capability for industrial protocols that provides visibility and control up to the protocol payload, thus supporting visibility and control over all network communication to and from each host. Likewise, the same ISFW performs the intra-VLAN communication.

Virtual domains (VDOMs) are very beneficial in an industrial IoT environment with microsegmentation, as some IIoT devices may not support IP-based routing. The FortiGate can be configured to run in both non-IP based mode (Layer 2) and IP-based mode (Layer 3) at the same time. This is also known as Transparent VDOM and NAT/Routed VDOM, respectively. Likewise, the Fortinet FortiLink functionality enables integration of FortiSwitch and FortiAP within the FortiGate. This assists with the configuration and management of the integrated FortiSwitch and FortiAP from within the FortiGate. Essentially, with FortiLink, the integrated FortiSwitch and FortiAP serve as extended network ports on the FortiGate NGFW.

The ability to segment and microsegment the industrial environment, including visibility into industrial protocols, is a key benefit of Fortinet's approach to OT security. Fortinet products, including FortiGate, FortiSwitch, FortiAP, and others, are integrated into the Fortinet Security Fabric, providing holistic protection of both the industrial and enterprise digital environment.



The virtual domains (VDOMs) functionality on the FortiGate offers flexibility by dividing the single FortiGate into multiple virtual firewall instances, where each virtual firewall instance within the same FortiGate can independently perform its own security functions.

Signaling Protection

As 5G technologies mature, the use of cellular access networks will become more common in industrial networks. These networks have a high signaling overhead. In the situation where there are large numbers of IIoT endpoints compared with the amount of data transferred, this can pose a risk of signaling storms—either intentional (as a result of a cyberattack) or unintentional (as a result of device malfunction).

The latter is of particular concern, because dealing with errors in embedded devices is particularly difficult. Often the most reliable way to return the device to a known state is to restart. This is a good solution in theory. However, this may be difficult to do in a live operational environment. Furthermore, an error condition may be caused by an external factor (e.g., high temperature, power outage, earthquake). If that factor impacts a large number of similar devices, then the result may be that all such devices simultaneously reattach to the network. The resulting overhead on the signaling infrastructure may cause outages not only for the devices involved but also for other services sharing the network.

FortiOS has a range of features designed to protect carrier networks, including protection from signaling storms. In addition, the Fortinet IPS function has the ability to define rules for specific network behavior, including rate-based rules. Because many IoT devices have a predictable packet rate, this can be used to detect unusual activity (possibly caused by malfunction or compromise) and remove such devices from the network to protect the signaling infrastructure.

IoT Platform Protection

An IoT platform is the critical heart of any IIoT service, and in larger networks it may be implemented as a hierarchy of platforms. All signaling and data will normally pass through one or more platform nodes; protecting those nodes against attack is very important. In the traditional IoT model, the IoT platform would be positioned in the cloud. But for IIoT, there are two issues with this approach:

- For event logic (such as adjusting an actuator based on a sensor reading), the round-trip time between devices and cloud may be too long and the reliability of a cloud connection may not be sufficient.
- Sending data into the cloud may present security risks, due to the transmission of private data over a public internet link.

The 3rd Generation Partnership Project (3GPP)—a consortium of standards organizations that develop protocols for mobile telecommunications—has proposed several solutions to specifically address these issues, including:

- The MEC architecture, where an instance of the 5G packet core is implemented close to or on the customer premises. This allows an IoT service platform and associated application servers to be located on-premises, which eliminates both the round-trip time and data privacy issues.
- A private 5G network, which is similar to the above except that the 5G packet core is dedicated to the end-user. This further eliminates any privacy issues and ensures complete control of the infrastructure.

One or both of the above solutions can be used to provide highly reliable, low-latency, high-bandwidth applications with all critical data remaining in the domain of the end-user.

From a security point of view, bringing the processing close to or onto the customer premises (known as “edge computing”) brings advantages. Transactions can be handled locally without sending data over a WAN link or public internet connection. Transactions that cannot be handled locally can exit to higher layers through a defined logical interface with an appropriate security policy applied.

In cases where data must be sent to the cloud over an untrusted network, encryption and integrity protection should be employed to guard against eavesdropping or tampering. FortiOS provides very mature and field-hardened TLS and Internet Protocol security (IPsec) implementations with extreme scaling, thanks to hardware acceleration using dedicated application-specific integrated circuits (ASICs) in FortiGate appliances or using central processing unit (CPU) acceleration capabilities in virtualized instances.

Logging and Monitoring

Centralized logging and monitoring enables observation of the entire IIoT ecosystem from a single point, usually a SOC or network operations center (NOC). This should include the ability to determine or configure baselines and provide access to logs and events that may result from deviations from the baselines or from malicious activity. The suitable place to incorporate logging and monitoring measures is within the conduits between Purdue Level 2 and Level 3 (Level 2.5) or between Level 3 and Level 4 (Level 3.5) or in Level 5—depending on the IIoT organization’s operating structure.

Fortinet solutions (including FortiAnalyzer, FortiManager, and FortiSIEM) can enable centralized logging and monitoring for the Fortinet technologies deployed both within the IIoT ecosystem and across the broader OT environment. They can also collect information from hundreds of other vendor devices that are part of the Fortinet Open Fabric Ecosystem.

Summary of Fortinet Solutions for IIoT Environments

Security Requirement	Applicable Purdue Levels	Communication Networks	Functional Domains	Technology Tiers	Fortinet Solutions
Asset Management	All Levels	All Networks	All Domains	All Tiers	FortiGate, FortiSwitch, FortiAP, FortiNAC, Fabric-Ready Partner Solutions
Application Visibility and Control	Levels 1-5	All Networks	All Domains	All Tiers	FortiGate, FortiSwitch, FortiAP
Intrusion Detection and Response	Levels 1-5	All Networks	All Domains	All Tiers	FortiGate, FortiSwitch, FortiAP, Fabric-Ready Partner Solutions
Network Access Control	Within and Between Levels 1-5	Between the Network Boundaries	All Domains	All Tiers	FortiGate, FortiSwitch, FortiAP, FortiAuthenticator, FortiToken, FortiNAC
Network Segmentation	Within and Between Levels 1-5	Between the Network Boundaries	All Domains	All Tiers	FortiGate, FortiSwitch, FortiAP
Logging and Monitoring	Within Level 3.5 or Level 3.5 and Level 5	Between the Network Boundaries	All Domains	All Tiers	FortiGate, FortiSwitch, FortiAP, FortiNAC, FortiAnalyzer, FortiManager, FortiSIEM, Fabric-Ready Partner Solutions

Figure 9: Fortinet technologies mapped to security requirements and IIoT functional domains, tiers, and networks.

Fortinet Enhanced Purdue Model

Despite the work done in recent years by various standards bodies such as the IIC, the Purdue model has not yet officially incorporated IIoT and wireless connectivity. This work is ongoing, but asset owners and security professionals cannot wait for the formal ratification process before implementing security measures. As a result, Fortinet has been promoting an enhanced Purdue model over the past several years. In order to be architecturally agnostic, Fortinet represents the IIoT device and platforms as well as wireless devices (be they IIoT or not) laterally in an unlayered “Zone 6” that physically resides in the security perimeter within OT. This is illustrated in Figure 10 below.

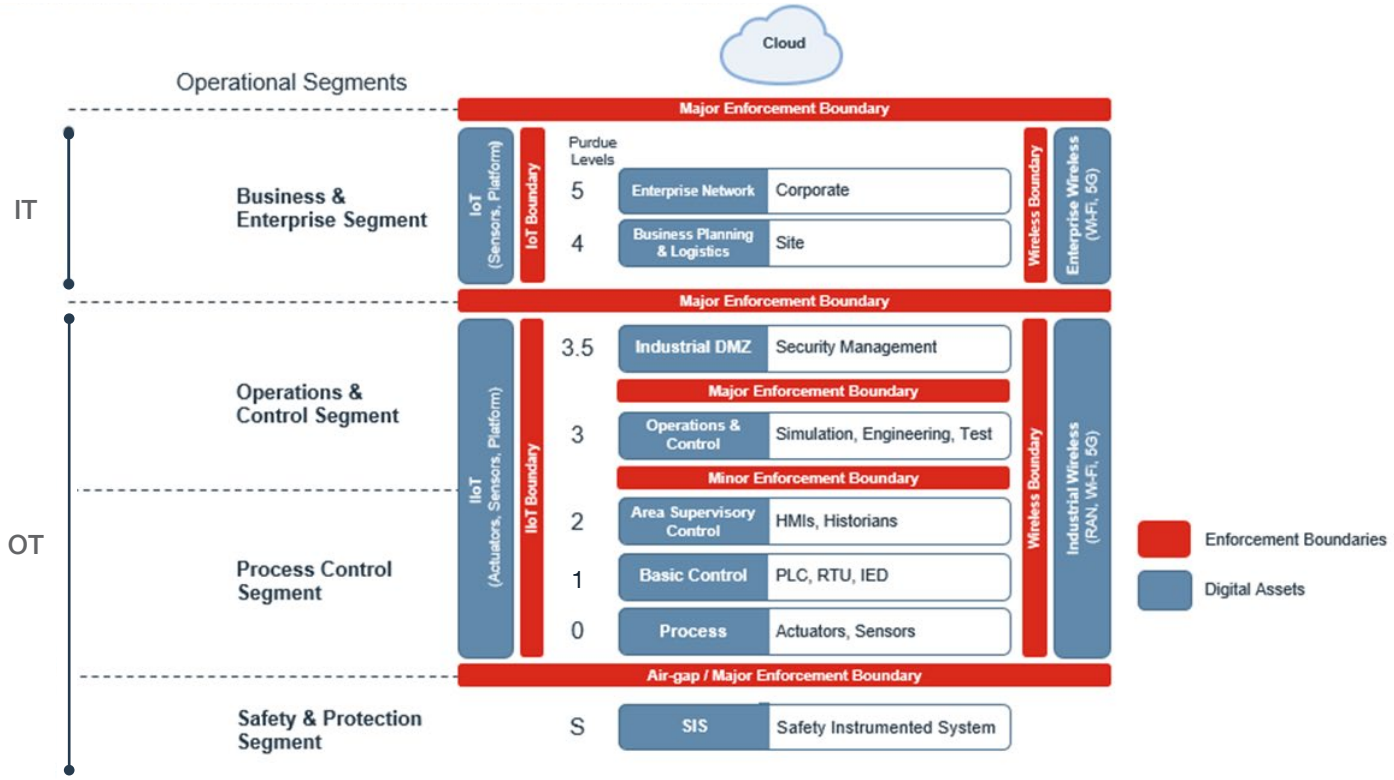


Figure 10: Enhanced Purdue model including IIoT and wireless.

Conclusion

Production environments are going through tremendous transformations due to wireless, 5G, and IIoT technologies. These changes are ushering in a new era of flexibility, productivity, and control for OT-based organizations. At the same time, these innovations are opening up new attack vectors for bad actors who prey on these critical aspects of business and public infrastructures. Although the standards for designing and protecting these infrastructures continue to evolve, operations and security management cannot simply wait for a final result. The threats are real today. It is therefore critically important to put in place a flexible security infrastructure with elements that can evolve along with today's changing wired and wireless OT environments.

Fortinet is totally focused on cybersecurity. As the industry's leading pure-play cybersecurity provider with over 20 years of experience protecting both IT and OT environments, Fortinet offers a full portfolio of integrated security solutions that not only work with each other but also interconnect with products from hundreds of other suppliers. This includes all of the major ICS and supervisory control and data acquisition (SCADA) offerings, asset and network industrial systems visibility products, and industrial systems integrators. As production and operational technology evolves, organizations can be sure that the Fortinet security investment made today will adapt and grow to meet future requirements.

[1] "Industrial Internet Reference Architecture," IIC, accessed December 30, 2020.

[2] "New ISA/IEC 62443 standard specifies security capabilities for control system components," ISA, accessed December 30, 2020.

[3] "Cybersecurity Framework," NIST, accessed December 30, 2020.

[4] "Open Fabric Ecosystem," Fortinet, accessed December 30, 2020.

[5] Josh Fruhlinger, "The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet," CSO, March 9, 2018.

February 9, 2021 3:00 AM

884983-0-0-EN

D:\Fortinet\2020 Old templates\White Paper\Purple White Paper\IIoT and 5G with Purdue Model\wp-iiot-and-5g-with-purdue-model-V3-292021\wp-iiot-and-5g-with-purdue-model-V3-292021