FORTINET

SOLUTION GUIDE

Securing Industrial Control Systems with Fortinet

IEC-62443 compliant end-to-end security

Executive Summary

In recent years, the Industrial Control Systems (ICS) upon which much of our critical infrastructure and manufacturing industry depends, have come under increasingly frequent and sophisticated cyber-attack.

In part, this is a consequence of the inevitable convergence of Operational Technology (OT) with Information Technology (IT). As in all spheres of computing, the advantages of increased network connectivity through open standards such as Ethernet and TCP/IP, as well as the cost savings derived from replacing dedicated proprietary equipment with off-the-shelf hardware and software, come at the cost of increased vulnerability.

However, while the impact of a security breach on most IT systems is limited to financial loss, attacks on ICS have the added potential to destroy equipment, threaten national security, and even endanger human life.

With this critical distinction also comes a troubling difference in the profile and motivations of potential attackers. While the lion's share of modern cybercrime is motivated by financial reward, ICS have recently become attractive targets for terrorism and cyber-warfare. As a consequence, the financial and human resources available to its perpetrators can be an order of magnitude greater than those of conventional cybercriminals. This is especially true of highly targeted state-sponsored attacks, of which STUXNET (first appearing back in 2010) is considered one of the most sophisticated examples so far.

The purpose of this solutions guide is to show how, in spite of these and many other challenges, Fortinet's Solutions can help to ensure the safety and reliability of ICS - and in particular those employing Supervisory Control and Data Acquisition (SCADA) - through the application of standards-compliant multi-layered network security.

Potential Vulnerabilities

Due to their unique history and conception, separate from the evolving world of IT, ICS present a number of unique challenges:

- Inherent lack of security: Much of the technology underpinning ICS, while extremely robust and reliable, was never designed to be accessible from remote networks, and so security relied instead upon restricted physical access, and the relative obscurity of its components (e.g. RTUs, PLCs etc.) and their (mostly serial) communications protocols (e.g. Modbus, RP-570, Profibus, Conitel etc.).

- The "air-gap" fallacy: The superficially seductive idea of creating an "air-gap" between the ICS and all other networks is no longer realistic for the vast majority of real-life applications. As more and more of today's ICS components rely on software updates and periodic patching, it is now virtually impossible to avoid at least occasional data transfer into the ICS. Even in the absence of permanent network connections (or those employing only unidirectional devices such as optical data diodes), 'air-gapped' networks are still vulnerable to the connection of infected PCs or storage devices such as USB drives (one of the infection vectors of STUXNET).

- Expanding Attack Surface: As proprietary, dedicated solutions are replaced with off-the-shelf hardware and software, employing open standards such as Ethernet, TCP/IP, and Wi-Fi, the number of potential vulnerabilities increases exponentially. The recent proliferation of mobile devices together with trends such as BYOD only exacerbate the problem further.

- Continued use of outdated hardware and software operating systems (sometimes pre-dating even the very notion of cybersecurity) which may be incompatible with standard modern defenses such as anti-virus software.

- Infrequent updates and patching due to the complexity, cost, and potential service disruption entailed. It is not always practical, for example, to interrupt a plant's operations whenever one of its operational servers needs patching.

- Large numbers of simple, unsecured telemetry devices such as sensors and pressure gauges, whose data, if manipulated, could nevertheless carry huge consequences for the safety and reliability of the overall system.

- Use of embedded software written with scant adherence to the security techniques and best practices of modern coding.

- Insufficient regulation of component manufacture and supply chain, introducing the possibility of equipment compromise, even prior to installation.

- Limited Access Control / Permission Management: As previously isolated or closed systems have been interconnected, the controls imposed on exactly who can access what, have not always kept pace with IT security best practice.

- Poor network segmentation: The standard security practice of partitioning networks into functional segments which, while still interconnected, nevertheless limit the data and applications that can overlap from one segment to another, is still underutilized within ICS as a whole.

- Lack of security expertise among the engineers who have traditionally designed and maintained the systems.

Addressing the Problem

The good news is that in recent years, the inherent problems and vulnerabilities of ICS have become more widely recognized, and the first steps have now been taken to rectify them.

One way this is occurring is through the help of government bodies such as the The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) in the US, and the Centre for Protection of National Infrastructure (CPNI) in the UK, both of which publish advice and guidance on security best practice for ICS.

Another way is through the definition of common standards such as ISA/IEC-62443 (formerly ISA-99). Created by the International Society for Automation (ISA) as ISA-99 and later renumbered 62443 to align with the corresponding International Electro-Technical Commission (IEC) standards, these documents outline a comprehensive framework for the design, planning, integration and management of secure ICS.

Although still a work in progress and some way from addressing all vulnerabilities at their most fundamental level, the standard provides practical guidance, such as the model of 'zones, conduits, boundaries and security levels', through which to address the most pressing deficiencies of ICS network security.

Implementation of the zones and conduits model, which is recommended by both ICS-CERT and CPNI, can greatly reduce the risk of intrusion, as well as the potential impact should such a breach still occur.

The basic strategy outlined in the standard, is to segment the network into a number of functional 'zones' (which may also include sub-zones), and then to clearly define the 'conduits' as all essential data and applications allowed to cross from one zone to another. Each zone is then assigned a security level from 0 to 5, with 0 representing the highest level of security and 5 the lowest. Strict access controls can then be imposed limiting access to each zone and conduit based on the authenticated identity of the user or device.

This is a strategy that maps extremely well to the range of capabilities delivered by Fortinet's Enterprise Solutions, and in particular the Internal Segmentation Firewall (ISFW).

Securing ISC / SCADA with Fortinet

As with any effective security implementation, the first step is to fully assess the business and operational risks and to define an appropriate strategy commensurate with those risks. A major part of this will include defining the zones, conduits, boundaries and security levels outlined in IEC-62443.

This will typically look something like the network represented in figure 1.

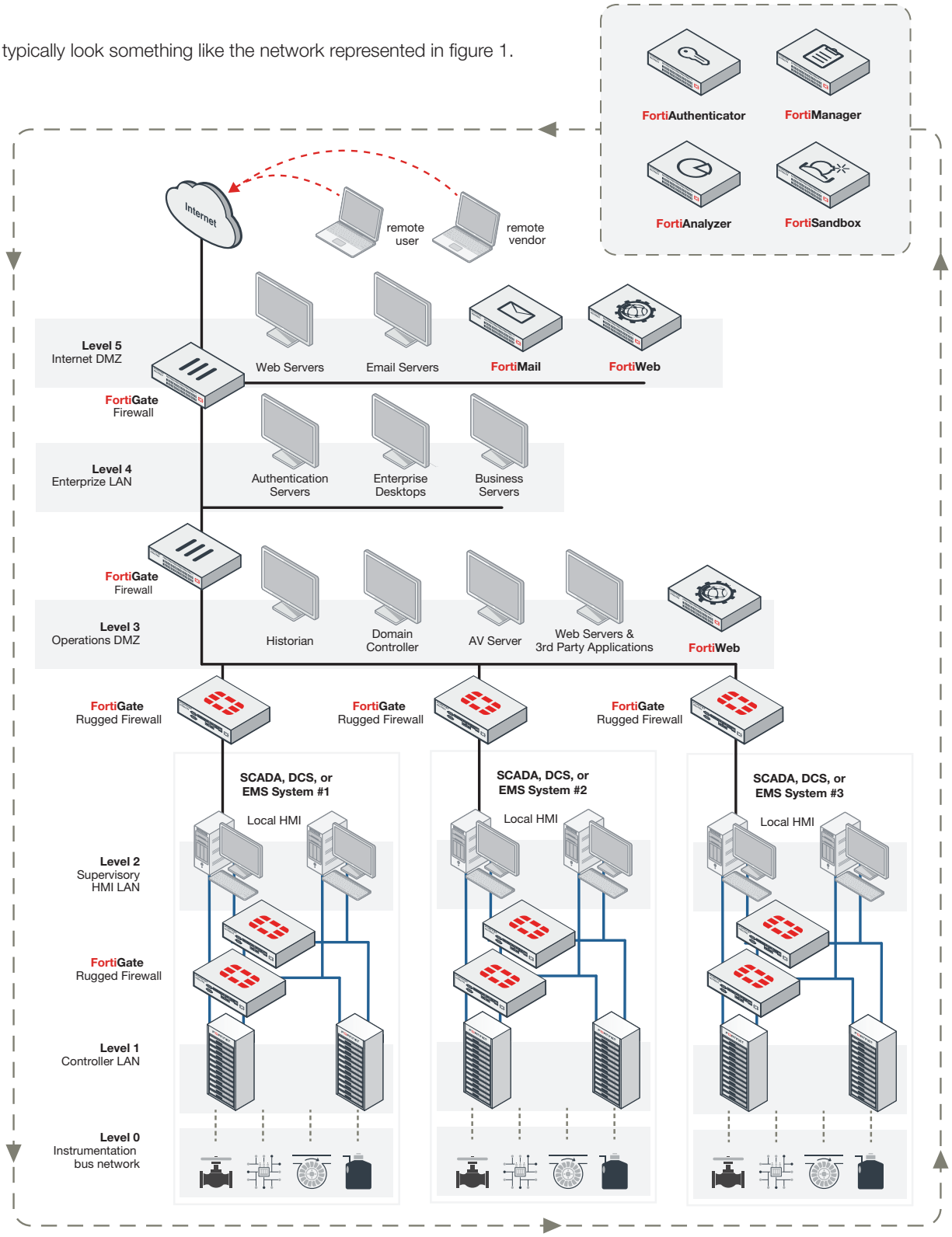

Figure 1: Security levels as depicted in the ISA S99 standard

Comprehensive multi-layered Security

With its multi-layered defense in depth, high availability design, and optional rugged form-factor, the FortiGate range of security appliances is the perfect choice for implementing the zones and conduits model, no matter how critical the ICS infrastructure, or how harsh the environment.

Using the deployment mode of "**Internal Segmentation Firewall**" (ISFW), which combines Functional and physical segmentation, the FortiGate combines advanced high-performance firewall functionality and robust two-factor authentication, with anti-virus, intrusion prevention, URL filtering, and Application Control. With a wide selection of high speed LAN interfaces and the hardware acceleration derived from its custom ASIC design, the FortiGate has been proven to deliver inter-zone performance in excess of 100Gbps.

Using the granular security policies available with FortiGate's ISFW deployment mode, ICS zones and conduits can be enforced based on criteria such as user identity, application, location, and device type. In this way, the FortiGate™ can effectively lock down each zone, ensuring that only legitimate, prescribed traffic, originating from authorized endpoints can pass from one zone to another.

For an alternative implementation of sub-zones, the FortiGate and FortiSwitch™ appliances also support 802.1Q VLAN traffic tagging, although in most critical deployments, the ISFW mode provides greater isolation and containment and is therefore recommended over the use of VLANs.

The embedded security of these highly flexible and scalable products comes from a combination of their operating system, FortiOS™, the FortiAuthenticator™ and FortiToken™ authentication solutions, and the automated, 24/7, self-learning, continuous threat response resources of FortiGuard™.

Centralized Management, logging and reporting

Management of the infrastructure, which is all consolidated through the FortiGate, is accomplished via FortiManager™ and FortiAnalyzer™, combining centralized configuration with reporting, visibility, event logging and analysis, to create a comprehensive, real-time network monitoring and control center

Specific ICS- / SCADA-aware functionality

Using predefined and continually updated signatures, the FortiGate can identify and police most of the common ICS / SCADA protocols (see list below) for the purpose of defining conduits.

- Bacnet
- DLMS/COSEM
- DNP3
- EtherCAT
- ICCP
- IEC-60870.5.104
- Modbus
- OPC
- Profinet

This is done through the configuration of security policies in which multiple services, such as IPS, AV, and Application Control can be mapped to each protocol.

In parallel to this specific protocol support, additional vulnerability protection is provided for applications and devices from the major ICS manufacturers (see list below) through a complementary set of signatures.

- ABB
- Advantech
- Elcom
- GE
- Rockwell
- Schneider
- Seimens
- Vedeer Root
- Yokogawa

This provides a more granular application-level control of the traffic between zones and enables the FortiGate to detect attempted exploits of known vulnerabilities relating to any of the supported vendors' solutions.

Zone Access Control with FortiAuthenticator and FortiToken

Applying granular control of the access to each zone and conduit based on both user and device is the role of FortiAuthenticator's integration with FortiGate and directory services.

FortiAuthenticator User Identity Management Appliances provide Two-factor Authentication, RADIUS, LDAP and 802.1X Wireless Authentication, Certificate management and Fortinet Single Sign-on. FortiAuthenticator is compatible with and complements the FortiToken range of Two-Factor Authentication Tokens for Secure Remote Access enabling authentication with multiple FortiGate network security appliances and third party devices. Together, FortiAuthenticator and FortiToken deliver scalable, cost-effective, secure authentication to your entire network infrastructure.

Securing the Historian with FortiDB

All central databases present an attractive target for cyber-attack, but those underpinning ICS may be especially vulnerable since, due to their history, security may not have been a major consideration in their deployment and scripting.

To help assess the current security level, address any vulnerabilities, and monitor all subsequent access for suspicious activity, FortiDB provides a flexible policy framework through which to secure these critical resources.

Securing the Web-based HMI with FortiWeb

While the cost and usability benefits of controlling the ICS through a web-based console are self-evident, the impact of intrusion or compromise to the back-end is clearly much greater within this environment than for most other web-servers.

Using advanced techniques to provide bidirectional protection against malicious sources, application layer DoS Attacks, and sophisticated threats like SQL injection and cross-site scripting, FortiWeb adds another crucial layer to your ICS defenses.

Securing the #1 Attack vector with FortiMail

Although not specific to ICS or its components, unsecured Email – especially when combined with social engineering – remains the #1 attack vector for the majority of known threats.

Protecting against inbound attacks, including advanced malware, as well as outbound threats and data loss, FortiMail™ provides a single solution combining anti-spam, anti-phishing, anti-malware, sandboxing, data leakage prevention (DLP), identity based encryption (IBE), and message archiving.

Responding to Advanced Persistent Threats

Most of the discussion so far has focused on the detection and blocking of attacks through the use of signatures, yet this approach relies on having encountered some close variant of the threat before. With the extensive threat response resources of FortiGuard continually monitoring thousands of live customer networks around the world, this is extremely likely, but with the stakes for ICS intrusion so high, it is essential to also prepare for attacks which have yet to be encountered.

In such a scenario, it becomes crucial that the intrusion is detected rapidly, its propagation limited, and its impact minimized. Here, a critical component of Fortinet's Advanced Persistent Threat Protection Framework is FortiSandbox™, which is designed to detect and analyze advanced attacks that might bypass more traditional signature-based defenses.

Government Accreditation and Assurance

Compliant with US Federal Government standard FIPS 140-2 level 2 for Cryptographic Modules, and International Common Criteria certification EAL 4+, Fortinet delivers robust, field-proven, protection that has been evaluated and tested by numerous third-party organizations to the highest levels of any multi-layered security solution.

Summary

Adequately securing ICS presents many significant challenges, some of which clearly go beyond the scope of this solutions guide. Yet by following the best practices set forth by ICS-CERT / CPNI, and deploying government accredited solutions such as those of the Fortinet portfolio outlined above, the probability of a successful cyber-attack, as well as its likely impact on the ICS, can be greatly reduced.

With dedicated support for the ICS / SCADA environment as well as its proven success as a leading provider of multi-layered enterprise security, Fortinet is uniquely positioned to help our industrial customers overcome their security challenges and protect the safety and reliability of our most critical infrastructure and services.

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

Slovakia:
csr_sales@fortinet.com
+421.903.516.455

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