FORTINET "RUGGED"

Fortinet delivers an industry-specific, tightly integrated solution that combines the connectivity and security you need for distributed industrial control systems in form factors that are designed for the extreme environments in which they must be deployed.

The Unique Challenges of Securing Industrial Control Systems

Background

Measurement and control systems have been utilized by energy producers, mining operations, utility companies, transportation systems, and similar organizations since the 1968 when the first programmable logic units were used to control systems at industrial plants. Since then more critical systems have become more automated and connected.

Just as information technology in knowledge-based enterprises, these "operational technologies" (OT) have resulted in great efficiency and cost improvements for process-intensive industries. Yet they also raise similar and significant operational security challenges. These issues are further complicated by environmental, geographic and regulatory issues. However they can be appropriately addressed by implementing ubiquitous security and posture control to protect human health and safety.

The threat posed to industrial control systems by advanced cyber-attacks continues to evolve daily. Active mitigation tactics are required to secure critical resources because the potential impact goes far beyond the very significant financial risk to commercial businesses – making security at paramount priority.

Benefits

- Top rated, industrial control-specific, protection to increase security from advanced threats
- Higher reliability and longer lifecycle from appliances designed for harsh environments
- Simpler deployment and management of tightly integrated security, networking and wireless
- Admission control capabilities that not only track devices but also the traffic they produce to

SECURED BY **FORTIGUARD.**

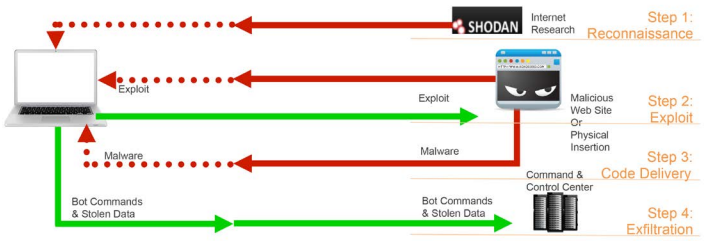
Challenges to Securing ICS

The sophistication of today's cybercriminals is one of the top challenges facing OT as well as IT. Attackers often follow a similar set of steps (or "kill chain") to penetrate industrial control systems.

- **Step1:** In the industrial control world, reconnaissance often involves searches on the web to identify HMI systems. In the case of the October 2014 ICS-CERT alert, cybercriminals sought out GE Cimplicity, Advantech/ Broadwin WebAccess, and Siemens WinCC. These systems registered themselves on the internet and were publically accessible through a Google search.

- **Step 2:** Identify vulnerabilities, such as CVE-2014-0751 of the Human Machine Interface (HMI) related to the October 2014 ICS-CERT alert, and launch exploit attacks to gain access and remotely execute code.

Figure 1: Typical Targeted Attack on IC System



- **Step 3:** Install malware on the system (Black Energy in the case of the October 2014 ICS-CERT) to communicate back out to the Cybercriminal for additional instructions.

- **Step 4:** Once the malicious code is running, it can potentially harvest information from the user and control system, move laterally within the organization and even start sending instructions to the controller.

Traditionally, "air gapping" or ensuring that HMI and control systems were only locally and physically accessible was the acknowledged method of security. However, mounting evidence of Internet connected HMI systems highlights the criticality of additional security measures:

1. Access Control: segmentation and strong authentication

2. Vulnerability Management: physical or virtual patching

3. Threat Prevention: IPS, Antimalware and Web Filtering for analysis of protocol, code and communications

4. Sandboxing and other monitoring to detect attacks that slip through

However there are additional challenges to deploying what are essentially IT Security controls to an OT environment.

- **Industry-specific systems, regulations and practices.** Most industrial control systems come from very different vendors and run proprietary operating systems, applications and protocols (GE, Rockwell, DNP3, Modbus). As a result, host-based security developed for IT is generally not available for ICS and many network security controls developed for common enterprise applications and protocols do not offer much in the way of support for those used by ICS.

- **Environmental conditions.** Industrial control systems can, literally, be physically located anywhere in the world, often with harsh environments. Very different from controlled, indoor IT environments.

- **Distributed, remote locations.** Industrial control systems generally span miles, often countries and even the world. As a result, access (both physical and Internet) can be limited and difficult.

Real-World Examples

With the exploding "Internet of Things," or dramatic increase in connected and intelligent systems, the number of different types of systems to be secured is nearly endless. However, here we provide brief, representative examples of systems, challenges and recommendations.

Midstream Pipeline

Pipelines span vast portions of countries to transport liquids and gases.

- **Industry-specific considerations:** Standard control systems in this industry provide the continuous monitoring required for safe operation. Recognition of these applications for the purpose of traffic management and, ideally, white listing as part of a positive security model are recommended.

- **Environmental conditions:** Further, such pipelines and their distribution shacks provide severely limited protection (enclosures, heating or cooling) from the elements, A dedicated form factor that can handle these extremes in temperature is highly recommended.

- **Distributed, remote locations:** Far flung operations require strong remote management and the ability to operate over limited bandwidth.

Transportation – Shipping

Multi-ton tankers are run by surprisingly small teams and traverse parts of the world where piracy is common.

- **Industry-specific considerations:** The keys to the kingdom for controlling a ship are the navigation systems. Fortinet recommends segmentation and strong access controls between the onboard HMI and ship control systems.

- **Environmental considerations:** Operating on the high seas, this security is ideally delivered in a rugged form factor that can withstand the physical motion on board, as well as the inevitable exposure to elements over time.

- **Distributed, remote locations:** Internet connectivity out at sea can be limited and often satellite-based. Support for integrated wireless access, ideally 3G/4G networks, is recommended.

Oil & Gas Rigs

Often floating far out in the middle of oceans, industrial control systems for oil & gas drilling are still highly automated and precise.

- **Industry specific considerations:** oil rigs are highly dependent on dynamic positioning systems and satellite communications given such limited bandwidth in their remote locations. Fortinet recommends introducing traffic management solutions with quality of service tracking that can recognize and prioritize these ICS applications, as well as shield the ICS systems from vulnerability exploit.

- **Environmental conditions:** Further, their location exposes systems and security to harsh weather conditions — in addition to hazardous proximity. Fortinet recommends special consideration to form factor including a full enclosed, Division 1 Class 2 appliance designed to be ignition and explosion proof.

- **Distributed, remote locations:** Internet connectivity out at sea can be limited and often satellite-based. Support for integrated wireless access, ideally 3G/4G networks, is recommended.

Electric Utility – Generators and Substations

By contrast, electric utility generators substations are located on land, but must span even the most remote areas to provide critical energy to all parts of any country. And depending on the method of generation, can represent an even greater risk and hazard- in the case of nuclear power for example.

- **Industry considerations:** Both the generation and distribution sides of the utility business are highly automated. Further, such systems are regulated by the North American Electric Reliability Corporation (NERC) and similar standards in various parts of the world.

Among these standards are provisions related to perimeter security, continuous threat monitoring and response and more that need to be considered. Fortinet recommends a highly reliable, small form factor device that integrates industry-specific security intelligence with networking that allows remote access without opening the control box.

- **Environmental Conditions:** Those substations are exposed to the elements, which run the full gamut of conditions based on climate. Hot, cold, dusty, wet, all that protects such systems and security is a metal container on site. Fortinet suggests a rugged form factor to address the extreme temperatures if nothing else.

- **Distributed, remote locations:** Electricity distribution is, as the name denotes, highly distributed. As a result, strong central management and reporting- given the regulatory requirements – need to be a part of any solution.

Fortinet Solution

Fortinet delivers a tightly integrated solution that combines the connectivity and security you need for distributed industrial control systems, in form factors that are designed for the extreme environments in which they must be deployed. Specifically, organizations benefit from:

1. Top rated security technologies, including industrial control-specific capabilities to protect critical infrastructure systems.

2. Integrated switching and wireless access to ensure connectivity as well as security for your automated systems anywhere in the world.

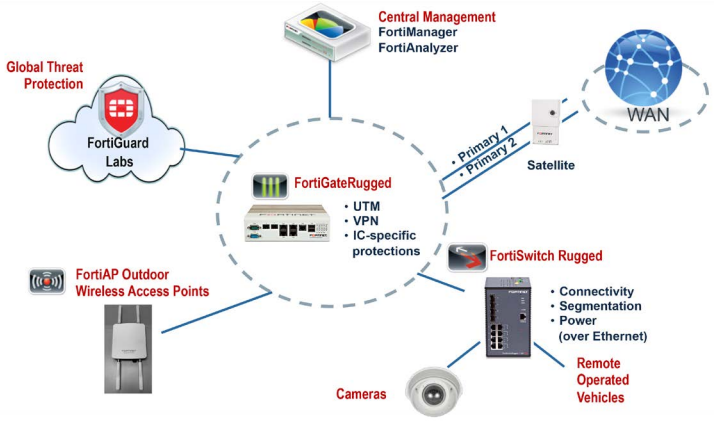
3. Strong remote configuration and management, as well as central monitoring and reporting, to maintain security, ensure high availability and demonstrate compliance.

4. Purpose-built devices to withstand extreme temperatures, harsh climates, and hazardous locations, in accordance with international substation automation standards, IEC 61850-3 and IEEE 1613, and other standards.

5. FortiGuard Labs threat expertise and intelligence, including proactive research focused on industrial control systems, vulnerabilities, threats and protections.

While use cases vary, the need for industry specific protections, connections and form factors does not.

Figure 2: Fortinet's Rugged Solution for Industrial Control Systems in Remote Locations



For more information visit http://www.fortinet.com/solutions/distributed_enterprise.html.

For more information visit www.fortiguard.com

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480