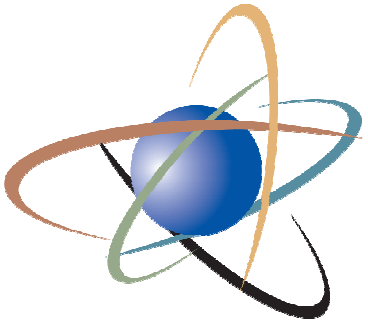


U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

Cyber Security and Industrial Automation Systems

William (Tim) Shaw – CISSP, C|EH, CPT
NRC Cyber Security Specialist

Presentation Outline

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- IACS and IT - Similarities and Differences
- Operational differences between IT and Plants
- The ‘digital’ environment in Industrial Facilities
- Potential Attack Vectors for Industrial Facilities
- Address vs. Implement – One size doesn’t fit all
- Challenges unique to IACS
- Summary/Conclusion

IACS and IT – Similarities and Differences

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Over the past two decades the computer-based technologies used for industrial automation have evolved from systems and products with highly customized and proprietary designs (both HW and SW) into systems and products that look, in many ways, very much like conventional IT/Business systems.

- This is because those IACS systems and products have migrated onto and incorporated commercial platforms and IT technologies such as x86 computers and servers, MS Windows operating systems, TCP/IP and Ethernet networking, Oracle and SQLserver RDBMS and web-based user interfaces and browser SW.

IACS and IT – Similarities and Differences

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- To a certain degree DCS and SCADA systems look just like conventional IT systems; except with some unusual peripheral devices and application programs. In fact some SCADA vendors now mainly sell software and allow customers to purchase and stage their own servers, PCs, LANs (and commercial software, including OS and networking.)

- For these reasons some organizations have put their IT departments in charge of supporting their computer-based industrial automation systems. This doesn't always work well due to differences in philosophy between traditional IT "best practices" and the operational requirements of an industrial plant/facility.

IACS and IT – Similarities and Differences

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- A major difference between plant operations and traditional IT is the issue of safety. No one is seriously injured if the email server has to be rebooted. No one dies if the web server goes down. But in many plants if the computer–based control/automation system crashes or mis-operates there is the possibility for injury and even death. Even rebooting such a system can be dangerous.

- IT systems tend to be replaced every few years and generally keep pace with technology. But plant automation systems are expected to operate for ten or more years and thus often incorporate old and even obsolete HW and SW.

IACS and IT – Similarities and Differences

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Patching and updating software is done almost daily on IT systems, even if there is no way to test these changes in advance of deployment. Plant systems often never get patched or updated due to the risk of introducing a problem ("if it ain't broken don't fix it!") and the lack of a test system on which to validate changes/patches.

- IT systems use HW/SW that is available from many sources or which has active vendor support. But plant automation systems may incorporate proprietary HW and SW and the original vendors may no longer exist (maybe acquired?) or no longer support their older equipment and systems.

- Plant systems use a lot of legacy communication protocols including those that have been converted to work over Ethernet and TCP/IP.

Dangerous Consequences

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Much of the critical (and dangerous) industrial infrastructure in the developed world is controlled (and protected) by computer-based "automation" systems and as such a malicious compromise of those systems has the potential for serious harm to plant workers, the 'public' and the environment.

Accidents and human error have had dramatic consequences. Just think of what might happen if someone set out to **intentionally** maliciously manipulate a critical control/automation system.

Chernobyl

Consequences of Cyber Attacks

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

In reality the consequences of IACS compromise could range from a small production loss to a major environmental disaster, and everything in between, based on the process:

- Unauthorized access, theft, or misuse of confidential information (product formulations, trade secrets, production schedules, etc.)
- Loss of integrity or reliability of process/production information
- Loss of system availability and/or accessibility
- Process upsets leading to compromised process functionality, inferior product quality, product contamination, lost production capacity, compromised process safety, or environmental releases
- Equipment and/or facility damage
- Personal injury or death
- Violation of legal and regulatory requirements (e.g. environmental)
- Risk to public health and confidence
- Threat to a nation's security (DHS)

Operational Differences between IT and Plants

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Most industrial plants operate 24/7 and it is expensive, and even dangerous, to try and shut them down. Computer-based automation systems are expected to operate 24/7 for ten or more years once installed and commissioned.

- Most IACS designs incorporate full redundancy (or some form of 'graceful degradation') and allow for "hot" repairs if something does fail. Most have a distributed design to limit the impact of a failure to a plant unit/train/work cell.

- Patching and SW updating are usually only done to fix problems that make the system/device unacceptably mal-functional. Cyber security isn't usually a consideration.

Operational Differences between IT and Plants

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Most industrial plants operate with 'lean' staffing and often lack personnel with networking, IT and cyber security expertise. Often I&C personnel with minimal training are called upon to perform IT functions.

- Safety (followed by cost) is a major overriding concern in all decision making.

- Many plants have old/orphaned systems that are no longer supported by their manufacturer and the philosophy is usually to prohibit ANY changes to such systems except for repairing failed hardware components.

- Plants use a lot of smart devices, many now with IP/Ethernet networking capabilities (and wireless), and these devices are not familiar to IT personnel and they use 'industrial' protocols also not familiar to IT personnel.

Obsolete and Proprietary HW

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NOVA 2 minicomputer

VAX/MicroVAX

VT100 Dumb Terminal

PDP-11 minicomputer

VAX Station

Proprietary CRT/Console
(8-bit microprocessor)

Proprietary Controller and I/O
(16-bit microprocessor)

Proprietary RTU and I/O
(16-bit microprocessor)

The 'Digital' Environment in Industrial Facilities

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Most US industrial plants (other than nuclear) converted to computer-based automation starting in the 1980s when DCS technology came on the market. Geographically distributed processes, such as power transmission and pipelines, began adopting SCADA technology in the 1970s. Plants that couldn't afford or justify DCS technology adopted PC/PLC technology when it became available in the late 1980s.

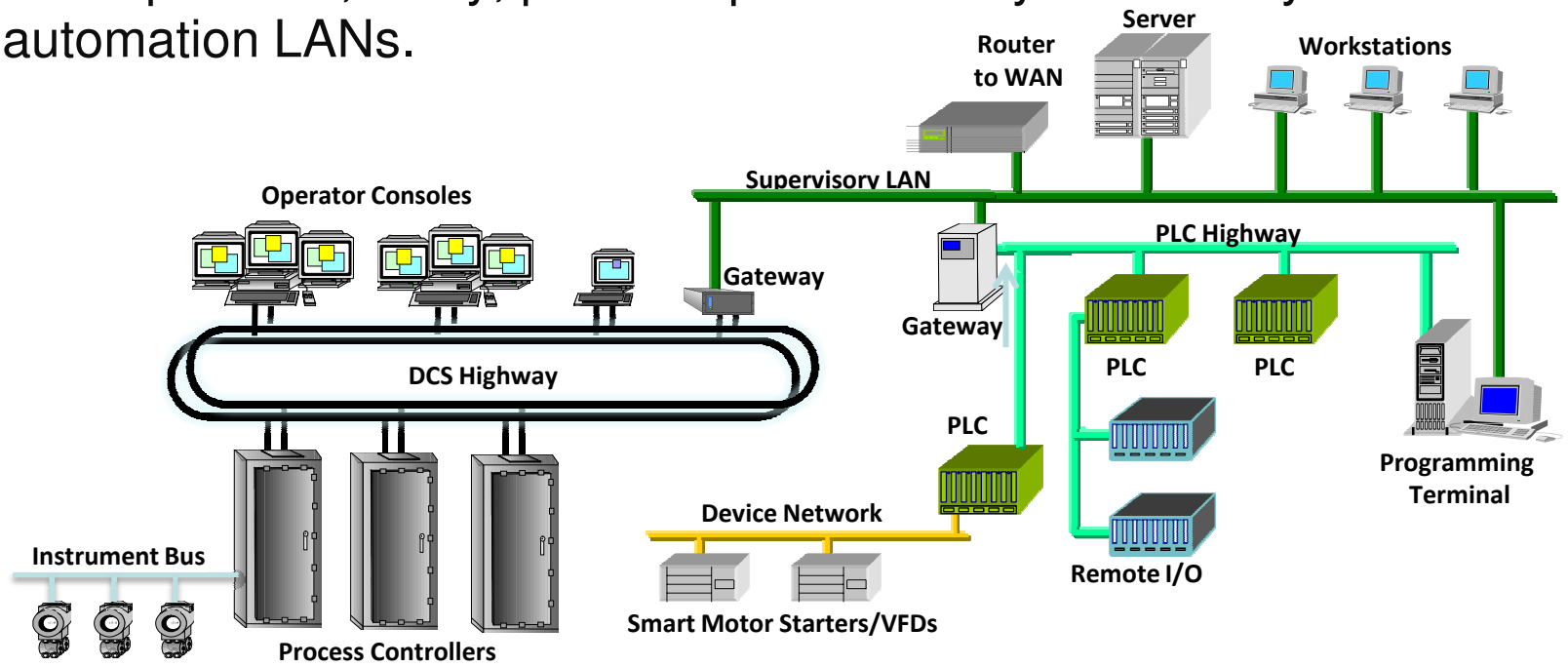
- Conventional panel and field instruments began being replaced with digital versions in the late 1980s and today almost all instruments and even control elements (e.g. valves) are "smart."

- In most plants you will find a number of local area networks. There are proprietary LANs for older DCS systems and PLC systems. There are a number of vendor-specific instrument "fieldbus" LANs in use today.

Plant Networking

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Today plant networks may be mainly Ethernet based and may be shared by multiple systems and subsystems. Plant networks may be multi-purposed and carry process control/data message traffic as well as video and even VoIP phone traffic. Plants (especially large ones) have also begun utilizing wireless networking, both of the IEEE 802.11 (Wifi) and “fieldbus” variety.
- In the past few, if any, plants implemented cyber security on their automation LANs.



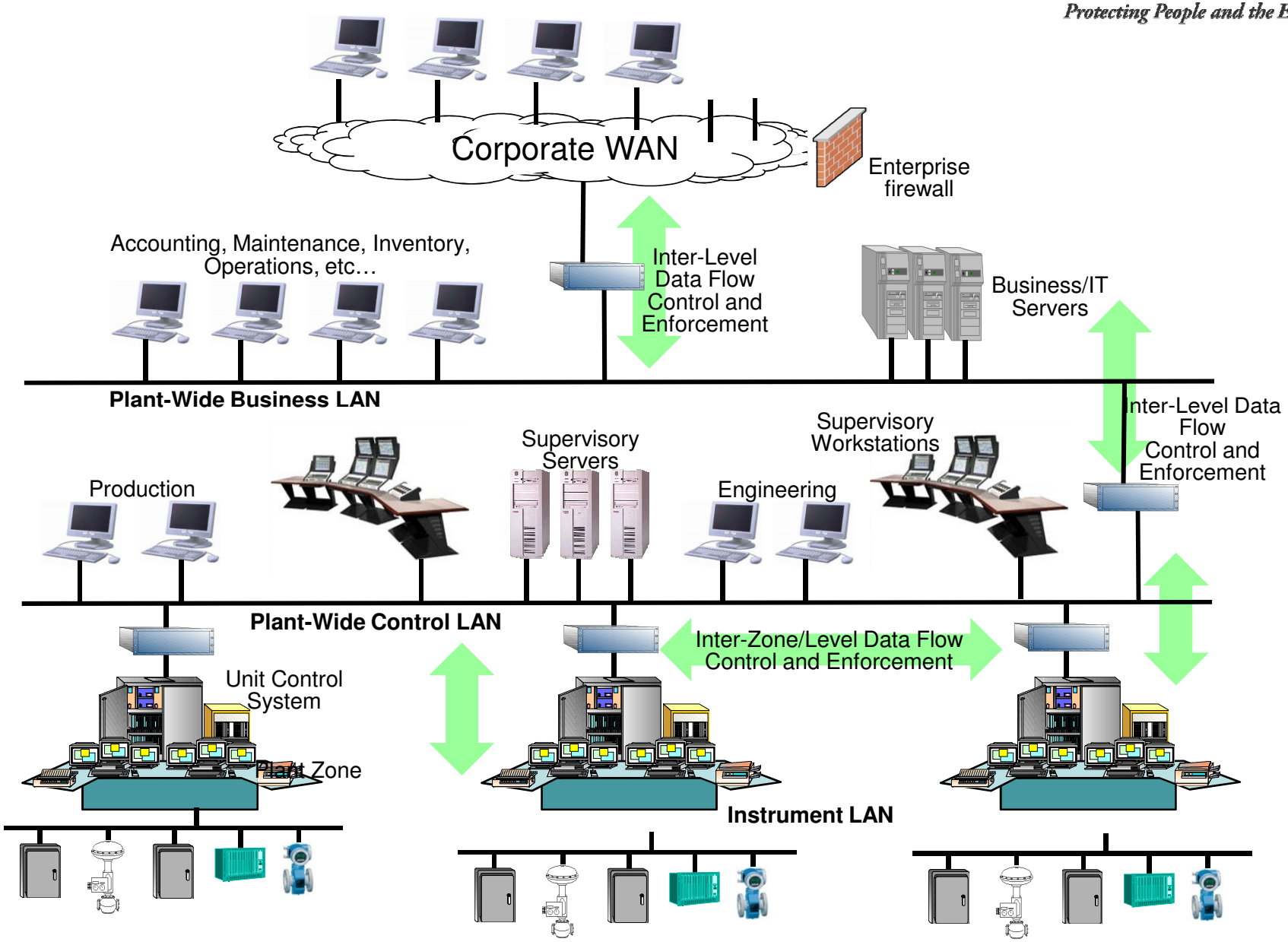
Plant Networking

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Most modern plants use a range of digital technologies and digital networks (LANs) and usually all of them are ‘bridged’ or interconnected to allow for plant-wide integrated data acquisition and control (both automatic and supervisory.)

Corporate IT Vertical Integration

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment



The 'Digital' Environment in Industrial Facilities

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

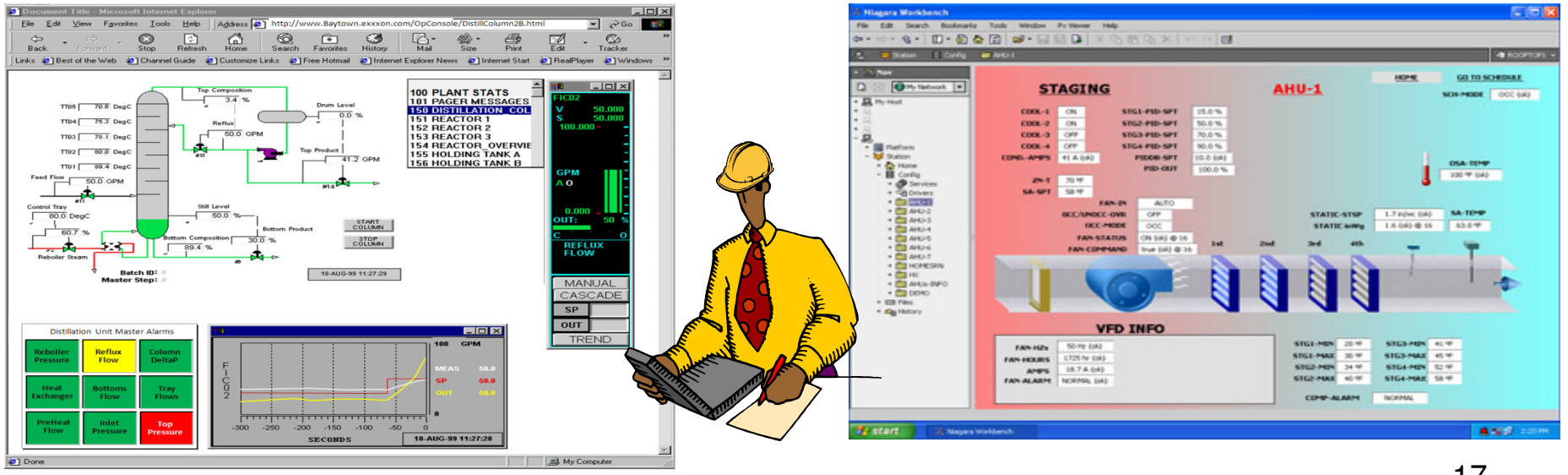
- Newer plants, or those upgraded recently, may have replaced much of the proprietary LAN technology with Ethernet versions (or with wireless technologies.)

- Some plants have begun creating wireless LANs that provide coverage all around the facility so that personnel can use this for their cell phones and for portable devices (e.g. a tablet PC providing a roving operator's console or access to a maintenance system or documentation/manuals.)

Web Technologies

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Web technology, combined with wireless networking, is being used in industrial facilities to enable personnel to access operational, process, production and maintenance data regardless of their location. This is very convenient, but opens up potential cyber vulnerabilities if adequate cyber security isn't used. Many plants have "guest" Wifi access with only basic security controls in place (e.g. a router) to prevent an unauthorized/malicious cross-over from the guest WLAN onto the plant LANs.



Lots of Smart Devices

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

PLCs and remote I/O

Digital panel instruments

Digital chart recorders

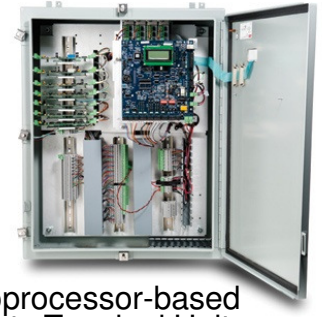
Smart control elements

Computer-based test equipment

Computer-based displays

Smart transmitters

Microprocessor-based controllers



Microprocessor-based
Remote Terminal Units

Smart Analytical Devices

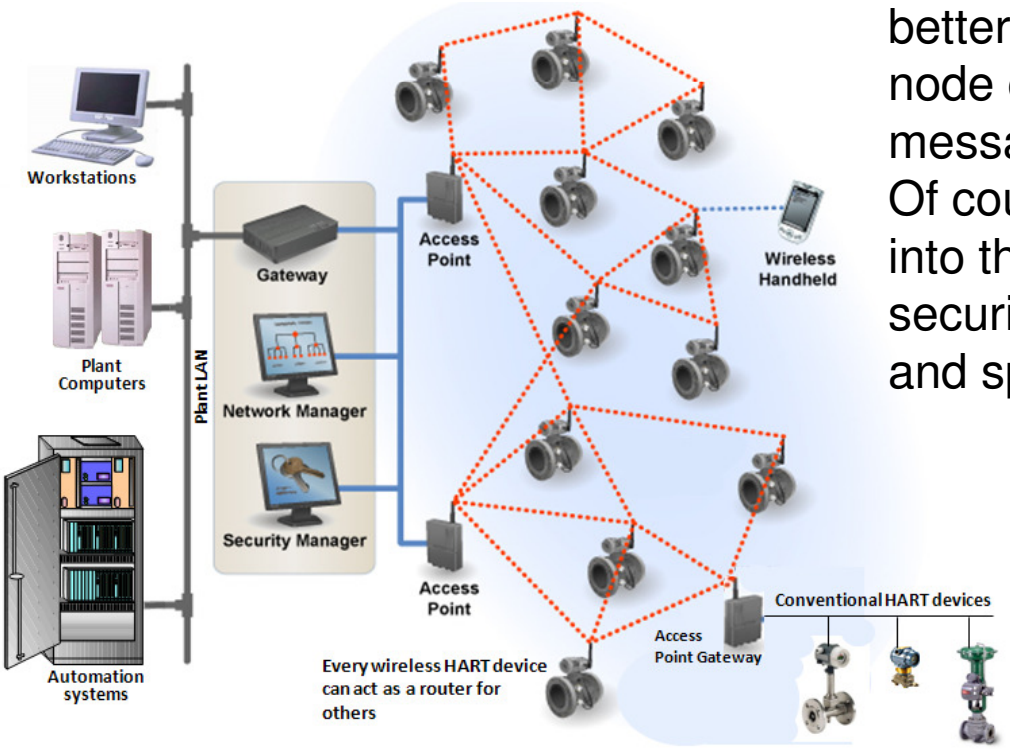
Digital protective relays

Digital protective relays

Wireless Instrumentation

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Wireless instrumentation networks have started gaining popularity in plants due to the elimination of signal wiring costs and the ability to move instruments if needed and to be able to locate instruments in places that would be impossible otherwise (e.g. on moving equipment and rotating platforms.) Many vendors offer wireless devices and there are several competing standards such as wirelessHART (shown on the left) and ISA.100. A mesh network provides better reliability and coverage since each node can provide store-and-forward message routing services to other nodes. Of course an Access Point can connect you into the mesh so it is critical to use the security features to block rouge connections and spoofed message traffic.



Potential Attack Vectors for Industrial Facilities

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Cyber attacks are not done with magic and hackers aren't wizards (even if some think they are.) There are only a handful of vectors/pathways that can be used to launch a cyber attack. The obvious ones are wired or wireless communication links. These can be high-bandwidth network (LAN or WAN) connections or simple point-to-point 'serial' links with another system/device. These can also be temporary links such as using a dial-in/out modem and phone line to connect to another system/device (or the Internet itself.)

- Sometimes you have pathways that you don't realize: a cell phone with a "hot spot" provides a path to the Internet for a laptop equipped with Wifi capabilities. An analyzer or subsystem comes with an (undocumented) integral cellular modem/gateway so that the vendor can remotely monitor and support the device. A system has an auto-answer modem and router so that the vendor can provide remote technical support via the telephone (and was left connected to a phone line after the system was commissioned.)

Potential Attack Vectors for Industrial Facilities

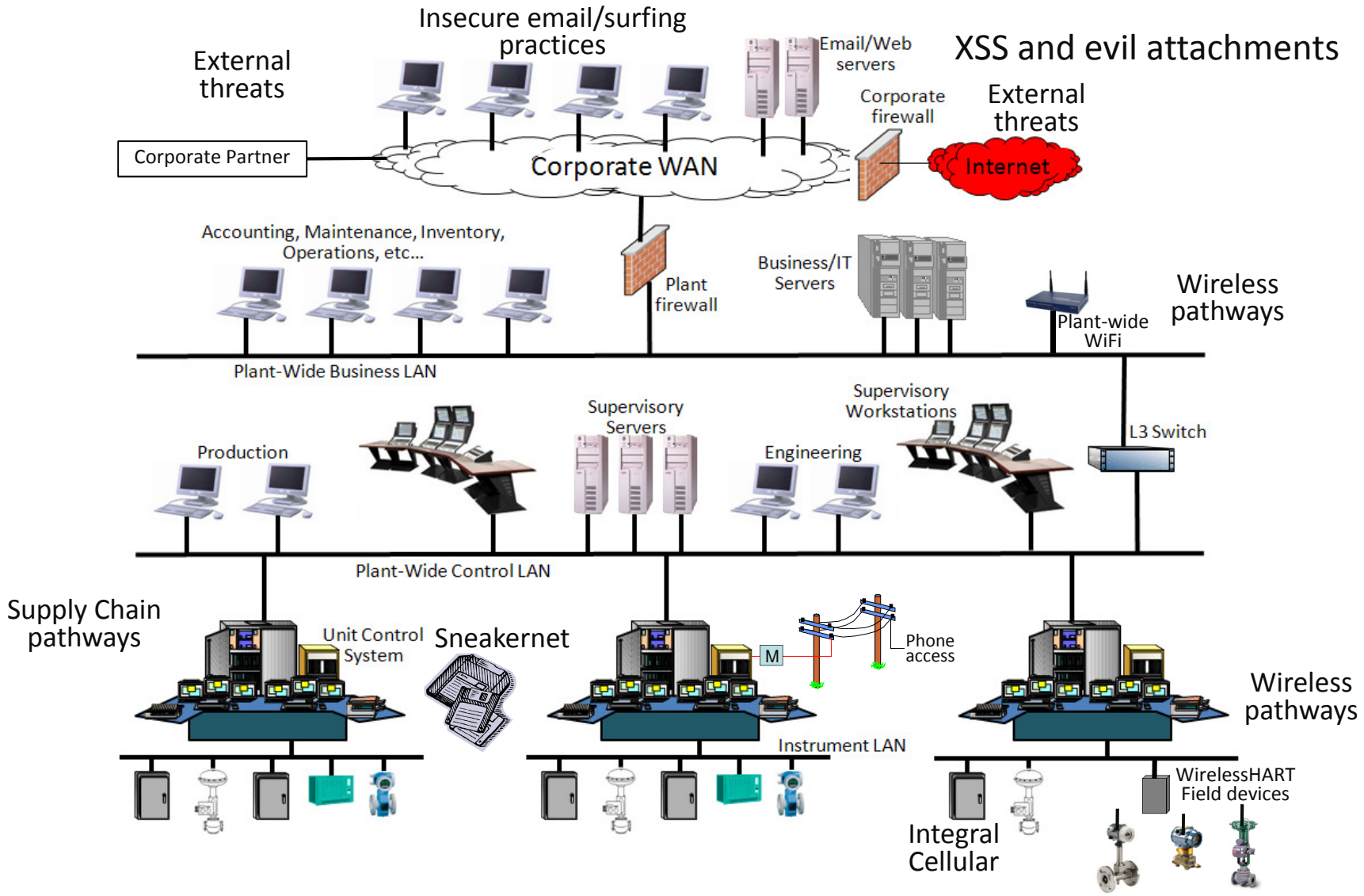
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Wireless connectivity comes in many forms today: laptop PCs with integral Wifi and Bluetooth adapters. PCMCIA cellular modems that connect to the cell phone system and onto the Internet. USB adapters that add Bluetooth or Wifi capabilities to any computer. Cell phones that support 'tethering'. A rogue AP attached to an internal network.

- Cyber attacks can be launched locally if the attacker has physical access to the computer or system. Cyber attacks can be launched through the use of infected computer-readable media or by connecting an infected device to a computer/system. Malware has been spread through network-connected shared peripherals such as a network printer or copy center.

Potential Points of Attack

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment



Less Obvious Attack Pathways

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

An obvious attack path for a system is any communication interface (wired and/or wireless) that connects that system to other systems or devices.

But the path too often overlooked, or underestimated, is the oldest one: SneakerNET. There is a vast array of portable devices and removable media that have the ability to deliver malware to, and be used to take sensitive information from, an inadequately protected system.

Less Obvious Attack Pathways

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Any USB port is particularly dangerous due to the bulk storage object concept that automatically mounts the file system of such a device. USB ports also support UPnP functions that allow devices to 'connect' and interoperate. Equally dangerous are the O.S. AutoRun or AutoPlay functions that try to find and 'play' the content on the inserted/mounted media.

Infected media/devices have been (are still) a well-used vector for delivering malware.

Supply Chain Threats

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

An attack vector that has come to the attention of cyber security professionals in the past few years is what is collectively known as the “supply chain” which is a general term for malicious activities in the design, construction or on-going support of your systems. If an attacker is completely rebuffed by your physical and cyber security measures, and willing to invest in a longer-term attack strategy, then your vendors could be used to attack your critical systems.

Supply Chain Threats

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

By either compromising your vendor or actually going to work for them (especially in product support or field service where they can abuse the 'trust relationship'), an attacker could potentially achieve any of the following:

- Including hidden functions in the original product software/firmware
- Producing/providing updates that contain a logic bomb, hidden function or a backdoor
- Providing security patches that are ineffective or that increase vulnerabilities
- Making malicious alteration of security policy settings (degrading protections)
- Malicious tampering to create vulnerabilities or implant malware
- Abusing poor end-point security for remote diagnostic support/access
- Use of infected test equipment and/or removable media in support activities
- Reinstallation of removed vulnerable applications (un-do the 'hardening')
- Creation of an unauthorized administrative account

Portable Devices

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

The discussion of portable devices generally does **not** extend to special-purpose microprocessor-based diagnostic and test equipment commonly used in plant/process environments. Most such devices do not have an interface that provides Ethernet or TCP/IP communications capability or a local file system that can be accessed via a USB connection. Most such devices have all of their software in ROM or flash and it is not possible (or it is very complicated and messy) to make changes to that programming in the field.

Most (but not all) will not be running any commercial OS; only special-purpose software is contained in the device. These portable devices do not pose the same level of cyber security threat as do laptop PCs and in general, if their use and physical access is properly managed, they do not pose a cyber threat.

Portable Devices

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Having said that be aware that there may be some types of test equipment that do actually contain a full-function computer with a COTS O.S. and assorted peripherals including network and USB connectivity. Such a device would potentially be as dangerous as a laptop PC as regards its ability to be used to harbor and deliver malware to systems/networks to which it is attached.

F.O. cable tester

Digital oscilloscope

Ethernet cable tester

F.O. light source

(W)LAN tester

HART/FF Calibrator

Digital multimeter

Address vs. Implement – One Size Doesn't Fit All

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

The NRC issued RG 5.71 in an effort to bring nuclear power plants up to an acceptable level of cyber security; specifically in regards to digital systems, devices and networks associated with safety, security and emergency preparedness functions.

That document included two appendices containing a range of cyber security 'controls' derived from NIST SP 800-53. Although that NIST document was focused on cyber security for government IT systems, many (and in some cases all) of these controls are also applicable to enhancing the cyber security of computer-based automation systems.

Address vs. Implement – One Size Doesn't Fit All

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Because of the range of functionality, complexity and capability found in digital devices, networks and systems (CDAs), the NRC staff realized that not every control could be (or should be) implemented in every case. The licensees were given the option of reviewing each CDA and determining which controls could be excluded, or replaced by an alternative countermeasure. In order to exclude a control, or to use an alternative, the licensee is required to perform an analysis and document the technical justifications. This analysis and decision process is what the NRC meant, in RG 5.71, by "addressing" all of the controls.

Some high-functionality CDAs, such as a modern DCS system or access control system, would probably benefit from the implementation of all of the security controls. Other CDAs, particularly low-functionality ones like smart transmitters, would probably be exempt from nearly all of the security controls. Rather than dictate a one-size-fits-all laundry list of security controls, the NRC allowed licensees to evaluate the controls on a case-by-case basis for each of their CDAs.

Picking The Right Controls

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

The application and selection of protective controls has a lot to do with the consequences of compromise and the functional sophistication or complexity of the system or device. Of course some controls may not be viable/possible for purely technical reasons.

Capability/Feature	Low Risk	Moderate Risk	High Risk
Basic Functionality	Factory set, no field changes	Field alterable with local connection and special vendor software	Can be completely altered either locally or remotely with Root/Admin password
Configuration	Limited minor parameter changes via local manual entry	Field alterable with local connection and special vendor software	Full range of changes possible with Root/Admin password
Operating System	None, vendor proprietary single-function program	Vendor customized version of a well-known COTS O.S.	Well-known COTS O.S. such as Unix, Linux, Windows, VxWorks
Peripherals	None	Manual support for portable media (USB) devices	Automatic support for portable media such as CD, DVD and USB
Communications	None	Serial industrial protocols (Modbus)	Wired or Wireless Ethernet/IP protocols

Simple Digital Instruments

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Some digital control devices (such as a smart transmitter) have little vulnerability to the vast array of cyber threats and attack vectors and can basically be kept 'cyber secure' through the use of physical security and physical security controls.
- Of course if you replace it with a wireless device or an Ethernet connected device the situation, and possible attack vectors, change dramatically

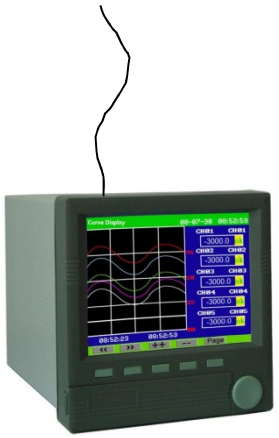
Device/Element: Foundation Fieldbus Single Measurement Transmitter Interface: 4-20mA analog signal with superimposed Digital Messaging			
Threats:	Consequences:	Attack Vector:	Countermeasures:
Physical damage to device	Loss of measurement	Physical access to device	Physical access controls
Modified scaling or ranging	Incorrect measurement value, control loop instability	Physical access or access to loop wiring with calibrator	Physical access controls and signal wiring in conduit
Modified alarm settings	No alarming or indication of dangerous value	Physical access or access to loop wiring with calibrator	Physical access controls and signal wiring in conduit
Placed off-line	Loss of measurement	Physical access or access to loop wiring with calibrator	Physical access controls and signal wiring in conduit

Complex Digital Instruments

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Some digital devices used for control are display-only and have either local setup and configuration via the available displays and controls and/or may be configured using vendor-specific software and a point-to-point local connection to the device.
- If the device supports Ethernet communications then you have to consider what could be done via that connectivity. In this case there is only asynchronous serial communication.

Serial Modus RTU



Device/Element: Multivariable Digital Chart Recorder Interface: Analog and contact I/O plus Modbus Serial for ReadOnly Access			
Threats:	Consequences:	Attack Vector:	Countermeasures:
Physical damage to device	Loss of trends and alarms	Physical access to device	Physical access controls
Modified scaling or ranging	Incorrect measurement trends and alarms	Physical access to device with laptop PC and vendor config software	Physical access controls management of config SW and laptop
Modified alarm settings	No alarming or indication of dangerous value	Physical access to device with laptop PC and vendor config software	Physical access controls management of config SW and laptop
Placed off-line	Loss of measurement trends and alarms	Physical access to device with laptop PC and vendor config software	Physical access controls management of config SW and laptop

Digital Controllers

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

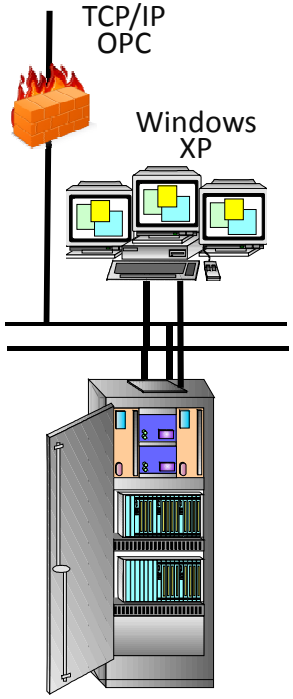
- A PLC that has Ethernet LAN capability and is performing critical control functions will accept downloads and commands from any other device that speaks its language.
- Current PLCs do not support authentication (other then simple passwords) and cannot differentiate the source of program downloads or commands but some support a physical key-lock switch for enabling/blocking program changes/downloads

Device/Element: Programmable Logic Controller **Interface: 100 BaseT Ethernet, Modbus/TCP, Embedded Web Server, Telnet**			
Threats:	Consequences:	Attack Vector:	Countermeasures:
Physical damage to device	Process/unit trip	Physical access to device	Physical access controls
Modified regulatory control logic	Create dangerous process conditions, possible injuries	Physical access to LAN with laptop PC and COTS config software	Isolate LAN via switches and routers and use firewalls to manage access
Modified or disabled safety logic	Ignore dangerous process conditions, possible injuries	Physical access to LAN with laptop PC and COTS config software	Isolate LAN via switches and routers and use firewalls to manage access
Disable communications (DOS attack)	Operators blind, process/unit trip required	Physical access to LAN with laptop PC and COTS config software	Isolate LAN via switches and routers and use firewalls to manage access

Computer-Based Automation System

United States Nuclear Regulatory Commission
Protecting People and the Environment

- A Full-Function DCS is capable of running all of the control and sequence (and basic safety) functions of a large plant, including all of the BOP activities. Advanced calculations and modeling can be supported by a single system.
- Modern DCS systems borrow heavily from the IT world as regards hardware platforms, O.S., networking, HMI, Relational databases, etc.



Device/Element: Distributed Control System (DCS)
Interface: 100 Base FO, MS Windows, RTLinux, TCP/IP, OPC, IIS, MySQL

Threats:	Consequences:	Attack Vector:	Countermeasures:
Physical damage to device	Process/unit trip	Physical access to device	Physical access controls
Modified regulatory control or safety logic	Create dangerous process conditions, possible injuries	Remote connectivity via Corporate WAN, via support access, via malware infection	Multi-layer DiD with strong boundary (DMZ) defenses, monitoring and full O&M controls
Op Console hijacking and manual override of controls	Explosive conditions, plant damage, death and injuries, threat to public health	Remote connectivity via Corporate WAN, via support access, via malware infection	Multi-layer DiD with strong boundary (DMZ) defenses, monitoring and full O&M controls
Disable communications (DOS attack)	Operators blind, process/unit trip, plant shutdown required	Remote connectivity via Corporate WAN, via support access, via malware infection	Multi-layer DiD with strong boundary (DMZ) defenses, monitoring and full O&M controls

Challenges Unique to IACS

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- In an operating plant environment it is often impossible to shut down or turn off the computer-based systems that you want to make more cyber secure. The process of hardening a system or installing a host-based intrusion detection package or even installing a host-resident firewall package may disrupt (even if only momentarily) the functioning of these systems. If you have to wait for an outage to do this work it could be many months or even years before the opportunity presents itself.

- If such as system is fully redundant then it may be possible to make these changes to the 'standby half' but you do loose redundancy while this is happening. With a distributed system design you may be able to make your changes to one component of the system at a time. But you will have to deal with the plant/process elements impacted by the temporary loss of that component. Some controllers and devices don't hold their process outputs in the current state when you restart them, which can cause a process disruption/upset. Also, you will generally produce a lot of alarms when you mess with these systems so operational personnel need to be prepared to deal with that situation.

Challenges Unique to IACS

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Performing these activities “hot” always poses a risk and potential safety hazard. Most computer-based automation systems don’t include any manual overrides that allow control actions to be performed (e.g. opening/closing contact outputs and manipulating analog outputs.) In most plants making changes “hot” requires a good deal of advance planning and preparation and coordination between operations, engineering, instrumentation and maintenance staffs. There may be a need to install temporary equipment and wiring to support plant operations while the changes are being made.

Patching and Updates

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- In an operating plant environment there may be a range of devices and systems performing control/automation functions. The age and technology base of these devices and systems can vary dramatically. You may have ‘orphaned’ systems and devices for which no vendor exists, let alone vendor support. You may have systems that are of a vintage that utilize early MS/Unix/Linux operating systems (e.g. DOS, Windows 98, Sun Solaris, VMS, etc.)
- In many instances the plant operational and I&C organizations may be loath to allow ANY messing with those devices/systems, including installing patches or updates. Or, they may permit patching only during an outage so the patching/updating can be tested and rolled-back if needed. It is always advisable to have plans for undoing changes if they don’t work out.

Patching and Updates

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- There my be no documentation, incomplete documentation or only poor/inaccurate documentation, for plant networks and wiring and for those old systems and devices (which makes patching, updating or modifying them even more risky.)
- Old systems may not have accurate or complete (or any) backups. The plant might have the media (tapes?) used to initially install and commission the system but they may never have made any subsequent backups. In some cases the backup media may prove to be unreadable or corrupt. Some plants may have updated their peripheral devices (e.g. going from reel-to-reel magnetic tape to cartridge tape) and never made a new backup.
- Getting a good backup made may be the critical first step before anything else can be done to an automation system or device.

Orphaned & Legacy IACS

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- In some cases a plant may have a digital control system that is outdated and no longer be supported by the vendor (or the vendor may no longer exist.) Spare parts may have to be found on eBay or purchased 'used' from others who have replaced such a system. (E.g. the US nuclear industry does a lot of this.)

- Though old, these systems may be sufficiently modern (1990s) to have Ethernet networking and use a Unix/Linux or Windows operating systems (and thus be susceptible to many cyber attack methodologies.) They may be a mix of newer and older technologies due to partial upgrades or system expansions.

Orphaned & Legacy IACS

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- The plant personnel may fear making any alteration or modifications to the system because of the possibility of 'breaking' it and shutting down the plant.
- The plant personnel may also feel that the systems are memory and processor limited and incapable of supporting any additional functions or programs. With systems based on Windows NT and 1990 computer technology, they may well be right.

Summary/Conclusion

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Although modern automation systems may look like IT systems, there are critical differences in best practices
- IT personnel usually will not be familiar with many of the specialized “smart” devices that are used for digital I&C, including their communication protocols
- Plant personnel often deal with IT issues but don’t actually have the proper training to know what they are doing or how it impacts security
- Modern industrial plants have a lot of digital technology and networks, and the evolution is towards universal Ethernet networking and wireless LANs

Summary/Conclusion

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Plant automation systems and devices are potentially vulnerable to a range of cyber attacks and there are many attack vectors/pathways that may be exploited including the supply chain and portable media and devices
- Operating plants pose a lot of challenges in regards to making changes to implement cyber security, mostly due to safety concerns
- The application of security controls to critical systems/devices/networks has to take into account the capabilities/functions of the CDA and the consequences of its compromise