WHITE PAPER

Securing SCADA Infrastructure

Introduction

Supervisory Control and Data Acquisition, or SCADA systems are specialized computer networks and devices that work in concert to monitor and control key processes involved in the management of machinery, equipment and facilities. Measurements taken from a variety of sensors (temperature, pressure, flow etc.) are used to make decisions, for example; to open a valve and release water from a tank when it fills up, or to initiate an emergency shutdown of a nuclear power plant. SCADA systems are typically deployed in three main areas:

Industrial process management – manufacturing, production, chemical processes, power generation, fabrication, and refining industries

Infrastructure management – water treatment and distribution, waste water collection and treatment, oil and gas pipelines, electrical power transmission and distribution, large communication systems

Facility management – offices, data centers, airports, ships etc; monitor and control HVAC, physical access, and energy consumption

SCADA devices communicate with the control system using protocols such as DNP v3, ICCP and MODBUS. Management information and reports are passed to and from SCADA devices via the following interfaces:

Human–machine interface – the HMI allows an operator to view and react to process status and events

Supervisory system – computers which monitor and send commands to control devices and processes

Remote terminal units – RTUs convert signals from process sensors to digital data and relay them to the supervisory system

Communications infrastructure – connects RTUs to the supervisory system

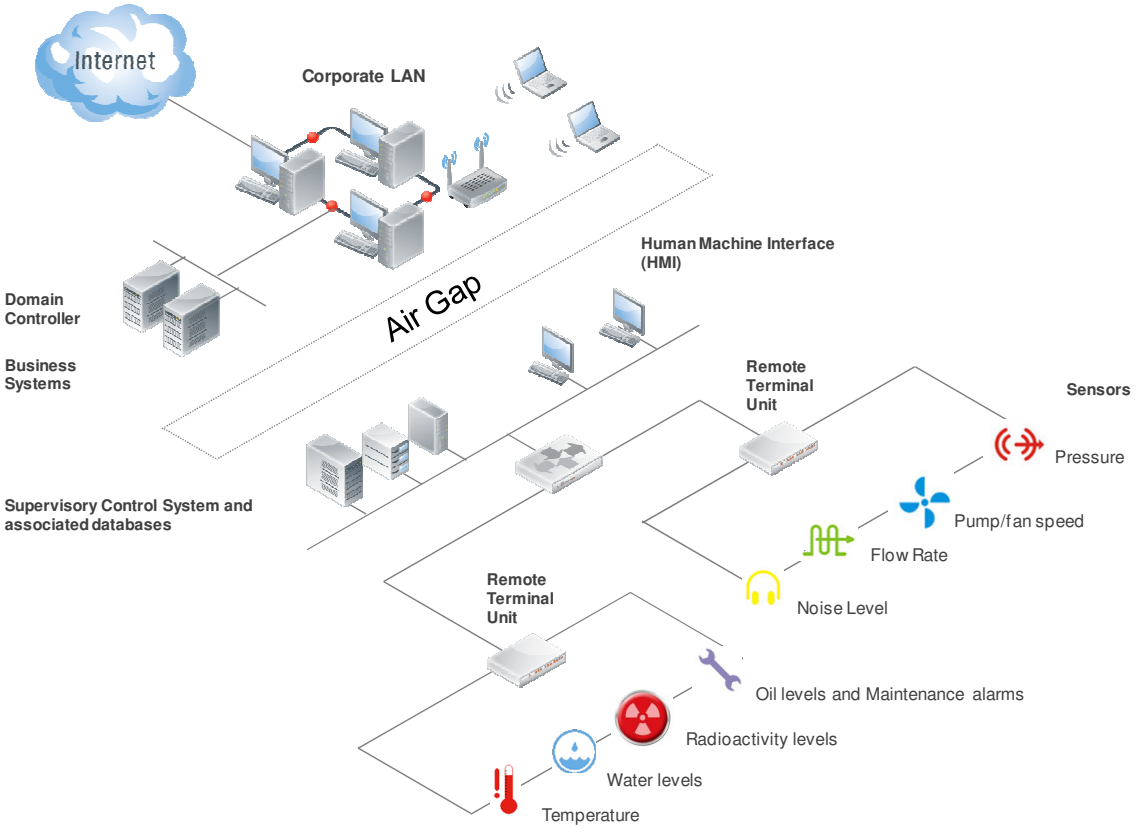

Figure 1: Industrial Control System with SCADA Network Architecture

The Importance of SCADA Systems

SCADA systems control some of the world's most critical national infrastructure including:

- Nuclear power stations
- Electrical distribution stations
- Water pumping and waste treatment plants
- Oil processing facilities
- Chemical plants

Loss of access to or misuse of these systems could result in severe physical damage, disruption and financial loss to a company. Therefore, security of these SCADA systems should be a high priority.

Traditionally, SCADA networks have been segregated from other corporate networks to minimize exposure to unsecure areas, such as the Internet. Recently however, more organizations are connecting SCADA networks with other potentially unsecure networks in order to cut costs, share operational information, or distribute ordering/billing data. Even when connecting SCADA networks to other networks is prohibited by corporate policy, incorrectly installed systems can unintentionally bridge networks together - putting SCADA networks and the processes they control at risk.

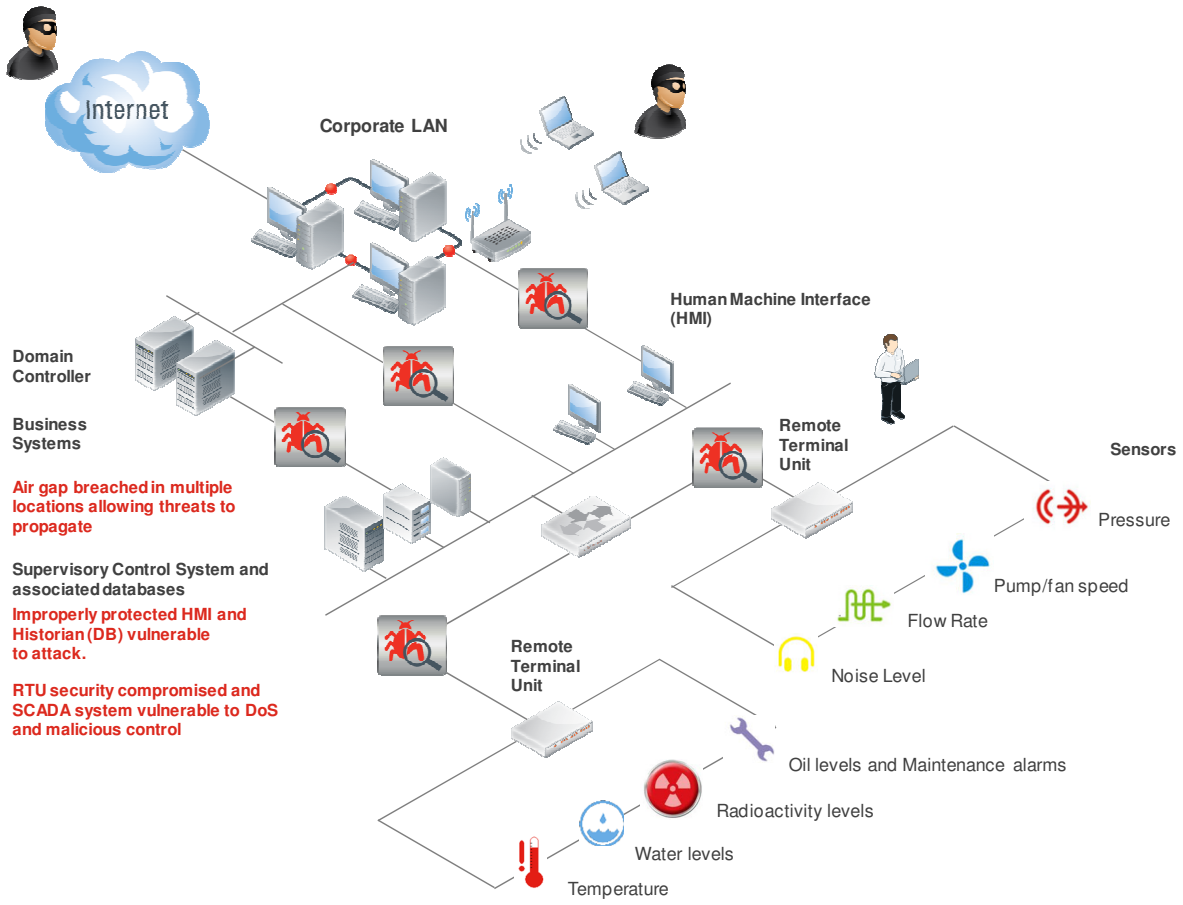

Figure 2: Security compromised SCADA network

Most SCADA protocols were never intended for use on publically accessible networks, and in some cases, not even on IP networks. MODBUS, a common SCADA protocol, was originally designed for use only within simple process control networks[1] to enable low speed serial communications between clients and servers. In order to communicate on an IP

[1] http://www.digitalbond.com/wiki/index.php/Modbus

network, MODBUS TCP merely encapsulates serial data within a TCP packet before sending it across the network. No additional protection has been added to secure communications sent using the protocol.

Often, security for SCADA systems consists of nothing more than a basic password which is passed in plain text from the control system to the RTUs. These unprotected passwords can easily be intercepted by malware and packet sniffers. In many cases, these passwords remain set to the manufacturer's default value. Some corporate IT policies require password changes on a monthly basis. However, this safety measure is rarely applied to SCADA systems because of the resources needed to manually change passwords on potentially hundreds of devices, and the risk to the company should these devices become inaccessible.

Threats to SCADA Systems

Security risk management can be defined as a balance between the impact of losing control of protected assets and the likelihood that a threat to the assets will be realized [2]. The level of risk to an asset can be stated as:

Risk = Threat x Vulnerability x Impact

The impact of losing control of protected assets can be determined by assessing the severity of the loss to the business or government entity. For example; malicious or accidental loss of access to a SCADA device could have minimal impact, such as the absence of a temperature reading or it could have a major impact, resulting in the total shutdown of a nuclear power plant. The impact will be specific to the system in question.

Threats are increasing daily as the systems have become a target for identification and attack. Something Fortinet have warned about and protected against however for several years.

Vulnerabilities have been increasing, partly due to the attention the systems are receiving. SCADA systems are often based on insecure legacy protocols that may or may not use adequate access controls e.g. default database passwords[3]. These systems are also subject to vulnerabilities in the host operating system (commonly Windows for the HMI). Patching of legacy systems can impact SCADA functionality so frequently run vulnerable, unpatched applications[4] on top of vulnerable operating systems. Following the September 11th terrorist attacks, these concerns prompted eminent US scientists to write an open letter to President Bush in which they warn:

"The critical infrastructure of the United States, including electrical power, finance, telecommunications, health care, transportation, water, defence and the Internet, is highly vulnerable to cyber attack. Fast and resolute mitigating action is needed to avoid national disaster[5]."

Main areas of concern include:

- Security and authentication in the design, deployment and operation of existing SCADA networks
- The premise that SCADA systems are secure because they use specialized protocols and have proprietary interfaces
- The premise that SCADA networks are secure because they have been physically secured
- The premise that SCADA networks are secure because they are not exposed to the Internet

Due to the mission-critical nature of a large number of SCADA systems, attacks on these systems have the potential to cause, either directly or indirectly, massive financial losses (through data theft or actual physical destruction), environmental disasters, and loss of life.

Richard Clarke, White House cyber security adviser from October 2001 to March 2003, also warns that "cyber terrorism is a significant threat" and that terrorist organisations are recruiting members with professional qualifications in areas such as Internet security and computer engineering[6]. Even as far back as 2002, the US and UK were aware of al-Qaeda's interest in SCADA systems following the capture of operatives with details of such systems in Afghanistan[7,8,9].

---

[2] http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf
[3] http://www.wired.com/threatlevel/2010/07/siemens-scada/
[4] See Browns Ferry example "Nuclear Plant Scrammed"
[5] http://pbs.gen.in/wgbh/pages/frontline/shows/cyberwar/vulnerable/
[6] http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/clarke.html
[7] US 'fears al-Qaeda hack attack' http://news.bbc.co.uk/1/hi/sci/tech/2070706.stm

Noted SCADA security expert Joe Weiss warns:

"My very, very, very strong feeling is if and when we get hit, we will never know why we were hit. All we will know is breakers are opening, valves are closing, certain things are happening. But we won't have a clue as to why." [10]

This was confirmed with great effect at the 2008 SANS Process Control and SCADA Security Summit[11], a gathering of more than 300 US, UK, Swedish and Dutch government officials, engineers and security managers from electric, water, oil, gas and other critical industries. There, US Central Intelligence Agency senior analyst Tom Donahue stated that:

"We have information from multiple regions outside the United States, of cyber intrusions into utilities, followed by extortion demands. We suspect, but cannot confirm, that some of these attackers had the benefit of inside knowledge. We have information that cyber attacks have been used to disrupt power equipment in several regions outside the United States. In at least one case, the disruption caused a power outage affecting multiple cities. We do not know who executed these attacks or why, but all involved intrusions occurred through the Internet." [12]

Companies often conceal security breaches such as those described above due to potential negative impact on their reputations. This makes it extremely difficult to assess the likelihood of attack, and therefore, the overall risk to SCADA systems. In a 2009 news article, a Department of Homeland Security Official was quoted as saying only that SCADA intrusions "are growing, and there were a lot last year." [13] However, some incidents have been well documented due to government reporting requirements or high profile court cases.

Slammer Worm Shuts Down Safety Systems at Nuclear Power Plant [14]

January 2003: A Slammer worm bypassed a network firewall at the Ohio Davis-Besse nuclear power plant (operated by FirstEnergy Corp.) disabling a safety monitoring system for nearly five hours. Even more disturbing, the Plant Process Computer crashed and was down for nearly six hours.

A Davis-Besse contractor had logged into an unsecured network, accidentally releasing the Slammer worm into the internal corporate network. A poorly documented T1 line had bridged the unsecured network with the internal corporate network, completely bypassing the firewall. Ironically, the firewall had been properly configured to block the port utilized by the Slammer worm. This was only one of multiple ingresses discovered by investigators into Davis-Besse's internal corporate network.

"This is in essence a backdoor from the Internet to the corporate internal network that was not monitored by corporate personnel," reads the April NRC filing by First Energy's Dale Wuokko. "Some people in the corporate network services department were aware of this T1 connection and some were not."

It is worth noting that the Slammer worm exploited a vulnerability in Microsoft's SQL Server 2000. This implies that vulnerabilities in the underlying operating system and applications were also inherited by the SCADA system.

Nuclear Plant Scrammed

April 2007: The US NRC reported that a safety VFD controller at the Browns Ferry nuclear power station stopped responding "due to excessive traffic on the plant ICS network". As a result, the nuclear reactor had to be "scrammed", or shut down in an emergency fashion by inserting control rods into the reactor[15]. The deluge of data was caused by a malfunctioning control device, known as a programmable logic controller (PLC). This in turn caused controllers for two of the water recirculation devices to lock up, forcing the operators to shut down the reactor.

Given the knowledge that PLCs are susceptible to such issues and with unauthorized access to the control network, it would be relatively easy for a rogue party to recreate this scenario.

---

8 "Cyber-Attacks by al-Qaeda Feared" Barton Gellman, Washington Post, June 27, 2002; Page A01

9 What are al-Qaeda's capabilities? http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/vulnerable/alqaeda.html

10 http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/vulnerable/scada.html

11 http://www.sans.org/scada08_summit/

12 http://www.sans.org/newsletters/newsbites/newsbites.php?vol=10&issue=5

13 **Wall Street Journal:** http://online.wsj.com/article/SB123914805204099085.html

14 http://www.securityfocus.com/news/6767

15 http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/2007/in200715.pdf

Project Aurora

September 2007: Declassified information about US Department of Homeland Security's Project Aurora was released. The purpose of the project, conducted in March of that year at the Department of Energy's Idaho lab, was to investigate the risk to electrical power systems by launching an experimental cyber attack. By changing the operating cycle of a generator, researchers managed to cause the generator to self-destruct, alarming the federal government and electrical industry about what might happen if such an attack were to be carried out on a large scale.

"What people had assumed in the past is the worst thing you can do is shut things down. And that's not necessarily the case. A lot of times the worst thing you can do, for example, is open a valve -- have bad things spew out of a valve," said Joe Weiss of Applied Control Solutions. [16]

These incidents show that SCADA networks can and have been actively targeted and attacked and that corporations and governments are aware of the problem and are preparing for such attacks[17, 18].

The highly advanced Stuxnet worm discovered in 2010[19], which includes the capability to reprogram PLCs hide the changes, is the first worm known to specifically target SCADA systems and critical industrial infrastructure. It was digitally signed with two authentic stolen certificates, making it difficult to detect, and could be upgraded remotely via peer to peer networking. Stuxnet used Windows vulnerabilities as the vector for infection, comprising multiple computers in the network via the host operating system. The virus payload was specifically targeted at interacting with SIMATIC WinCC and SIMATIC Siemens STEP 7 industrial process control systems and further more at motors running at a certain frequency, a very specific target.

Iran Admits Stuxnet Worm Infected PCs at Bushehr Nuclear Reactor Facility [20]

September 2010: Iran admits that the Stuxnet worm had infected at least 30,000 computers in the country. The worm, which researchers have dubbed the most sophisticated malware ever, targets Windows PCs that manage large-scale SCADA systems at manufacturing and utility companies.

"The studies show that few PCs of Bushehr nuclear power plant workers are infected with the virus," Mahmoud Jafari, the facility's project manager, told Iran's state-run Islamic Republic News Agency. Jafari denied that the worm had caused major damage to SCADA systems or that Stuxnet had delayed the reactor's completion.

However, Iranian state media later reported that the virus was mutating and causing widespread damage to industrial equipment in Iran.

The Stuxnet worm is estimated to have taken several man years to develop and uses complex programming techniques, cryptography and a command and control structure. Clearly, protections are needed to guard against threats such as Stuxnet and similar targeted viruses. This is not made any easier by SCADA vendors using inadequate security measures in their products including hard coded, publically known, database passwords[21].

The Fortinet IPS engine protects against the Windows vulnerabilities used by Stuxnet, while Fortinet antivirus protections block the virus and dll files used by the worm: A true defence-in-depth solution. More details can be found on the Fortinet Blog http://blog.fortinet.com/stuxnet-a-comprehensive-faq/

When Fortinet first introduced SCADA protection measures several years ago, SCADA security was not something you would hear about in the mainstream press. However, today, with the spotlight on SCADA systems following Stuxnet, have become a prime focus for both Government Agencies trying to ensure they are adequately secured and hackers trying to exploit them.

---

[16] http://www.cnn.com/2007/US/09/27/power.at.risk/index.html?eref=rss_topstories
[17] http://www.washingtonpost.com/wp-dyn/content/article/2010/02/16/AR2010021605762.html
[18] http://www.cpni.gov.uk/About/whatIs.aspx
[19] http://blog.fortinet.com/stuxnet-a-comprehensive-faq/
[20] http://www.computerworld.com/s/article/9188147/Iran_admits_Stuxnet_worm_infected_PCs_at_nuclear_reactor
[21] http://www.wired.com/threatlevel/2010/07/siemens-scada/

Stuxnet-style SCADA attack kept quiet after US gov tests[22]

May 2011: Security researchers decided to cancel a planned demonstration of security holes in industrial control systems from Siemens following requests from the German manufacturer and a security response team. Dillon Beresford, a security analyst at NSS Labs, and independent security researcher Brian Meixell were due to make a presentation – entitled Chain Reactions–Hacking SCADA – at the TakeDown Conference in Dallas on Wednesday.

Cyber-security of continent's power grid 'chaotic,' report warns [23]

November 2011: The cyber-security of the North American power grid is "in a state of near chaos," according to a report by a respected U.S. energy consultancy monitoring the industry's transition to wireless digital technologies.

The white paper by Pike Research reveals that a $60 smart phone application can bypass security measures and allow direct communications between the phone and some control systems (ICS) that regulate breakers, relays, feeders and the flow of electricity. The news comes on the heels of a warning from the cyber-security arm of the U.S. Department of Homeland Security that the hacker collective known as Anonymous appears intent on exploiting the ICS vulnerabilities within the energy industry.

The type of organizations utilizing SCADA, often manufacturing or energy and utilities, bring them under fire from hacking groups targeting large corporate or organizations with government ties. A recent US Department of Homeland Security Bulletin warned of interest in SCADA systems from the hacker group Anonymous [24] who have been targeting a large biotech company and posted to Twitter the results of browsing the directory tree for a Siemens SIMATIC SCADA system which they had been developing attack code for.

In an intriguing turn of events a recently reported breach of the Illinois water system from IP addresses originating in Russia which reportedly resulted in damage to a pump [25], was emphatically denied by the Department of Homeland security.

The Illinois SCADA hack: DHS said it never happened [26]

November 2011: According to a message to the official ICS-CERT (Industrial Control Systems-Computer Emergency Response Team) mailing list about 12 hours ago, both the FBI and the DHS are adamant no such breach occurred. The message also confirms the previously unnamed water authority to be the Curran-Gardner Public Water District as claimed in our previous report.

Whilst in this instance, it may be true that the pump failure was no more than a lack of proper servicing, it does highlight the concern there is about such an incident and the fact that this is possible and very likely to happen. In apparent irritation at attempts by the U.S. Department of Homeland Security (DHS) to downplay the threat of cyber-attacks on critical infrastructure in the alleged attack on the Illinois water plant, a self-styled vigilante hacker subsequently divulged details of other utility systems which could be easily accessed using remote access tools via the internet[27] to prove the risk, posting screenshots of the system to back up his claim.

Whilst they have been working on SCADA security for several years, developing signatures to protect against customers against attack, Fortinet 's Threat Research Team, FortiGuard Labs have predicted 2012 to be the year of SCADA vulnerabilities.

---

[22] http://www.theregister.co.uk/2011/05/19/scada_vuln_talk_cancelled/
[23] http://www.ottawacitizen.com/technology/Cyber+security+continent+power+grid+chaotic+report+warns/5715690/story.html
[24] http://www.theregister.co.uk/2011/10/18/anonymous_threatens_scada/
[25] http://www.crn.com/news/security/231903424/security-expert-says-illinois-water-system-hacked.htm
[26] http://www.itwire.com/business-it-news/security/51333-the-illinois-scada-hack-dhs-said-it-never-happened
[27] http://www.scmagazineuk.com/attacker-says-scada-system-was-protected-by-three-character-password/article/217323/

Fortinet's FortiGuard Labs Reveals 2012 Threat Predictions:- SCADA Under the Scope[28]

December 2012: For over a decade, Supervisory Control and Data Acquisition- (SCADA) based threats have been a concern, because they are often connected to critical infrastructure such as power and water grids, which are not always operating on a closed circuit. Many new human machine interface (HMI) devices that interact with these systems have Web interfaces for logging in that can be circumvented to access back end systems. Groups such as Anonymous have already found an assortment of Web-based vulnerabilities simply by picking targets and scouring code. In 2012, FortiGuard predicts new SCADA vulnerabilities will be discovered and exploited with potentially devastating consequences.

Securing SCADA Networks

There are several important steps that should be taken in order to secure SCADA networks:

- Patch host operating systems, applications and SCADA components
- Control application communications between SCADA networks and other networks
- Control application communications within SCADA networks
- Control what and who are allowed to interact with SCADA networks and systems
- Monitor all networks closely and react quickly to viruses and attacks

Unfortunately, due to their criticality, patching of SCADA systems is not always possible in the timescales needed to prevent an exploit. The next best solution is to use a defence-in-depth strategy by applying application layer security at both the host RTU and at the network level. What is required is a consolidated security system which offers tightly integrated multiple detection mechanisms including:

- Stateful, application aware firewalls
- Anti-virus detection
- Application control
- Web filtering
- VPNs
- Automated updates to antivirus and IPS signature databases
- Known SCADA Exploits already in antivirus and IPS databases
- Network Anomaly and DoS prevention
- Database protection
- Web application protection

Fortinet Security for SCADA Networks

Fortinet is the leading provider of Unified Threat Management (UTM) systems and rated by Gartner, IDC and Frost & Sullivan as the leaders their respective reviews. Fortinet provides firewall, secure remote access, antivirus protection, intrusion prevention, Web content filtering, anti-spam protections and much more; all in a single appliance. Fortinet has a range of security solutions designed specifically for a SCADA environment and to secure the SCADA network. Some features and protections that should be considered when planning security for SCADA networks have been summarized below.

Government Certifications

Fortinet has a long history of products which have been successfully validated against FIPS 140-2 and EAL4+ security certifications. The use of FortiOS in a FIPS approved mode of operation is a requirement of Government agencies and customers alike where assurances of data security are needed.

FIPS PUB 140-2 requirements are defined by the National Institute of Standards and Technology (NIST) – a US federal agency that develops new security standards. FIPS testing is designed to ensure that secure traffic is protected from

[28] http://www.fortinet.com/press_releases/121213.html

tampering and unauthorized disclosure. When using a FIPS-certified version of FortiOS in the FIPS-compliant mode of operation, weak cryptographic algorithms and unsecure management services are disabled to ensure that traffic is protected with the strongest methods possible. Cryptographic and integrity self-tests are also instated and executed when cryptographic encrypt and decrypt operations are performed. These measures mitigate any anomalous system activity that might introduce unforeseen issues. FIPS certification is also a prerequisite for US Government-sanctioned Common Criteria evaluations when specific security functional requirements of FortiOS are further scrutinized and tested.

Common Criteria focuses on functionality related to product security and management services. Common Criteria is an international standard (ISO/IEC 15408) which is recognized by over 20 countries world-wide. Common Criteria evaluations are conducted by ISO 17025 accredited labs who evaluate product design and subject FortiOS to thorough testing to ensure that security weaknesses and potential vulnerabilities are mitigated. Successful certifications confirm that the Target of Evaluation can be adopted by customers world-wide for use in environments where assurance in the deployed security solution is paramount.

High-Availability and Network Resilience

Availability of the SCADA network and its elements is critical for secure operation. All Fortinet products from the FortiGate-50B and up support high-availability (HA) deployment. Multiple devices can be configured in an active-passive or active-active mode to provide resilience in the case of failure. Should a device fail, session failover ensures a safe transition to the backup device. Where HA is not an option, a range of fail-open capable devices are available. Device level power resilience is available from the FortiGate-310B where an external AC to DC power supply can be connected as a backup to the main AC power supply. High-end devices support dual power supplies for internal power resilience. HA clustering also has the benefit of providing zero downtime upgrade capability, further minimising disruption to the network infrastructure.

At the network level, the FortiGate appliance range allows multiple WAN links to be connected, providing ISP level resilience. Multiple VPNs can be configured over these links to ensure secure, resilient ISP level redundancy. Where required, such as at remote or mobile locations, FortiGate devices can be configured to utilize a 3G modem to enable communication with the control system. This can be combined with other fixed line methods in order to provide backup “out-of-band” access to the SCADA network.

High Throughput / Low Latency VPN

SCADA systems are inherently insecure and their protocols are commonly easily intercepted in transit. To protect SCADA network traffic, Fortinet provides high throughput, low latency, VPN connections. Fortinet ASIC technology accelerates encryption and decryption processes and reduces the risk of data interception in a geographically diverse network.

The Fortinet SSL VPN can be utilized to deliver secure remote access to SCADA devices via Telnet (an inherently insecure protocol itself), SSH, RDP, VNC etc., further enhancing security while maintaining manageability of the SCADA network.

Transparent Mode

Management of SCADA networks is of critical importance due to the sensitivity of the systems they control. Changes and network downtime are to be avoided at all cost. In order to minimize deployment risk while still providing security, Fortinet includes a transparent deployment methodology, allowing the device to be inserted into the network as a layer 2 bridge. This can be done without any change to the existing layer 3 network structures.

Intrusion Prevention

Because Fortinet devices are installed on the wire they can act as both intrusion detection and active prevention systems, in other words they are able to intercept malicious traffic before it impacts the network. Intrusions are detected using the following methods:

Network anomaly and DoS mitigation – Detects unusual activity such as traffic that violates protocol standards or exceeds thresholds. This includes oversized ICMP packets, out of order TCP packets (FIN without SYN), and SYN floods or other packet storms which indicate a denial of service attack, such as the one that affected the Browns Ferry Nuclear Power plant.

Signature detection – Fortinet provides worm IPS signatures to protect against network propagation (such as that responsible for the Davis-Besse nuclear power plant shut down and Stuxnet propagation and C&C activity), Windows, Linux and UNIX signatures to protect against vulnerabilities in unpatched operating systems, and application signatures to protect against application vulnerabilities such as MS SQL, IIS, Apache, Exchange etc.

Fortinet uses SCADA IPS signatures developed both in-house by the FortiGuard Threat Research team and in collaboration with industry. These signatures protect against vulnerabilities in MODBUS, ICCP, DNP v3 and other proprietary SCADA protocols. Additionally, the system protects against host OS and application vulnerabilities and can detect dial home activity of many botnets (see Application Control below). As Fortinet develops new signatures, real-time updates are dynamically pushed to FortiGate appliances, ensuring that they are always up-to-date.

Application Control

Application Control detects and restricts application use on the network based on behavioural analysis and classification. There are over 1600 different applications in the database including P2P, remote access, bots, etc. Applications can be denied by default and allowed on a case-by-case basis, useful for locking down highly critical networks.

A specific application class for SCADA allows protocols such as DNP v3 to be allowed or blocked but additionally for DNP v3 reads/writes to be allowed or denied as required. Using the default deny policy, all applications that do not match the SCADA description can be blocked by default whilst allowing the SCADA traffic to pass unimpeded, regardless of which port is being used. The FortiGuard Threat Research team are also available to develop custom applications detections on request.

Network Antivirus

To stop the spread of viruses around an organisation, Fortinet provides network-based virus scanning for HTTP, FTP and email protocols. With high-speed ASIC acceleration, you can be assured that your network will be protected without impacting performance.

VLAN Support

While not a best practice for high-security networks such as those carrying SCADA traffic, VLANs are often employed to keep SCADA and corporate traffic separate using the same physical network to reduce cost while enhancing security. All Fortinet devices support 802.1Q VLAN traffic tagging.

Multiple Networks / DMZs and Virtual Firewalls

Even entry level Fortinet devices have the ability to create multiple networks, enabling segregation of SCADA and corporate data traffic at the physical interface or VLAN level. This is critically important where business systems from the corporate network interact with SCADA system components, breaching the network security “air gap”. If direct connectivity is unavoidable, it should at least be secured from attack.

Another important benefit of multiple network segments and DMZs is at remote sites where an engineer may require Internet access for email or other communication. Should an engineer logon from an infected laptop which attempts to scan, infect or breach the SCADA network, this will be prevented and logged. Corporate security policies can also be applied to restrict access to downloadable content by category or to block downloading of malicious content. To further increase security, networks can be segregated using Virtual Domains. VDOMs logically partition a physical firewall, ensuring that traffic cannot traverse between networks.

Identity Based Policies

A key requirement of standards provided by organisations such as ISA99, CPNI and NIST is to segregate networks and only allow authorised users to access SCADA systems. Providing a totally separate network for these users may not be feasible so users need to be identified and given access based on their user credentials. With Fortinet Identity Based Policies, credentials such as AD login can be harnessed to provide user or role based access control to the required resources.

Ruggedized Form Factor

Fortinet have a range of products designed for deployment within harsh environments common to SCADA deployments such as manufacturing locations, electrical sub-stations etc. These devices include protection against electromagnetic interference, a wide range of operating temperature and extended shock protection.

Wide Range of Products

Fortinet offers a wide range of products - from small office to carrier class devices - all with robust multi-threat protection capabilities. This allows Fortinet to deliver the right level of security at the right price point for any size business or application. With cost-effective entry level appliances offering full security functionality, Fortinet devices can be deployed at all points in a SCADA network, even at RTUs, providing consolidated, high-speed protection for the entire network.

Centralized Management, Logging and Reporting

Fortinet offer a wide range of appliances to protect the core and the distributed RTUs. With the potential for a large number of devices, FortiManager is essential to simplify management, reduce operational costs, enable separation of duties and deliver change control across a large Fortinet estate. FortiAuthenticator centralizes log collection and reporting delivering visibility of threats across the whole network as well as detailed reporting and trend analysis.

Database Security

At the core of all SCADA systems will be a management system with a backend database, sometimes referred to as the historian. Often database administration will not be a core function of the person managing the SCADA infrastructure and as such, it may end up deployed in an insecure fashion. Default administrator passwords, vulnerable supplied applications and poor configuration can all lead to insecurities in the database and ultimately the whole system. FortiDB enables you to quickly asses the security level of your database and once steps have been taken to rectify any security issues, will inform you if your database systems deviate from this secure state.
In addition to this vulnerability detection capability, the solution also allows you to monitor the database for unusual activity within the database; e.g. access from unusual locations, unusual times, changes of data types, querying of large volumes of data and to alert appropriately.

Web Application Security

Web-based HMIs (Human Machine Interface, the SCADA GUI) are becoming more and more popular due to the lower cost, and flexibility of development, cross platform nature and familiarity and ubiquity of the browser. The benefit of web based applications means they can be easily accessed remotely; however this can also be the downfall of a SCADA system. FortiWeb web application firewall protects web-based applications and internet-facing data. Automated protection and layered security protects web applications from sophisticated attacks such as SQL Injection, Cross Site Scripting attacks, buffer overflow exploits and data loss.

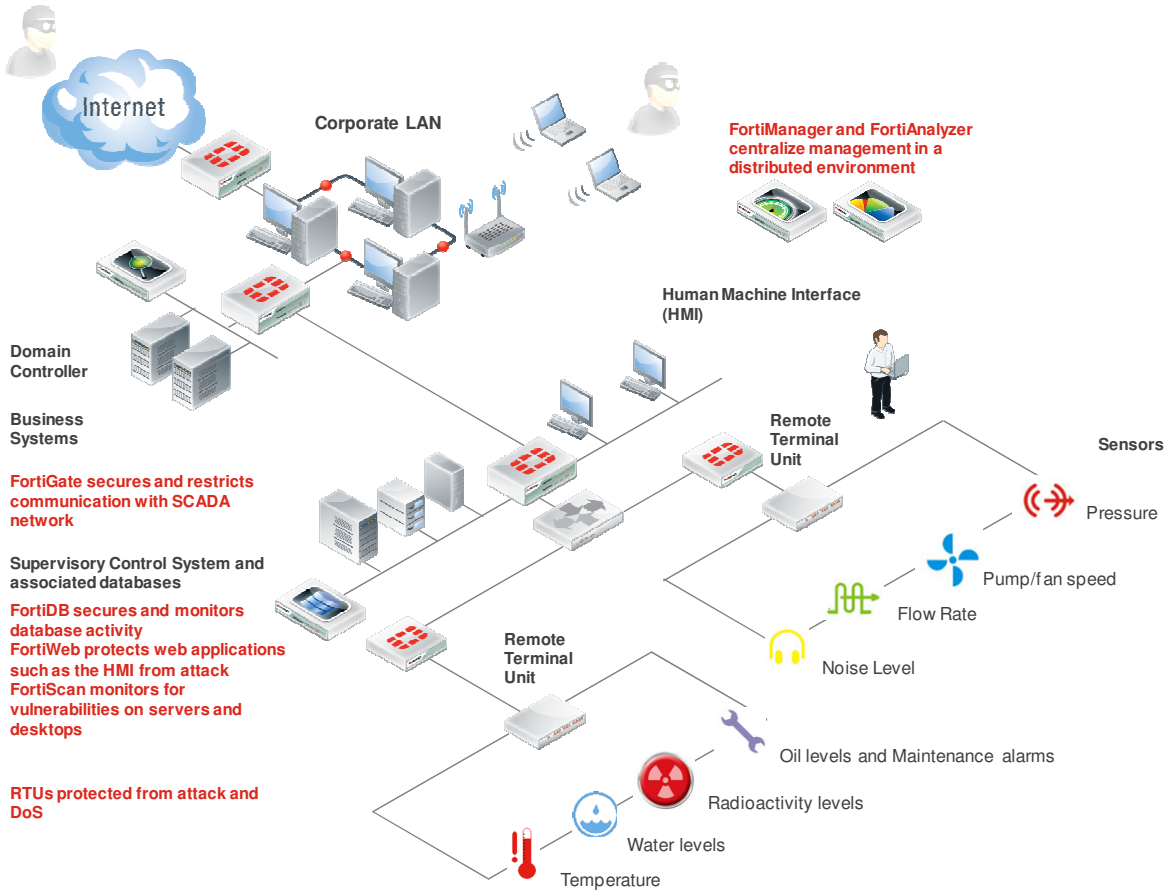

Figure 3: Fortinet secured SCADA network

Summary

It is clear that steps are being taken to secure SCADA protocols, however immediate action is required to prevent exploitation of insecure legacy protocols as well as the underlying insecure host operating systems. SCADA systems often cannot adhere to the corporate patching regime due to the risk of instability, so stringent external security must be applied.

Fortinet secures SCADA systems with a complete range of network security services designed specifically for SCADA including data leak prevention, wireless network security, intrusion protection, application control, secure remote access and firewalling services. With FIPS 140-2 and Common Criteria EAL4+ certification, Fortinet are an ideal partner to help you meet such critical security requirements. FortiGate unified threat management provides true defence-in–depth capabilities to "virtually patch" vulnerable systems, minimising disruption to the SCADA network. With a wide range of products, Fortinet delivers protection to all areas of the network; from low-end appliances to directly protect RTU/PLU devices to powerful, high performance, low latency systems that aggregate VPNs from remote locations, protect control systems, and mitigate risk at network borders. With FortiDB securing your database assets, and FortiScan providing desktop and server vulnerability detection and patch management and FortiWeb securing web based HMI systems, Fortinet are the only security vendor with the breadth of products required to provide cost–effective, end–to-end security for your most complicated and critical network.

GLOBAL HEADQUARTERS
Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1.408.235.7700
Fax +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE – FRANCE
Fortinet Incorporated
120 rue Albert Caquot
06560, Sophia Antipolis, France
Tel +33.4.8987.0510
Fax +33.4.8987.0501

APAC SALES OFFICE – SINGAPORE
Fortinet Incorporated
61 Robinson Road, #09-04 Robinson Centre
Singapore 068893
Tel +65-6513-3730
Fax +65-6223-6784

WP-SCADA-R2-201112