Testimony of
Joseph M. Weiss

Control Systems Cyber Security Expert

before the

Committee on Commerce, Science, and Transportation
U.S. Senate

March 19, 2009

Control Systems Cyber Security—The Current Status of Cyber Security of Critical Infrastructures

Good afternoon Mr. Chairman and Members of the Committee. I would like to thank the Committee for your invitation to discuss the current status of cyber security of the control systems utilized in our nation's critical infrastructure.

I am a nuclear engineer who has spent more than thirty years working in the commercial power industry designing, developing, implementing, and analyzing industrial instrumentation and control systems. I have performed cyber security vulnerability assessments of power plants, substations, electric utility control centers, and water systems. I am a member of many groups working to improve the reliability and availability of critical infrastructures and their control systems, including the North American Electric Reliability Council's (NERC) Control Systems Security Working Group (CSSWG), the Instrumentation Systems and Automation Society (ISA) S99 Manufacturing and Control Systems Security Committee, the National Institute of Standards and Technology (NIST) Industry-Grid Working Group, Institute for Electrical and Electronic Engineers (IEEE) Power Engineering Society Substations Committee, International ElectroTechnical Commission (IEC) Technical Committee 57 Working Group 15, and Council on Large Electric Systems (CIGRÉ) Working Group D2.22- Treatment of Information Security for Electric Power Utilities (EPUs). I would like to state for the record that the views expressed in this testimony are mine.

Until 2000, my focus strictly was to design and develop control systems that were efficient, flexible, cost-effective, and remotely accessible, without concern for cyber security. At about that time, the idea of interconnecting control systems with other networked computing systems started to gain a foothold as a means to help lower costs and improve efficiency, by making available operations-related data for management "decision support." Systems of all kinds that were not interconnected with others and thereby could not share information ("islands of automation") became viewed as an outmoded philosophy. But at the same time, there was no corresponding appreciation for the cyber security risks created. To a considerable extent, a lack of appreciation for the potential security pitfalls of highly interconnected systems is still prevalent today, as can be witnessed in many articles on new control systems and control system conferences. As such, the need for organizations to obtain information from operational control system networks to enable ancillary business objectives has often unknowingly led to increased cyber vulnerability of control system assets themselves.

The timing of this hearing is fortuitous as the Stimulus Bill has recently been approved which is stimulating work on the Smart Grid, the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) cyber security standards are being updated, the Chemical Facility Anti-Terrorism Standards (CFATS) is being reviewed, and the water industry R&D Roadmap has been issued. In each case, I believe there are shortcomings that can have significant impacts on the security of our critical infrastructures if they are not adequately addressed.

Introduction[2]

Industrial Control Systems (ICS)[3] are an integral part of the industrial infrastructure providing for the national good. While sharing basic constructs with Information Technology (IT) business systems, ICSs are technically, administratively, and functionally more complex and unique than business IT systems. Critical infrastructure protection focuses on protecting and maintaining a safe and reliable supply of electric power, oil, water, gasoline, chemicals, food, etc. Computer cyber vulnerabilities are important if they can affect the safe, functional performance of these systems and processes. One should view current ICS cyber security as where mainstream IT security was fifteen years ago – it is in the formative stage and needs support to leapfrog the previous IT learning curve.

The convergence of mainstream IT and ICS systems require both mainstream and control system expertise. It is the successful convergence of these systems and organizations that will enable the promised secure productivity benefits. To ensure that ICS are adequately represented, include subject matter experts with control systems experience in all planning meetings that could affect these systems.

Generally cyber security has been the purview of the Information Technology (IT) department, while control system departments have focused on equipment efficiency and reliability – not cyber security. This has led to the current situation where some parts of the organization are now sensitized to security while others are not as yet aware of the need. Industry has made progress in identifying control system cyber security as an issue while not appreciating the full gravity of the matter. There is a significant difference between the security philosophies of enterprise IT and ICS. The purpose of enterprise security is to protect the data residing in the servers from attack. The purpose of ICS security is to protect the ability of the facility to safely and securely operate, regardless of what may befall the rest of the network.

Cyber refers to electronic communications between systems and/or individuals. This term applies to any electronic device with serial or network connections. For this White Paper, the umbrella term "cyber" addresses all electronic impacts on ICS operation including:

- intentional targeted attacks,
- unintended consequences such as from viruses and worms,
- unintentional impacts from inappropriate policies, design, technologies, and/or testing,

[2] The testimony is based on the White Paper prepared for the Center for Strategic and International Studies, "Assuring Industrial Control System (ICS) Cyber Security", by Joe Weiss, dated August 25, 2008.

[3] It should be noted that many of the acronyms used in industrial controls may be similar to acronyms used in government or other applications but with different meanings. Examples are ICS, IED, and IDS. In order to avoid confusion all acronyms have been spelled out the first time they have been used.

- Electro Magnetic Pulse (EMP),
- Electro Magnetic Interference (EMI),
- other electronic impacts

The umbrella term "ICS" includes:
- automated control systems (ACS)
- distributed control systems (DCS),
- programmable logic controllers (PLC),
- supervisory control and data acquisition (SCADA) systems,
- intelligent electronically operated field devices, such as valves, controllers, instrumentation
- intelligent meters and other aspects of the Smart Grid
- networked-computing systems

An ICS is actually a system of systems. A crude distinction between mainstream IT and control systems is that IT uses "physics to manipulate data" while an ICS uses "data to manipulate physics." The potential consequences from compromising an ICS can be devastating to public health and safety, national security, and the economy. Compromised ICS systems can, and have, led to extensive cascading power outages, dangerous toxic chemical releases, and explosions. It is therefore important to implement an ICS with security controls that allow for reliable, safe, and flexible performance.

The design and operation of ICS and IT systems are different. Different staffs within an organization conceive and support each system. The IT designers are generally computer scientists skilled in the IT world. They view "the enemy of the IT system" as an attacker and design in extensive security checks and controls. The ICS designers are generally engineers skilled in the field the ICS is controlling. They view "the enemy of the ICS" not as an attacker, but rather system failure. Therefore the ICS design uses the "KISS" principle (keep it simple stupid) intentionally making systems idiot-proof. This approach results in very reliable but paradoxically, cyber-vulnerable systems. Moreover, the need for reliable, safe, flexible performance precludes legacy ICS from being fully secured, in part because of limited computing resources. This results in trade-off conflicts between performance/safety and security. These differences in fundamental approaches lead to conflicting technical, cultural, and operational differences between ICS and IT that need addressing.

CIA Triad Model – Confidentiality, Availability, and Integrity:
- Confidentiality describes how the system or data is accessed
- Integrity describes the accuracy or completeness of the data
- Availability describes the reliability of accessing the system or data

Traditional IT systems employ the best practices associated with "Confidentiality, Integrity, Availability" (CIA) triad model – in that order of importance. The placement of rigorous end user access controls and additional data encryption processes provide confidentiality for critical information.

Traditional ICS systems employ the best practices associated with "Confidentiality, Integrity, Availability" (CIA) triad model – in the reverse order; AIC- Availability, Integrity, Confidentiality. Extra emphasis is placed on availability and message integrity.

The converged ICS/IT model would employ the best practices associated with "Confidentiality, Integrity, Availability" (CIA) triad model – in an equally balanced way. The compromise of any of the triad will cause the system to fail and become unusable.

It is important to point out another major difference between IT and ICS systems. In an IT system, the end user generally is a person, in an ICS system the end user generally is a computer or other highly intelligent control device. This distinction lies at the heart of the issue around securing an ICS in a manner appropriate to current need.

IT systems strive to consolidate and centralize to achieve an economy of scale to lower operational costs for the IT system. ICS systems by necessity are distributed systems that insure the availability and reliability of the ICS and the systems that the ICS controls. This means that remote access is often available directly from field devices reducing the effectiveness of firewalls at the Central Demilitarized Zone (DMZ) and requiring additional protection at remote locations. The limited computer processing power in the field devices precludes use of many computer resource-intensive IT security technologies such as remote authentication servers. Newer ICS designs do, or will, employ advanced high-speed data networking technologies. Thus, what used to be a single attack vector (the host) increases by the number of smart field devices (Intelligent Electronic Devices [IED], smart transmitters, smart drives, etc.).

The use of mainstream operating system environments such as Windows, UNIX, and Linux for running ICS applications leave them just as vulnerable as IT systems. While at the same time, the application of mainstream IT security technical solutions and/or methods will help to secure more modern ICS host computers and operator consoles (i.e., PCs). In technologies such as Virtual Private Networks (VPN) used to secure communications to and from ICS networks, IT security focuses on the strength of the encryption algorithm, while ICS security focuses on what goes into the VPN. An example of this concern was demonstrated by one of the Department of Energy's National Laboratories of how a hacker can manipulate widely used "middleware" software running on current mainstream computer systems without a great deal of difficulty. In this sobering demonstration, using vulnerabilities in OPC code ("OLE for Process Control"), the system appears to be functioning properly even though it is not; while displaying incorrect information on, or withholding correct information from, system operator consoles.

Certain mainstream IT security technologies adversely affect the operation of ICS, such as having components freeze-up while using port scanning tools or block encryption slowing down control system operation - basic Denial of Service (DOS). IT systems are "best effort" in that they get the task complete when they get the task completed. ICS systems are "deterministic" in that they must do it NOW and cannot wait for later as that will be too late.

To enable proper security, these examples demonstrate the mandate to understand the ICS and control processes and to evaluate the impacts of potential security process and actions upon those systems and processes prior to implementation.

Figure 1 is used to illustrate the distinction between ICS and business IT considerations. A person is shown (see yellow arrow for location) at the bottom cylindrical torus to provide a perspective of size. In this nuclear plant case, the box shown in the figure (on the left side approximately one-quarter of the way up, see green arrow for location) is one of two main coolant pumps each consuming enough power to power approximately 30,000-50,000 homes. A power plant of this design suffered a broadcast storm resulting in a DOS. In a typical broadcast storm creating a DOS, the impact is disruption of communications across a computer network, potentially resulting in shutdown of computers as a consequence. This broadcast storm DOS shutdown the

equipment controlling the pumps eventually resulting in the shutdown of the nuclear plant. The term DOS has a completely different meaning when talking about desktops being shutdown compared to major equipment in nuclear plants and other major facilities being shutdown or compromised.

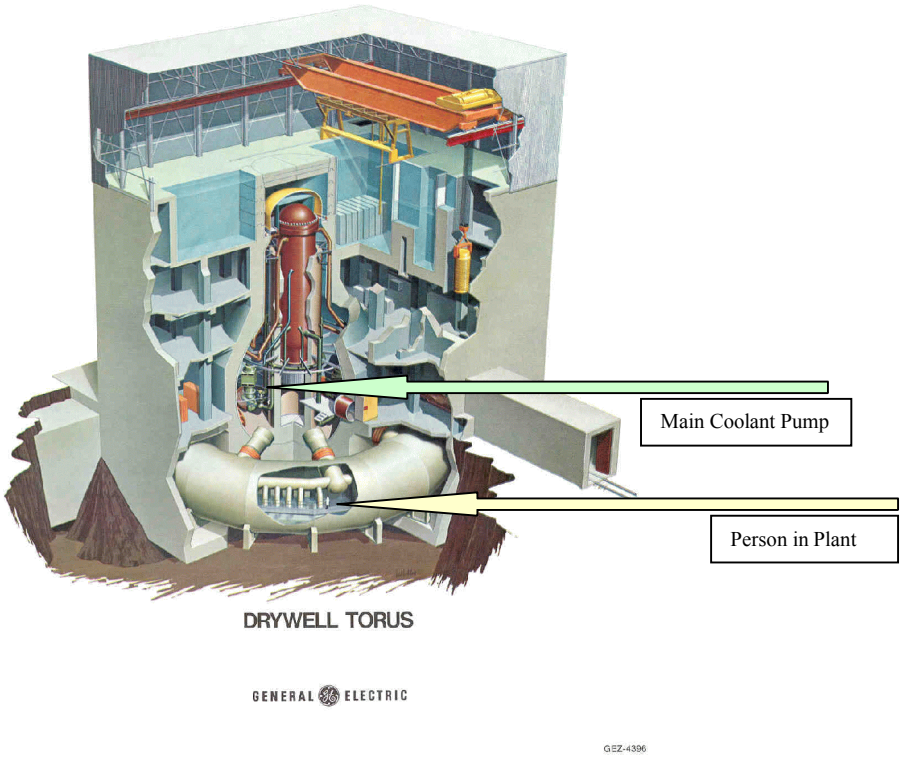

Figure 1 Nuclear Power Plant Denial of Service

Need for Understanding

In the past, the people that implemented a system, whether Business IT or ICS, were intimately familiar with the processes and systems being automated. Today, few people possess this kind of system knowledge. Rather they design and implement systems based upon design concepts handed to them. In the case of an ICS, the designer and implementer may not even know what the end device does, how it does it, or even what it looks like. The system designer and implementer may not be in the same country as the controlled device. This disconnect allows for loss of understanding about the impacts of miss-operation of a device, device failure, or improper communication with the device.

The more complex the ICS application, the more detailed knowledge of the automated ICS processes are required: how it is designed and operated; how it communicates; how it is interconnected with other systems and ancillary computing assets. Only with this knowledge can appreciation of the cyber vulnerabilities of the system as a whole can begin. There is a current lack of ICS cyber security college curricula and ICS cyber security professional certifications.

Figure 2 characterizes the relationship of the different types of special technical skills needed for ICS cyber security expertise, and the relative quantities of each at work in the industry today. Most people now becoming involved with ICS cyber security typically come from a mainstream IT background and not an ICS background. This distinction needs to be better appreciated by government personnel (e.g., DHS NCSD and S&T, DOE, EPA, etc.) responsible for ICS security. This lack of appreciation has resulted in the repackaging of IT business security techniques for control systems rather than addressing the needs of field ICS devices that often have no security or lack the capability to implement modern security mitigation technologies. This, in some cases, inadvertently results in making ICS systems less reliable without providing increased security. An example of the uninformed use of mainstream IT technologies is utilizing port scanners on PLC networks.

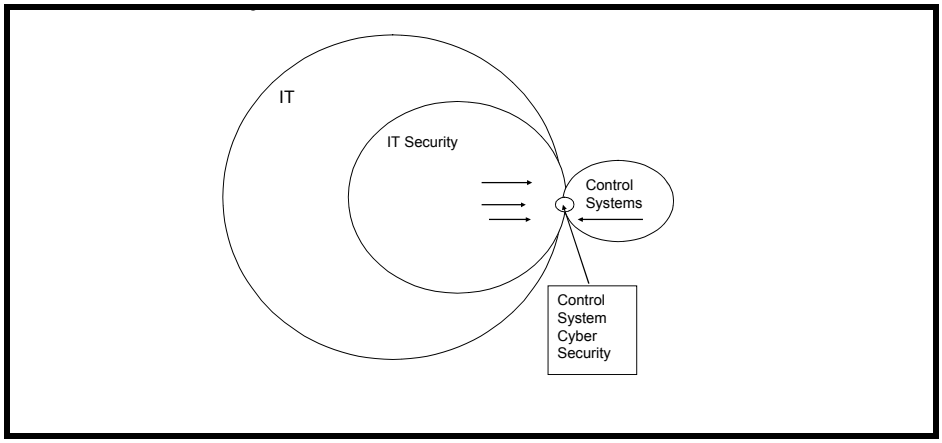

Figure 2 - Relationship and Relative Availability of ICS Cyber Security Expertise

In figure 2, we see that IT encompasses a large realm, but does not include ICS processes. It is true that IT evaluation and design models can be used to develop an ICS; the major difference is that within the Business IT model all tasks have a defined start and a defined end. In the process control model, the process is a continuous loop. Generally, the IT community avoids the continuous loop, while the ICS community embraces the continuous loop. It is the continuous loop that enables an ICS to operate efficiently and safely. As an example,, automated meters "read and record the value from a meter every second". The meter will happily read and record forever, and be proud that it is doing its function.

A common misconception deals with the availability of knowledge about an ICS. There are only a limited number of DCS, SCADA, and PLC suppliers A few of the major suppliers include ABB, Areva, Alsthom, Emerson, General Electric, Honeywell, Invensys, Metso Automation, Rockwell Automation, Schneider, Siemens, Telvent, and Yokogawa. Approximately half of the suppliers are US-based while the other half are European or Asian-based. The US suppliers provide systems to North America and throughout the world, except to "unfriendly" countries. The ICS systems provided internationally are the same systems provided in North America with the same architecture, same default vendor passwords, and same training. Sales of electric industry SCADA/Energy Management Systems include the system source code, meaning that the software used in North American SCADA systems is available world-wide. Some of the largest implementations of ICS systems originating in the United States are implemented in the Middle East and China. A number of North American control system suppliers have development activities in countries with dubious credentials (e.g. a major North American control system

supplier has a major code writing office in China and a European RTU manufacturer has code written in Iran). There are cases where US companies will remotely control assets throughout the world from North America (and vice versa). The non-North American-based ICS suppliers provide the same systems to North America as those provided to countries NOT friendly to us. There are cases where non-North American companies will remotely control assets in North America from Europe or Asia. Additionally, ICS engineers willingly share information. This truly is a global issue.

An example of information-sharing concerns is the SCADA Internet email-based discussion list from Australia where people from around the world can discuss SCADA/control system issues. Unfortunately, this includes questions from individuals from suspect countries about ICS systems, processes, or devices they do not have, but that we do. This approach works in a benign world – unfortunately, we don't live in one.

There is a reticence by commercial entities to share information with the U.S. government. Few "public" ICS cyber incidents have been documented (probably less than 10), yet there have been more than 125 actual ICS incidents. Even the "public" cases may not be easily found as they are buried in public documents such as the National Transportation Safety Board (NTSB) report on the Bellingham, WA Pipeline Disaster[4] or nuclear plant Operating Experience Reports. An interesting anecdote was a presentation made by a utility at the 2004 KEMA Control System Cyber Security Conference on an actual SCADA system external attack. This event shut down the SCADA system for two weeks. However, since power was not lost, the utility chose not to inform local law enforcement, the FBI, or the Electric Sector ISAC since they did not want their customers to know. This is one of the reasons it is not possible to provide a credible business case for control system cyber security.

The prevailing perception is the government will not protect confidential commercial information and organizations such as ISACs will act as regulators. That is, if two organizations have the same vulnerabilities and only one is willing to share the information, the organization sharing the information will be punished as not being cyber secure while the organization does not share will be viewed as cyber secure by default. This has Sarbanes-Oxley implications as well. It is one reason why the US CERT, which is government-operated, does not work as effectively as needed. Therefore, a "Cyber Incident Response Team (CIRT) for Control Systems" by a global non-governmental organization with credible control system expertise is required. This organization would collect and disseminate information used to provide the necessary business cases for implementing a comprehensive ICS system security program. Models for this approach include CERT, InfraGard, or FAA[5]. Specific details can be provided if desired. The InfraGard model for public-private information sharing requires more sharing with the ICS community by the FBI so industry can protect themselves if a cyber attack has been detected. The FBI's "cone of silence" is not adequate. As identified by numerous government reports following the 9/11 disaster, there is a need to "connect the dots" to determine if there are patterns in events that should be followed-up. In this case, the dots that need to be connected are with ICS cyber incidents to determine if policies, technologies, and testing are adequate to address these incidents.

Operationally, there are differences between mainstream IT and ICS systems. Of primary concern is maintenance of systems. Like all systems, periodic maintenance and tuning is required

[4] "Pipeline Accident Report Pipeline Rupture and Subsequent Fire in Bellingham, Washington June 10, 1999", National Transmission Safety Board Report NTSB/PAR-02/02 PB2002-916502.

[5] http://asrs.arc.nasa.gov/overview/immunity.html

to insure effective operation which must be scheduled in advance so as not to cause system impacts. Shutting down a major industrial plant may cost as much as several hundred thousand dollars per minute.

The current state of the IT world insures a high degree of intelligence and processing capability on the part of the various devices within an IT system. The standard implementation provides centralized control points for authentication and authorization of IT activities. The lifetime of the equipment in an IT network, typically, ranges from 3 to 7 years before anticipated replacement and often does not need to be in constant operation. By the very nature of the devices and their intended function, ICS devices may be 15 to 20 years old, perhaps older, before anticipated replacement. Since security was not an initial design consideration, ICS devices do not have excess computing capacity for what would have been considered unwanted or unneeded applications.

As can be seen, device expectations are different for ICS and IT systems, and this very difference generates two incredibly complex problems: how to authenticate access, and how to patch or upgrade software.

Of considerable importance is intra- and inter- systems communication in both the IT and ICS realms. ICS systems are intended to operate at all times, whether connected to other systems or not. This independence makes the ICS very flexible, indeed. The age of the equipment makes it difficult to authenticate communications properly. Not just between servers, but between servers and devices, devices and devices, workstations and devices, devices and people,… The older technologies do not have the ability, by want of adequate operating systems, to access centralized authentication processes. By want of the ability of the ICS network to be broken into very small chunks, the use of centralized authentication is impractical, using the technologies of today. In an IT network, the authentication rules take place in the background and are hidden, for the most part, from the end user. In an ICS network, the authentication rules take place in the foreground and require interaction with the end user, causing delay and frustration.

Patching or upgrading an ICS has many pitfalls. The field device must be taken out of service which may require stopping the process being controlled. This in turn may cost many thousands of dollars and impact thousands of people. An important issue is how to protect unpatchable, unsecurable workstations such as those still running NT Service Pack 4, Windows 95, and Windows 97. Many of these older workstations were designed as part of plant equipment and control system packages and cannot be replaced without replacing the systems. Additionally, many Windows patches in the ICS world are not standard Microsoft patches but have been modified by the ICS supplier. Implementing a generic Microsoft patch can potentially do more harm than the virus or worm against which it was meant to defend. As an example, in 2003 when the Slammer worm was in the wild, one ICS supplier sent a letter to all of their customers stating that the generic Microsoft patch should not be installed as it WOULD shut down the ICS. Another example was a water utility that patched a system at a Water Treatment Plant with a patch from the operating system vendor. Following the patch, they were able to start pumps, but were unable to stop them!

The disconnection between senior management in charge of Operations from senior management in charge of security is leading to vendors being tasked to build new technology for reliability, not security purposes. The mantra of “from the plant floor to the Boardroom” is being followed without seriously asking the question of why an executive in the Boardroom would want to control a valve in a plant or open a breaker in a substation. Several years ago, a heat wave caused failures of a large number of electric transformers. In order to address this, the vendor installed

temperature sensing and decided that getting information out to the largest possible audience was the best way to proceed. Consequently, the new transformer was built with a Microsoft IIS webserver integrally built into the transformer (Figure 3). Cyber vulnerable technologies such as Bluetooth and wireless modems are being built-in to ICS field devices. As one vendor claims: "They now have a Bluetooth connection for their new distribution recloser. If your line folks and/or engineers would like to sit in the truck on those rainy days checking on the recloser..." This means it is possible to get onto the SCADA network far downstream of the corporate firewall. In many cases, it is not possible to bypass the vulnerable remote access without disabling the ICS devices.

UNIT SUBSTATIONS NOW WEB-ENABLED TO SIMPLIFY ACCESS TO POWER TRANSFORMER DATA

Aug. 29, 2005 – Equipped with an Ethernet interface and Web server, Vendor A Unit Substations now provide simple, affordable access to power system information – including transformer coil temperatures – using a standard Web browser. The pre-engineered equipment ships in standard lead-times and connects to a customer's existing Ethernet Local Area Network much like adding a PC or printer.

Unit substations include a Temperature Controller, which provides remote access to transformer data, in addition to its primary role in controlling cooling fans. With a simple click of a mouse, it is easy to monitor transformer coil temperatures per phase, and verify cooling fan status at a glance. Among the many potential benefits, these new capabilities make it possible to correlate circuit loading with transformer temperatures to extend equipment life.

The typical unit substation incorporates Medium Voltage Metal-Enclosed Switchgear on the primary side and Low Voltage Switchgear or Low Voltage Switchboard on the secondary.

Vendor A was the first manufacturer in the world to embed an Ethernet interface and Web server into its power distribution equipment, allowing customers easier access to power system information. The family of power distribution equipment includes medium and low voltage switchgear, unit substations, motor control centers, switchboards and panelboards.

Figure 3 Distribution Transformer with Built-in Webserver

A great concern is the integration of ICS systems with other systems such as Geographical Information Systems (GIS) or customer information systems. The unintended consequences of incompatible software or inappropriate communications have caused significant cyber incidents. This is an insidious problem because the individual systems work as designed, while the vulnerability is the interconnection of individually secure systems. In one case, the rebooting of a control system workstation that was not even on the control system network directly led to the automatic shutdown of a nuclear power plant. In this case, both the workstation and the PLC worked exactly as designed – two rights made a wrong. In another instance, incompatible software turned a fossil power plant into a "yo-yo" causing it to swing from maximum load to minimum load and back, within configured parameters, for three hours causing extreme stress to the turbine rotor.

There are currently very few forensics to detect or prevent these types of events, thus pointing to the need for additional or improved monitoring and logging. This lack of ICS cyber forensics has two aspects. The first is for performing forensics on COTS operating systems (e.g., Windows). The second and more challenging issue is how to perform cyber forensics on an antique 1200 baud modem to determine if a cyber event has occurred. Technologies exist, but will removing a hard drive actually impact the restart and operation of an ICS?

One final concern almost seems trivial but isn't. In most tabletop exercises, the ultimate fix is to "pull the plug" (isolate the ICS from all others). Unfortunately, in complex ICS implementations, it may not be possible to know if the ICS really has been isolated. Consequently, a very important issue is to determine how an organization can tell if the ICS has been isolated and also if any Trojans have been left that can affect restart.

Why do we care

It is often, but mistakenly, assumed that a cyber security incident is always a premeditated targeted attack. However, NIST defines a Cyber Incident[6] as: "An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability (CIA) of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Incidents may be intentional or unintentional." Unintentional compromises of CIA are significantly more prevalent and can have severe consequences, but this does not seem to be part of many current discussions of ICS cyber security. The direct cause of many ICS cyber incidents are unintentional human error. This phenomenon must be addressed by cyber security standards if they are to be effective. It is important to note that protecting ICS from these unintentional compromises also protects them from intentional compromise and outside threat.

Contacts throughout industry have shared details and adverse affects of more than 125 confirmed ICS cyber security incidents to date. The incidents are international in scope (North America, South America, Europe, and Asia) and span multiple industrial infrastructures including electric power, water, oil/gas, chemical, manufacturing, and transportation. With respect to the electric power industry, cyber incidents have occurred in transmission, distribution, and generation including fossil, hydro, combustion turbine, and nuclear power plants. Many of the ICS cyber

[6] National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006. http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

incidents have resulted from the interconnectivity of systems, not from lack of traditional IT security approaches such as complex passwords or effective firewalls. Impacts, whether intentional or unintentional, range from trivial to significant environmental discharges, serious equipment damage, and even deaths.

Figure 4 shows the result of a Bellingham, WA, pipe rupture which an investigation concluded was not caused by an intentional act. Because of the detailed evaluation by NTSB, this is arguably the most documented ICS cyber incident. According to the NTSB Final Report, the SCADA system was the proximate cause of the event. Because of the availability of that information, a detailed post-event analysis was performed which provided a detailed time line, examination of the event, actions taken and actions that SHOULD HAVE been taken [7].

Figure 4 Bellingham, WA Gasoline Pipeline Rupture

Figure 5 is a picture of the Idaho National Laboratory (INL) demonstration of the capability to intentionally destroy an electric generator from a cyber attack.[8]

[7] "Bellingham, Washington Control System Cyber Security Case Study", Marshall Abrams, MITRE, Joe Weiss, Applied Control Solutions, August 2007, http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Bellingham_Case_Study_report%2020Sep071.pdf

[8] http://news.yahoo.com/s/ap/20070927/ap_on_go_ca_st_pe/hacking_the_grid_13

Figure 5 INL Demonstration of Destroying Large Equipment via a Cyber Attack

An attempt was made to categorize the severity of these events. The prevailing view has been there have been no significant ICS cyber incidents, but that industry will respond when a significant event occurs. Consequently, a database of ICS cyber incidents was examined to determine the level of severity of these incidents. Arbitrarily, three levels of severity were developed based on impacts:

Severe
This represents failures, omissions, or errors in design, configuration, or implementation of required programs and policies which have the potential for major equipment and/or environmental damage (more than millions of dollars); and/or extreme physical harm to facilities' personnel or the public; and/or extreme economic impact (bankruptcy).

Example: The Bellingham, WA gasoline pipeline rupture's impact was 3 killed, $45M damage, and bankruptcy of the Olympic Pipeline Company. Forensics were not available to determine the actual root cause. This incident would not have been prevented by mainstream IT security policies or technologies.

Moderate
This represents failures, omissions, or errors in design, configuration, or implementation of required programs and policies which have the potential for moderate equipment and/or environmental damage (up to hundreds of thousands of dollars) with at most some physical harm to facility personnel or the public (no deaths).

Examples: 1) Maroochy (Australia) wireless hack caused an environmental spill of moderate economic consequence. This incident would not have been prevented by mainstream IT security policies or technologies. 2) Browns Ferry 3 Nuclear Plant Broadcast Storm could have been caused by a bad Programmable Logic Controller (PLC) card, insufficient bandwidth, or caused by mainstream IT security testing. Forensics were not available to determine the actual root cause. This incident would not have been prevented by mainstream IT security policies or technologies.

Minor
This represents failures, omissions, or errors in design, configuration, or implementation of required programs and policies which have the potential for minimal damage or economic impact (less than $50,000) with no physical harm to facility personnel or the public.

Example: Davis Besse Nuclear Plant cyber incident caused by a contractor with a laptop contaminated by the Slammer worm plugging into the plant Safety Parameter Display System. This incident could have been prevented by mainstream IT security policies.

From the incident database, many of the incidents would have been judged to be Moderate or Severe. Most would not have been detected nor prevented by traditional IT security approaches because they were caused by the system interconnections or inappropriate policies or testing – not by mainstream IT cyber vulnerabilities. In order to improve security and avoid vast expenditures on systems and equipment without real improvements in automation network security, there is a critical need to examine previous ICS cyber incidents to determine if there are patterns in these incidents, what technologies would detect such events, and what policies should be followed. For mainstream IT security approaches to be effective, they need to be combined with ICS expertise that appreciates potential impact on facilities. Examination of ISA SP99 requirements and risk definitions and tools such as the Cyber Security Self-Assessment Tool (CS2SAT)[9] make it clear that consequences must be understood in terms of the effects on facilities, major impact on equipment, environmental concerns, and public safety.

One way to move towards cross-sector convergence in cyber security ways and means is for all stakeholders to use the same terminology and to eliminate duplicative or overlapping sets of security standards' requirements. NIST offers a set of high-quality publications addressing most of the relevant managerial, administrative, operational, procedural, and technical considerations. Each of these publications, such as SP 800-53, have been put through a significant international public vetting process, including, to the extent possible, by authorities in the national security domain. NIST offers its documents to all organizations interested in using them as a basis for developing in-common standards within the ICS community. The recent Nuclear Regulatory Commission Draft Regulatory Guide 5022 specifically references NIST SP 800-53 and other appropriate NIST documents.

Incentives versus Regulation

Because I am very familiar with the electric power industry, I will focus on that segment. However, the information and experience from this segment generalizes across the entire critical infrastructure.

When the EPRI Enterprise Infrastructure (cyber security) Program was initiated in 2000, control system cyber security was essentially a non-factor – it was a problem of omission. Immediately following 9/11, the Federal Energy Regulatory Commission (FERC) attempted to provide incentives for security improvements by issuing a letter that would allow security upgrades to be included in the rate base. For various reasons, very few utilities took advantage of the offer and little was done. Consequently, in 2003 FERC approached the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Working Group with an ultimatum – do something or FERC would do it to you. In order to preclude regulations, industry promised they would produce cyber security requirements that would comprehensively secure the electric enterprise. The electric industry eventually developed the NERC CIP series of standards and the nuclear industry developed the Nuclear Energy Institute (NEI) guidance documents (NEI-0404). Instead of providing a comprehensive set of standards to protect the electric infrastructure, the NERC CIPs and NEI-0404 were ambiguous and with multiple exclusions. The industry went from being vulnerable because of lack of knowledge to now being vulnerable because of

[9] US CERT Control Systems Security Program, http://csrp.inl.gov/Self-Assessment_Tool.html

excluding systems and technologies and then claiming compliance. The electric industry has demonstrated they cannot secure the electric infrastructure without regulation. Other industrial verticals have similarly defaulted. Therefore, regulation is needed.

Recommendations

- Develop a clear understanding of ICS cyber security
- Develop a clear understanding of the associated impacts on system reliability and safety on the part of industry, government and private citizens
- Define "cyber" threats in the broadest possible terms including intentional, unintentional, natural and other electronic threats such as EMP
- Develop security technologies and best practices for the field devices based upon actual and expected ICS cyber incidents
- Develop academic curricula in ICS cyber security
- Leverage appropriate IT technologies and best practices for securing workstations using commercial off-the-shelf (COTS) operating systems
- Establish standard certification metrics for ICS processes, systems, personnel, and cyber security
- Promote/mandate adoption of the NIST Risk Management Framework for all infrastructures or at least the industrial infrastructure subset
- Establish a global, non-governmental Computer Emergency Response Team (CERT) for Control Systems staffed with control system expertise for information sharing
- Establish a means for vetting experts rather than using traditional security clearances
- Establish, promote, and support an open demonstration facility dedicated to best practices for ICS systems
- Provide regulation and incentives for cyber security of critical infrastructure industries
- Include Subject Matter Experts with control system experience at high level cyber security planning sessions
- Change the culture of manufacturing in critical industries so that security is considered as important as performance and safety

Summary

Recognize that first and foremost, ICS systems need to operate safely, efficiently, and securely which will require regulation. ICS cyber vulnerabilities are substantial and have already caused significant impacts including deaths. Security needs to be incorporated in a way that does not jeopardize the safety and performance of these systems. One should view ICS cyber security as where mainstream IT security was fifteen years ago – it is in the formative stage and needs support to leapfrog the previous IT learning curve. There is a convergence of mainstream IT and control systems that will require both areas of expertise. To ensure that ICS are adequately represented, include subject matter experts with control systems experience in all planning meetings that could affect these systems. The prevailing perception is the government will not protect confidential commercial information and organizations such as ISACs will act as regulators. This has Sarbanes-Oxley implications as well. It is one reason why the US CERT, which is government-operated, does not work as effectively as needed and a "CIRT for Control Systems" by a global non-governmental organization with credible control system expertise is required.