CONTROL ENGINEERING

Lessons Learned: Making Industrial Networking Better.

Sponsor Profile 2

NERC Assante Interview 3

Cyber Security: the Human Factor 6

Control Network Security Lessons From Stuxnet 8

Cyber Security Standard Aims at Critical Infrastructure in Process Industries 11

White Paper: Smart Grid 13

Sponsor Profile

NERC Assante Interview

Cyber Security: the Human Factor

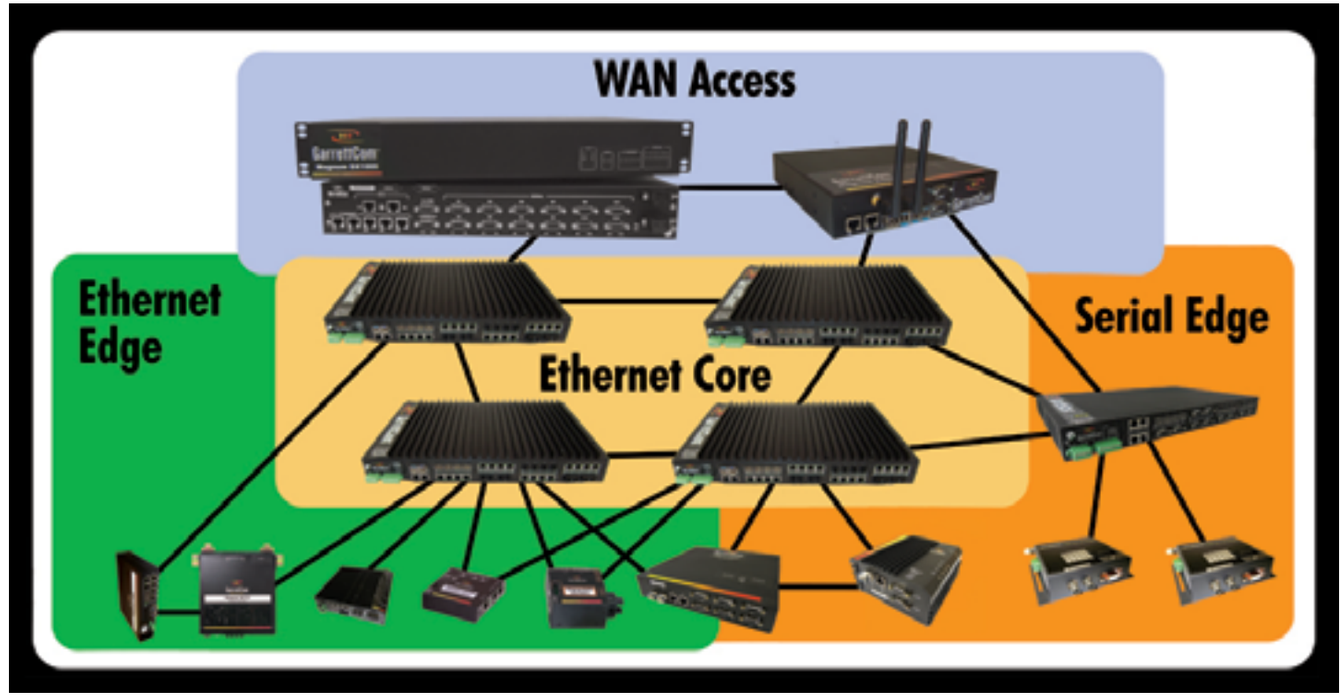
Control Network Security Lessons From Stuxnet

Cyber Security Standard Aims at Critical Infrastructure in Process Industries

White Paper: Smart Grid

GarrettCom®: Industrial Networking at its Best™.

With an installed base of more than 10 million node connections, GarrettCom®, Inc. is an industry



leader in providing premium networking solutions for challenging industrial environments, including power utility substations, video surveillance, transportation, industrial automation, and mobile networking applications in trains, tanks and other environments subject to shock and vibration. Today the company works with 75 percent of the top 100 power utilities in North America, as well as top-tier industrial system integrators worldwide. A wholly-owned subsidiary of Belden®, Inc., it has been producing reliable innovative industrial networking products, designed and manufactured in the U. S. A., since 1989.

GarrettCom's Magnum™ line of Ethernet™ switches, routers, terminal servers, and wireless communications products provides a comprehensive industrial network architecture encompassing a switched Ethernet core, distributed edge devices for both Ethernet and Serial protocols, and secured connections to various WAN services. The Magnum product line offers one of the broadest selections of hardened switches and routers, including PoE connectivity options, to industrial facilities around the world, and is noted for its configurability and ease-of-use GUI-based management software. The company is ISO 9001 certified for networking products design, marketing and manufacturing.

Well regarded by the industry as a thought leader in industrial networking issues, GarrettCom has published more than 50 whitepapers on industrial networking topics and is expert at innovative solutions derived from integrated industrial applications.

END

Sponsor Profile

NERC Assante Interview

Cyber Security: the Human Factor

Control Network Security Lessons From Stuxnet

Cyber Security Standard Aims at Critical Infrastructure in Process Industries

White Paper: Smart Grid

Cyber security advice from NERC

In an interview with Control Engineering, Michael Assante, chief security officer of NERC, offers some observations and practical advice about the industrial cyber security climate.

Author, Peter Welander, Control Engineering

In 2009, Control Engineering cyber security contributor Matt Luallen caught up with Michael Assante, chief security officer of NERC at the SANS Institute SCADA Summit.

CE: What is NERC?

Assante: Just to give everyone a quick introduction, NERC is the North American Electric Reliability Corporation. We're a self-regulatory organization made up of our stakeholders and professional staff who work towards ensuring reliability of the North American bulk power system.

CE: In the auspices of cyber security, for NERC specifically, there are the critical infrastructure protection standards and there are a number of asset owners that are being regulated by this. In 2008 the GAO identified 18 critical infrastructures. Many of our readers are involved in other areas that could eventually be designated as critical infrastructure that would fall under these standards moving forward. Those could include water and waste water treatment, other energy sectors, certain areas of manufacturing, aviation, transportation, railroads, and others. What can you say to try to prepare some of these other entities as to what they may have to deal with?

Assante: That's a great observation. I think there are really two things to think about when it comes to CIP standards: One you alluded to when the GAO did a survey of the 18 CIKRs, and they looked at what the requirements are that the different energy sectors are driving towards. They looked to see if the CIP standards were unique and if they were the only requirements specific to control systems that would fall under the environment of operating the electric system. That's important to note because we're really pioneering a model for how to protect infrastructure relative to security risk, and cyber security risk in particular. That's going to have an impact on the market, it's going to have an impact obviously on the owners and operators, those folks that are actually in the regulatory regime that we have, who have to adhere to these requirements. In the bulk power system, that includes not only transmission operators, but providers and generation, so the technology cuts across the landscape of real traditional SCADA systems and SCADA EMS. It also includes industrial control system technology you might find in a generation plant or facility. So the impact to the marketplace is across technology disciplines, it's not only things like protection but also

SCADA and DCS platforms.

So I think you'll see the market evolve as people try to sell products into the power system. As a provider, you're going to want to understand the burden that the utility or the purchaser will have in bringing the technology into the environment and making it CIP compliant. I hope that providers are seeing this as an opportunity. Some vendors are very proactively looking at that and understanding the requirements so when they design their systems, they can design them to integrate well into environments that need to be CIP compliant. They're thinking about, 'How do I provide more security in my systems for my buyers,' and I think that that will be a benefit for all other sectors. If you're selling a control system that is used in a power application, it might also easily be used in a water treatment or a waste water application as well, so if more security gets delivered to the end customer, it's going to help all sectors.

I think that the second thing to consider is that as the electric sector learns its lessons and improves its standards and continues to live in this area, other sectors that are anticipating similar regulation will start moving that way, depending on how the federal regulatory scene looks. So you've got to consider that as we gain some ground, hopefully we'll learn some lessons and the other sectors can incorporate those lessons. We provide a model, but I would suspect that no area should think that it wouldn't be facing the same type of

Lessons Learned: Making Industrial Networking Better.

Sponsor Profile

NERC Assante Interview

Cyber Security: the Human Factor

Control Network Security Lessons From Stuxnet

Cyber Security Standard Aims at Critical Infrastructure in Process Industries

White Paper: Smart Grid

circumstances in the near future. Hopefully as we advance, we'll be pretty open about how the system is working. It's a very transparent process, which is one of the strengths of the self-regulatory model. It is very open and deliberate.

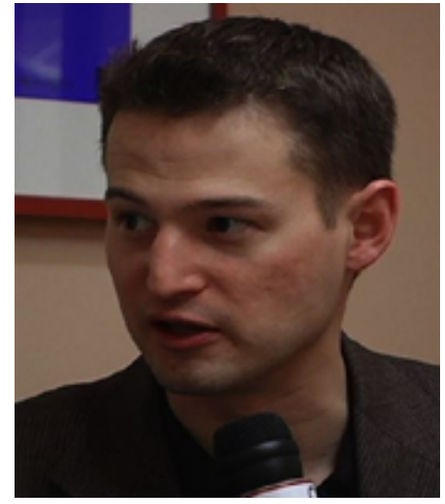
CE: That said, as we look at typical control systems, they are highly reliable, and highly safe in nature. Looking at the plants involved, often there are lives at stake, and once again the question is being knocked around, isn't security already addressed with safety in the system? How would you go about trying to address that type of question? Are you trying to say there's a difference between the two?

Assante: Well, I believe we're in a time of really rapid technological change, especially in some of these industrial environments. You can think about how telecommunication has changed in the last ten years. We're in a real change state where technology is doing two things: first, it's redefining the relationship between the provider and the customer, and that's very exciting. There are lots of benefits, and further efficiencies to consider, but by this pace and scale of change that's occurring it's redefining all of our assumptions, including the engineering assumptions that relate to protecting systems and safety. In the electric sector, clearly, protection of the system is a key mandate. We have always, and we still do, relied upon redundancy with the new system. It's an ac network that gives us some level of protection and survivability for contingencies, but when you start rapidly changing technology, you have to consider how that technology could be exploited. That becomes the key way to start, that's why your assumptions have to start changing. So, if your operating safety controls are embedded in the technology, software or hardware, then you have to start re-examining it. Ask yourself, 'One the safeties I rely upon is truly a digital device, so what happens if attackers gain access to what was just a safety system before? What if they have access to both: the primary controls system and the safety system?' Under that circumstance the old assumption goes away. Now you have to say, 'Wait a minute, someone could manipulate the safety systems so that the set points are no longer what I thought they were.' They start setting up contingencies now that could result in great harm, or would do harm, and you know at the network level it's starting to redefine what was purpose-built protection, or purpose-built safety. There are lots of reasons to integrate them today, whether to integrate at the network level, or there's a mesh network and sensors are now only available. So the control system or the safety system is segregated now more by function than by true network segregation, or it's just logical controls. These are really important things to understand because, like you suggested, as your assumption changes it really changes how you need to think about risk and the system, and I believe technology is changing at that pace.

In the utility world, advanced metering technology and smart grid technology have some really unbelievable benefits associated with them. But I'll give you an example of where we've made a big philosophical assumption shift. Before we protected the availability of generation resources, mounting to the grid, the movement of power on the ac network, and the grid itself, but never really worried about load. But now, with new technology we can start using load response and start using demand response management to curtail load when needed in peak times during system stress. When you start relying upon those as safeties of the system, they become a set of technologies that create a potential vulnerability point. If somebody could get to them, make them go away all at once, or make them not available when we need them, then really you're looking at risk to the bulk power system from the very edge of the system. So for now, user loading represents a new potential risk to the system. So that's how technology in our industries redefines risk. I suspect that's occurring in every single critical infrastructure protection sector.

CE: So, let's turn to the idea of incident response. How can asset owners understand that they should look at what types of incidents may occur and plan beforehand, so that they know in given situations how they're going to respond. You can't plan for every type of situation, but if your architecture supports being able to respond for at least a few certain types of incidents, it's going to be that much better off. One simple example is preparing for air gapping in an extreme situation. Do you have any comments or recommendations here?

Assante: Yes, specifically to control systems, I think incident response is critical. A lot of times we're kind of



Lessons Learned: Making Industrial Networking Better.

Sponsor Profile

NERC Assante Interview

Cyber Security: the Human Factor

Control Network Security Lessons From Stuxnet

Cyber Security Standard Aims at Critical Infrastructure in Process Industries

White Paper: Smart Grid

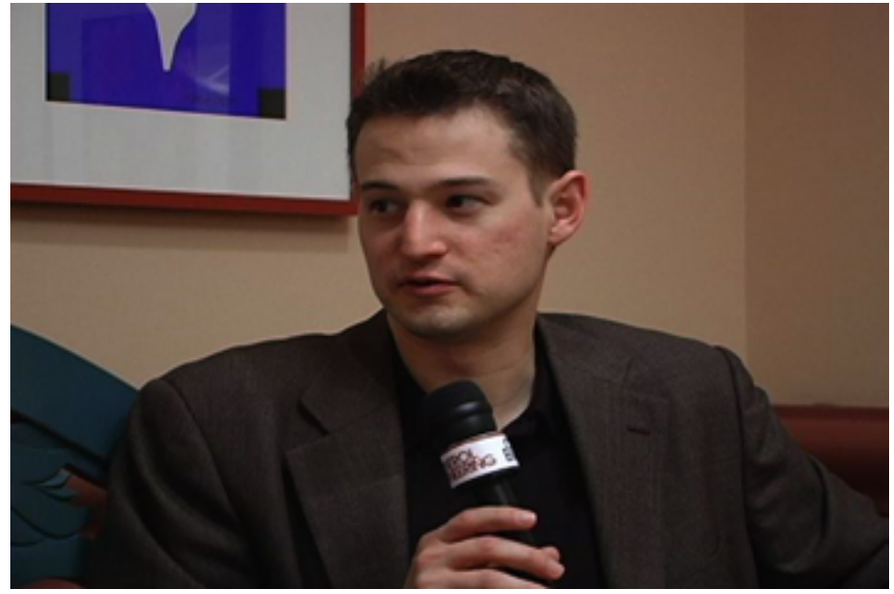
in this age of enlightenment, we're talking about prevention and security at the perimeter, and we're going to put a lot of investment and effort into that. But in the control system world you really have to have a strategy of designing a good incident response plan, and it starts with using scenarios to say, 'Well, what if this happened?' You have to take a consequence-based view to that in order for you to really start organizing your thinking for responding to incidents. You need to know the edge of that envelope. For example, could I lose a controller? Well that's one thing, but do I use the same controller on a large enough scale, and is there a way through, whether it's a compromise at a firmware level, that I have to worry about losing all of my controllers? And if I did lose all of my controllers, what does that mean to a plan for how we respond to incidents? So, while developing these scenarios you can do a tabletop exercise and consider what the consequences could be. That's a good starting point, and what you need to do is bring in the process managers, the business units, the technologists, and the support people together and say, 'Let's go through that exercise.'

I think you want to look at incident response in four main areas. First, you need to consider what your technical ability is to observe and categorize the situation that you're in, so when something is occurring in your area, how will you know about it? What's the key observable? So if you can identify those key observables, you know what to look for, and you know you're in situation 'A' instead of a situation 'D,' so you put the right response to the right incident. So that's an area for people to develop. They think it takes quite a bit of work, but it's the area that a lot of people need to address.

The second question is, 'How do I coordinate and communicate through an incident?' So, is it good enough that the facility itself starts the communication process or do I need to start alerting the supply chain? How quickly does that happen? Do I need to alert the rest of the business unit? For a utility example, I'm interconnected, so I need to alert my interconnected utilities, but then also what about through ICCP up to the control area? And then what's my responsibility in a broader sense to the ISAC or to government obligations? And so how to coordinate and communicate is an important element to an incident response plan.

The third part, which is an art, not a science, is how do we minimize the physical consequences to a technical incident within the system? It takes a unique thought process to get to a good answer there. In the utility example you'd be looking at a situation when you lose a specific link or node, you start thinking about how you would operationally try to reconfigure the system. The same thing can apply in another industrial control system environment. If I lost a part of the process, does that mean I could try to contain it within that sub-process and know that we could continue to operate at this level? Can I try to pull the electronic tethers away from other parts that may be compromised? Where are those controls and levers to start pushing buttons to start severing ties?

The final part of the incident response recovery side is understanding where the investment needs to be. What's on the shelf? What's not on the shelf? What's realistic in terms of authorities necessary to put resources to recover from a problem? That requires a real business continuity approach. There's a technical incident response element and then you have to back it up to the overall business continuity plan to make sure the two are aligned with each other, because the worst thing you can have is a plant that doesn't have the authority to spend the kind of money they need at the moment to get themselves to recover. If you haven't done the full business impact assessment, you don't realize you're actually losing X millions a day so therefore giving them these authorities makes a lot of sense. So, incident response is a real critical area. When looking at control system security that needs to be addressed.



END

Sponsor Profile

NERC Assante Interview

Cyber Security: the Human Factor

Control Network Security Lessons From Stuxnet

Cyber Security Standard Aims at Critical Infrastructure in Process Industries

White Paper: Smart Grid

Cyber Security: The Human Factor

You've installed state-of-the-art security equipment on your control system to keep out the bad guys. But do your people leave the front door open?

Peter Welander, Control Engineering

At the opening of an episode of NBC's sitcom, The Office, the corporate IT guy is sitting at Pam's computer, trying to flush out a virus as Jim and Pam look on.
IT guy: "Generally, it's not a good idea to click on any internet offers that you haven't requested. What was the exact offer?"
Pam: "It was for a video."
IT guy: "What kind of video?"
Pam: (embarrassed) "A celebrity sex tape."
Jim: "Really? What kind of celebrity?"
Pam: "Not relevant."
Jim: "How much did you pay for it?"
Pam: "Not relevant."
Jim: "You paid for it?!?"
Pam: "It all happened so fast!"
Their situation, while humorous, is all too real. Your people can be the weakest security link. In some cases an unhappy employee can cause deliberate sabotage, but these situations are less frequent than people doing stupid things. Or sometimes people fall for a social engineering scam that makes them open the door to a virus or hacker.

Here are four examples that illustrate key points:

No. 1: Imagine your office phone rings. The caller says he's from IT and asks you to help solve a network problem by changing your password. If you've had any cyber security training, you know that you really shouldn't do that sort of thing, right? The IRS did a test just like this. Here is a brief excerpt from the summary of results:

"The IRS has nearly 100,000 employees and contractors on approximately 240 computer systems and over 1,500 databases. Using social engineering tactics, we determined IRS employees, including managers, are not complying with the rudimentary computer security practices of protecting their passwords. As a result, the IRS is at risk of providing unauthorized persons access to taxpayer data that could be used for identity theft and other fraudulent schemes.

"We made 102 telephone calls to IRS employees, including managers and a contractor, and posed as computer support helpdesk representatives. Under this scenario, we asked for each employee's assistance to correct a computer problem and requested that the employee provide his or her username and temporarily change his or her password to one we suggested. We were able to convince 61 (60%) of the 102 employees to comply with our requests. Only 8 of the 102 employees in our sample contacted...the IRS computer security organization to validate our test as being part of an official audit."

No. 2: A hacker who was caught and convicted for breaking into VoIP systems said his job wasn't all that hard. Finding Web interfaces on devices using Google search strings was simple, but he still had to get past a password to do anything. As the hacker put it, "The way we got into them is that most of the telecom administrators were using the most basic password, 'Cisco' or 'admin.' They weren't hardening their boxes at all."

No. 3: One attack vector for hackers to get into a company is to scatter thumb drives around the parking lot and grounds of the subject company. People going to work find them and can't resist plugging one in. File names that show up sound interesting (a celebrity sex tape, for example) so someone will open one out of curiosity. A program launches that makes the person's computer contact the hacker and allows a way to get in. It all happens so fast.

This approach has been used both to break into systems, and as a test to see how well cyber security training has been engrained into individual employees. If you don't believe this is a way that malware spreads, remember Stuxnet? Here's an excerpt from an advisory distributed by Siemens last summer when it was trying to contain the problem: "Siemens was notified about the malware program (Trojan) that is targeting the Siemens software Simatic WinCC and PCS 7 on July 14. The company immediately assembled a team of experts to evaluate the situation and is working with Microsoft and the distributors of virus scan programs, to analyze the likely consequences and the exact mode of operation of the virus. It has so

Lessons Learned: Making Industrial Networking Better.

Sponsor Profile

NERC Assante Interview

Cyber Security: the Human Factor

Control Network Security Lessons From Stuxnet

Cyber Security Standard Aims at Critical Infrastructure in Process Industries

White Paper: Smart Grid

far been established that the Trojan, which spreads via USB sticks and uses a Microsoft security breach, can affect Windows computers from XP upward."

The handy thumb drive is considered a serious threat because it is a very effective medium for stealing data or injecting malware. While some suggest disabling auto-run options for thumb drives and CDs, others feel that isn't nearly enough protection. A more effective but drastic approach is to fill unused USB ports on a server with epoxy or make sure there are locked covers over any computer ports.

No. 4: More sinister are those unhappy employees who deliberately set out to cause problems. Consider the story of a former systems administrator at Medco Health Solutions who created a logic bomb and planted it in the company's network. The bomb would have disabled records in Medco's customer database spread over 70 servers that allows pharmacists to check customer's existing medication use before issuing a new prescription.

Yung-Hsun Lin, the administrator, allegedly wrote the code in October 2003, as he was expecting to be laid off. He set the code to execute the following April. Lin was not laid off, but left the bomb in place. When the day arrived, the bomb fizzled due apparently to coding errors. Lin fixed the problem and reset the bomb to go off in April 2005.

In January 2005, a co-worker stumbled across the malicious code, and the IT department removed it safely. Eventually it was traced back to Lin and he was arrested by FBI agents in December 2006. Medco estimates that it cost between $70,000 and $120,000 to clean up the problem. Had the bomb worked, the physical damage this could have done to patients due to medication problems is impossible to determine. Lin pleaded guilty and was sentenced in 2008 to 30 months in jail and ordered to pay $81,200 in restitution to his old company. At the time of the sentencing, U.S. Attorney Christopher J. Christie said, "Disgruntled or rogue employees are a real threat to corporate technology infrastructures and can cause extensive damage. The results of this prosecution send a message to systems administrators and employees, and industry should feel comfortable and confident in coming to us when just such cases arise."

Procedures vs. creating security culture

Procedures are important, but people have to understand their role in keeping a plant safe. The DHS reports that social engineering is one of the biggest attack vectors. Sean McGurk, director of the control systems security program (CSSP) for the U.S. Department of Homeland Security (DHS), says, "How often do we see vulnerabilities and exploits that are conducted as a result of poor operational practices because people don't understand the need for security."

Marty Edwards, Idaho National Laboratory DHS CSSP manager, outlines the kind of cultural change that needs to happen: "One of the biggest challenges we have in security—whether it's in control systems, or IT, or physical security—is creating that security culture, and you can do that regardless of the vintage of the equipment that you have. It's your personnel. It's your training. It's the culture that they operate in."

From a safety perspective, industrial and processing areas have had that culture for some time, says Edwards. "You don't do anything in a plant without thinking about what the safety ramifications are," he adds. "We must instill that same culture, so that before I do anything, I think about the security ramifications. Should I post a network drawing at a user group conference that contains all the most intimate details of our control system? That's a change that everybody can make immediately, and it costs a lot less than replacing equipment."

The moral of these stories is that technical solutions alone cannot secure a system. But on the other hand, even the best trained and conscientious people cannot stop a determined hacker from invading a weak system. Hardening involves people and systems. The two must work together to minimize vulnerabilities. If you want some ideas of how to suggest good security policies to technical and non-technical employees, the DHS offers some very practical and understandable tips at http://www.us-cert.gov/cas/tips/.

Peter Welander is a CFE Media content manager. Reach him at PWelander@cfemedia.com.

END

Sponsor Profile

NERC Assante Interview

Cyber Security: the Human Factor

Control Network Security Lessons From Stuxnet

Cyber Security Standard Aims at Critical Infrastructure in Process Industries

White Paper: Smart Grid

Control Network Security Lessons From Stuxnet

A UK Expert Describes How Stuxnet And Other Threats To Industrial Infrastructure Cyber Security Are Prompting National And International Action. Technology Update, February 2011, Monthly Control Engineering, North American Edition.

Dr. Richard Piggin, consultant - 02/03/2011

Industrial control systems have long life cycles. Older systems were designed with little or no regard for cyber security and are interconnected in ways never envisaged. The mistaken belief in "security through obscurity"—the use of specialized systems, protocols, and proprietary interfaces as the basis of secure systems—is obsolete in the wake of recent incidents. Add to this the increasing complexity, proliferation of access points, wireless communications and wider use of common operating systems, and wider use of the Internet, and it is understandable why governments are keen to promote cyber security.

Information on industrial protocols is widely available, and some systems have already been specifically targeted. These include the Modbus protocol and more recently the Stuxnet trojan/virus, which affected Siemens WinCC SCADA, Step 7 Programming Software and Simatic PLCs. While fixes were quickly developed, Stuxnet was a game-changer in terms of its complexity and reach, and as it and other breaches of security continue to be analyzed, governments are responding with general and sector-specific guidance to protect critical national infrastructures.

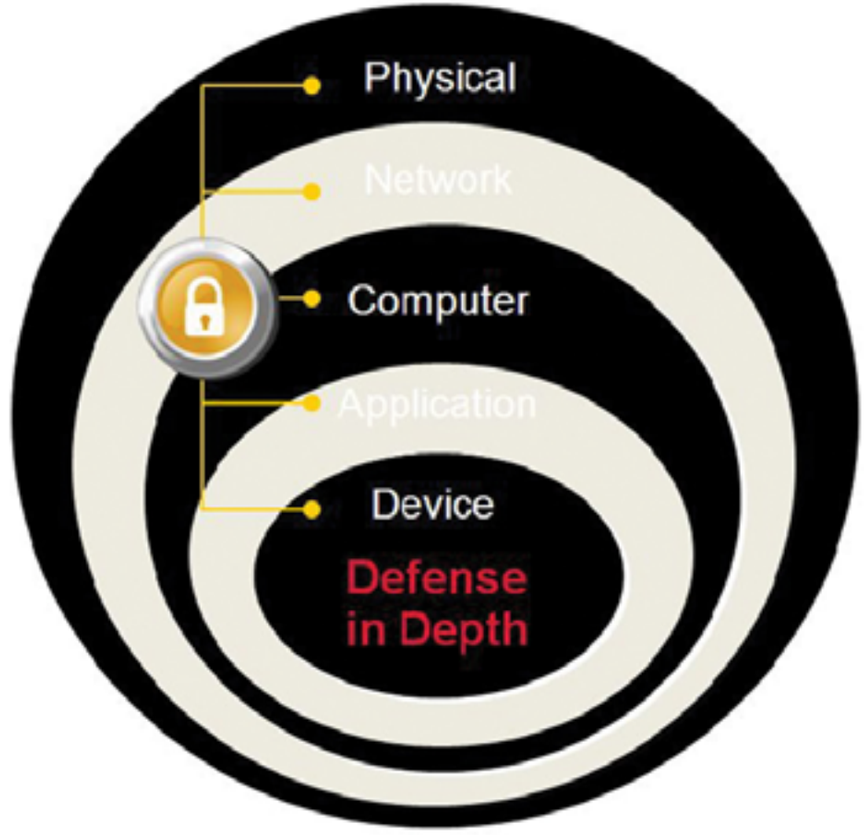
Critical national infrastructure

The critical national Infrastructure comprises facilities, systems, sites, and networks necessary for the delivery of the essential services upon which daily life depends. This covers nine sectors: communications, emergency services, energy, finance, food, government, health, transport, and water. Like the U.S. Department of Homeland Security, the UK's Centre for the Protection of National Infrastructure (CPNI) works with the operators of essential services and with lead government departments to identify critical national infrastructure and to help protect it.

An often cited example to illustrate the risk is the "drive-by wireless hacking" by an Australian ex-employee of a Queensland sewage treatment plant. He used his knowledge of the control system to hack the system 46 times and release millions of liters of waste into public waterways.

The CIA has confirmed a cyber attack caused power outages in multiple cities (including New Orleans in 2008). The CIA also provided information on intrusions into utilities that were followed by extortion demands. The U.S. government has been taking the potential reconnaissance of the power grid by Russia and China seriously, considering the potential for terrorist attack, and this year formed the United States Cyber Command. This group is responsible for directing the defense of U.S. Defense Department networks and conducting military cyberspace operations.

In the UK, the Centre for the Protection of National Infrastructure (CPNI) is the government authority that provides protective security advice to the national infrastructure. Specific SCADA advice is offered by the CPNI in a series of process control and SCADA security good practice guidelines. Much is a result of the work of the U.S. National Institute of Standards and Technology (NIST) and is sponsored by U.S. Homeland Security.



Sponsor Profile

NERC Assante Interview

Cyber Security: the Human Factor

Control Network Security Lessons From Stuxnet

Cyber Security Standard Aims at Critical Infrastructure in Process Industries

White Paper: Smart Grid

Stuxnet—an unusually complex threat

The Stuxnet trojan/virus is the first publicly known "worm" to target industrial control systems. The threat posed by Stuxnet has been portrayed as beyond anything seen before. Its goal was to sabotage a real-world industrial plant, not disrupt abstract IT systems. It was aimed at industrial control systems with the intention to reprogram PLCs in a manner that would sabotage the plant, hiding the changes from programmers or users.

Stuxnet has highlighted the potential to directly attack industrial control systems used in critical national infrastructure, including energy, water, and transport sectors. Research by Symantec (September 2010) showed that nearly 60% of the approximately 100,000 hosts infected by Stuxnet were located in Iran, with relatively high infection rates also seen in India and Indonesia. This has led to speculation that Stuxnet's goal was disruption of Iran's delayed Bushehr nuclear power plant, or the uranium enrichment plant at Natanz.

Stuxnet has been described by Symantec as one of the most complex threats the company has analyzed. Features include:

- Four zero-day exploits, which are exploits that are unknown, undisclosed to the software vendor, or for which no security fix is available. This is a rarity for any virus, and would be considered wasteful by most hackers.
- MS Windows rootkit, which is software that enables privileged access to a computer while hiding its presence.
- First-ever "PLC rootkit," which infected PLC programs while remaining undetectable.
- Antivirus evasion.
- Two stolen Taiwanese digital signatures to authenticate Windows software.
- Complex process injection and hooking code to prevent programmers from seeing the infected code.
- Network infection routines.
- Privilege escalation.
- Peer-to-peer updates.
- Remote command and control.
- Identified vulnerabilities

How does this virus spread? Since PCs used for control system programming are not normally connected to the Internet, Stuxnet replicates via removable USB drives—exploiting a vulnerability that enables auto-execution. It then spreads across the local area network via a Microsoft Windows Print Spooler vulnerability, and via a Windows Server Remote Procedure Calls vulnerability.

Stuxnet copies and executes on remote computers through network shares and Siemens WinCC database servers (SCADA software). It also copies itself into Siemens Step 7 PLC program projects and executes when a project is loaded, and updates versions via peer-to-peer communication across a LAN. Stuxnet communicates with two command and control servers originally located in Denmark and Malaysia to enable code download and execution for the updating of versions. Stuxnet may have the ability to change command and control servers, although this has not been observed as yet.

Inside the PLC

Stuxnet fingerprints specific PLC configurations that use the Profibus industrial network for distributed I/O. The particular configurations were gleaned using earlier versions of Stuxnet. If the fingerprint does not match the target configuration, Stuxnet remains benign. If the fingerprint matches, the code on the PLCs is modified with the infected programming software and the changes are hidden.

The modified code prevents the original code from running as intended and causing the plant equipment to operate incorrectly, potentially sabotaging the system under control. This is achieved by interrupting processing of code blocks, injecting network traffic on the Profibus network, and modifying output bits of PLC I/O. How this affects the individual plant system depends on how the control system is connected to the PLC and distributed network I/O via Profibus.

The future threat Stuxnet poses is as a blueprint for attacks on real-world infrastructure, providing generic methods to reprogram industrial control systems. However, the level of sophistication and complexity of Stuxnet, which require significant resources, make it unlikely similar threats will develop overnight.

To address the vulnerabilities revealed by Stuxnet, the series of process control and SCADA security good practice guidelines from CPNI and NIST include a series of sector "road maps" for securing the water, electricity, and chemical sectors. There is an emphasis on cost-effective security for legacy systems and new architecture designs and secure communications.

Standards in this area are blossoming as well, including work being done by the International Society of Automation (ISA), which published ISA99 Parts 1 and 2 that deal with industrial automation and control systems security. Part 1 serves as the foundation for all subsequent standards in the ISA99 series. Meanwhile IEC is also working on ICS standards and is considering work already done in ISA.

In the first public speech given by Britain's secret intelligence agency GCHQ, Chief Ian Lobban highlighted the "real and credible" threat facing the UK's Critical Infrastructure from terrorists, organized criminals, and hostile foreign governments. He demanded a swifter response to match the speed with which "cyber events" occurred, and stated that the UK's future economic prosperity rested on ensuring a defense against such assaults. The challenge is to implement appropriate measures while

Sponsor Profile

NERC Assante Interview

Cyber Security: the Human Factor

Control Network Security Lessons From Stuxnet

Cyber Security Standard Aims at Critical Infrastructure in Process Industries

White Paper: Smart Grid

continuing the process of assessment, adjustment, and review in light of emerging vulnerabilities, threats, and consequences.

Dr. Richard Piggin [rpiggin(at)iee.org] is a UK-based network and security consultant. He works with the IEC Network and System Security and Cyber Security working groups, and is involved in developing IEC 62443 Security for Process Measurement and Control – Network and System Security.

What Is A Threat?

According to the National Institute of Standards and Technology (NIST) Guide to Industrial Control Systems (ICS) Security, potential cybersecurity incidents may include the following:

- Blocked or delayed flow of information through control system networks, which could disrupt control system operation.
- Unauthorized changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment, create environmental impacts, and/or endanger human life.
- Inaccurate information sent to system operators, either to disguise unauthorized changes, or to cause the operators to initiate inappropriate actions, which could have various negative effects.
- Control system software or configuration settings modified, or software infected with malware, which could have various negative effects.
- Interference with the operation of safety systems, which could endanger human life.

Best Practices For Industrial Control Network Protection

In the UK, the Centre for the Protection of National Infrastructure (CPNI) is the government authority that provides protective security advice to the national infrastructure. Specific SCADA advice is offered by the CPNI in a series of process control and SCADA security good practice guidelines.

- The foundation of the best practice is three guiding principles:
- Protect, Detect, and Respond - It is important to be able to detect possible attacks and respond in an appropriate manner to minimize the impacts.
- Defense in Depth - No single security measure itself is foolproof as vulnerabilities and weaknesses could be identified at any point in time. To reduce these risks, implementing multiple protection measures in series avoids single points of failure.
- Technical, Procedural, and Managerial protection measures - Technology is insufficient on its own to provide robust protection.

Recommendations from the National Institute of Standards and Technology (NIST) include:

- Restricting physical access to the ICS network and devices.
- Protecting individual ICS components from exploitation. This includes deploying security patches in as expeditious a manner as possible, after testing; disabling all unused ports and services; restricting ICS user privileges to only those that are required; tracking and monitoring audit trails; and using security controls such as antivirus software and file integrity checking software where feasible to prevent, deter, detect, and mitigate malware.
- Maintaining functionality during adverse conditions. This involves designing the ICS so that each critical component has a redundant counterpart. Additionally, if a component fails, it should fail in a manner that does not generate unnecessary traffic on the ICS or other networks, or does not cause another problem elsewhere, such as a cascading event.
- Restoring the system after an incident. Incidents are inevitable and an incident response plan is essential.

For further reading:
Stuxnet as a Precision Weapon
Cybersecurity standard aims at critical infrastructure in process industries
Securing Legacy Control Systems

Sponsor Profile

NERC Assante Interview

Cyber Security: the Human Factor

Control Network Security Lessons From Stuxnet

Cyber Security Standard Aims at Critical Infrastructure in Process Industries

White Paper: Smart Grid

Cyber Security Standard Aims At Critical Infrastructure In Process Industries

The International Instrument Users Association (WIB) Releases Comprehensive Cyber Security Standard To Protect Critical Industrial Computer Systems From Cyber Attack.
11/16/2010

The International Instrument Users Association (WIB), an international organization that represents global manufacturers in the industrial automation industry, announced the second version of the Process Control Domain Security Requirements For Vendors document – the first international standard that outlines a set of specific requirements focusing on cyber security best practices for suppliers of industrial automation and control systems.

"We are pleased to announce today the second version of our cyber security standard," said Alex van Delft, competence manager for process control at DSM and chairman of the WIB. "This is an important step in the ongoing process to improve the reliability of our critical manufacturing and production systems, and provides end-users the ability to communicate their expectations about the security of process automation, control, and safety systems."

With industrial networks being increasingly connected to the hostile IT world, and the frequency and sophistication of malware growing exponentially, industrial stakeholders must act today to protect their critical systems. Whether it is a targeted attack like Stuxnet, or an accidental disruption, a single cyber incident can cost millions of dollars in lost revenue, jeopardize employee and public safety, and potentially disrupt national critical infrastructure.

"Our increasingly connected production systems are facing a growing threat on a daily basis and we must do all we can to ensure a safe and secure operational environment," said Peter Kwaspen, strategy and development manager, EMEA control and automation systems at Shell Projects & Technology. "This document provides the common language we need to communicate our expectations around security to our suppliers and the framework to work together to help improve the overall security posture for our critical systems."

Led by major companies such as Shell, BP, Saudi Aramco, Dow, DuPont, Laborelec, Wintershall, and dozens of other end-users, as well as leading vendors such as Invensys, Sensus, and multiple government agencies, the group spent two years developing the requirements and piloting a certification program to ensure a functional, scalable, and ultimately valuable result.

"The security requirements outlined in the document went through a year of comments and revisions from over 50 global stakeholders and were subjected to a thorough pilot certification program over the last eight months," said Jos Menting, cyber security advisor GDF Suez Group. "We've now come to a truly functional cyber security standard based on the needs of end-users and it is now up to us, the end-users, to take advantage of this effort and insist that our vendors are certified."

Members of the WIB Plant Security Working Group have already started implementing the requirements into their procurement processes and others around the world are heeding the call. "Shell has mandated conformance to the WIB standard for all vendors supplying systems to be deployed in Shell's process control environment starting January 1, 2011," said Ted Angevaare, PACO EMEA control and automation systems team leader. "These requirements will become a standard part of the procurement language saving us a significant amount of time and effort."

Leading suppliers of industrial process control and automation systems are also starting the process of integrating the requirements into their organizations. "Adopting the WIB's security requirements ensures that Invensys has a set of measurable practices in place that enforce a safer and more secure critical infrastructure. Not only do the requirements provide current-state measures, they allow us to continue to improve and adapt to the ever-changing security landscape," said Ernie Rakaczky, program manager for control systems cyber security at Invensys Operations Management. "From our perspective, this program is a major shift, not only focusing on tactics, but one that puts into place strategic elements that address operational change."

Cyber security at all stages of the industrial product lifecycle

The WIB standard is designed to fit the needs of end-users — the system owner/operators — and reflects the unique requirements for industries like oil and gas, electric power, smart grid, transportation, pharmaceutical, and chemical. The goal is to address cyber security best practices and allocate responsibility at various stages of the industrial system lifecycle: Organizational practices, product development, testing, commissioning, maintenance, and support.

"Security is not a one-time application, but rather a process in which every stakeholder must contribute in order to achieve any significant improvement in operational reliability," said Auke Huistra, project manager at National Infrastructure against Cyber Crime (NICC). "The WIB requirements are designed with this principle at its core and we are encouraging critical infrastructure stakeholders in The Netherlands to integrate the requirements into their cyber security plans."

The requirements were also constructed to address a broad range of cyber security topics relevant to industrial stakeholders; from high-level requirements for vendor's internal security policies, procedures, and governance, to specific requirements

Lessons Learned: Making Industrial Networking Better.

concerning access, authentication, data protection, default password protection, and patch management. When a vendor's solution complies with this set of requirements, the solution is considered by the WIB to be Process Control Domain Security Compatible.

The requirements are further broken down into 3 levels designed to reflect various starting points of global suppliers and provide a scalable framework to plan improvements over time. In the program, there are Gold, Silver and Bronze levels, each consisting of a set requirements designed to verify that applicable policies and practices are in place, enabled and practiced by the vendor.

Successful global cooperation

From the beginning, industry leaders recognized that given the global nature of industrial cyber security, any effort to standardize cyber security best practices would require stakeholder cooperation from different industry sectors and in different regions of the world. The WIB association was the ideal conduit to guide creation of the standard given its independent nature and membership composition. Moreover, the initiative needed to reflect and incorporate the important cyber security activities happening internationally. Many government agencies, industry working groups, and standards bodies were consulted to ensure harmony. For example, major industry standards efforts such as ISA SP99, NIST 800-53, NISTIR 7628, and various international government regulations such as NERC/CIP were reviewed and incorporated where appropriate or expanded to ensure testability. The WIB executive committee has started the process of introducing the WIB PCD requirements into the CEN/CENELEC and IEC international standards framework.

Download a copy of the standard: www.wib.nl/download.html or www.isssource.com/wib

Edited by Peter Welander, pwelander@cfemedia.com

Visit the Control Engineering Plant Safety & Security Channel for more information.

END

Sponsor Profile

NERC Assante Interview

Cyber Security: the Human Factor

Control Network Security Lessons From Stuxnet

Cyber Security Standard Aims at Critical Infrastructure in Process Industries

White Paper: Smart Grid

Sponsor Profile

NERC Assante Interview

Cyber Security: the Human Factor

Control Network Security Lessons From Stuxnet

Cyber Security Standard Aims at Critical Infrastructure in Process Industries

White Paper: Smart Grid

9 Lessons Learned from Smart Grid Implementations

How Smart Grid Technology Is Blazing the Trail for All Industrial Networks

By Jim Krachenfels, GarrettCom Marketing Manager

Planning for the Smart Grid has had a huge impact on the way power utilities manage their operating data and control networks. The convergence of IP technology, Smart Grid imperatives and the increased need for security as characterized in the NERC CIP regulations in North America has provided an opportunity for power utilities to rethink their operating strategies and come up with innovative ways to integrate the new and the old in order to position themselves for the future. This exercise has generated a body of knowledge that is instructive for all industrial networking applications.

IP – the Game-changing Factor Enabling Smart Grid

IP is a game-changing technology that is the basis for three compelling benefits for power utilities — particularly in the areas of substation automation and power transmission and distribution processes

- the overall reduction of operations expense from creating an IP-based infrastructure that integrates operational and non-operational data
- viable distributed intelligence applications that allow decision making in remote locations as well as in the central operations or central offices
- comprehensive grid operations and grid management security

As the power utility community has grappled with these opportunities and issues, nine lessons have emerged that can be applied to any industrial networking system

1. Plan for scalable bandwidth to handle the steadily increasing demand for data

2. Explore heavier-duty switches and routers to support expanding demands for more equipment attachments

3. Expect to integrate wireless communications for simple, cost-effective data links to remote sites

4. Upgrade to equipment with precision timing features to enable synchronized data management and control actions

5. Know how to integrate serial equipment into your complex IP network — it's not going away any time soon

6. Choose switches with flexible port configurations to easily integrate various types of new and existing equipment

7. Integrate a strategy for cyber security as well as a physical security to keep control networks safe

8. Bring corporate IT into data management as a partner

9. Understand that developing an outstanding industrial network is a work in process, not a one-time event

The joint imperatives of 9/11 and the Smart Grid have created a massive

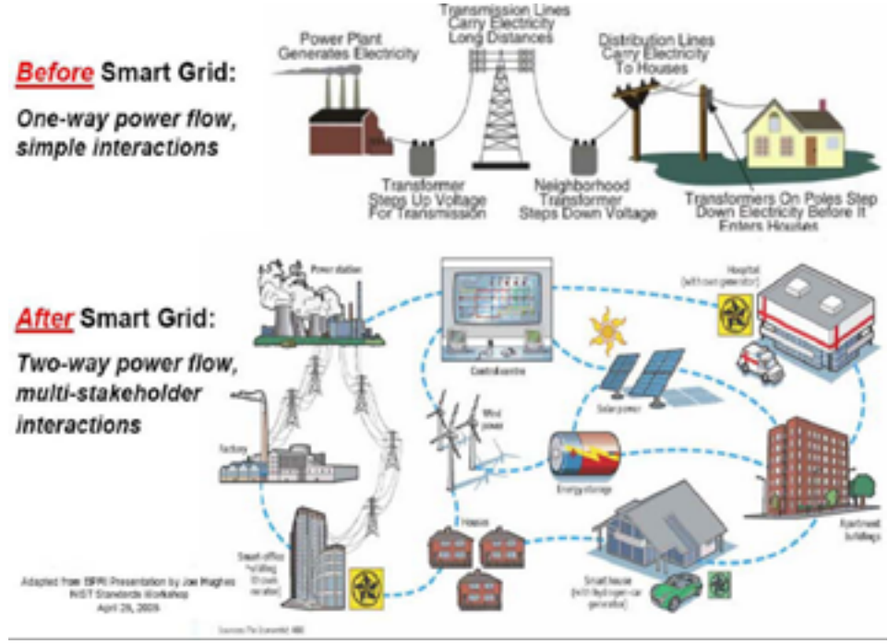


Figure 1

amount of development and retrofit activity in power utilities. The need to protect the security of power installations and the data that is passing in increasing quantities within and among substations and central offices is high. While the utilities are struggling with this issue, Smart Grid requires two-way communications with users to encourage smart use of power. Opening communication while protecting the privacy of the users and the security of the transmissions adds another layer of complexity.

Government organizations such as NERC (North American Electric Reliability Corporation), standards groups such as IEC, and industry organizations such as The International Instrument Users Association (WIB), have all contributed to the development of protocols, standards and requirements for addressing these challenges. (WIB is the first international standard that outlines a set of specific requirements focusing on cyber security best practices for suppliers of industrial automation and control systems). Power utilities themselves, separately and through cooperative efforts, have also provided insights and ideas.

Smart Grid = Increased Complexity

Daniel Wong, Principal Engineer, Protection & Control at AltaLink, summarized the opportunity—and the challenges—using Fig. 1 at the 2011

Lessons Learned: Making Industrial Networking Better.

DistribuTECH Conference & Exposition. Suddenly, a relatively simple operation became more complex with two-way communication and multiple stakeholders replacing a simple one-way transaction from an omnipotent and (from the user's standpoint) arbitrary source. Not only did control functions increase in complexity, but also non-operational data management increased dramatically, and because it was transported far beyond the boundaries of a single facility, issues including timing and security had to be addressed at a much more comprehensive level.

This is a starting point for understanding the nine lessons and their relationship to a broader range of industrial applications.

The Basics: Bandwidth, Capacity and Hardening

It should be clear from Fig.1 that additional bandwidth is necessary to successfully implement any Smart Grid strategy. Fiber backbones are a basis of most large-scale data management strategies because of fiber's excellent properties for providing high bandwidth over long distances, noise immunity, and inherent security features (because it is not easy to tap). Fiber is also flexible enough to support the installation of new nodes as demand on the network increases. With increased acceptance, coupled with the steep rise in the cost of copper, fiber is seen as a cost-effective alternative and a secure alternative to dedicated T1 or dial up lines, and it is well matched with IP infrastructure solutions.

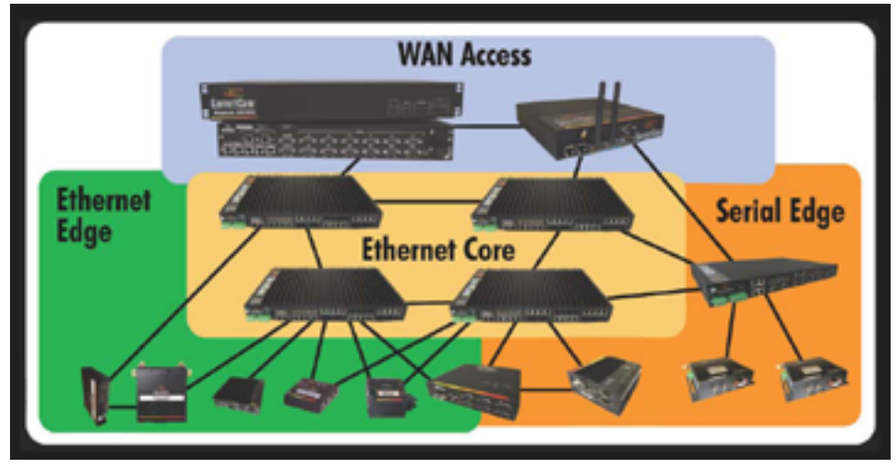


Figure 2

Just as the numbers of entities on the overall Smart Grid infrastructure are increasing, so are the numbers of nodes required within each of those entities. Using a substation as an example (Fig. 2), it is possible to observe the increasing number of intelligent IP-enabled devices available for connection—from sensors and monitors all the way to new security devices such as video cameras, card readers, and intelligent access control devices including fingerprint or iris scanners.

To cleanly support data and control systems demand generated from increased substation complexity, designers need to be able to choose Ethernet switches and routers equipped with varying numbers of ports. Particularly at the core of the network, it is inefficient and expensive to pile multiple low-port-count switches together, wasting two ports per device for connectivity, and this practice results in additional and unnecessary points of failure. Where larger port-count devices were once deployed only in climate-controlled central offices, today one sees installations of 24-port and 36-port switches at the nerve center of the substation, where the environmental conditions demand substantial hardening—in fact, substation-level hardening. These larger substation switches connect with smaller-port-count switches installed as the deployment approaches the network edge.

There are a number of components needed to create a hardened, robust switch, but the most significant are

- Extended temperature range for extreme environments (-40°C to +85°C)
- Strong EMC design to protect against electrical magnetic interference (EMI), which is often prevalent in substation environments
- Convection-cooling, eliminating the need for fans as a potential point of failure in hot, high-particulate environments, and protecting against the intrusion of dust and dirt
- Shock and vibration resistance
- Fiber configurability to support security and high-bandwidth demands
- DC power as well as AC to support installation in areas requiring specialized power sources
- Redundancy options to ensure high availability

WHAT IS INDUSTRIAL ETHERNET?

It is important to note that "Industrial Ethernet" is more than just a marketing phrase; it describes the environment in which an Ethernet device must operate. Hardened Ethernet switches are a complete rethinking and redesign of office-based Ethernet components. Electronics in extreme industrial environments can be subjected to high levels of EMI, heat and moisture, as well as dust, dirt, and corrosive chemicals. In addition, required levels of availability may exceed those for a commercial environment. It's never good when the network goes down in an office, but it's likely to have a more serious impact if an electrical blackout causes hundreds of thousands of subscribers to lose power.

Sponsor Profile

NERC Assante Interview

Cyber Security: the Human Factor

Control Network Security Lessons From Stuxnet

Cyber Security Standard Aims at Critical Infrastructure in Process Industries

White Paper: Smart Grid

The ability to support increased bandwidth and an increasing number of IEDs, combined with the ability to survive in extreme environments are all critical to substation success.

Transport Flexibility –Wireless, Ethernet, Serial

Another aspect of Smart Grid networks is the increasing demand for wireless connectivity both for the larger grid and within specific facilities. Distributed alternative power generation resources, as well as the need for two-way communications at users' meters, often require wireless connectivity support. Wireless provides an alternative to support the needs of the growing infrastructure, and, in fact, the use of wireless connectivity in developing countries has allowed some of them to accelerate their infrastructure development. Within a facility, wireless is increasingly being used, along with Power over Ethernet (PoE), for security applications and other specific functions where wiring is difficult or uneconomical.

'Wireless" is not a monolithic concept, and the broad variety of wireless connectivity options are beyond the scope of this paper. Nonetheless, it is important in planning a network to ensure that wireless connectivity is an option, at least at the router level, to support growing demand for this type of connectivity.

At the other end of the spectrum, serial equipment is here for the long run. In power utilities, much of the networking equipment installed to date has used serial connectivity—and it has been there for decades. Serial is still popular in new equipment installations today. While some utilities may have some Greenfield projects where they are deploying fully IP-based networks, most will be using serial components for years to come.

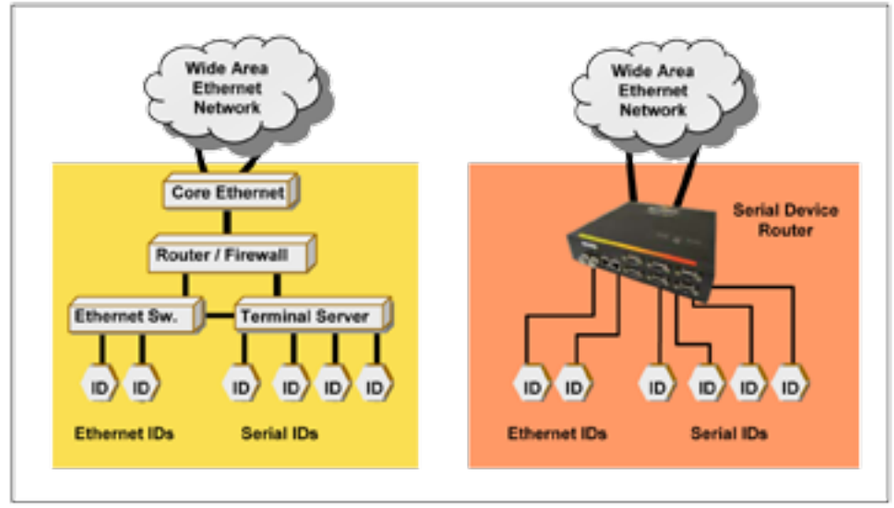


Figure 3

IP technology advances are making it possible to more fully utilize and integrate serial data, and, in fact, include it in IP security protocols. For this reason, ease in connecting serial devices into the IP architecture is a high priority. Terminal servers and routers that support both Ethernet and serial devices reduce complexity and also provide greater security options (see Fig. 3).

A typical substation will have IEDs and other equipment outfitted with a wide range of standard Ethernet and serial connectors. Modular technologies that support the mixing and matching of blocks of ports on individual switches and routers provide cost-effective and easy-to-deploy alternatives to fixed-port boxes.

"But I thought Arizona was on Mountain Time . . ."

Continued integration has made precision timing much more important as well. Most of us are well aware of the challenges in communication that result from coordinating different time zones, especially since some states don't follow daylight savings practices. Within a Smart Grid infrastructure, the challenge is even more complex.

In the case of a security incident, it is necessary to ensure that the time stamps on data from various cameras and intrusion detection devices are synchronized to a universal clock to ensure that accurate sequencing of events can be tracked. Internally, when there are operational events, it is equally necessary to make sure that comparisons of data—even from serial devices in the network—are based upon a single time standard. An example of a time code standard is IRIG-B, developed by Inter-Range Instrumentation Group, the standards body of the Range Commanders Council; it offers a standard by which it is possible to synchronize geographically separated instruments throughout a power delivery system.

Decision Making at the Source and the Expanded Role of Security

The good and the bad news about IP is that it makes it possible to transfer and manage large amounts of data over geographically separated areas. This enables informed decision-making at remote locations—from determining whether a user should be provided access to certain operational or non-operational data to helping a commercial power user to decide when to schedule power-hungry but discretionary activities. In addition to the challenges of ensuring consistent system-wide timing synchronization, flexible access to information in a distributed environment creates security issues that need to be addressed to ensure the integrity of the operation.

Lessons Learned: Making Industrial Networking Better.

Sponsor Profile

NERC Assante Interview

Cyber Security: the Human Factor

Control Network Security Lessons From Stuxnet

Cyber Security Standard Aims at Critical Infrastructure in Process Industries

White Paper: Smart Grid

Many industrial facilities are watching what is happening in the power utility industry because of stringent NERC mandates. NERC created a series of security requirements for the power utility industry that were meant to protect critical assets. These requirements have impacted how power utilities manage their business. A set of requirements that is expected to evolve over time CIP requirements today address the following network components of a substation security

- CIP-002: Critical Cyber Asset (CCA) Identification—which require identification of switches, routers, and data concentrators with access to the outside world
- CIP-005: Electronic Security Perimeter(s)— which requires switches and routers with access to the outside world to be protected by access control applications such as firewalls
- CIP-006: Physical Security of CCAs—which typically requires an integrated cyber and physical security strategy to protect the communication cabinet and the SCADA cabinet—and, in fact, the entire plant
- CIP-007: System Security Management—which includes test procedures, ports and services, patch management, prevention of intrusion by malicious software account management, and security status monitoring via syslogs
- CIP-009: Recovery Plans for CCAs—which include change control and basic recovery kits or protocols

While some utilities have adopted an attitude of removing as many critical assets from the inter-facility communications network as possible, the momentum toward shared data networks is huge because of the possibilities offered in terms of operational efficiency and distributed decision-making. In addition, as StuxNet proved in 2010, even unconnected systems can fall victim to the good old 'Adidas network" as employees intentionally or unintentionally expose systems to malicious attacks.

Developing a strong cyber (and physical) security strategy is critical in today's world.

Fig. 4 shows a network that is wide open to attack.

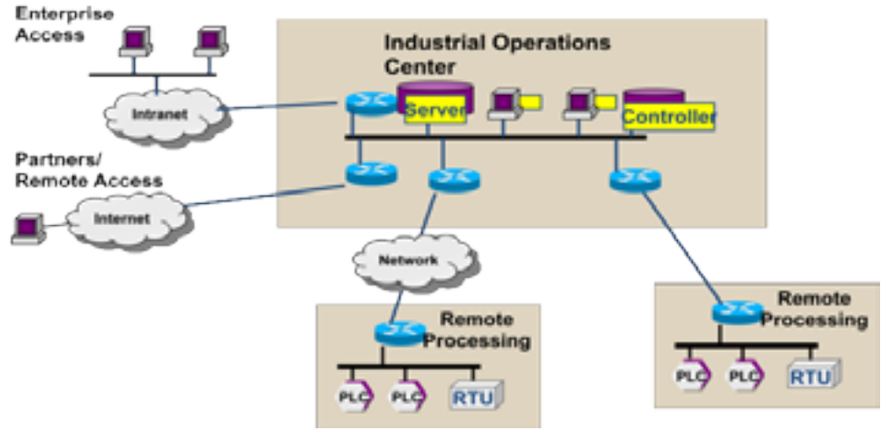


Figure 4

Fig. 5 shows the same type system with a stringent physical and cyber security layer inserted.

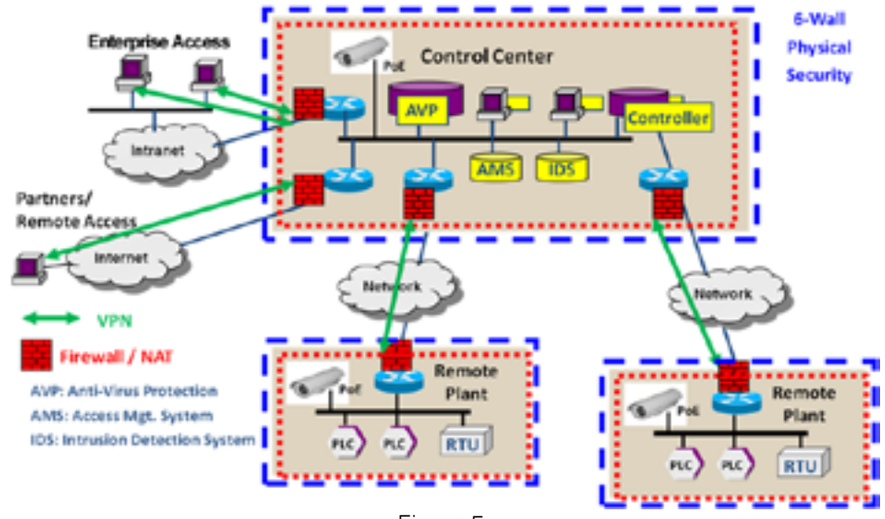


Figure 5

Sponsor Profile

NERC Assante Interview

Cyber Security: the Human Factor

Control Network Security Lessons From Stuxnet

Cyber Security Standard Aims at Critical Infrastructure in Process Industries

White Paper: Smart Grid

Fig. 6 goes one step further, implementing CIP 007 requirements for access control.

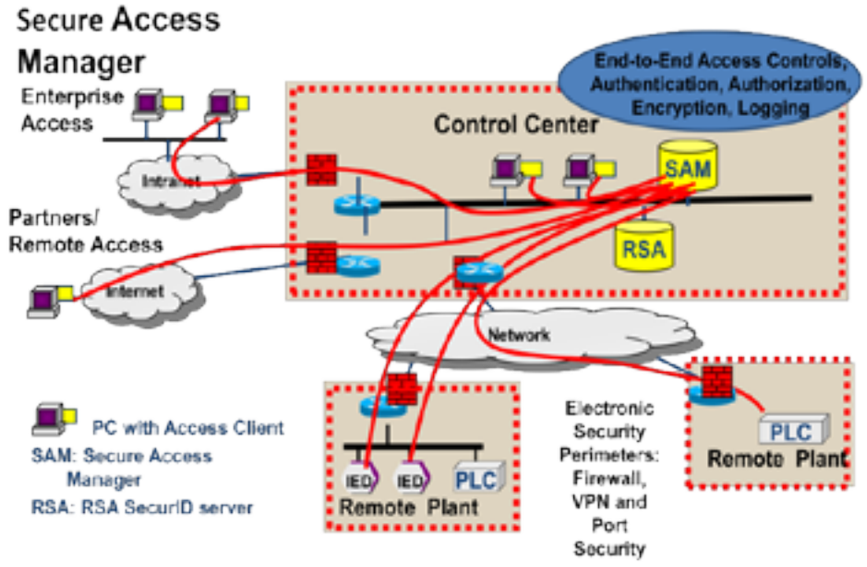


Figure 6

Some of the components involved in implementing a power utility security strategy are

- Physical security: Cyber security starts with physical security. If outsiders cannot gain access to the premises, it is harder for them to access sensitive data.
- Firewalls: It is necessary to protect cyber assets with firewalls at the cyber perimeters of critical cyber assets just as the physical perimeter is protected.
- Port access control: In addition to denying access to the building, disallowing unauthorized devices to be plugged into ports on switches and routers makes for a more secure environment.
- Password health and authentication: Prudent practices should include changing passwords regularly — and making sure that they are long enough and complex enough that they are difficult to crack. Authentication is more secure than simple authorization (which only ensures the person accessing the system is using the right code); it goes one step further by ensuring that the person or device requesting access is who he says he is.
- Encryption: Fiber cabling is much more secure than copper when used to relay data between secure locations. Sending encrypted data adds an extra level of protection outside secure facilities.
- VPNs and VLANs: Virtual Private Networks and Virtual LANS both provide extra layers of security for transmissions over multi-purpose transport networks.
- Employee training: Security is only as good as the practices that are in place. Employees, without meaning to create a security breach, can be lax with passwords, security codes and other primary measures unless they are educated — and reminded — about the importance of security.

For more information on cyber security, see GarrettCom's white paper titled "Cyber Security for Industrial Applications".

Working Well Together

As is made clear by the discussion on security, operational facilities are more hard-pressed than ever to seamlessly integrate data flow with corporate IT. While conflicting priorities and needs have traditionally made the two groups "friendly adversaries" at best and outright enemies at worst, there is a growing body of stories on how the two groups have collaborated to bring about the best results. Simply put, the two groups have very different goals and objectives in many cases — the precision timing issues and maintenance schedules on the plant floor can conflict with corporate information flows. In one memorable situation, a customer recounted the story where plant work was disrupted when a single IP network was installed and a corporate data run consumed all available bandwidth for plant operations and shut down the factory's night shift production line. However, multi-discipline workgroups are identifying and solving these types of problems — and providing more information and greater efficiencies across entire organizations.

An Ongoing Project

In power utilities, as well as other industrial facilities, there is a growing understanding that creating an efficient network is a work in progress. Progress is measured in increments and phrases: from quality circles and CPI (Continuous Process Improvement) to the planned phasing in of NERC-CIP requirements to the practical demands of resource planning. In the latter case, it is rarely feasible to implement the wholesale overhaul of physical plants that have hundreds of thousands — or millions of dollars invested in equipment that has not reached the end of its life cycle.

The Blue Ridge EMC Story

Blue Ridge EMC recently executed an upgrade as a result of both NERC and Smart Grid. In order to plug into the Smart Grid, the first order of business was being able to provide reliable, IP-based

Sponsor Profile

NERC Assante Interview

Cyber Security: the Human Factor

Control Network Security Lessons From Stuxnet

Cyber Security Standard Aims at Critical Infrastructure in Process Industries

White Paper: Smart Grid

communications services in its demanding service area in northwestern North Carolina. Much of the territory it serves is located in the Appalachian Mountain range.

Blue Ridge had to provide communications to remote locations at a reasonable cost to enable its TWACS AMR System to remotely read electric power meters with a granularity of up to an hour. AMR would save costs and reduce vehicle rolls (often difficult or impossible during severe winter weather). In designing the network for the substations, Blue Ridge followed NERC CIP standards, which helped to insure network security and reliability.

Fiber connectivity at substations is the logical choice for backhauling meter reading and load analysis data to the corporate office. Where IEDs have been installed, engineers can analyze fault data and the dispatchers in the operations center can ping individual meters to determine exactly where an outage has occurred.

Network Equipment Requirements

To build out this project, Blue Ridge Telecom/IT team needed switching equipment that was hardened to withstand the electrical and environmental extremes found in substations and beyond in the distribution system. In addition, new equipment had to be compatible with the existing network equipment; had to meet today's NERC CIP requirements (as well as be flexible enough to support anticipated future directions); and had to be easily monitored and managed remotely.

Security gateways made by Astaro Corp. and Magnum 6K Ethernet Managed Switches from GarrettCom, Inc., formed the basis of the communications network. Where fiber has been deployed, it is connected directly to the Magnum switch at the substation. To securely transmit information over the DSL lines, the security gateways act as a firewall between the substation network and the internet. The network switching equipment protects the substation network and transmits data over a separate DSL line to corporate. All unused ports on the Magnum switches are disabled to further enhance security. Fiber was used to deploy multiple VLANs to segregate engineering applications and corporate Ethernet traffic; DSL does not support VLANs, and therefore works best in distribution stations that have minimal transmission equipment.

With its new system in place, Blue Ridge enjoys both the additional flexibility of the Smart Grid and the security afforded by its expanded, secure IP network.

Summary

The combination of NERC and Smart Grid initiatives requires a major review of power utilities assumptions and objectives in collecting, managing and analyzing data. Consequently, the nine lessons discussed become increasingly critical to success

1) Plan to scale bandwidth to accommodate increasing demand for data
2) Look for a family of industrial-strength switches and routers to support expanding demands for equipment attachment — ranging from 24- and 36-port boxes for centralized data management to small four-port units to support the edge
3) Expect wireless requirements and have a plan for integrating them
4) Ensure that distributed data is synchronized
5) Create an architecture that can easily integrate serial equipment into the IP network
6) Choose equipment with flexible port configurations for easy integration of any IEDs
7) Build in cyber and physical security — it is no longer an option
8) Bring corporate IT into the loop as a partner
9) Prepare for phased continuous evolution of your network

GarrettCom is dedicated to stepping up to the plate with solutions that combine high availability networking technologies, industrial-strength design, flexibility, and innovative cyber-security solutions. These solutions are engineered to support industrial networking customers that devise, maintain, and improve the systems that support the expanding needs for operational and non-operational data in the 21st century. The challenges industries face today can become a springboard to more efficient, more effective operational practices. Through the use of standards-compliant hardware and software, an innovative approach to new data and data management requirements, and a broad portfolio of IP technologies and products, GarrettCom is working with customers to deliver the bandwidth, redundancy, reliability, and security to provide an extensible infrastructure that will serve them for years to come.

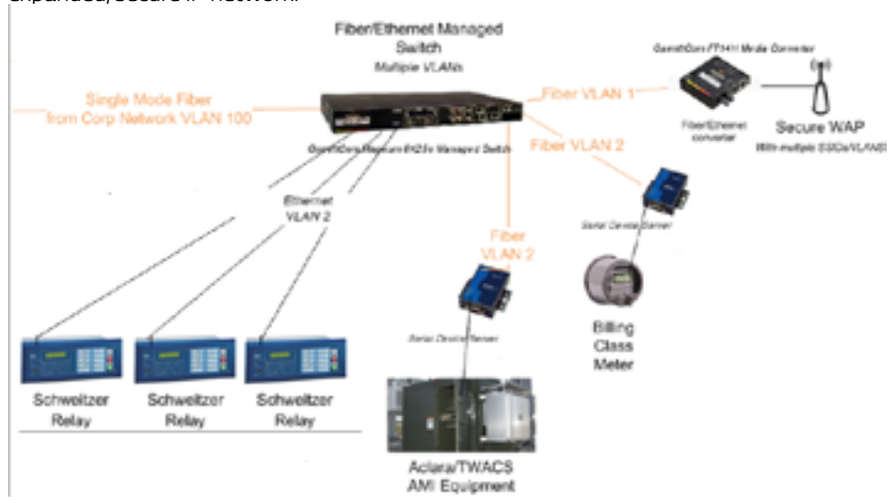


Fig. 7 shows the new substation and distribution layout that is a combination of Ethernet-connected IEDs and serial links.