Nuclear Cyber Security

Section One	Lesson Plan
Section Two	Module PPT
Section Three	Pre Assessment Test & Answer Key Post Assessment Test & Answer Key
Section Four	Module Glossary & Acronyms

RCNET

RCNET Nuclear Cyber Security Module

Topic

RCNET module on Securing SCADA (Supervisory Control And Data Acquisition) Systems. This module will help you understand and identify the necessary steps taken to secure your SCADA environment.

Module Introduction / Brief Lesson Description

We will discuss all three controls with a focus on SCADA systems.
This module will facilitate the increasingly urgent need to strengthen the security of our industrial networks and automation systems. Even though the attacks themselves will continue to evolve, the methods provided here will help to prepare against the inevitable advancement of industrial network threat.

Learning Objectives / Outcomes

Upon completion of this module, students will be able to:

1. Develop and reinforce a common language and understanding of Industrial Control System (ICS) cybersecurity as well as the important considerations that come with cyber-to-physical operations within these environments.
2. Demonstrate the necessary cyber-to-physical knowledge to better understand the importance of ICS operational drivers and constraints that require specific safety protection, communications needs, system management approaches, and cybersecurity implementations.
3. Know the adversary's approaches to attacking an ICS SCADA environment to be better prepared to defend that environment.
4. Develop a better understanding of where specific attack vectors exist, as well as the tools to use to discover vulnerabilities and exploit them along with specific capabilities available on servers, workstations, and applications, students will now learn network-specific defense approaches.
5. Better understand attacks targeting the types of web servers used on many ICS devices for management purposes.
6. Discuss essential ICS-related server and workstation operating system capabilities, implementation approaches, and system management practices.
7. Examine concepts that benefit SCADA ICS systems such as system hardening, log management, monitoring, alerting, and audit approaches, then look at some of the more common applications and databases used in ICS environments across multiple industries.
8. Implement technologies used to defend ICS networks.
9. Discuss the various models, methodologies, and industry-specific regulations that are used to govern what must be done to protect critical SCADA ICS systems.

Procedure for Using the RCNET Module

This module was designed to be taught over a period of six lecture hours, as outlined below. However, the teacher may modify this curriculum, as needed, to fit into specific program allowances.

Prior to Starting:	Review module material included in this packet	
	Gather module materials, included and not included in this packet (see the **List of Materials** section)	
	Print class set of the pre-assessments to hand out during class.	
	If providing hard copies of the PPT, print class set to hand out after the pre-assessment.	
Day One, Hours 1-2:	1	Introduce topic. Ask questions to generate discussion. (See Lecture Notes, included with PPT, for specific questions.)
	2	Start student presentation. Introduce the topic, module introduction, learning objectives, and module topics
	3	STOP the PPT.
	4	Administer Pre-Assessment. Explain to students that this assessment is to gauge their pre-existing knowledge of Cyber Security and will not count as a grade in the course.
	5	Collect pre-assessments for grading.
	6	Hand out pre-printed student slides (if using).
	7	If time permits, continue module, using PPT and lecture notes
	8	Pause at Slide 19 in Section 1 to perform the interactive exercise. (see **Interactive Activity** section for specific details)
	9	If time permits, continue module, using PPT and lecture notes
	10	End day one of module.
Day Two, Hours 3-4:	11	Briefly review topics discussed on previous day.
	12	Review results of pre-assessment. Tests can be handed back to students for discussion, but should be re-collected at the end of the discussion.
	13	Continue module, using PPT and lecture notes. Engage students in module by asking questions in lecture notes and allowing open discussion.
	14	End day two of module.
Day Three, Hours 5-6:	15	Briefly review topics discussed on previous days.
	16	Continue module, using PPT and lecture notes. Engage students in module by asking questions in lecture notes and allowing open discussion.
	17	Review takeaways and learning objectives to prepare students for post assessment.
	18	Administer Post-Assessment. The post-assessment can be administered by any of the following methods: -- Same day with open books/notes -- Same day without books/notes -- Next day to allow students time to study on their own -- At a later day in the campus assessment center
	19	Collect post-assessment, grade with provided key and provide feedback to students.

List of Materials

Below is a list of required and optional materials for this RCNET module. Materials may be modified for specific program allowances.

Required:	*RCNET Module - Nuclear Cyber Security* PPT with Lecture Notes
	AV equipment with connection to a computer equipped with Microsoft PowerPoint
Optional:	Printed class set of *RCNET Module - Nuclear Cyber Security* PPT student handout (master included in this packet)
	Printed class set of Pre -Assessment (master included in this packet)
	Printed class set of Post -Assessment (master included in this packet)
	Supplemental & Enrichment Material (included in this packet)

Lesson Plan & Scope of Work

1. Introduction, Learning Objectives, & Module Topics

Slide 1

This RCNET training is on Securing SCADA (Supervisory Control And Data Acquisition) Systems. This module will help you understand and identify the necessary steps taken to secure your SCADA environment.

Industrial control system (ICS) is a general term that encompasses several types of control systems used in industrial production, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other smaller control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures.

We will discuss all three controls with a focus on SCADA systems.
This module will facilitate the increasingly urgent need to strengthen the security of our industrial networks and automation systems. Even though the attacks themselves will continue to evolve, the methods provided herein should help to prepare against the inevitable advancement of industrial network threat.

Slide 2 Suggested ACADs and sample Program Courses where this module may fit into your nuclear program.

ACADs

1.1.9.2.6 Davis-Besse Nuclear Power Station event
5.1.1.2.1.12 theory of operations of plant electrical components
5.1.2 Plant Systems and Components Knowledge
5.1.2.15 Identify abnormal system and component indications and diagnose the probable causes

P**rogram Courses**

ETP 1230 Power Plant Systems
ETP 1220 Power Plant Fundamentals
ETI 1000 Industrial Plant Tools Equipment
ETI 1701 Industrial Safety

EET 1724C Electronic Design Software Tools
EET 1724C Electronic Design Software Tools

ETP 2930 Special Topics in Electrical Power Technology
ETP 2941 Professional Internship for Maintenance Technicians

Slide 3 Learning Objectives

Upon completion of this module, students will be able to:

1. Develop and reinforce a common language and understanding of Industrial Control System (ICS) cybersecurity as well as the important considerations that come with cyber-to-physical operations within these environments.

2. Demonstrate the necessary cyber-to-physical knowledge to better understand the importance of ICS operational drivers and constraints that require specific safety protection, communications needs, system management approaches, and cybersecurity implementations.

3. Know the adversary's approaches to attacking an ICS SCADA environment to be better prepared to defend that environment.

4. Develop a better understanding of where specific attack vectors exist, as well as the tools to use to discover vulnerabilities and exploit them along with specific capabilities available on servers, workstations, and applications, students will now learn network-specific defense approaches.

	5. Better understand attacks targeting the types of web servers used on many ICS devices for management purposes. 6. Discuss essential ICS-related server and workstation operating system capabilities, implementation approaches, and system management practices. 7. Examine concepts that benefit SCADA ICS systems such as system hardening, log management, monitoring, alerting, and audit approaches, then look at some of the more common applications and databases used in ICS environments across multiple industries. 8. Implement technologies used to defend ICS networks. 9. Discuss the various models, methodologies, and industry-specific regulations that are used to govern what must be done to protect critical SCADA ICS systems
Slide 4	This module is broken down into five sections: 1. What is Cyber Security & SCADA?, 2. ICS attack surface 3. Nuclear Case studies 4. Specific actions that can be taken to increase the security of SCADA networks 5. Roles and responsibilities of management to ensure the security of SCADA networks
2. What is Cyber Security & SCADA?	
Slide 5	Section one is an overview of SCADA systems, followed by a look at some answers to questions about Cyber-security as well as a video clip about Stuxnet and finally identify seven high-level findings that impact control systems today.
Slide 6	A SCADA (Supervisory Control And Data Acquisition) system is a purely software layer, normally applied a level above control hardware within the hierarchy of an industrial network. As such, SCADA systems do not perform any control, but rather function in a supervisory fashion. The focus of a SCADA is data acquisition and the presentation of a centralized Human Machine Interface (HMI), although they do also allow high level commands to be sent through to control hardware - for example the instruction to start a motor or change a set-point. SCADA systems are tailored towards the monitoring of geographically diverse control hardware, making them especially suited for industries such as utilities distribution where plant areas may be located over many thousand square kilometers
Slide 7	SCADA systems historically distinguish themselves from other ICS systems by being large scale processes that can include multiple sites, and large distances. These processes include industrial, infrastructure, and facility-based processes.
Slide 8	(SCADA) is an industrial control system which is used in many modern industries like energy, manufacturing, power, water transportation, etc. SCADA systems organize multiple technologies that allows to process, gather and monitor data at the same time to send instructions to those points that transmit data. In today's world, almost anywhere you can observe SCADA systems, whether it's a waste water treatment plant, supermarkets, industries or even in your home. As the power system deals with power generation, transmission and distribution sectors, monitoring is the main aspect in all these areas. Thus the SCADA implementation of power system improves the overall efficiency of the system for optimizing, supervising and controlling the generation and transmission systems. SCADA function in the power system network provides greater system reliability and stability for integrated grid operation

Slide 9	The control hardware that communicates with a SCADA is referred to as an Remote Terminal Unit (RTU) and is usually a type of specialized PLC. The device to which the RTUs communicate is known as a Master Terminal Unit (MTU). The remote location of RTUs imposes many restraints on the system and is a core aspect of the manner in which SCADA systems are designed. The functions of SCADA in power generation include: Continuous monitoring of Speed and Frequency Geographical monitoring of coal delivery and water treatment processes Supervising the status of circuit breakers, protective relays and other safety related operations Generation operations planning Active and reactive power control Turbine protection Load scheduling Historical data processing of all generation related parameters
Slide 10	The term SCADA is usually used to describe systems in which the monitoring and control of a large industrial campus is centralized. Most control functions are performed automatically by RTUs or PLCs, with central control functions being restricted to supervisory level intervention. A PLC may control the flow of coolant for an industrial process, for example, but an operator may be able to override flow controls or initiate emergency action. Data acquisition starts with the RTU or PLC, and includes sensor readings and equipment status data that are transmitted to the SCADA supervisory system. The data thus acquired is put into human-readable format so that an operator can use it to make a decision whether or not to intervene or adjust control parameters. In the longer term, historical data can be collected and used for auditing and process performance analysis.

Slide 11	The following two slides will discuss the various personnel and the roles in a SCADA work place.
Slide 12	Base Knowledge- Training focuses on security behaviors for individuals who interact with, operate, or support Industrial Control Systems. Training program may introduce ICS, the risks or types of ICS attacks, basic system and network defense sand controls, as well as typical SCADA ICS governance and policy best practices. Program goal should change human behavior in a SCADA ICS environment and reduce risk. Essentials Knowledge- Training program should provide a foundational set of standard skills and knowledge for industrial cybersecurity professionals. The training should ensure that the workforce involved in supporting and defending industrial control systems are trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats. Mastery Knowledge- Training should be role specific and focus on individual and organizational needs to advance knowledge, skills, and ability in a specific field. Expert Knowledge- Training should focus on coordinated response and improvement of team capabilities. This level is typically achieved in joint exercises and projects. Technical Leader- Training should focus on management and technical team development as well as methods for interacting with other teams and communicating technical concepts to non-technical
Slide 13	The following is a list of all the specific roles in an Industrial Control System environment.

Engineering

Process Engineer
- Electrical, Controls, and Mechanical Engineer
- Project Engineer
- Systems and Reliability Engineer
- OT Developer
- PLC Programmer
- Emergency Operations Manager
- Plant Networking
- Control/Instrumentation Specialist
- Protection and Controls
- Field Engineer
- System Integrator Operations

Support Staff

- Remote Maintenance & Technical Support
- Contractors (engineering)
- IT and Physical Security Contractor
- Procurement Specialist
- Legal
- Contracting Engineer
- Insurance
- Supply-chain Participant
- Inventory Management/Lifecycle Management
- Physical Security Specialist

IT Cybersecurity

- ICS Security Analyst
- Security Engineering and Architect
- Security Operations
- Security Response and Forensics
- Security Management (CSO)
- Audit Specialist
- Security Tester

Operations Technology

- Operator
- Site Security POC
- Technical Specialists (electrical/mechanical/chemical)
- OT Security
- ICS/SCADA Security
- ICS/SCADA Programm

Management

IT Staff

	• Plant Manager • Risk/Safety Manager • BU Management • C-level Management	• Networking and Infrastructure • Host Administrator • Database Administrator • Application Development • ERP/MES Administrator
Slide 14	The following section will go over cyber-security and how it relates to SCADA systems	
Slide 15	Industrial Control Systems (ICS) have been in existence for decades in the United States. These systems are relatively unknown to the general public and were designed to control our critical infrastructure such as utilities (electricity, nuclear power, and water treatment plants). Until recently, these systems were connected to company networks by privately owned IT networks based on private line technology. Public utility companies have begun to connect ICS networks to public networks such as the Internet as they transition to TCP/IP based networks. This trend is accomplishing the much needed modernization of the nation's IT networks supporting the critical infrastructure and setting the groundwork for developing the federally mandated Smart Grid. The ICS network transition to public networks has many benefits and risks. The increased risk to the smart grid must be addressed and an increase in training to better prepare individuals responsible for defending SCADA environments	
Slide 16	Shared learning translates into results - effective security requires the integration of cybersecurity professionals, ICS support staff, and engineers. Tremendous gains are being achieved in industrial applications by sharing and analyzing data, but we need professionals who can address the security challenges.	
Slide 17	Security in industrial networks bears a strong resemblance to that of commercial networks due to the growing overlap of the technologies used in both. While many of the same threats exist to both networks, the additional requirements and considerations of industrial networks mean that security may often be more difficult to implement. The goal of network security is to provide confidentiality, integrity of information, availability, authentication, authorization, auditability, non-reputability and protection from third parties. Securing industrial networks has become a prerequisite for securing critical infrastructure at a national level especially where Nuclear Power Plants are concerned. This is true for all industrialized nations and a greater dependence on the development and implementation of industrial network security is realized as greater levels of automation and computer-dependence is implemented within chemical processing, utility distribution and discrete manufacturing	

Slide 18	Note the Benefit Enrollment in the email and how easy it is to fool someone. Discuss the video clip and go over the following points in regards to Stuxnet: Stuxnet specifically targets PLCs, which allow the automation of electromechanical processes such as those used to control machinery on factory assembly lines, amusement rides, or centrifuges for separating nuclear material. Stuxnet has three modules: a worm that executes all routines related to the main payload of the attack; a link file that automatically executes the propagated copies of the worm; and a rootkit component responsible for hiding all malicious files and processes, preventing detection of the presence of Stuxnet. Stuxnet is typically introduced to the target environment via an infected USB flash drive. The worm then propagates across the network, scanning for Siemens Step7 software on computers controlling a PLC.
Slide 19	With over eight million sensors that emulate over six thousand applications – from Apple laptops, to ATM machines, to critical infrastructure systems, to closed-circuit TV cameras - the Norse Intelligence Network gathers data on who the attackers are and what they're after. Norse delivers that data through the Norse Appliance, which pre-emptively blocks attacks and improves your overall security ROI, and the Norse Intelligence Service, which provides professional continuous threat monitoring for large networks. Ask students about what information could be assessed from this site. Go over the information with them and ask what they could deduce from it. Ask students about what information could be assessed from this site. Go over the information with them and ask what they could deduce from it and why this is important. (You would know where the threats are coming from and which attacks are being used)
Slide 20	Respondents to the Consulting-Specifying Engineer 2015 Electrical and Power Study identified seven high-level findings impacting the electrical and power industries today. They are discussed in the next two slides.
Slide 21	1.Threat levels: Forty-seven percent of respondents perceive their control systems to be moderately threatened by cyber attacks, while 25% say theirs are highly threatened and 8% are at a severe threat level. 2.Most concerning threat: Malware from a random source is the most concerning control system threat for 35% of respondents. Another 18% are worried about theft of intellectual property, and 8% fear attacks from "hacktivists" with a political or environmental agenda. 3.Vulnerable system components: The top most vulnerable system components within respondents' organizations are connections to other internal systems (70%), computer assets (70%), network devices (67%), and wireless communication devices and protocols used in automation systems (60%). 4.Vulnerability assessments: One in four respondents reported that their organizations have performed some type of vulnerability assessment within the past three months. The average facility has checked their vulnerabilities within the past seven months

Slide 22	5.Cyber-related incidents: Nearly half of respondents have experienced a malicious cyber incident into their control system networks and/or control system cyber assets—that they are aware of—within the past 24 months. Forty-three percent of these attacks were accidental infections, 8% were targeted in nature, and 38% were both accidental and targeted. 6.Mobile devices: Thirty percent of organizations do not allow mobile devices—such as smart phones and tablets—to connect to networks or enter work areas, while 21% allow network access, and 15% allow them in the work areas only. 7.Training: Half of respondents said their organizations train employees on identifying things that may indicate a cyber incident or attack, and another 34% train them on identifying social engineering attacks.
Slide 23	**Takeaways** SCADA - Supervisory Control And Data Acquisition – is software layer, normally applied a level above control hardware within the hierarchy of an industrial network. Cyber Security is the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation. Cyber Security is necessary for all levels of employees, from entry to upper. The demand for expertise and technical know-how increase with each level of added responsibility. Nuclear Technicians must develop cybersecurity skills to defend national critical infrastructure.

3. SCADA ICS Attack Surface	
Slide 24	There has been an increase of publicly disclosed vulnerabilities in Supervisory Control and Data Acquisition (SCADA) software systems. This wave of reports underlines the ever increasing interest in analyzing the security of such systems. We are going to discuss the vulnerable components of SCADA software systems. SCADA systems related to industrial processes are broken up into manufacturing, production, electric grids and large communication systems that make large use of these technologies. The principal question is: are governments able to secure their infrastructures from cyber-attacks? SCADA components are considered privileged targets for cyber-attacks. By using cyber tools, it is possible to destroy an industrial process. This was the idea used on the attack to the nuclear plant in Natanz, in order to interfere with Iranian nuclear program. Despite the fact that western countries have been the first to explore the possibility of a cyber-offensive using a cyber-weapon, and in spite of the high interest of the US government in the matter, governments are conscious that the infrastructures of respective countries are still vulnerable to cyber-attacks. This section discusses the challenges of the attack surfaces SCADA environments face today.
Slide 25	The Attack Surface describes all of the different points where an attacker could get into a system, and where they could get data out. The Attack Surface of an application is: the sum of all paths for data/commands into and out of the application, and the code that protects these paths (including resource connection and authentication, authorization, activity logging, data validation and encoding), and all valuable data used in the application, including secrets and keys, intellectual property, critical business data, personal data and PII, and the code that protects these data (including encryption and checksums, access auditing, and data integrity and operational security controls). Examples of attack surface in the real world include: --Open ports on outward facing web and other servers, code listening on those ports --Services available on the inside of the firewall --Code that processes incoming data, email, XML, office documents, industry-specific custom data exchange formats (EDI) --Interfaces, SQL, web forms --An employee with access to sensitive information is socially engineered When considering attack surface to develop a defense-in-depth architecture, there are three basic interrelated considerations that develop from our examples: Network Attack Surface, the attack will often be delivered via a network Software Attack Surface, with a primary focus on web applications Human Attack Surface, social engineering, errors, trusted insider, death and disease

Slide 26	Revealing system data or debugging information helps an adversary learn about the system and form a plan of attack. An information leak occurs when system data or debugging information leaves the program through an output stream or logging function. Information and resources are available to potential adversaries and intruders of all calibers around the world. With the available information, it is quite possible for an individual with very little knowledge of control systems to gain unauthorized access to a control system with the use of automated attack and data mining tools and a factory-set default password.
Slide 27	Information leakage happens whenever a system that is designed to be closed to an eavesdropper reveals some information to unauthorized parties nonetheless. For example, when designing an encrypted instant messaging network, a network engineer without the capacity to crack encryption codes could see when messages are transmitted, even if he could not read them.
Slide 28	When trying to keep information confidential, an attacker can often infer some of the information by using statistics. Have students think of some other examples and discuss.
Slide 29	In situations where data should not be tied to individual users, but a large number of users should be able to make queries that "scrub“(purge) the identity of users, it may be possible to get information about a user -- e.g., by specifying search terms that are known to be unique to that user.
Slide 30	Translucent Databases deals with the issue of building applications that store and manipulate sensitive data in a very accessible and pragmatic fashion. This is the link to the book referred to in slide: http://www.amazon.com/Translucent-Databases-2Nd-Authentication-Steganography/dp/1441421343/ref=asap_bc?ie=UTF8 In situations where data should not be tied to individual users, but a large number of users should be able to make queries that "scrub" the identity of users, it may be possible to get information about a user - e.g., by specifying search terms that are known to be unique to that user.
Slide 31	The accidental leaking of sensitive information through sent data refers to the transmission of data which is either sensitive in and of itself, or useful in the further exploitation of the system through standard data channels. Implementation: The final decision as to what data is sent is made at implementation time. Ensure that any possibly sensitive data specified in the requirements is verified with designers to ensure that it is either a calculated risk or mitigated elsewhere.
Slide 32	Control systems are a device, or set of devices, that manages, commands, directs or regulates the behavior of other devices or systems. Industrial control systems are used in industrial production for controlling equipment or machines. Industrial control system (ICS) is a general term that encompasses several types of control systems used in industrial production, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other smaller control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures
Slide 33	The control server hosts the DCS or PLC supervisory control software that communicates with lower-level control devices. The control server accesses subordinate control modules over an ICS network. ICSs are typically used in industries such as electrical, water, oil, gas and data. Based on data received from remote stations, automated or operator-driven supervisory commands can be pushed to remote station control devices, which are often referred to as field devices. Field devices control local operations such as opening and closing valves and breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions.

Slide 34	SCADA systems operate widely dispersed control systems and acquire system data for monitoring and control at the central server, or MTU. MTU (Master Terminal Unit) or SCADA Server, is the device that acts as the master in a SCADA system. The data acquisition process is integral to system functions, the acquired data critical to operational integrity. SCADA systems control crucial infrastructure, including the power grid, oil and gas pipelines, railway traffic, water distribution, and waste treatment plants. Any significant disruption to a critical SCADA system could directly threaten public health and safety. SCADA may include some or all of the components defined above, plus additional specialized components not described here.
Slide 35	The following slides will discuss some possible incident scenarios that can create vulnerabilities within SCADA control systems.
Slide 36	Unauthorized changes made to programmed instructions in PLCs, RTUs, DCS, or SCADA controllers, alarm thresholds changed, or unauthorized commands issued to control equipment, which could potentially result in damage to equipment (if tolerances are exceeded), premature shutdown of processes (such as prematurely shutting down transmission lines), causing an environmental incident, or even disabling control equipment Password policies are needed to define when passwords must be used, how strong they must be, and how they must be maintained. Without a password policy, systems might not have appropriate password controls, making unauthorized access to systems more likely
Slide 37	As a direct result of the intrinsic vulnerabilities of the SCADA protocol, attackers having access to the process network can easy impersonate a set of PLCs and provide false information to the SCADA server. The effect of this attack has a significant chain effect. In fact, since the information provided by the PLCs to the Master is aggregated and provided to the operational databases, and then used by the diagnostic systems and by the high level control centers, a similar attack could drive the operators in a completely wrong direction, with potentially catastrophic effects. A possible implementation of that attack scenario could be the following: 1. The attacker (or the malware written by the attacker), perform a DOS against a set of PLCs in order to block the data flow between them and the SCAD/Master. 2. The attacker (or the malware) impersonates the blocked PLCs 3. The attacker (or the malware) provides false data to the Master
Slide 38	Always avoid default values for any system Almost all are public information that can be acquired through the internet. The Real-time Control System (RCS) is a software system developed by NIST based on the Real-time Control System Reference Model Architecture, that implements a generic Hierarchical control system. The RCS Software Library is an archive of free C++, Java and Ada code, scripts, tools, make files, and documentation developed to aid programmers of software to be used in real-time control systems .
Slide 39	Interfering with the mechanics of safety at sites can lead to some SCADA networks potentially vulnerable to disruption of service, process redirection, or manipulation of operational data that could result in public safety concerns and/or serious disruptions to the nation's critical infrastructure. Items typically found in this are include all items identified in Level 0 and 1 with a dedicated purpose for a safety control function like; acoustic monitoring, liquid chemistry monitoring, vibration monitoring, emission monitoring and in most safety systems there exists a control function that serves to protect the operation and personnel.

Slide 40	Stuxnet is a great example. Stuxnet specifically targets PLCs, which allow the automation of electromechanical processes such as those used to control machinery on factory assembly lines, amusement rides, or centrifuges for separating nuclear material. Exploiting four zero-day flaws, Stuxnet functions by targeting machines using the Microsoft Windows operating system and networks, then seeking out Siemens Step7 software. Define: Virus- A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting (i.e., inserting a copy of itself into and becoming part of) another program. A virus cannot run by itself; it requires that its host program be run to make the virus active. Worm- A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively. Trojan Horse- A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.
Slide 41	The question of whether the data processed by the system is sensitive and subject to compromise or loss, must be examined in order to determine how best to protect it. The question should be asked; Is the data returned by the process of a sensitive nature such that loss, modification or compromise of the data, either intentional or unintentional, will cause serious harm to the organization's mission? Discuss.
Slide 42	**Takeaways**: Unauthorized changes made to programmed instructions in PLCs, RTUs, DCS, or SCADA controllers, could potentially result in damage to equipment. False information sent to control system operators either to disguise unauthorized changes or to initiate inappropriate actions by system operators. Control system software or configuration settings modified, producing unpredictable results. Safety systems operation that have been interfered with could lead to vulnerabilities. Malicious software (e.g., virus, worm, Trojan horse) introduced into the system. Recipes (i.e., the materials and directions for creating a product) or work instructions modified in order to bring about damage to products, equipment, or personnel.

4. Nuclear Case Studies	
Slide 43	Section III will discuss actual case studies. These case studies help us to understand that a successful cyber-attack on a control system could result in significant physical damage, loss of life, and cascading effects that could disrupt or destroy critical infrastructure at a local, regional, and even national level. In addition, significant cyberattacks could also undermine public confidence in the safety, security, and reliability of critical infrastructure. Lessons learned from these studies help critical infrastructure owners and operators do the following: --Identify potential weaknesses or gaps within their ICS network --Understand cybersecurity threats and vulnerabilities --Establish a baseline security posture and pursue risk mitigation options, as appropriate
Slide 44	Case Study #1 Davis-Besse Worm Infection - 2003 at the Davis-Besse Nuclear Power Plant
Slide 45	The design of Slammer was simple; it did not write itself to the hard drive, delete files, or obtain system control for its author. It settled in system memory and searched for other hosts to infect. Removing the worm was as simple as rebooting the server after closing network port 1434, Slammer's point of entry. Installing a patch Microsoft had released six months earlier would eliminate the vulnerability Slammer exploited and prevent another infection. The traffic generated by the worm clogged the corporate and control networks. For four hours and fifty minutes, plant personnel could not access the Safety Parameter Display System (SPDS)
Slide 46	Case Study #2 Browns Ferry Shutdown at the Browns Ferry Nuclear Plant
Slide 47	The condensate demineralizer used a programmable logic controller (PLC); the recirculation pumps depend on variable frequency drives (VFD) to modulate motor speed. Both kinds of devices have embedded microprocessors that can communicate data over the Ethernet LAN. However, both devices are prone to failure in high traffic environments. A device using Ethernet broadcasts data packets to every other device connected to the network. Receiving devices must examine each packet to determine which ones are addressed to them and to ignore those that are not. Without the recirculation pumps, the power plant could not cool the reactor, making a shutdown
Slide 48	Case Study #3 Hatch Automatic Shutdown at Hatch Nuclear Power Plant

Slide 49	This innocent mistake demonstrates how malicious hackers could make simple changes to a business network that end up affecting a nuclear reactor—even if they have no intent to interfere with critical systems. It also demonstrates that plant operators, in this case, did not fully understand the dependencies between network devices. This would make it difficult to identify and protect all the vulnerabilities in a process control system. Due to the growing network connections between control systems and office computers, even seemingly simple actions can have unexpected results. The computer was used to collect diagnostic data from the process control network; the update was designed to synchronize data on both networks.
Slide 50	Case Study #4 Iranian Nuclear Program Map of Iranian Nuclear Plant Sites
Slide 51	It is a misconception that PCS are immune from attack since they are not connected to the internet but Stuxnet did not rely on an internet connection at Natanz. It traveled between computers on worker's thumb drives and infected components destined for Natanz at their source in the Iranian chain of supply. The Stuxnet attack against the Iranian nuclear program demonstrates the impact that a sophisticated adversary with a detailed knowledge of process control systems can have on critical infrastructures. Stuxnet is believed to have destroyed 984 centrifuges at Iran's uranium enrichment facility in Natanz. Lessons learned: (1)Stuxnet spread between sites on USB sticks. Poor USB device control is a best practice violation, and so we took action. Some of us glued USB ports shut. (2) Stuxnet spread across networks for months using zero-day vulnerabilities. Zero-days happen in all software; there is no avoiding them. (3) Stuxnet spread through IT/OT firewalls on SQLServer connections using a Siemens S7 hard-coded password. Hard-coded passwords are a serious best-practice violation.
Slide 52	Case Study #5 South Houston Water System Compromise at South Houston Water Supply Plant

Slide 53	This hack was the result of a vulnerable web server. A hacker identified as 'pr0f' has provided evidence of a successful penetration of South Houston's water supply network. The attacker went on to say, "I'm not going to expose the details of the box. No damage was done to any of the machinery; I don't really like mindless vandalism. It's stupid and silly. On the other hand, so is connecting interfaces to your SCADA machinery to the internet. I wouldn't even call this a hack, either, just to say. This required almost no skill and could be reproduced by a two year old with a basic knowledge of Simatic," PasteBin is a site that has recently (in the last several years) proven to be a popular repository for sensitive data leaks and exposure. This site allows you to "subscribe" to alerts based on content triggers from spidering PasteBin. The link to the site is: http://pastebin.com/
Slide 54	This slide shows a screen shot recently posted online, allegedly from remote access to SCADA systems for the City of South Houston. The posting is said to have been in response to statements Department of Homeland Security's Peter Boogaard made as reported by The Register regarding apparent damage to a water system in Illinois stemming from a cyber attack.
Slide 55	Case Study #6 Havex Trojan. Currently, there is a popular remote access Trojan Horse called Havex that is being used to target Industrial Control Systems. The attack vectors include phishing emails, redirects to compromised web sites and most recently, trojanized update installers on at least 3 industrial control systems (ICS) vendor web sites. It gathers information about industrial control devices and then sends that information back to its command-and-control (C&C) server for the attackers to analyze. Those behind the operation are specifically interested in targeting organizations that use ICS and SCADA (supervisory control and data acquisition) applications. The purpose is to scan local area networks for devices that respond to OPC (Open Platform Communications) requests in addition to more traditional attacks like spam emails and Web-based exploits.

Slide 56	Mitigations to consider : --Enforce strict access control lists and authentication protocols for network level access to OPC clients and servers. --Always keep your patch levels up to date, especially on computers that host public services accessible through the firewall, such as HTTP, FTP, mail, and DNS services. --Maintain up-to-date antivirus signatures and engines, and apply them based on industrial control system vendor recommendations. --Build host systems, especially critical systems such as servers, with only essential applications and components required to perform the intended function. Where possible remove or disable any unused applications or functions to limit the attack surface of the host. --Implement network segmentation through V-LANs to limit the spread of malware. --Exercise caution when using removable media (USB thumb drives, external drives, CDs).
Slide 57	**Takeaways:** --PCS are not immune from attack since they are not connected to the internet. --PCS are not immune from attack since they are different from ordinary computers. --Vulnerabilities are more complicated than both skeptics and alarmists realize. The Davis-Besse incident shows that even operators who try to monitor and protect every connection cannot be sure they know about all of them. Stuxnet traveled on portable thumb drives to infect computers that were not connected to the internet. All four incidents demonstrate that PCS have become interoperable with ordinary computers, making them vulnerable. Alarmists often invoke the danger of hackers taking control of a power plant, but these incidents show how unintelligent computer viruses and even malfunctions in small devices can have big unexpected effects. This suggests that although nuclear facilities are vulnerable to attack, a malicious hacker would have difficulty making sure an attack works precisely as planned. Even so, states are working to make cyber attacks more precise, supplementing their methods with intelligence from other sources.

5. Increase the Security of SCADA Networks: Specific Actions	
Slide 58	Section IV will discuss specific actions to increase the security of SCADA networks. The President's Critical Infrastructure Protection Board and the Department of Energy have developed the steps outlined here to help any organization improve the security of its SCADA networks. These steps are not meant to be prescriptive or all-inclusive. However, they do address essential actions to be taken to improve the protection of SCADA networks. Briefly introduce the sub-sections: --Identify all connections to SCADA networks --Disconnect unnecessary connections to the SCADA network --Evaluate and strengthen connections to the SCADA Network --Harden SCADA networks by removing or disabling unnecessary services --Do Not Rely on Proprietary Protocols to Protect Your System --Implement the security features provided by device and system vendors --Establish strong controls over any backdoor into the SCADA network --Implement internal and external intrusion detection systems 24/7 --Audits SCADA devices and networks to identify security concerns --Conduct physical security surveys and assess all remote sites --Establish SCADA "Red Team" to identify and evaluate susceptible attack
Slide 59	Identify and evaluate the following types of connections: --Internal local area and wide area networks, including business networks --The Internet --Wireless network devices, including satellite uplinks --Modem or dial-up connections --Connections to business partners, vendors or regulatory agencies --Develop a comprehensive understanding of all connections to the SCADA network, and how well these connections are protected
Slide 60	To ensure the highest degree of security of SCADA systems, isolate the SCADA network from other network connections to as great a degree as possible. They must be designed and implemented properly to avoid introduction of additional risk through improper configuration. Strategies such as utilization of "demilitarized zones" (DMZs) and data warehousing can facilitate the secure transfer of data from the SCADA network to business networks.

Slide 61	Since the SCADA network is only as secure as its weakest connecting point, it is essential to implement firewalls, intrusion detection systems (IDSs), and other appropriate security measures at each point of entry. --Strategically place IDSs at each entry point to alert security personnel of potential breaches of network security --Organization management must understand and accept responsibility for risks associated with any connection to the SCADA network. --Use this information in conjunction with risk management processes to develop a robust protection strategy for any pathways to the SCADA network. --Configure firewall rules to prohibit access from and to the SCADA network, and be as specific as possible when permitting approved connections. --Example: an Independent System Operator (ISO) should not be granted "blanket" network access simply because there is a need for a connection to certain components of the SCADA system
Slide 62	Examples of services to remove from SCADA networks include automated meter reading/remote billing systems, email services, and Internet access. An example of a feature to disable is remote maintenance. Also, numerous secure configuration guidelines for both commercial and open source operating systems are in the public domain, such as the National Security Agency's series of security guides. Do not permit a service or feature on a SCADA network unless a thorough risk assessment of the consequences of allowing the service/feature shows that the benefits of the service/feature far outweigh the potential for vulnerability exploitation. Work closely with SCADA vendors to identify secure configurations and coordinate any and all changes to operational systems to ensure that removing or disabling services does not cause downtime, interruption of service, or loss of support
Slide 63	It is extremely not to rely on proprietary protocols or factory default configuration settings to protect your system Demand that vendors disclose any back doors or vendor interfaces to your SCADA systems, and expect them to provide systems that are capable of being secured. You should know of any back doors into your system. Preferably, there should not be any.
Slide 64	Analyze each SCADA device to determine whether security features are present. Most older SCADA systems (most systems in use) have no security features whatsoever Some newer SCADA devices are shipped with basic security features, but these are usually disabled to ensure ease of installation Factory default security settings (such as in computer network firewalls) are often set to provide maximum usability, but minimal security Set all security features to provide the maximum level of security Allow settings below maximum security only after a thorough risk assessment of the consequences of reducing the security level

Slide 65	War driving is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer, smartphone or personal digital assistant (PDA). War dialing is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers by malicious hackers who specialize in breaching computer security - for guessing user accounts (by capturing voicemail greetings), or locating modems that might provide an entry-point into computer or other electronic systems. Successful "war dialing" or "war driving" attacks could allow an attacker to bypass all other controls and have direct access to the SCADA network or resources To minimize the risk of such attacks, disable inbound access and replace it with some type of callback system
Slide 66	Intrusion detection system monitoring is essential 24 hours a day; this capability can be easily set up through a pager. Additionally, incident response procedures must be in place to allow an effective response to any attack. To complement network monitoring, enable logging on all systems and audit system logs daily to detect suspicious activity as soon as possible
Slide 67	Establish strong controls over any medium that is used as a backdoor in a SCADA network via very secure authentication. Many commercial and open-source security tools are available that allow system administrators to conduct audits of their systems/networks to identify active services, patch level, and common vulnerabilities. The use of these tools will not solve systemic problems, but will eliminate the "paths of least resistance" that an attacker could exploit. Track corrective actions and analyze this information to identify trends Retest systems after corrective actions have been taken to ensure that vulnerabilities were actually eliminated. Scan non-production environments actively to identify and address potential problems
Slide 68	You must identify and eliminate single points of failure. The security of the site must be adequate to detect or prevent unauthorized access. Do not allow "live" network access points at remote, unguarded sites simply for convenience. Conduct a physical security survey and inventory access points at each facility that has a connection to the SCADA system. Identify and assess any source of information, including remote telephone/computer or network/fiber optic cables that could be tapped; radio and microwave links that are exploitable; computer terminals that could be accessed; and wireless local area network access points

Slide 69	Use a variety of people who can provide insight into weaknesses of the overall network, SCADA systems, physical systems, and security controls. It is important to feed information resulting from the "Red Team" evaluation into risk management processes to assess the information and establish appropriate protection strategies. People who work on the system every day have great insight into the vulnerabilities of your SCADA network and should be consulted when identifying potential attack scenarios and possible consequences. Ensure that the risk from a malicious insider is fully evaluated, given that this represents one of the greatest threats to an organization.
Slide 70	**Takeaways:** Identify all connections to SCADA networks Disconnect unnecessary connections to the SCADA network Evaluate and strengthen connections to the SCADA Network Harden SCADA networks by removing or disabling unnecessary services Do Not Rely on Proprietary Protocols to Protect Your System Implement the security features provided by device and system vendors Establish strong controls over any backdoor into the SCADA network Implement internal and external intrusion detection systems 24/7 Audits SCADA devices and networks to identify security concerns Conduct physical security surveys and assess all remote sites Establish SCADA "Red Teams" to identify and evaluate possible attacks
6. Management Actions to Increase the Security of SCADA Networks	
Slide 71	Section V will discuss actions management can take to increase the security of SCADA networks. --Clearly define cyber security roles, responsibilities, and authorities --Document network architecture and identify critical systems --Establish a Rigorous, Ongoing Risk Management Process --Establish a Network Protection Strategy Based on the Principle of Defense-in-depth --Clearly Identify Cyber Security Requirements --Establish effective configuration management pocesses --Conduct Routine Self-Assessments --Establish system backups and disaster recovery plans --Senior organizational leadership should establish expectations for cyber security performance and accountability --Establish policies and conduct training
Slide 72	Key personnel need to be given sufficient authority to carry out their assigned responsibilities. Too often, good cyber security is left up to the initiative of the individual, which usually leads to inconsistent implementations and ineffective security. 1. Establish a cyber security organizational structure that defines roles and responsibilities and clearly identifies how cyber security issues are escalated and who is notified in an emergency. 2. Organization personnel need to understand the specific expectations associated with protecting information technology resources through the definition of clear and logical roles and responsibilities.

Slide 73	**LEVEL 0-** Process Control Instrumentation Bus Network Includes the functions involved in transitioning from cyber to physical and from physical to cyber. Items typically found in this zone include; sensors, actuators, motors, process specific automation machinery and field instrumentation devices.
	LEVEL 1- Control Devices include the functions involved at site specific operating environments. Items typically found in this zone include; dedicated operator workstation, Programmable Logic Controllers, control processors, programmable relays, Remote Terminal Units, and process specific microcontrollers
	LEVEL 2- Supervisory Control LAN include the functions involved with operating the real-time control system. Items typically found in this zone include; control center operation workstations, Human Machine Interfaces (HMI), engineering workstations, security event collectors, operations alarm systems, communications front ends, data historians, and network / application administrator workstations.
	LEVEL 3- Operations Support include the functions involved in managing the operations environment. Items typically found in this zone include; operations scheduling resources, reliability tracking tools, operations simulation and modeling tools, contingency analysis tools, replicated historians, and data visualization utilities. There may also be dedicated operations specific IT services such as DHCP, LDAP, DNS, and file servers.
	LEVEL 4- Business Unit or Plant Network IT shared services for a local site, business unit, or subsidiaries. Items typically found in this zone include; local file and print servers, local phone systems, site directory replicas, site specific remote access solutions, security event aggregators, and site specific Internet access points.
	LEVEL 5- Enterprise Business Network corporate level applications used to support Enterprise Business and User Goals. Items typically found in this zone include; Internet access points, Email servers, customer facing web servers, internal web servers, CRM systems, HR systems, corporate directory architectures, enterprise document management systems, and remote access VPN endpoints.
Slide 74	An in-depth understanding of the functions that the systems perform and the sensitivity of the stored information is required. Stress that documenting the information security architecture and its components is critical to understanding the overall protection strategy, and identifying single points of failure. Without this understanding, risk cannot be properly assessed and protection strategies may not be sufficient. Documenting the information security architecture and its components is critical to understanding the overall protection strategy, and identifying single points of failure
Slide 75	Identification of residual risk with an in-place network protection strategy is fundamental to risk management, as well as acceptance of that risk by management. Risk assessments form the technical basis of this understanding and are critical to formulating effective strategies to mitigate vulnerabilities and preserve the integrity of computing resources. Initially, perform a baseline risk analysis on a current threat assessment to develop a network protection strategy. Due to rapidly changing technology and the emergence of new threats on a daily basis, an ongoing risk assessment process is also needed so that routine changes can be made to the protection strategy to ensure it remains effective.

Slide 76	The Defense-In-Depth strategic framework, a multi-layered approach to security, comprehensively addresses security architecture and is accomplished by identifying vulnerabilities across operational, network and host platforms. Countermeasures are deployed at each level to provide security encompassing the entire ICS architecture. Single points of failure must be avoided, and cyber security defense must be layered to limit and contain the impact of any security incidents. Utilize technical and administrative controls to mitigate threats from identified risks to as great a degree as possible at all levels of the network. Defense-in-depth must be considered early in the design phase of the development process, and must be an integral consideration in all technical decision-making associated with the network. Each layer must be protected against other systems at the same layer. Example, to protect against the insider threat, restrict users to access only those resources necessary to perform their job functions.
Slide 77	A formal program is essential for establishing a consistent, standards-based approach to cyber security throughout an organization and eliminates sole dependence on individual initiative. Formalized policies and procedures are typically used to establish and institutionalize a cyber security program. Policies and procedures also inform employees of their specific cyber security responsibilities and the consequences of failing to meet those responsibilities. Establish requirements to minimize the threat from malicious insiders, including the need for conducting background checks and limiting network privileges to those absolutely necessary. As part of identifying cyber security requirements, include user agreements and notification and warning banners. Provide guidance regarding actions to be taken during a cyber security incident and promote efficient and effective actions during a time of crisis.
Slide 78	Configuration management begins with well-tested and documented security baselines for your various systems and needs to cover both hardware configurations and software configurations. Changes to hardware or software can easily introduce vulnerabilities that undermine network security, therefore processes are required to evaluate and control any change to ensure that the network remains secure.
Slide 79	A sign of a mature organization is one that is able to self-identify issues, conduct root cause analyses, and implement effective corrective actions that address individual and systemic problems. Self-assessment processes that are normally part of an effective cyber security program include routine scanning for vulnerabilities, automated auditing of the network, and self-assessments of organizational and individual performance.
Slide 80	System backups are an essential part of any plan and allow rapid reconstruction of the network. Routinely exercise disaster recovery plans to ensure that they work and that personnel are familiar with them. Make appropriate changes to disaster recovery plans based on lessons learned from exercises.

Slide 81	It is important for individuals to be held accountable for their performance as it relates to cyber security. It is essential that senior organizational leadership establish a structure for implementation of a cyber security program and an expectation for strong cyber security and communicate this to their subordinate managers throughout the organization This includes managers, system administrators, technicians, and users/operators. This structure will promote consistent implementation and the ability to sustain a strong cyber security program.
Slide 82	Release data related to the SCADA network only on a strict, need-to-know basis, and only to persons explicitly authorized to receive such information. "Social engineering," the gathering of information about a computer or computer network via questions to naive users, is often the first step in a malicious attack on computer networks. The more information revealed about a computer or computer network, the more vulnerable the computer/ network is. Never divulge data related to a SCADA network, including the names and contact information about the system operators/administrators, computer operating systems, and/or physical and logical locations of computers and network systems over telephones or to personnel unless they are explicitly authorized to receive such information. People can be a weak link in an otherwise secure network. Conduct training and information awareness campaigns to ensure that personnel remain diligent in guarding sensitive network information, particularly their passwords.
Slide 83	Takeaways: Clearly define cyber security roles, responsibilities, and authorities. Document network architecture and identify critical systems. Establish a Rigorous, Ongoing Risk Management Process. Establish a Network Protection Strategy Based on the Principle of Defense-in-depth. Clearly Identify Cyber Security Requirements. Establish effective configuration management processes. Conduct Routine Self-Assessments. Establish system backups and disaster recovery plans. Senior organizational leadership should establish expectations for cyber-security performance and accountability. Establish policies and conduct training.

Slide 84	Security is the degree of resistance to, or protection from harm. The attacks on SCADA systems in future are not only going to increase but will be highly sophisticated, particularly when SCADA systems would provide a potential terrain of war for the nation states. For reasons of efficiency, maintenance, and economics, data acquisition and control platforms have migrated from isolated in-plant networks using proprietary hardware and software to PC-based systems using standard software, network protocols, and the internet. The downside of this transition has been to expose SCADA systems to the same vulnerabilities and threats that plague Windows-based PCs and their associated networks. The main reason for SCADA failure is communication network failure. PLCs and PCs have low failure rates compared to communication network. The availability of the communication network should be increased for a more reliable SCADA system. Any defense strategy to be used for SCADA systems should have a judicious blend of security and usability in real time. Any process of live forensic should meet the test of nonrepudiation on procedural aspect of process, technology, science and integrity of the data has to be assured, so that it is admissible in court of Law. Only a judicious use of technology and common sense would help to keep the SCADA systems secure. More research is required in designing live forensic platforms that could be applicable to SCADA
Slide 85	Module Takeaways: Sections 2 & 3 What is Cyber Security & SCADA? 1. SCADA - Supervisory Control And Data Acquisition – is software layer, normally applied a level above control hardware within the hierarchy of an industrial network. 2. Cyber Security is the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation. 3. Cyber Security is necessary for all levels of employees, from entry to upper. The demand for expertise and technical know-how increase with each level of added responsibility. 4. Nuclear Technicians must develop cybersecurity skills to defend national critical infrastructure. SCADA ICS Attack Surface 1. Unauthorized changes made to programmed instructions in PLCs, RTUs, DCS, or SCADA controllers, could potentially result in damage to equipment. 2. False information sent to control system operators either to disguise unauthorized changes or to initiate inappropriate actions by system operators. 3. Control system software or configuration settings modified, producing unpredictable results. 4. Safety systems operation that have been interfered with could lead to vulnerabilities. 5. Malicious software (e.g., virus, worm, Trojan horse) introduced into the system. 6. Recipes (i.e., the materials and directions for creating a product) or work instructions modified in order to bring about damage to products, equipment, or personnel.
Slide 86	Module Takeaways: Sections 4 & 5 Nuclear Case Studies 1. PCS are not immune from attack since they are not connected to the internet. 2. PCS are not immune from attack since they are different from ordinary computers 3. Vulnerabilities are more complicated than both skeptics and alarmists realize.

	Increase the security of SCADA Networks: Specific Actions 1. Identify all connections to SCADA networks 2. Disconnect unnecessary connections to the SCADA network 3. Evaluate and strengthen connections to the SCADA Network 4. Harden SCADA networks by removing or disabling unnecessary services 5. Do Not Rely on Proprietary Protocols to Protect Your System 6. Implement the security features provided by device and system vendors 7. Establish strong controls over any backdoor into the SCADA network 8. Implement internal and external intrusion detection systems 24/7 9. Audit SCADA devices and networks to identify security concerns 10. Conduct physical security surveys and assess all remote sites 11. Establish SCADA "Red Teams" to identify and evaluate possible attacks
Slide 87	Module Takeaways: Section 6 Management actions to increase the security of SCADA Networks 1. Clearly define cyber security roles, responsibilities, and authorities 2. Document network architecture and identify critical systems 3. Establish a Rigorous, Ongoing Risk Management Process 4. Establish a Network Protection Strategy Based on the Principle of Defense-in-depth 5. Clearly Identify Cyber Security Requirements 6. Establish effective configuration management processes 7. Conduct Routine Self-Assessments 8. Establish system backups and disaster recovery plans 9. Senior organizational leadership should establish expectations for cyber security performance and accountability 10. Establish policies and conduct training

Lessons Learned & Takeaways

What is Cyber Security & SCADA?
SCADA - Supervisory Control And Data Acquisition – is software layer, normally applied a level above control hardware within the hierarchy of an industrial network.
Cyber Security is the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.
Cyber Security is necessary for all levels of employees, from entry to upper. The demand for expertise and technical know-how increase with each level of added responsibility.
Nuclear Technicians must develop cybersecurity skills to defend national critical infrastructure.
SCADA ICS Attack Surface
Unauthorized changes made to programmed instructions in PLCs, RTUs, DCS, or SCADA controllers, could potentially result in damage to equipment.
False information sent to control system operators either to disguise unauthorized changes or to initiate inappropriate actions by system operators.
Control system software or configuration settings modified, producing unpredictable results.
Safety systems operation that have been interfered with could lead to vulnerabilities.
Malicious software (e.g., virus, worm, Trojan horse) introduced into the system.

Recipes (i.e., the materials and directions for creating a product) or work instructions modified in order to bring about damage to products, equipment, or personnel.
Nuclear Case Studies
PCS are not immune from attack since they are not connected to the internet.
PCS are not immune from attack since they are different from ordinary computers
Vulnerabilities are more complicated than both skeptics and alarmists realize.
Increase the security of SCADA Networks: Specific Actions
Identify all connections to SCADA networks
Disconnect unnecessary connections to the SCADA network
Evaluate and strengthen connections to the SCADA Network
Harden SCADA networks by removing or disabling unnecessary services
Do Not Rely on Proprietary Protocols to Protect Your System
Implement the security features provided by device and system vendors
Establish strong controls over any backdoor into the SCADA network
Implement internal and external intrusion detection systems 24/7
Audit SCADA devices and networks to identify security concerns
Conduct physical security surveys and assess all remote sites
Establish SCADA “Red Teams” to identify and evaluate possible attacks
Management actions to increase the security of SCADA Networks
Clearly define cyber security roles, responsibilities, and authorities
Document network architecture and identify critical systems
Establish a Rigorous, Ongoing Risk Management Process
Establish a Network Protection Strategy Based on the Principle of Defense-in-depth
Clearly Identify Cyber Security Requirements
Establish effective configuration management processes
Conduct Routine Self-Assessments
Establish system backups and disaster recovery plans

Senior organizational leadership should establish expectations for cyber security performance and accountability
Establish policies and conduct training

References

Knapp, Eric D., and Joel Thomas Langill. Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems. Syngress, 2014.
Knapp, Eric D., and Raj Samani. Applied cyber security and the smart grid: implementing security controls into the modern power infrastructure. Newnes, 2013
Radvanovsky, Robert, and Jacob Brodsky, eds. Handbook of SCADA/control systems security. CRC Press, 2013.
Abbas, Hosny, Future SCADA challenges and the promising solution: the agent-based SCADA. International Journal of Critical Infrastructures 01/2014; 10(3/4):307 - 333. DOI: 10.1504/IJCIS.2014.066354
21 Steps to Improve Cyber Security of SCADA Networks, Office of Energy Assurance, U.S. Department of Energy, http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf
Macaulay, Tyson, and Bryan L. Singer. Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS. CRC Press, 2011
Zetter, Kim. Countdown to zero day: Stuxnet and the launch of the world's first digital weapon. Crown, 2014.
Falliere, Nicolas, Liam O. Murchu, and Eric Chien. "W32. stuxnet dossier." White paper, Symantec Corp., Security Response 5 (2011).
Albright, David, Paul Brannan, and Christina Walrond. "Stuxnet malware and natanz: Update of isis december 22, 2010 report." ISIS, February 15 (2011).
Murchu, Liam O., Stephen Doherty, and Eric Chien. Stuxnet 0.5: The missing link. Symantec, 2013
Byres, Eric, Andrew Ginter, and Joel Langill. "How Stuxnet spreads–A study of infection paths in best practice systems." Tofino Security, white paper (2011).

Assessments

Pre-Assessment (Answer Key Included)
Post-Assessment (Answer Key Included)

Supplemental & Enrichment Material

Web Sites:
https://ics-cert.us-cert.gov/
https://scadahacker.com/
http://ics-isac.org/
http://www.nist.gov/energy-portal.cfm
https://www.esisac.com/
http://www.nerc.com/Pages/default.aspx
http://krebsonsecurity.com/
http://www.samuraistfu.org/
http://www.pbs.org/wgbh/nova/military/cyberwar-threat.html

https://www.f-secure.com/weblog/archives/00002718.html
http://www.cnet.com/news/hacker-says-he-broke-into-texas-water-plant-others/
http://www.slideshare.net/guest85a34f/dhs-ics-security-presentation
http://www.darkreading.com/risk/stuxnet-five-years-later-did-we-learn-the-right-lesson/a/d-id/1319740
https://scadahacker.com/library/
http://andrewmohawk.com/category/security/pastebin-security/
http://large.stanford.edu/courses/2015/ph241/holloway1/
Twitter Feeds:
https://twitter.com/SCADAhacker
https://twitter.com/ICSCERT
https://twitter.com/ICSISAC
https://twitter.com/SANSInstitute
https://twitter.com/infosec
https://twitter.com/briankrebs
Training:
http://ics.sans.org/
https://niccs.us-cert.gov/training/tc/search/detail/1439
http://www.isaca.org/Education/Training/On-Site-Training/Pages/default.aspx?cid=sem_1104935&appeal=sem&gclid=CjwKEAjw1Iq6BRDY_tK-9OjdmBESJABlzoY7gq8VrXqj06ldhUzS2kiDWfweY9D2TTbB68b4SPhV-BoCcRzw_wcB
https://scadahacker.com/training.html
Video:
http://www.pbs.org/wgbh/nova/military/cyberwar-threat.html

RCNET

Nuclear Cyber Security

RCNET Nuclear Cyber Security

ACADs

1.1.9.2.6 Davis-Besse Nuclear Power Station event

5.1.1.2.1.12 theory of operations of plant electrical components

5.1.2 Plant Systems and Components Knowledge

5.1.2.15 Identify abnormal system and component indications and diagnose the probable causes

Program Courses

ETP 1230 Power Plant Systems
ETP 1220 Power Plant Fundamentals
ETI 1000 Industrial Plant Tools Equipment
ETI 1701 Industrial Safety

EET 1724C Electronic Design Software Tools
EET 1724C Electronic Design Software Tools

ETP 2930 Special Topics in Electrical Power Technology
ETP 2941 Professional Internship for Maintenance Technicians

Learning Objectives

Upon completion of this module, student will be able to:

1. Develop and reinforce a common language and understanding of Industrial Control System (ICS) cybersecurity as well as the important considerations that come with cyber-to-physical operations within these environments.
2. Demonstrate the necessary cyber-to-physical knowledge to better understand the importance of ICS operational drivers and constraints that require specific safety protection, communications needs, system management approaches, and cybersecurity implementations.
3. Know the adversary's approaches to attacking an ICS SCADA environment to be better prepared to defend that environment.
4. Develop a better understanding of where specific attack vectors exist, as well as the tools to use to discover vulnerabilities and exploit them along with specific capabilities available on servers, workstations, and applications, students will now learn network-specific defense approaches.
5. Better understand attacks targeting the types of web servers used on many ICS devices for management purposes.
6. Discuss essential ICS-related server and workstation operating system capabilities, implementation approaches, and system management practices.
7. Examine concepts that benefit SCADA ICS systems such as system hardening, log management, monitoring, alerting, and audit approaches, then look at some of the more common applications and databases used in ICS environments across multiple industries.
8. Implement technologies used to defend ICS networks.
9. Discuss the various models, methodologies, and industry-specific regulations that are used to govern what must be done to protect critical SCADA ICS systems.

3

Module Topics

- SCADA Systems Overview
- Personnel
- Cyber-Security
- Seven High-level Findings Impacting Control Systems today

What is Cyber Security & SCADA?

- ICS Attack Surface
- Information Leaks
- Control Systems
- Possible Incident Scenarios

SCADA ICS Attack Surface

- Davis-Besse Worm Infection
- Browns Ferry Shutdown
- Hatch Automatic Shutdown
- Iranian Nuclear Program
- Houston Water System Compromise
- Havex Trojan

Nuclear Case Studies

- List of specific actions to take to increase the security of SCADA networks

Increase the security of SCADA Networks: Specific Actions

- List of the roles and responsibilities of management to ensure the security of SCADA systems

Management actions to increase the security of SCADA Networks

4

Introduction

- SCADA Systems Overview
- Personnel
- Cyber-Security
- Seven High-level Findings Impacting Control Systems today

5

SCADA Systems Overview

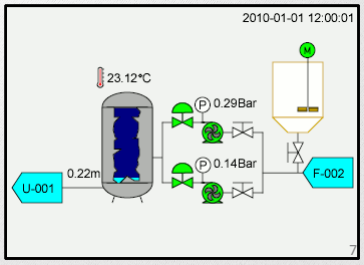
SCADA - Supervisory Control And Data Acquisition

- A purely **software layer**, normally applied a level above control hardware within the hierarchy of an industrial network.
- SCADA systems do not perform any control, but rather **function in a supervisory fashion**.
- The focus of a SCADA is **data acquisition** and the presentation of a centralized Human Machine Interface (HMI)

6

SCADA SYSTEM

- **SCADA** (Supervisory Control and Data Acquisition) is a type of industrial control system (ICS).
- Industrial control systems are computer controlled systems that **monitor and control industrial processes** that exist in the physical world.



SCADA Field of Applications

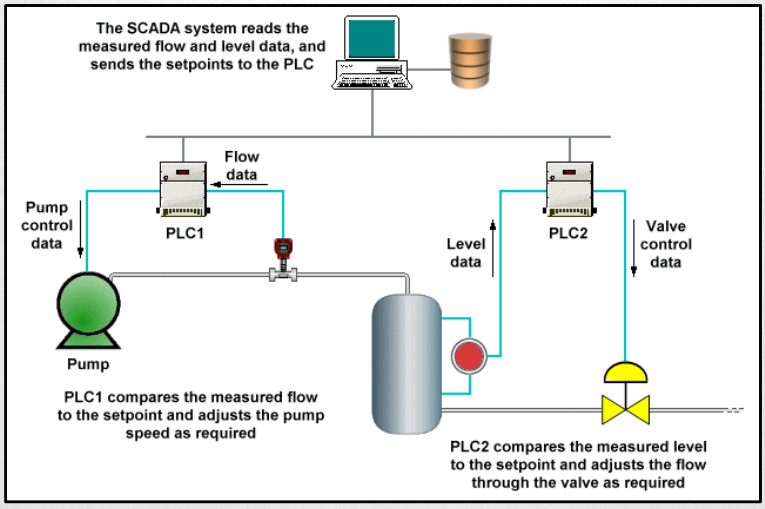
- **Industrial processes** include those of manufacturing, production, power generation, fabrication, and refining, and may run in continuous, batch, repetitive, or discrete modes.
- **Infrastructure processes** may be public or private, and include water treatment and distribution, wastewater collection and treatment, oil and gas pipelines, electrical power transmission and distribution, wind farms, civil defense siren systems, and large communication systems.
- **Facility processes** occur both in public facilities and private ones, including buildings, airports, ships, and space stations. They monitor and control heating, ventilation, and air conditioning systems (HVAC), access, and energy consumption.

Common SCADA System Components

- **A human–machine interface or HMI:** is the apparatus or device which presents processed data to a human operator, and through this, the human operator monitors and controls the process.
- **A supervisory (computer) system:** gather (acquire) data on the process and sending commands (control) to the process.
- **Remote terminal units (RTUs):** connect to sensors in the process, convert sensor signals to digital data and send digital data to the supervisory system.
- The device to which the RTUs communicate is known as a **Master Terminal Unit** (**MTU**).
- **Programmable logic controller (PLCs):** used as field devices because they are more economical, versatile, flexible, and configurable than special-purpose RTUs.
- **Communication infrastructure:** connect the supervisory system to the remote terminal units.

9

A Typical SCADA System

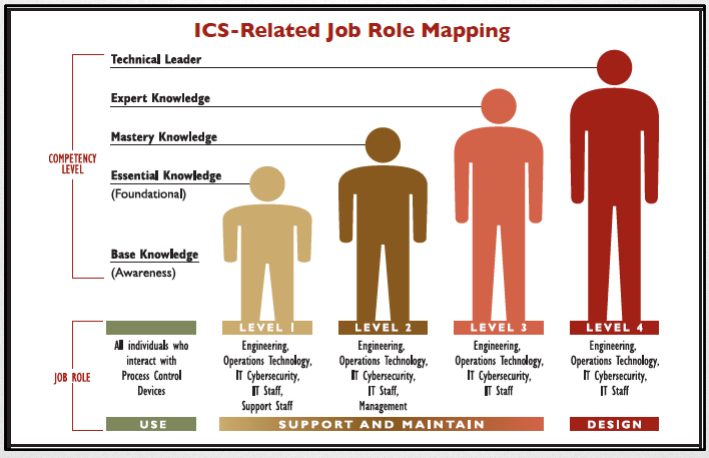


10

Personnel

11

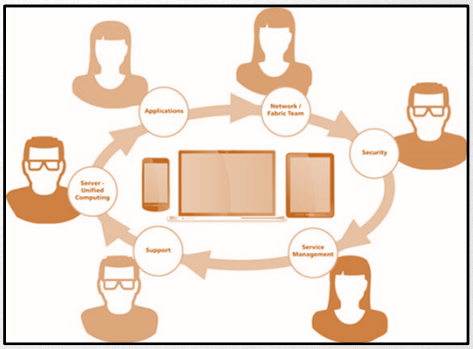
Job Role to Competency Level Recommendation



12

Job Role Groupings

- Engineering
- Operations
- Technology
- Management
- Support Staff
- IT Cybersecurity
- IT Staff



13

Cyber Security

14

What is Cyber Security?

- The activity or process, ability or capability, or state whereby **information and communications systems and the information contained therein are protected from and/or defended** against damage, unauthorized use or modification, or exploitation.

National Initiative for Cybersecurity Careers and Studies (NICCS)

15

Why Is It Important?

- Preparation is critical because ICS incidents are **occurring with increasing frequency** and damaging systems.
- Control systems are widely deployed and need your attention because there is no **such thing as a system that is too small**.
- Up-to-date ICS knowledge and security skills can help **keep our critical systems safe**.

16

How Does it Relate to Nuclear Technicians?

- Security professionals and control system engineers must develop **cybersecurity skills** to **defend national critical infrastructure**
- It is essential that SCADA environments ensure that the workforce involved in supporting and defending industrial control systems is **trained to keep the operational environment safe, secure, and resilient** against current and emerging cyber threats

17

Cyber-Security Video

18

Interactive Activity

Norse maintains the world's largest dedicated threat intelligence network.

19

Seven High-level Findings Impacting Control Systems Today

20

Control Engineering 2015 Cyber Security Study identified seven high-level findings impacting control systems today (1)

1. Threat levels
2. Most concerning threat
3. Vulnerable system components
4. Vulnerability assessments

21

Control Engineering 2015 Cyber Security Study identified seven high-level findings impacting control systems today (1)

5. Cyber-related incidents
6. Mobile devices
7. Training

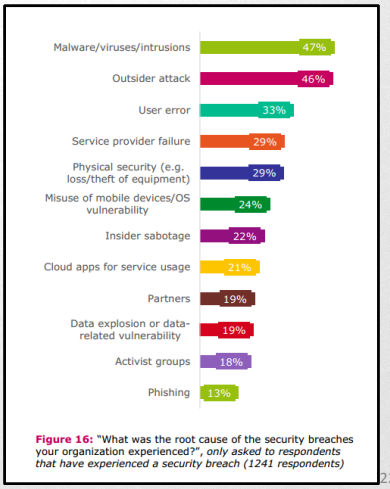


Figure 16: "What was the root cause of the security breaches your organization experienced?", *only asked to respondents that have experienced a security breach (1241 respondents)*

22

Takeaways

What is Cyber Security & SCADA?

- SCADA - Supervisory Control And Data Acquisition – is software layer, normally applied a level above control hardware within the hierarchy of an industrial network.
- Cyber Security is the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.
- Cyber Security is necessary for all levels of employees, from entry to upper. The demand for expertise and technical know-how increase with each level of added responsibility.
- Nuclear Technicians must develop cybersecurity skills to defend national critical infrastructure.

23

SCADA ICS Attack Surface

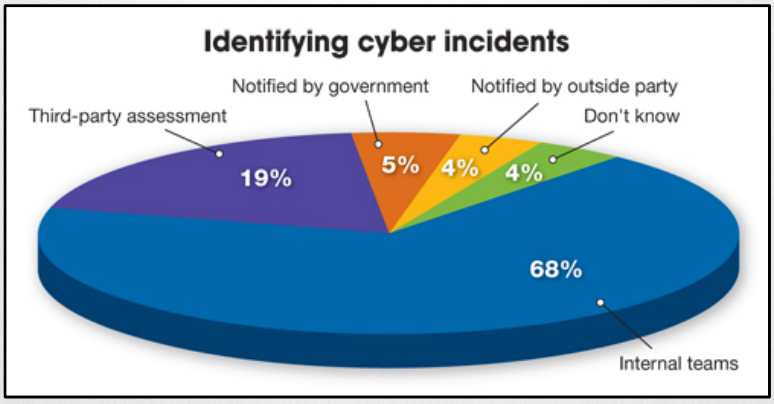
- ICS Attack Surface
- Information Leaks
- Control Systems
- Possible Incident Scenarios

24

ICS Attack Surface

25

ICS Attack Surface



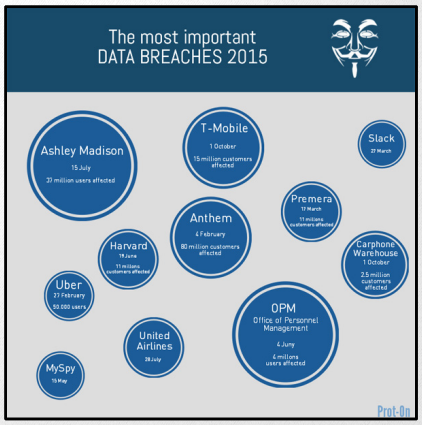
26

Information Leaks

27

Three types of Leaks

- Accidental leaking of sensitive information through **data queries**.
- Accidental leaking of sensitive information through **error messages.**
- Accidental leaking of sensitive information through **sent data**.



28

Accidental leaking of sensitive information through *data queries*

- When trying to keep information confidential, an attacker can often **infer** some of the information by **using statistics**

29

Accidental leaking of sensitive information through *data queries*

- **Consequences**
  - Confidentiality: Sensitive information may possibly be disclosed through data queries accidentally.
- **Exposure period**
  - Design: Proper mechanisms for preventing this kind of problem generally need to be identified at the design level.
- **Avoidance and mitigation**
  - This is a complex topic. See the book *Translucent Databases* for a good discussion of best practices.

30

Accidental leaking of sensitive information through *sent data*

- **Consequences**
  - Confidentiality: Data leakage results in the compromise of data confidentiality.
- **Exposure period**
  - Requirements specification: Information output may be specified in the requirements documentation.
- **Avoidance and mitigation**
  - Requirements specification: Specify data output such that no sensitive data is sent.

31

Control Systems

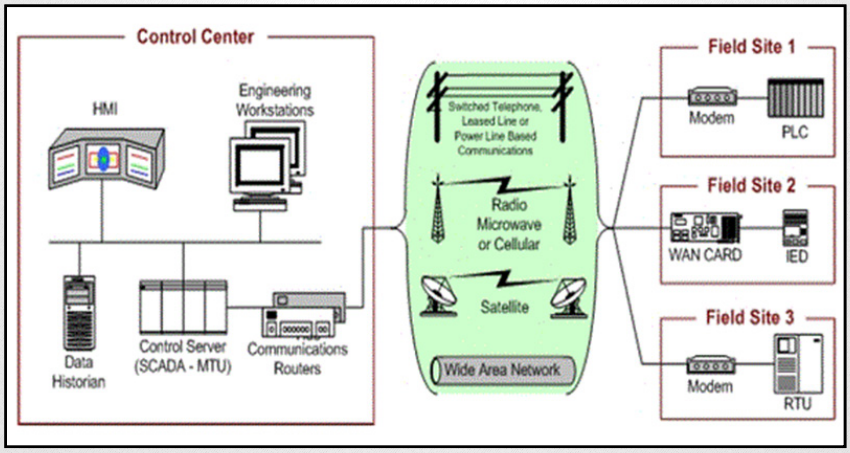
32

Control Systems

- Control systems operation disrupted by delaying or **blocking the flow of information** through corporate or control networks, thereby **denying availability of the networks** to control system operators or causing information transfer **bottlenecks** or **denial of service** by IT-resident services (such as DNS).

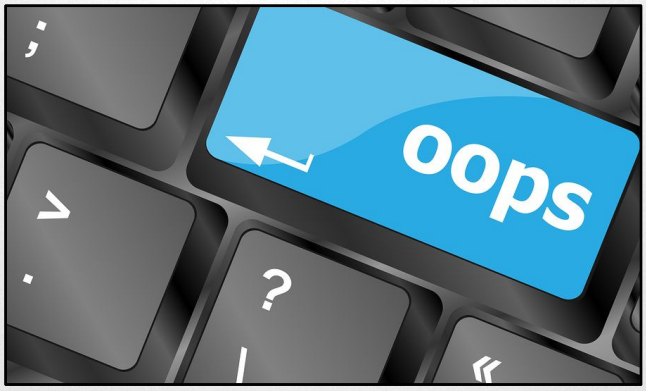
33

Control Systems



34

Possible Incident Scenarios



35

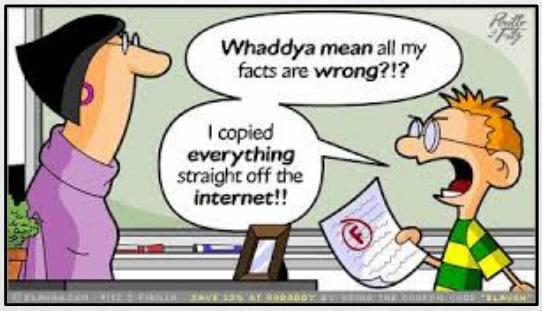
Unauthorized Changes

- **Unauthorized changes** made to programmed instructions in **PLCs, RTUs, DCS, or SCADA** controllers, could potentially result in **damage to equipment**.

36

False Information

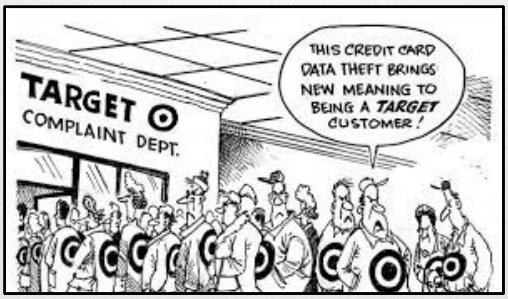
- **False information** sent to control system operators either to **disguise unauthorized changes** or to initiate **inappropriate actions** by system operators.



37

Control System Software

- Control system software, or configuration settings modified, produce **unpredictable results**.



38

Safety Systems

- Safety systems operations that have been interfered with could lead to **vulnerabilities**.

39

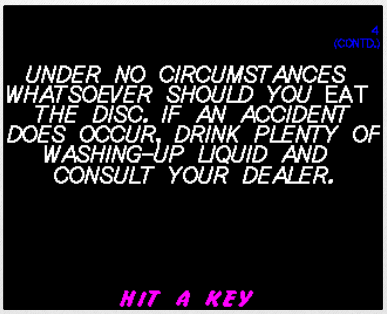
Malware

- Malicious software (e.g., **virus, worm, Trojan horse**) introduced into the system

40

Work Instructions Modified

- Recipes (i.e., the materials and directions for creating a product) or **work instructions modified** in order to bring about damage to products, equipment, or personnel.



41

Takeaways

SCADA ICS Control Systems

- Unauthorized changes made to programmed instructions in PLCs, RTUs, DCS, or SCADA controllers, could potentially result in damage to equipment.
- False information sent to control system operators either to disguise unauthorized changes or to initiate inappropriate actions by system operators.
- Control system software or configuration settings modified, producing unpredictable results.
- Safety systems operation that have been interfered with could lead to vulnerabilities.
- Malicious software (e.g., virus, worm, Trojan horse) introduced into the system.
- Recipes (i.e., the materials and directions for creating a product) or work instructions modified in order to bring about damage to products, equipment, or personnel.

42

Nuclear Case Studies

- Davis-Besse Worm Infection- 2003
- Browns Ferry Shutdown- 2006
- Hatch Automatic Shutdown- 2008
- Iranian Nuclear Program
- Houston Water System Compromise- 2012
- Havex Trojan- 2014

43

Davis-Besse Worm Infection - 2003

Davis-Besse Nuclear Power Plant

44

Davis-Besse Worm Infection

- In January of 2003, the Slammer worm began exploiting a vulnerability in Microsoft SQL Server.
- Within **10 minutes**, it had infected **75,000 servers worldwide—90% of vulnerable hosts**.
- The Slammer worm infected computer systems at the Davis-Besse nuclear power plant in Ohio.
- The worm travelled from a consultant's network, to the corporate network of First Energy Nuclear (the licensee for Davis-Besse) and then to the process control network for the plant.

45

Browns Ferry Shutdown

Browns Ferry Nuclear Plant

46

Browns Ferry Shutdown

- The August 2006 shutdown of Unit 3 at the Browns Ferry nuclear plant near Athens, Alabama, demonstrates that **not just computers**, but even **critical reactor components**, could be disrupted and disabled by a cyber attack.
- Unit 3 was manually shutdown after the failure of both reactor recirculation pumps and the condensate demineralizer controller.

47

Hatch Automatic Shutdown - 2008

Hatch Nuclear Power Plant

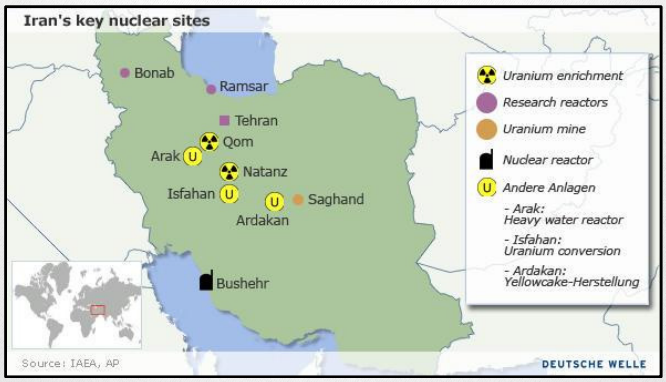
48

Hatch Automatic Shutdown

- In March 2008, Unit 2 of the Hatch nuclear power plant near Baxley, Georgia, automatically shutdown after an engineer **applied a software update** to a **single computer** on the plant's **business network**.
- When the engineer rebooted the computer, the synchronization program reset the data on the control network.
- The control systems **interpreted the reset as a sudden drop** in the reactor's water reservoirs and initiated an automatic shutdown

49

Iranian Nuclear Program



Iranian Nuclear Plant Sites

50

Iranian Nuclear Program

- Between November 2009 and late January 2010 Stuxnet is believed to have **destroyed 984 centrifuges at Iran's uranium enrichment facility** in Natanz
- The Stuxnet worm **targeted specific PCS components** used in the Iranian centrifuge cascades
- The PLCs controlled the frequency converters to modulate the speed at which the centrifuges spun.
- Stuxnet commanded the PLCs to speed up and slow down the spinning centrifuges, destroying some of them, while **sending false data** to plant operators to make it **appear the centrifuges were behaving normally**.

51

South Houston Water System Compromise- 2012

South Houston Water Supply Plant

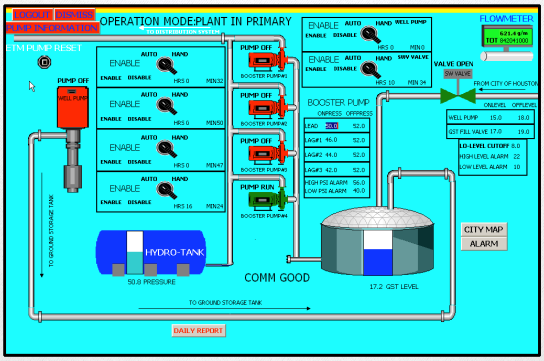
52

South Houston's Water Supply Network

- In November 2011, a hacker identified as **'pr0f'** provided evidence of a successful penetration of South Houston's water supply network.
- The hacker posted this in Pastebin, *"I don't really like mindless vandalism. It's stupid and silly. On the other hand, so is **connecting interfaces to your SCADA machinery to the internet**. I wouldn't even call this a hack, either, just to say. This required almost no skill and could be reproduced by a two year old with a basic knowledge of Simatic."*

53

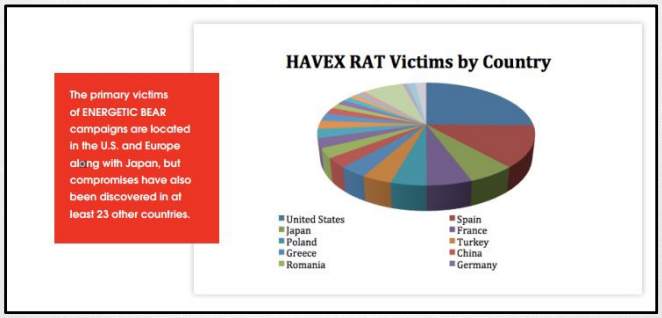
South Houston Water System Compromise- 2012



Asked how he gets into systems, **pr0f** said:
"As for how I did it, it's usually a **combination of poor configuration of services, bad password choice, and no restrictions** on who can access the interfaces."

54

Havex Trojan - 2014-Present



- Havex is **known** to have been used in **targeted attacks** against various industrial sectors, particularly the **energy sector** and **will continue in the future**.

55

Havex Trojan - 2014-Present

- Havex **Remote Access Trojans (RATs**) provide cybercriminals with **unlimited access** to infected endpoints. Targeted attacks against **energy sector** organizations took place in September 2013 and were perpetrated by a group of attackers with links to the **Russian Federation**.
- The majority of the victims are located in Europe, though, at least one company in **California** was also observed sending data to the Command & Control servers
- Attackers hack into the website of industrial control system (ICS) manufacturers and **poison their legitimate software downloads.**

56

Takeaways

Nuclear Case Studies

- PCS are not immune from attack since they are not connected to the internet.
- PCS are not immune from attack since they are different from ordinary computers.
- Vulnerabilities are more complicated than both skeptics and alarmists realize.

57

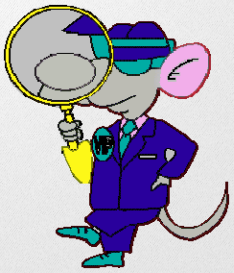
Increase the Security of SCADA Networks: Specific Actions

- Identify all connections to SCADA networks
- Disconnect unnecessary connections to the SCADA network
- Evaluate and strengthen connections to the SCADA Network
- Harden SCADA networks by removing or disabling unnecessary services
- Do Not Rely on Proprietary Protocols to Protect Your System
- Implement the security features provided by device and system vendors
- Establish strong controls over any backdoor into the SCADA network
- Implement internal and external intrusion detection systems 24/7
- Audits SCADA devices and networks to identify security concerns
- Conduct physical security surveys and assess all remote sites
- Establish SCADA “Red Teams” to identify and evaluate possible attacks

58

Identify all connections to SCADA networks

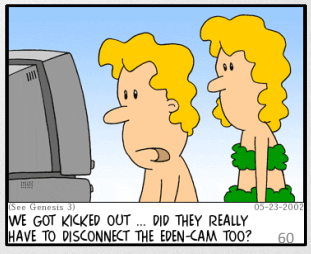
- Conduct a thorough **risk analysis** to assess the risk and necessity of **each connection** to the SCADA network.



59

Disconnect unnecessary connections to the SCADA network

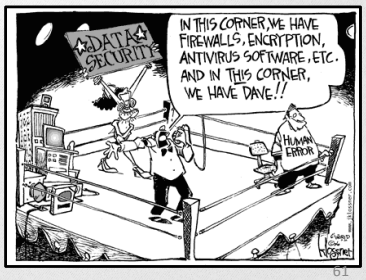
- Any connection to another network introduces **security risks**, particularly if the connection creates a pathway from or to the Internet
- **Isolation** of the SCADA network must be a primary goal to provide needed protection



60

Evaluate and strengthen the security of any remaining connections to the SCADA Network

- Conduct **penetration testing or vulnerability analysis** of any remaining connections to the SCADA network to evaluate the protection posture associated with these pathways



61

Harden SCADA networks by removing or disabling unnecessary services

- SCADA control servers built on commercial or open-source operating systems can be **exposed to attack through default network services**.
- To the greatest degree possible, remove or disable unused services and network daemons to reduce the risk of direct attack. This is particularly important when SCADA networks are interconnected with other networks.

62

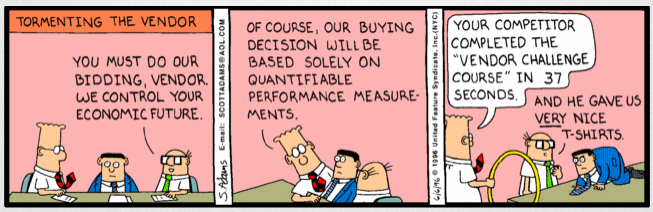
Do Not Rely on Proprietary Protocols to Protect Your System

- Some SCADA systems use unique, proprietary protocols for communications between field devices and servers.
- Often the security of SCADA systems is **based solely on the secrecy of these protocols**. Unfortunately, obscure protocols provide very little "real" security.

63

Implement the security features provided by device and system vendors

- SCADA system owners must insist that their **system vendor implement security features** in the form of product patches or upgrades.



64

Establish strong controls over any medium that is used as a backdoor into the SCADA network

- Where backdoors or vendor connections do exist in SCADA systems, **strong authentication** must be implemented to ensure secure communications.
- Modems, wireless, and wired networks used for communications and maintenance represent a **significant vulnerability** to the SCADA network and remote sites.

65

Implement internal and external intrusion detection systems and establish 24-hour-a-day incident monitoring

- To be able to effectively respond to cyber attacks, establish an **intrusion detection strategy** that includes alerting network administrators of malicious network activity originating from **internal** or **external sources.**

66

Perform technical audits of SCADA devices and networks, and any other connected networks, to identify security concerns

- Technical audits of SCADA devices and networks are critical to ongoing security effectiveness and Analyze identified vulnerabilities to determine their significance, and **take corrective actions as appropriate.**

67

Conduct physical security surveys and assess all remote sites connected to the SCADA network to evaluate their security

- Any location that has a connection to the SCADA network is a **target**, especially **unmanned** or **unguarded remote sites.**

68

Establish SCADA "Red Teams" to identify and evaluate possible attack scenarios

- Establish a "**Red Team**" to identify potential attack scenarios and evaluate potential system vulnerabilities.

69

Takeaways

Increase the Security of SCADA Networks: Specific Actions

- Identify all connections to SCADA networks
- Disconnect unnecessary connections to the SCADA network
- Evaluate and strengthen connections to the SCADA Network
- Harden SCADA networks by removing or disabling unnecessary services
- Do Not Rely on Proprietary Protocols to Protect Your System
- Implement the security features provided by device and system vendors
- Establish strong controls over any backdoor into the SCADA network
- Implement internal and external intrusion detection systems 24/7
- Audits SCADA devices and networks to identify security concerns
- Conduct physical security surveys and assess all remote sites
- Establish SCADA "Red Teams" to identify and evaluate possible attacks

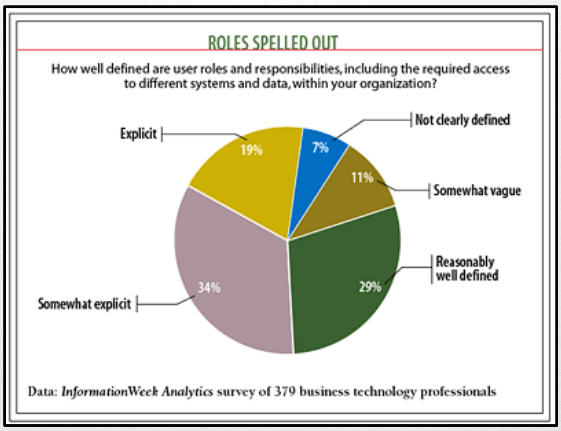
70

Management Actions to Increase the Security of SCADA Networks

- Clearly define cyber security roles, responsibilities, and authorities
- Document network architecture and identify critical systems
- Establish a Rigorous, Ongoing Risk Management Process
- Establish a Network Protection Strategy Based on the Principle of Defense-in-depth
- Clearly Identify Cyber Security Requirements
- Establish effective configuration management processes
- Conduct Routine Self-Assessments
- Establish system backups and disaster recovery plans
- Senior organizational leadership should establish expectations for cyber security performance and accountability
- Establish policies and conduct training

71

Clearly define cyber security roles, responsibilities, & authorities for managers, system administrators, & users



72

Levels of Responsibility

- ***LEVEL 0*** - Process Control Instrumentation Bus Network
- ***LEVEL 1*** - Control Devices
- ***LEVEL 2*** - Supervisory Control LAN
- ***LEVEL 3*** - Operations Support
- ***LEVEL 4*** - Business Unit or Plant Network
- ***LEVEL 5*** - Enterprise Business Network

73

Document network architecture & identify systems that serve critical functions or contain sensitive information that require additional levels of protection

- It is essential that **organizations design their networks with security in mind** and continue to have a strong understanding of their network architecture throughout its lifecycle.

Establish a Rigorous, Ongoing Risk Management Process

- A thorough understanding of the risks to network computing resources from denial-of-service attacks and the vulnerability of sensitive information to compromise is essential to an **effective cyber security program**.

75

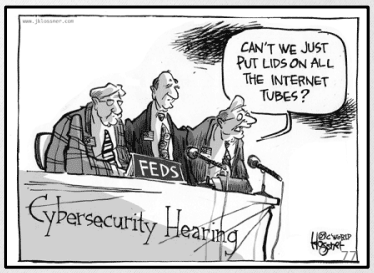
Establish a Network Protection Strategy Based on the Principle of Defense-in-depth

- A **fundamental principle** that must be part of any network protection strategy is **defense-in-depth**.

76

Clearly Identify Cyber Security Requirements

- Organizations and companies need **structured security programs** with mandated requirements to establish expectations and allow personnel to be held accountable.



Establish effective configuration management processes

- **Configuration Management** is a fundamental management process needed to **maintain a secure network**.

78

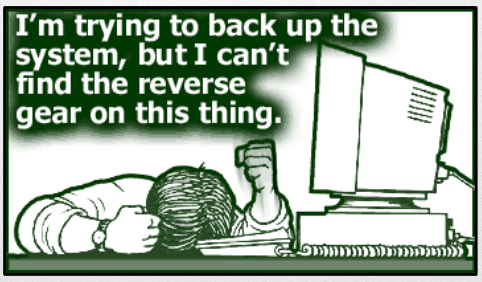
Conduct Routine Self-Assessments

- **Robust performance evaluation** processes are needed to provide organizations with feedback on the effectiveness of **cyber security policy** and **technical implementation**.

79

Establish system backups & disaster recovery plans

- Establish a **disaster recovery plan** that allows for **rapid recovery** from any emergency (including a cyber attack)



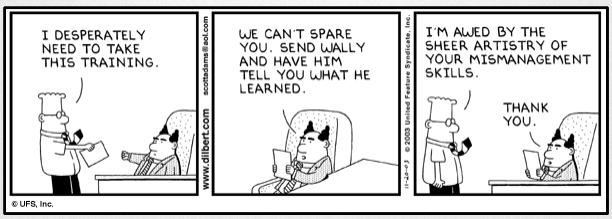
80

Senior organizational leadership should establish expectations for cyber security performance & hold individuals accountable for their performance

- Effective cyber security performance requires **commitment and leadership** from senior managers in the organization.

81

Establish policies and conduct training to minimize the likelihood that organizational personnel will **inadvertently disclose sensitive** information regarding SCADA system **design, operations, or security controls.**



82

Takeaways

Management Actions to Increase the Security of SCADA Networks

- Clearly define cyber security roles, responsibilities, and authorities
- Document network architecture and identify critical systems
- Establish a Rigorous, Ongoing Risk Management Process
- Establish a Network Protection Strategy Based on the Principle of Defense-in-depth
- Clearly Identify Cyber Security Requirements
- Establish effective configuration management processes
- Conduct Routine Self-Assessments
- Establish system backups and disaster recovery plans
- Senior organizational leadership should establish expectations for cyber security performance and accountability
- Establish policies and conduct training

83

Future Challenges

- The attacks on SCADA systems in the future are not only **going to increase** but will be **highly sophisticated**, particularly when SCADA systems would provide a **potential terrain of war** for the nation states.

84

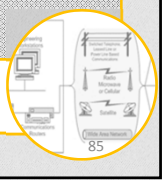
Module Takeaways

- SCADA - Supervisory Control And Data Acquisition – is software layer, normally applied a level above control hardware within the hierarchy of an industrial network.
- Cyber Security is the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.
- Cyber Security is necessary for all levels of employees, from entry to upper. The demand for expertise and technical know-how increase with each level of added responsibility.
- Nuclear Technicians must develop cybersecurity skills to defend national critical infrastructure.

What is Cyber Security & SCADA?

- Unauthorized changes made to programmed instructions in PLCs, RTUs, DCS, or SCADA controllers, could potentially result in damage to equipment.
- False information sent to control system operators either to disguise unauthorized changes or to initiate inappropriate actions by system operators.
- Control system software or configuration settings modified, producing unpredictable results.
- Safety systems operation that have been interfered with could lead to vulnerabilities.
- Malicious software (e.g., virus, worm, Trojan horse) introduced into the system.
- Recipes (i.e., the materials and directions for creating a product) or work instructions modified in order to bring about damage to products, equipment, or personnel.

SCADA ICS Attack Surface



85

Module Takeaways

- PCS are not immune from attack since they are not connected to the internet.
- PCS are not immune from attack since they are different from ordinary computers
- Vulnerabilities are more complicated than both skeptics and alarmists realize.

Nuclear Case Studies

- Identify all connections to SCADA networks
- Disconnect unnecessary connections to the SCADA network
- Evaluate and strengthen connections to the SCADA Network
- Harden SCADA networks by removing or disabling unnecessary services
- Do Not Rely on Proproprietary Protocols to Protect Your System
- Implement the security features provided by device and system vendors
- Establish strong controls over any backdoor into the SCADA network
- Implement internal and external intrusion detection systems 24/7
- Audit SCADA devices and networks to identify security concerns
- Conduct physical security surveys and assess all remote sites
- Establish SCADA "Red Teams" to identify and evaluate possible attacks

Increase the security of SCADA Networks: Specific Actions

86

Module Takeaways

- Clearly define cyber security roles, responsibilities, and authorities
- Document network architecture and identify critical systems
-
- Establish a Rigorous, Ongoing Risk Management Process
- Establish a Network Protection Strategy Based on the Principle of Defense-in-depth
- Clearly Identify Cyber Security Requirements
- Establish effective configuration management processes
- Conduct Routine Self-Assessments
- Establish system backups and disaster recovery plans
- Senior organizational leadership should establish expectations for cyber security performance and accountability
- Establish policies and conduct training

Management actions to increase the security of SCADA Networks

87

RCNET Nuclear Cyber Security Module Name:_____

*PRE Assessment **TEST*** Date:_____

*This assessment is designed to determine your pre-existing knowledge about securing SCADA systems and their nuclear applications. This assessment should be taken prior to starting the **RCNET Nuclear Cyber Security Module** and will not count as a grade.*

Please write the correct answer directly on this test.

1. The three categories for SCADA Field applications are: Check all that apply.
    a) Industrial processes
    b) Infrastructure processes
    c) Facility processes
    d) Personnel process

2. A Remote terminal units (RTUs) purpose is to:
    a) Gathers (acquire) data on the process and sending commands (control) to the process
    b) Connect to sensors in the process, convert sensor signals to digital data and send digital data to the supervisory system
    c) Used as field devices because they are more economical, versatile, flexible, and configurable than special-purpose RTUs
    d) Connect the supervisory system to the remote terminal units.

3. List the seven job role groupings in an Industrial Control System environment.

    _____

    _____

    _____

    _____

    _____

    _____

    _____

    _____

4. True / False: It is essential that SCADA environments ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

5. According to *Control Engineering* 2015 Cyber Security Study, what are the most concerning threats?

6. Examples of attack surface in the real world include the following except:
    a) Open ports on outward facing web and other servers, code listening on those ports
    b) Services available on the inside of the firewall
    c) Using an intrusion detection system
    d) Code that processes incoming data, email, XML, office documents
    e) Interfaces, SQL, web forms

7. In reference to information leaks, what are the three ways accidental leaking of sensitive information can be done:

8. There are some possible incident scenarios that can create vulnerabilities within SCADA control systems. What is the concern about control system software?

9. A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program. What type of malware is this?
    a) Virus
    b) Worm
    c) Trojan Horse

10. What is the name of the worm that infected the Iranian nuclear power plant?
    a) Natanz
    b) Havex
    c) Stuxnet
    d) SQL Map

11. A new Trojan horse called Havex is targeting SCADA systems. This Trojan is referred to as a RAT. What does the RAT acronym stand for?
    a) Real Active Trojan
    b) Real-time attacking Trojan
    c) Remote Access Trojan

12. One of the specific actions to increase the security of SCADA networks is to identify all connections. Name four of the six connections.

    _____

    _____

    _____

    _____

    _____

    _____

    _____

    _____

13. Evaluate and strengthen the security of any remaining connections to the SCADA Network requires a type of testing. What testing method is used in this process?
    a) Pentesting
    b) Throughput Testing
    c) Load Balancing Testing

d) CPU Threshold Testing

14. You can Harden SCADA networks by removing or disabling unnecessary what?
    a) Cabling
    b) Wireless
    c) Services
    d) Backups

15. True / False: Modems, wireless, and wired networks used for communications and maintenance represent a significant vulnerability to the SCADA network and remote sites

16. It is important to document the information security architecture and its components because it is critical to understanding:
    a) Fundamentals to risk management
    b) The overall protection strategy and identifying single points of failure
    c) Factory default security settings
    d) Help identify SCADA vendors

17. Initially, perform a _____ risk analysis based on a current threat assessment to use for developing a network protection strategy.
    a) Standard
    b) Sequential
    c) Baseline
    d) Single

18. An Established Network Protection Strategy Based on the Principle of _____.
    a) Job Functions
    b) Organization
    c) Firewall Security
    d) Defense-in-depth

19. What can allows for rapid recovery from any emergency (including a cyber attack)
    a) Memory Allocation
    b) Long Passwords
    c) Backups
    d) Non-use of wireless networks

20. True / False: Establish policies and conduct training to minimize the likelihood that organizational personnel will inadvertently disclose sensitive information regarding SCADA system design, operations, or security controls.

RCNET Nuclear Cyber Security Module Name:_____

PRE Assessment ***ANSWER KEY*** Date:_____

This assessment is designed to determine your pre-existing knowledge about securing SCADA systems and their nuclear applications. This assessment should be taken prior to starting the ***RCNET Nuclear Cyber Security Module*** *and will not count as a grade.*

Please write the correct answer directly on this test.

1. The three categories for SCADA Field applications are: Check all that apply.
   - **a) Industrial processes**
   - **b) Infrastructure processes**
   - **c) Facility processes**

2. A Remote terminal units (RTUs) purpose is to:
   - **b) Connect to sensors in the process, convert sensor signals to digital data and send digital data to the supervisory system**

3. List the seven job role groupings in an Industrial Control System environment.
   - **Engineering**
   - **Operations**
   - **Technology**
   - **Management**
   - **Support Staff**
   - **IT Cybersecurity**
   - **IT Staff**

4. **True**/False: It is essential that SCADA environments ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

5. According to *Control Engineering* 2015 Cyber Security Study, what are the most concerning threats?
   Malware from a random source is the most concerning control system threat for 35% of respondents. Another 18% are worried about theft of intellectual property, and 8% fear attacks from "hacktivists" with a political or environmental agenda

6. Examples of attack surface in the real world include the following except:
   - **c) Using an intrusion detection system**

7. In reference to information leaks, what are the three ways accidental leaking of sensitive information can be done:
   - **Data queries**
   - **Error messages**
   - **Sent data**

8. There are some possible incident scenarios that can create vulnerabilities within SCADA control systems. What is the concern about control system software?
   Configuration settings modified, producing unpredictable results.

9. A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program. What type of malware is this?
   c) Trojan Horse

10. What is the name of the worm that infected the Iranian nuclear power plant?
    c) Stuxnet

11. A new Trojan horse called Havex is targeting SCADA systems. This Trojan is referred to as a RAT. What does the RAT acronym stand for?
    c) Remote Access Trojan

12. One of the specific actions to increase the security of SCADA networks is to identify all connections. Name four of the six connections.
    - **Internal local area and wide area networks, including business networks**
    - **The Internet**
    - **Wireless network devices, including satellite uplinks**
    - **Modem or dial-up connections**
    - **Connections to business partners, vendors or regulatory agencies**
    - **Develop a comprehensive understanding of all connections to the SCADA network, and how well these connections are protected**

13. Evaluate and strengthen the security of any remaining connections to the SCADA Network requires a type of testing. What testing method is used in this process?
    a) Pentesting

14. You can Harden SCADA networks by removing or disabling unnecessary what?
    c) Services

15. **True**/False: Modems, wireless, and wired networks used for communications and maintenance represent a significant vulnerability to the SCADA network and remote sites

16. It is important to document the information security architecture and its components because it is critical to understanding:
    b) The overall protection strategy and identifying single points of failure

17. Initially, perform a _____ risk analysis based on a current threat assessment to use for developing a network protection strategy.
    c) Baseline

18. An Established Network Protection Strategy Based on the Principle of _____.
    d) Defense-in-depth

19. What can allows for rapid recovery from any emergency (including a cyber attack)
    c) Backups

20. **True**/False: Establish policies and conduct training to minimize the likelihood that organizational personnel will inadvertently disclose sensitive information regarding SCADA system design, operations, or security controls.

RCNET Nuclear Cyber Security Module Name:_____

*POST Assessment **TEST*** Date:_____

*This assessment is designed to determine what you have learned about securing SCADA systems and their nuclear applications. This assessment should be taken after completing the **RCNET Nuclear Cyber Security Module** and will count as a grade.*

Please write the correct answer directly on this test.

1. The three categories for SCADA Field applications are: Check all that apply.
    a) Industrial processes
    b) Infrastructure processes
    c) Facility processes
    d) Personnel process

2. A Remote terminal units (RTUs) purpose is to:
    a) Gathers (acquire) data on the process and sending commands (control) to the process
    b) Connect to sensors in the process, convert sensor signals to digital data and send digital data to the supervisory system
    c) Used as field devices because they are more economical, versatile, flexible, and configurable than special-purpose RTUs
    d) Connect the supervisory system to the remote terminal units.

3. List the seven job role groupings in an Industrial Control System environment.

    _____

    _____

    _____

    _____

    _____

    _____

    _____

    _____

4. True / False: It is essential that SCADA environments ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

5. According to *Control Engineering* 2015 Cyber Security Study, what are the most concerning threats?

6. Examples of attack surface in the real world include the following except:
    a) Open ports on outward facing web and other servers, code listening on those ports
    b) Services available on the inside of the firewall
    c) Using an intrusion detection system
    d) Code that processes incoming data, email, XML, office documents
    e) Interfaces, SQL, web forms

7. In reference to information leaks, what are the three ways accidental leaking of sensitive information can be done:

8. There are some possible incident scenarios that can create vulnerabilities within SCADA control systems. What is the concern about control system software?

9. A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program. What type of malware is this?
    a) Virus
    b) Worm
    c) Trojan Horse

10. What is the name of the worm that infected the Iranian nuclear power plant?
    a) Natanz
    b) Havex
    c) Stuxnet
    d) SQL Map

11. A new Trojan horse called Havex is targeting SCADA systems. This Trojan is referred to as a RAT. What does the RAT acronym stand for?
    a) Real Active Trojan
    b) Real-time attacking Trojan
    c) Remote Access Trojan

12. One of the specific actions to increase the security of SCADA networks is to identify all connections. Name four of the six connections.

    _____

    _____

    _____

    _____

    _____

    _____

    _____

    _____

13. Evaluate and strengthen the security of any remaining connections to the SCADA Network requires a type of testing. What testing method is used in this process?
    a) Pentesting
    b) Throughput Testing
    c) Load Balancing Testing

d) CPU Threshold Testing

14. You can Harden SCADA networks by removing or disabling unnecessary what?
    a) Cabling
    b) Wireless
    c) Services
    d) Backups

15. True / False: Modems, wireless, and wired networks used for communications and maintenance represent a significant vulnerability to the SCADA network and remote sites

16. It is important to document the information security architecture and its components because it is critical to understanding:
    a) Fundamentals to risk management
    b) The overall protection strategy and identifying single points of failure
    c) Factory default security settings
    d) Help identify SCADA vendors

17. Initially, perform a _____ risk analysis based on a current threat assessment to use for developing a network protection strategy.
    a) Standard
    b) Sequential
    c) Baseline
    d) Single

18. An Established Network Protection Strategy Based on the Principle of _____.
    a) Job Functions
    b) Organization
    c) Firewall Security
    d) Defense-in-depth

19. What can allows for rapid recovery from any emergency (including a cyber attack)
    a) Memory Allocation
    b) Long Passwords
    c) Backups
    d) Non-use of wireless networks

20. True / False: Establish policies and conduct training to minimize the likelihood that organizational personnel will inadvertently disclose sensitive information regarding SCADA system design, operations, or security controls.

RCNET Nuclear Cyber Security Module Name:_____

POST Assessment ***ANSWER KEY*** Date:_____

This assessment is designed to determine what you have learned about securing SCADA systems and their nuclear applications. This assessment should be taken after completing the ***RCNET Nuclear Cyber Security Module*** *and will count as a grade.*

Please write the correct answer directly on this test.

1. The three categories for SCADA Field applications are: Check all that apply.
    a) **Industrial processes**
    b) **Infrastructure processes**
    c) **Facility processes**

2. A Remote terminal units (RTUs) purpose is to:
    b) **Connect to sensors in the process, convert sensor signals to digital data and send digital data to the supervisory system**

3. List the seven job role groupings in an Industrial Control System environment.
    - **Engineering**
    - **Operations**
    - **Technology**
    - **Management**
    - **Support Staff**
    - **IT Cybersecurity**
    - **IT Staff**

4. **True**/False: It is essential that SCADA environments ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

5. According to *Control Engineering* 2015 Cyber Security Study, what are the most concerning threats?
    Malware from a random source is the most concerning control system threat for 35% of respondents. Another 18% are worried about theft of intellectual property, and 8% fear attacks from "hacktivists" with a political or environmental agenda

6. Examples of attack surface in the real world include the following except:
    c) **Using an intrusion detection system**

7. In reference to information leaks, what are the three ways accidental leaking of sensitive information can be done:
    - **Data queries**
    - **Error messages**
    - **Sent data**

8. There are some possible incident scenarios that can create vulnerabilities within SCADA control systems. What is the concern about control system software?

    Configuration settings modified, producing unpredictable results.

9. A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program. What type of malware is this?

    c) Trojan Horse

10. What is the name of the worm that infected the Iranian nuclear power plant?

    c) Stuxnet

11. A new Trojan horse called Havex is targeting SCADA systems. This Trojan is referred to as a RAT. What does the RAT acronym stand for?

    c) Remote Access Trojan

12. One of the specific actions to increase the security of SCADA networks is to identify all connections. Name four of the six connections.
    - **Internal local area and wide area networks, including business networks**
    - **The Internet**
    - **Wireless network devices, including satellite uplinks**
    - **Modem or dial-up connections**
    - **Connections to business partners, vendors or regulatory agencies**
    - **Develop a comprehensive understanding of all connections to the SCADA network, and how well these connections are protected**

13. Evaluate and strengthen the security of any remaining connections to the SCADA Network requires a type of testing. What testing method is used in this process?

    a) Pentesting

14. You can Harden SCADA networks by removing or disabling unnecessary what?

    c) Services

15. **True**/False: Modems, wireless, and wired networks used for communications and maintenance represent a significant vulnerability to the SCADA network and remote sites

16. It is important to document the information security architecture and its components because it is critical to understanding:
    b) The overall protection strategy and identifying single points of failure

17. Initially, perform a _____ risk analysis based on a current threat assessment to use for developing a network protection strategy.
    c) Baseline

18. An Established Network Protection Strategy Based on the Principle of _____.
    d) Defense-in-depth

19. What can allows for rapid recovery from any emergency (including a cyber attack)
    c) Backups

20. **True**/False: Establish policies and conduct training to minimize the likelihood that organizational personnel will inadvertently disclose sensitive information regarding SCADA system design, operations, or security controls.

GLOSSARY

Access Points - is a networking hardware device that allows a device to connect to a network. In the sentence, "Conduct a physical security survey and inventory ***access points*** at each facility that has a connection to the SCADA system", refers to any point where a hardware device connects to the SCADA system or network.

Attack Surface is the attack surface of a system or asset refers to the collectively exposed portions of that system or asset. A large attack surface means that there are many exposed areas that an attack could target, while a small attack surface means that the target is relatively unexposed.

Control Server is a server that hosts the supervisory control system, typically a commercially available application for DCS or SCADA system.

Control System is a system in which deliberate guidance or manipulation is used to achieve a prescribed value for a variable. Control systems include SCADA, DCS, PLCs and other types of industrial measurement and control systems.

Data acquisition begins at the RTU or PLC level and includes meter readings and equipment status reports that are communicated to SCADA as required. Data is then compiled and formatted in such a way that a control room operator using the HMI can make supervisory decisions to adjust or override normal RTU (PLC) controls.

Defense-in-Depth is a fundamental principle that must be part of any network protection strategy to defend their network.

Denial of Service (DoS) The prevention of authorized access to a system resource or the delaying of system operations and functions.

Digital Control System (DCS) is a control system for a process or plant, wherein control elements are distributed throughout the system. This is in contrast to non-distributed systems, which use a single controller at a central location. In a DCS, a hierarchy of controllers is connected by communications networks for command and monitoring.

Energy Management System (EMS) is essentially a SCADA server tailored for the energy industry. In some cases this will refer to a large electrical network, and in other products this refers to the energy used within a building.

Field Device Equipment that is connected to the field side on an ICS. Types of field devices include RTUs, PLCs, actuators, sensors, HMIs, and associated communications.

Field Site A subsystem that is identified by physical, geographical, or logical segmentation within the ICS. A field site may contain RTUs, PLCs, actuators, sensors, HMIs, and associated communications.

Human Machine Interface (HMI) sometimes called the (Man Machine Interface) MMI or (Human Computer Interface) HCI. These are nodes at which control engineers monitor their plants, factories, pipelines, and field devices. Often found in control rooms, but sometimes dispersed across the plant.

Industrial Control Systems (ICS) a system that performs the functions of target acquisition, tracking, data computation, and engagement control, primarily using electronic means and assisted by electromechanical devices.

Intrusion Detection System (IDS). Intrusion detection systems perform deep-packet inspection and pattern matching to compare network packets against known "signatures" of malware or other malicious activity in order to detect a possible network intrusion. IDS operates passively by monitoring networks either in-line or on a tap or span port, and providing security alerts or events to a network operator.

Intrusion Prevention System (IPS). Intrusion protection systems perform the same detection functions of an IDS, with the added capability to block traffic. Traffic can typically be blocked by dropping the offending packet(s), or by forcing a reset of the offending TCP/IP session. IPS works in-line, and therefore may introduce latency.

Logging- In computing, a logfile is a file that records either events that occur in an operating system or other software runs, or messages between different users of communication software.

Malware- Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code (malware).

Management Controls is the security controls (i.e., safeguards or counter measures) for an information system that focus on the management of risk and the management of information security.

Modbus is a serial communications protocol originally in 1979 for use with its programmable logic controllers (PLCs). Simple and robust, it has since become a *de facto* standard communication protocol, and it is now a commonly available means of connecting industrial electronic devices. Modbus enables communication among many devices connected to the same network, for example a system that measures temperature and humidity and communicates the results to a computer.

Remote Terminal Unit or sometimes Remote Telemetry Unit (RTU) is a microprocessor used to transmit telemetry back from the field and to control devices in the field. They are often widely geographically dispersed, and use diverse wireless communications accordingly. They can run simple safety logic programs for redundancy and to reduce control delays.

Password Fuzzing is a software testing technique used to discover coding errors and security loopholes in software, operating systems or networks by inputting massive amounts of random data, called fuzz, to the system in an attempt to guess passwords.

Phishing is the tricking individuals into disclosing sensitive personal information by claiming to be a trustworthy entity in an electronic communication (e.g., internet web sites).

Port is the entry or exit point from a computer for connecting communications or peripheral devices.

Programmable logic controllers (PLCs) connect to sensors in the process and convert sensor signals to digital data. PLCs have more sophisticated embedded control capabilities (typically one or more IEC 61131-3 programming languages) than RTUs. PLCs do not have telemetry hardware, although this functionality is typically installed alongside them.

Protocol A set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems.

Red Team- Penetration testers can play the role of a "***Red Team***" to assess an organizations security to provide a more realistic picture of the security readiness than exercises, role playing, or announced assessments.

SCADA-IDS is a SCADA aware Intrusion Detection System. An IDS designed for use in SCADA and ICS networks. SCADA-IDS devices support pattern matching against the specific protocols and services used in control systems, such as Modbus, ICCP, DNP3, and others. SCADS-IDS is passive, and is therefore suitable for deployment within a control system, as it does not introduce any risk to control system reliability.

SCADA-IPS is a SCADA aware Intrusion Prevention System. An IPS system designed for use in SCADA and ICS networks. SCADA-IPS devices support pattern matching against the specific protocols and services used in control systems, such as Modbus, ICCP, DNP3, and others. SCADA-IPS is active and can block or blacklist traffic, making it most suitable for use at control system perimeters. SCADA-IPS is not typically deployed within a control system for fear of a false positive disrupting normal control system operations.

SCADA Server is the device that acts as the master in a SCADA system.

Scrub- In situations where data should not be tied to individual users, but a large number of users should be able to make queries that "**scrub**" or erase the identity of users.

Security Controls The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability.

Security Plan Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.

Security Policy Security policies define the objectives and constraints for the security program. Policies are created at several levels, ranging from organization or corporate policy to specific operational constraints (e.g., remote access). In general, policies provide answers to the questions "what" and

"why" without dealing with "how." Policies are normally stated in terms that are technology-independent.

Spoofing Modbus- To exploit this hole, an attacker could simply change their IP address to match the Modbus (this is known as **"spoofing"**) and send their malicious packets to the Client marked with TCP port 80 as his source port.

SQL Injection is a code injection technique, used to attack data-driven applications, in which malicious **SQL** statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).

Stuxnet is an advanced cyber-attack against an industrial control system, consisting of multiple zero-day exploits used for the delivery of malware that then targeted and infected specific industrial controls for the purposes of sabotaging an automated process. Stuxnet is widely regarded as the first cyber-attack to specifically target an industrial control system.

Supervisory station refers to the servers and software responsible for communicating with the field equipment (RTUs, PLCs, SENSORS etc.), and then to the HMI software running on workstations in the control room, or elsewhere. In smaller SCADA systems, the master station may be composed of a single PC.

Supervisory Control and Data Acquisition (SCADA) refers to the systems and networks that communicate with industrial control systems to provide data to operators for supervisory purposes, as well as control capabilities for process management.

Telemetry system is typically used to connect PLCs and RTUs with control centers, data warehouses, and the enterprise. Examples of wired telemetry media used in SCADA systems include leased telephone lines and WAN circuits.

Vulnerability refers to a weakness in a system that can be utilized by an attacker to damage the system, obtain unauthorized access, execute arbitrary code, or otherwise exploit the system.

Vulnerability Assessment is the process of scanning networks to find hosts or assets, and probing those hosts to determine vulnerabilities. Vulnerability assessment can be automated using a vulnerability assessment scanner, which will typically examine a host to determine the version of the operating system and all running applications, which can then be compared against a repository of known software vulnerabilities to determine where patches should be applied.

Worm is a standalone malware computer program that replicates itself in order to spread to other computers.

War Dialing is the technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers and malicious hackers who specialize in breaching computer security - for guessing user accounts (by capturing voicemail greetings), or locating modems that might provide an entry-point into computer or other electronic systems

War Driving is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer, smartphone or personal digital assistant (PDA).

Acronyms & Abbreviations

AC Alternating Current
ACL Access Control List
AGA American Gas Association
API American Petroleum Institute
ARP Address Resolution Protocol
BCP Business Continuity Plan
CIDX Chemical Industry Data Exchange
CIGRE International Council on Large Electric Systems
CIP Critical Infrastructure Protection
CMVP Cryptographic Module Validation Program
COTS Commercial Off-the-Shelf
CPNI Centre for the Protection of National Infrastructure
CPU Central Processing Unit
CSE Communications Security Establishment
CSRC Computer Security Resource Center
CSSC Control System Security Center
CVE Common Vulnerabilities and Exposures
DCOM Distributed Component Object Model
DCS Distributed Control System(s)
DETL Distributed Energy Technology Laboratory
DHS Department of Homeland Security
DMZ Demilitarized Zone
DNP Distributed Network Protocol
DNS Domain Name System
DOE Department of Energy
DoS Denial of Service
DRP Disaster Recovery Plan
EAP Extensible Authentication Protocol
EMS Energy Management System
EPRI Electric Power Research Institute
ERP Enterprise Resource Planning
FIPS Federal Information Processing Standards
FISMA Federal Information Security Management Act
FTP File Transfer Protocol
GAO Government Accountability Office
GPS Global Positioning System
HMI Human-Machine Interface
HSPD Homeland Security Presidential Directive
HTTP Hypertext Transfer Protocol
HTTPS Hypertext Transfer Protocol Secure
HVAC Heating, Ventilation, and Air Conditioning
I/O Input/Output
I3P Institute for Information Infrastructure Protection
IAONA Industrial Automation Open Networking Association

ICMP Internet Control Message Protocol
ICS Industrial Control System(s)
IDS Intrusion Detection System
IEC International Electrotechnical Commission
IED Intelligent Electronic Device
IEEE Institute of Electrical and Electronics Engineers
IETF Internet Engineering Task Force
IGMP Internet Group Management Protocol
INL Idaho National Laboratory
IP Internet Protocol
IPS Intrusion Prevention System
IPsec Internet Protocol Security
ISA The Instrumentation Systems and Automation Society
ISID Industrial Security Incident Database
ISO International Organization for Standardization
IT Information Technology
ITL Information Technology Laboratory
LAN Local Area Network
MAC Media Access Control
MES Manufacturing Execution System
MIB Management Information Base
MTU Master Terminal Unit (also Master Telemetry Unit)
NAT Network Address Translation
NCSD National Cyber Security Division
NERC North American Electric Reliability Council
NFS Network File System
NIC Network Interface Card
NISCC National Infrastructure Security Coordination Centre
NIST National Institute of Standards and Technology
NSTB National SCADA Testbed
OLE Object Linking and Embedding
OMB Office of Management and Budget
OPC OLE for Process Control
OS Operating System
OSI Open Systems Interconnection
PCSF Process Control System Forum
PDA Personal Digital Assistant
PIN Personal Identification Number
PID Proportional – Integral - Derivative
PIV Personal Identity Verification
PLC Programmable Logic Controller
PP Protection Profile
PPP Point-to-Point Protocol
R&D Research and Development
RADIUS Remote Authentication Dial In User Service
RBAC Role-Based Access Control
RFC Request for Comments
RMA Reliability, Maintainability, and Availability

RPC Remote Procedure Call
RPO Recovery Point Objective
RTO Recovery Time Objective
RTU Remote Terminal Unit (also Remote Telemetry Unit)
SC Security Category
SCADA Supervisory Control and Data Acquisition
SCP Secure Copy
SFTP Secure File Transfer Protocol
SIS Safety Instrumented System
SMTP Simple Mail Transfer Protocol
SNL Sandia National Laboratories
SNMP Simple Network Management Protocol
SP Special Publication
SPP-ICS System Protection Profile for Industrial Control Systems
SQL Structured Query Language
SSH Secure Shell
SSID Service Set Identifier
SSL Secure Sockets Layer
TCP Transmission Control Protocol
TCP/IP Transmission Control Protocol/Internet Protocol
TFTP Trivial File Transfer Protocol
TLS Transport Layer Security
UDP User Datagram Protocol
UPS Uninterruptible Power Supply
US-CERT United States Computer Emergency Readiness Team
USB Universal Serial Bus
VFD Variable Frequency Drive
VLAN Virtual Local Area Network
VPN Virtual Private Network

Suggested Reading:

Knapp, Eric D., and Joel Thomas Langill. *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Syngress, 2014.

Knapp, Eric D., and Raj Samani. *Applied cyber security and the smart grid: implementing security controls into the modern power infrastructure*. Newnes, 2013.

Radvanovsky, Robert, and Jacob Brodsky, eds. *Handbook of SCADA/control systems security*. CRC Press, 2013.

Abbas, Hosny, *Future SCADA challenges and the promising solution: the agent-based SCADA. International Journal of Critical Infrastructures 01/2014; 10(3/4):307 - 333. DOI: 10.1504/IJCIS.2014.066354*

21 Steps to Improve Cyber Security of SCADA Networks, Office of Energy Assurance, U.S. Department of Energy, http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf.

Macaulay, Tyson, and Bryan L. Singer. *Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS*. CRC Press, 2011.

Zetter, Kim. *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. Crown, 2014.

White Papers:

Falliere, Nicolas, Liam O. Murchu, and Eric Chien. "W32. stuxnet dossier." *White paper, Symantec Corp., Security Response* 5 (2011).

Albright, David, Paul Brannan, and Christina Walrond. "Stuxnet malware and natanz: Update of isis december 22, 2010 report." *ISIS, February* 15 (2011).

Murchu, Liam O., Stephen Doherty, and Eric Chien. *Stuxnet 0.5: The missing link*. Symantec, 2013.

Byres, Eric, Andrew Ginter, and Joel Langill. "How Stuxnet spreads–A study of infection paths in best practice systems." Tofino Security, white paper (2011).

W. Broad, J. Markoff, and D. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," New York Times, 15 Jan 11.

D. Kushner, "The Real Story of Stuxnet," IEEE Spectrum **53**, No. 3, 48 (2013).

B. Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack," Strategic Insights **10**, 15 (2011).

K. Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (Crown, 2014).

J. Grayson, "Stuxnet and Iran's Nuclear Program," Physics 241, 7 Mar 11

October 2015: The Industrial Control System Cyber Kill Chain *SANS Institute*

August 2015: The Sliding Scale of Cyber Security *SANS Institute*

June 2015: The State of Security in Control Systems Today: A SANS Survey *SANS Institute*
May 2015: The Perfect ICS Storm *SANS Institute*

August 2014: An Abbreviated History of Automation & Industrial Controls Systems and Cybersecurity *SANS Institute*

January 2014: Industrial Control Systems (ICS) Cybersecurity Response to Physical Breaches of Unmanned Critical Infrastructure Sites Whitepaper *SANS Institute*

Web Sites:

https://ics-cert.us-cert.gov/

https://scadahacker.com/

http://ics-isac.org/

http://www.nist.gov/energy-portal.cfm

https://www.esisac.com/

http://www.nerc.com/Pages/default.aspx

http://krebsonsecurity.com/

http://www.samuraistfu.org/

http://www.pbs.org/wgbh/nova/military/cyberwar-threat.html

https://www.f-secure.com/weblog/archives/00002718.html

http://www.cnet.com/news/hacker-says-he-broke-into-texas-water-plant-others/

http://www.slideshare.net/guest85a34f/dhs-ics-security-presentation

http://www.darkreading.com/risk/stuxnet-five-years-later-did-we-learn-the-right-lesson/a/d-id/1319740

https://scadahacker.com/library/

http://andrewmohawk.com/category/security/pastebin-security/

http://large.stanford.edu/courses/2015/ph241/holloway1/

Twitter Feeds:

https://twitter.com/SCADAhacker

https://twitter.com/ICSCERT

https://twitter.com/ICSISAC

https://twitter.com/SANSInstitute

https://twitter.com/infosec

https://twitter.com/briankrebs

Training:

http://ics.sans.org/

https://niccs.us-cert.gov/training/tc/search/detail/1439

http://www.infosecinstitute.com/

http://www.isaca.org/Education/Training/On-Site-Training/Pages/default.aspx?cid=sem_1104935&appeal=sem&gclid=CjwKEAjw1Iq6BRDY_tK-9OjdmBESJABlzoY7gq8VrXqj06ldhUzS2kiDWfweY9D2TTbB68b4SPhV-BoCcRzw_wcB

https://scadahacker.com/training.html

Example Course: SANS Institute

ICS410: ICS/SCADA Security Essentials (5 Day Course)

This course provides a foundational set of standardized skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

The course is designed for the range of individuals who work in, interact with, or can affect industrial control system environments, including asset owners, vendors, integrators, and other third parties. These personnel primarily come from four domains:

- IT (includes operational technology support)
- IT security (includes operational technology security)
- Engineering
- Corporate, industry, and professional standards

Video: http://www.pbs.org/wgbh/nova/military/cyberwar-threat.html