



Setting the Standard for Automation™

Why Cyber Security is Harder for Industrial Facilities

Meet the Speaker



William (Tim) Shaw – PhD, CISSP, C|EH, CPT
Chief Security & Automation Architect
Industrial Automation and Control Systems

Over 40 years of industry experience designing and deploying DCS, SCADA and PLC based industrial control and automation systems in a range of industries including Electric power, Oil and Gas pipelines, Refining, Water and Waste-Water, Petrochemical, Steel, Glass, Pharmaceuticals, Wind Turbines, Nuclear Power and Substation Automation. He is the Author of Computer Control of BATCH Processes and Cyber Security for SCADA Systems as well a co-author of Industrial Data Communications. Shaw is a subject matter expert to the ISA where he teaches several courses on I&C, SCADA and DCS technologies as well as basics of process measurement, industrial cyber security, telecommunications and networking and database management for industrial automation systems. Shaw is a former Adjunct Assistant Professor of Computer Science at Loyola University in Baltimore and currently teaches on-line classes for the U of Kansas. Shaw is a Certified Information System Security Professional a Certified Ethical Hacker and Certified Penetration Tester. He is also a Contributing Editor for Security Topics to Electric Energy T & D Magazine.

Industrial Facilities Face Real Cyber Threats

International threat-actors (China, North Korea, Russia, etc.) are actively attempting to establish footholds in automation systems for critical infrastructure (Pipeline/Power grid/Transportation) and many others too!

They have had a lot of success even if they have not elected to use their footholds for anything (so far) but industrial espionage and I.P. theft

Even product vendors have been compromised via out-sourced manufacturing and software development (e.g. recent 'back-door' found in major vendor of Switches/Security Appliances; 'back-door' found in domestic power meters; malware spread by HP printers....)

Establishing Cyber Security is Difficult in General

There are many ways for the bad guys to get into your plant systems:

- Network interconnections with a Corporate WAN
- Plant connections to the Internet
- Poor Email and web browsing practices
- Portable computer devices (laptops, tablets, cell phones)
- Infected computer media (CD/CVD, USB drives, memory sticks)
- Dial-in access for remote personnel and vendor support
- Supply chain (vendor personnel, patches, updates, infected products)

Management Doesn't Always Believe

In spite of regulatory pressures and government mandates and reading about cyber attacks and data breaches in the news almost daily there are still a surprising number of industrial facilities that have not implemented an adequate cyber security program to protect their critical systems/devices

Just as worrisome (or maybe more) are the plants where they think they **have** provided adequate protections; but in reality their digital systems are actually still vulnerable (often due to lack of security technology expertise or misguided “help” from corporate IT or vendors)

You still hear upper-level managers saying “it won’t happen here” and “it hasn't happened here” (even when it actually has!)

There Seems to be Lots of Help Available

IT consultants and IT product vendors are willing to provide all sorts of advice, services and cyber toys (for a price);

Corporate IT says it can just swing by and fix things in no time, just the same way they have for the corporate business systems;

And yet time passes and industrial facilities continue to be inadequately protected against cyber threats.

Is there any logical reason why this is so?

One Challenge are the On-Going Myths

Our systems are vendor proprietary and not susceptible to cyber attacks

Our systems are isolated so no attacker can get to them

Our systems are so old that no one knows about them

Our plant isn't important so no one would attack it

We are protected by our Corporate IT department's firewall

Our systems are redundant so an attack would have little impact

It Can't Happen Here!

Some industrial facilities believe that their physical security measures (fences, gates, video surveillance and guards) provide adequate cyber protection for critical digital assets,

Especially since they probably also believe those digital assets to be “isolated” and thus impossible to attack, and therefore don’t think they need anything further.

The definition of the term “isolated” would seem to be clear; you can look it up in a dictionary (anyone remember those?) I thought I understood the term..



It Can't Happen Here!

I have had plant personnel swear up and down that a particular critical digital system was “isolated”

Except of course when Engineering Lead Fred X needs to dial into it from home (or connect to it across the Internet) during an emergency.

Oh, and of course when the system vendor needs remote access to diagnose a problem and download a ‘fix’

And of course any of the technicians can walk up to the system and connect a laptop or insert a CD at any time, because all of them are totally trustworthy.

It Can't Happen Here!

Possibly we need a new term such as “usually isolated” or “somewhat isolated” or maybe “occasionally isolated” in order to more accurately describe the actual status of such systems?

Maybe the plant management team is unaware of the Stuxnet attack on the really well isolated Iranian fuel enrichment facility?

Maybe they are unaware that hackers can locate and attack remote access connections, both dial-in and cross-network? And they LOVE wireless!

Maybe they are unaware that insider sabotage is one of the leading (and growing) causes of unplanned plant outages and plant system failures – and we are not talking about radicalized followers of ISIS.

It Can't Happen Here!

Most malicious insiders are just Bob from the instrument shop who got a crappy review, was just informed that he has to pay more for his medical insurance next year and who got no cost of living raise the past three years....

And he feels like a little payback is in order

(My apologies to any actual 'Bob' who works in the instrument shop.)



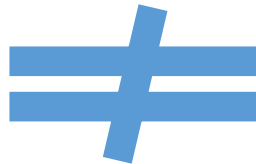
IT Isn't the Same as Industrial Automation

A modern plant automation system can look a LOT like a conventional IT business system - PCs running MS Windows, servers running MS Windows and maybe a SQL Server RDBMS, Ethernet switches and CAT5 cables, LAN-connected Printers and NAS storage devices. All pretty much the same as the IT folks use. So why not just let the IT folks “do their thing”?

Some corporations have even moved their automation and instrumentation groups under IT because of this fact...



But the truth is



Industrial Facilities Pose Special Challenges

Establishing and maintaining adequate cyber security in a plant environment is harder than many folks think due to a number of factors that are unique to industrial facilities, be they continuous or BATCH processes or even discrete manufacturing plants.

You have to contend with issues that are outside the experience and expertise of conventional IT departments, IT consultants and IT product vendors.

The Consequences of Mistakes are Different

When IT messes up productivity drops
and work slows down and you can't
get your email or print that report...



When you mess up productivity may
drop and thing may slow down, but on
the other hand if you REALLY mess up
things can get very exciting!

The Problem Seems so Big as to be Impossible



I know of plants where the I&C group identified several hundred (or more) digital automation assets but had no idea of how to go about classifying them based on the consequences of their cyber compromise and the need for cyber protections (or lack thereof)

Faced with what seemed to be a manpower intensive (and hugely expensive) task of protecting everything they had identified, some groups just choose a wait-and-see (and hope nothing bad happens) posture

All Digital Assets are NOT Created Equal

Not every digital asset/system in a facility needs the same level of cyber protection, and many don't need any cyber protections at all, the trick is in knowing which is which.

Unlike an IT operation where you have servers, PCs and network elements (all of which are 'computers') an industrial facility has a range of digital assets including smart instruments and control elements,

Large and complex DCS, PLC and SCADA systems MAY need a lot of protection, but digital protective relays, digital trend recorders, analyzers, smart instruments and other intelligent devices may only need limited or even no cyber protections at all.

Industrial Automation involves Strange Devices

Things you have to deal with

Basically just about everything IT deals with is a computer with a Windows or Linux OS, Ethernet-TCP/IP a CD/DVD a keyboard/mouse and USB ports

You have all sorts of “smart” devices full of microprocessors, but that’s where the similarity ends!

Things IT has to deal with

Why Cyber Security is Harder for Industrial Facilities



One-Size-Fits-All Doesn't Work for Industrial

A one-size-fits-all approach to cyber security (such as many IT organizations use) merely leads to unnecessary complexity and frustration in an industrial facility

In the IT world there are not that many types of digital assets and many IT organizations standardize on a handful of software and hardware platforms, so it is possible to devise a cyber security approach that standardizes the technical controls and countermeasures to be applied to all digital assets

An example of this is the government's FISMA cyber security standard for their IT systems which can be met by applying the NIST SP 800-53 standard and its huge list of cyber security "controls"

Also, most IT departments regularly update their assets every few years to keep them current with evolving computer and networking technologies.

One-Size-Fits-All Doesn't Work for Industrial

In an industrial facility adopting such an approach usually ends up creating a massive (and totally useless) paperwork nightmare where I&C personnel have to waste time documenting all the “exceptions” to the standard policy

Also a lot of digital IACS and I&C equipment in industrial facilities is quite old and not even close to being up-to-date with current computer and networking technologies and so often incompatible with standard IT cyber security technologies

It is common to require a 20-year operating life and product support when procuring large automation systems, and I know of DCS and SCADA systems still running that are nearing double that time-span (even though the original vendors have faded into history)

Limited-Functionality Automation Devices

There are a wide range of “smart” devices used for industrial automation. They range from actual general purpose computers (like a server or PC running Windows or Linux) down to simple devices with no peripherals or interfaces running proprietary, special-purpose EEPROM-based programming. The susceptibility of such devices to cyber attack, and thus their need for cyber security controls, will vary greatly based on their technical design and features.



You Call That a Computer?

Many digital assets in an industrial facility are not “computers” (even though they contain microprocessors and executable program code)






Most (if not all) conventional cyber countermeasures and technical ‘controls’ can’t be applied to many of these devices

Fortunately many of these digital assets do not need to be protected against cyberattack

Many low-functionality digital assets are actually nearly immune to cyber compromise but, not knowing this, efforts are often made to protect them anyway

Protection should be Based on Vulnerability

DECREASING VULNERABILITY TO CYBERATTACK

	Cyber Asset	Alterability	Cyber Compromisable
	Programmable Scientific calculator	<ul style="list-style-type: none"> Programming field alterable Configuration field alterable Data field alterable Local user interaction Remote user interaction 	Not possible to be cyber attacked because of 'hard-coded' programming and lack of a 'cyber' means for accessing or changing the stored programming. (Physical alteration is required.)
	Smart Transmitter with HART protocol communications	<ul style="list-style-type: none"> Programming field alterable Configuration field alterable Data field alterable Local user interaction Remote user interaction 	Not likely to be cyber attacked because of 'hard-coded' programming. Parameters and configuration can be field-altered, including via the HART interface, but the actual program running in the device can't be accessed or altered. No Ethernet, TCP/IP
	Quarter DIN single loop PID temperature controller with 'FFieldbus' Interface	<ul style="list-style-type: none"> Programming field alterable Configuration field alterable Data field alterable Local user interaction Remote user interaction 	Not likely to be cyber attacked because of 'hard-coded' programming. Parameters and configuration can be field-altered via front panel and Fieldbus interface, but the actual program running in the device can't be accessed or altered. No Ethernet, TCP/IP
	PLC with Ethernet communications module and Modbus/IP communications	<ul style="list-style-type: none"> Programming field alterable Configuration field alterable Data field alterable Local user interaction Remote user interaction 	Can be cyber attacked because of Ethernet, TCP/IP networking. Can use Modbus protocol to alter PLC logic (but not programming of the processor board). Com/Ethernet interface module vulnerable to program alteration.
	Windows XP Pro PC running HMI package, TCP/IP Ethernet networking and OPC process data connectivity	<ul style="list-style-type: none"> Programming field alterable Configuration field alterable Data field alterable Local user interaction Remote user interaction 	Can definitely be cyber attacked due to Windows OS, Ethernet, TCP/IP networking and use of OPC which uses RPC functions known to be vulnerable to attack.

Why Cyber Security is Harder for Industrial Facilities

You Call That a Computer?

Part of the problem here are the vendors/manufacturers. They publish spec sheets and manuals that give a lot of information about their products, but almost never provide information about the cyber vulnerabilities (or cyber security) of their products – possibly because they don't know?

I sat on the phone with a vendor's engineer one day asking question after question in order to finally determine that indeed, their device would not be vulnerable to an infected USB "thumb drive" being inserted due to limits in their USB port support software.

It would have been nice to find that data published in one of their manuals.

You Call That a Computer?

It should be noted that the ISA initiated a program called ISAsecure to provide a means for vendors and manufacturers to submit their products to a 3rd-party testing and assessment organization (exida in the US) in order to have a cyber security rating determined for those products

Vendor
their USB port support software.

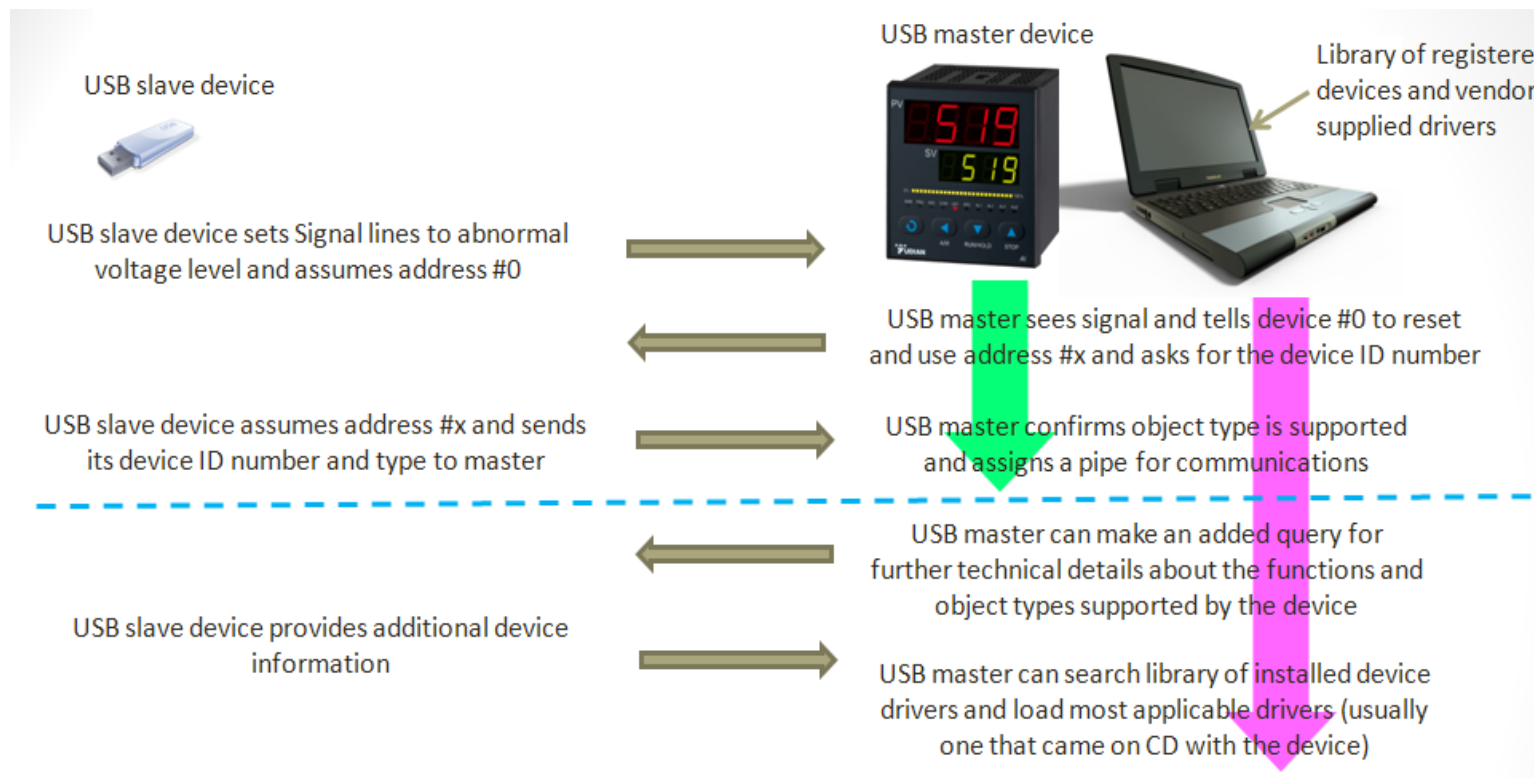
Manufacturers. They publish specifications about their products, but their vulnerabilities (or cyber security) don't know?

Today asking question after question, their device would not be working inserted due to limits in

It would have been nice to find that data published in one of their manuals.

Watch Out! It Has a USB Port!

Unlike a PC, a limited-functionality smart device has no 'library' of vendor-provided or generic drivers and won't **enumerate** the 'slave' USB device. It will have been factory-programmed to support just a specified subset of associated USB functions: e.g. read/write CDA memory buffer to/from USB bulk storage device



Is it REALLY Vulnerable to Cyberattack?

Vendor documentation rarely tells you if their “smart” device uses ROM, EEPROM or flash memory to hold their program code; yet knowing this can tell you if a device is essentially immune to any form of cyberattack (and therefore probably requires no protections).

IT folks generally don’t think about such issues since everything they deal with tends to be a computer with a bootstrap BIOS program, lots of RAM, possibly a file system and hard drive, Ethernet ports and a COTS operating system – and that pretty much guarantees that the device is vulnerable to some form of cyberattack, and will need to be protected.

Is it REALLY Vulnerable to Cyberattack?

The following is a non-prioritized list of some attributes which, in combination, may justify taking minimal, if any, steps to protect a digital asset from cyber attack:

- The lack of field-alterable software (alterable by cyber means)
- Only bulk replacement of total firmware load via USB/Memory stick
- Contains no information of value to an adversary
- Restricted-capability USB support
- Read-Only remote data access
- The lack of a file system
- The lack of an O.S. (especially a COTS one) with application call-able services
- Integral multi-level/multi-user password protection
- No Ethernet or restricted-capability Ethernet-TCP/IP support
- No wireless communications
- Does not control/operate critical equipment

Plant Operations aren't like IT Operations

Many of the automation systems in operating facilities are required to run continuously 24/7 until such time as the plant reaches a scheduled shutdown or outage – which might not be for several years.

Many security approaches, such as installing patches and updating (or eliminating) applications and installing specialized countermeasures such as a host-based intrusion detection system require at least rebooting of the systems to which they are applied, if not actually temporarily requiring removing those systems from operation

This is usually not a big deal in the IT world but, due to potential adverse safety and production impacts such actions may not be possible/allowed in an operating plant environment until the next (scheduled) outage

Plant Operations aren't like IT Operations


But during an outage the plant personnel are usually busy supporting the plant/process/automation changes in order to get the facility back up and into operation again and have little time left to support cyber security activities

Some of the more complex automation systems may be fully redundant, and so it would seem obvious that you could do your cyber security work on the standby portions of the system and then switch over and work on the primary portions

Sounds good on paper, but in reality only a plant with a low-risk, stable process, would likely consider doing this. Making redundancy just work as advertised has always been a challenge to automation system vendors and few plants would want to mess with a properly functioning automation system.

Getting “Long In the Tooth” but still Kicking

A lot of plant automation systems are categorized as being ‘legacy’ and have little if any vendor support (and spare parts have to be found on EBAY) and thus are considered as “no touch” - following the ancient wisdom which recommends that: “if it ain’t broke, don’t fix it!”

Such orphan systems may be running on hardware and operating system platforms that are semi-modern and might even use Ethernet networking - but no one at the plant has in-depth technical knowledge of the system and IT would probably laugh (or put a lot of “lol”s and  emoticons in their email response) if asked to support the system

IT might even ask why that old system hasn’t just been replaced with something modern? I feel sure that most plant managers could probably explain the reason that has not happened better than I ever could.

Some IT Best-Practices are Dangerous

IT strategies for convenience may actually degrade plant cyber security. Corporate IT people don't generally like to go to industrial facilities. They (plants, not IT folks) are dirty and smelly and loud and things occasionally go boom

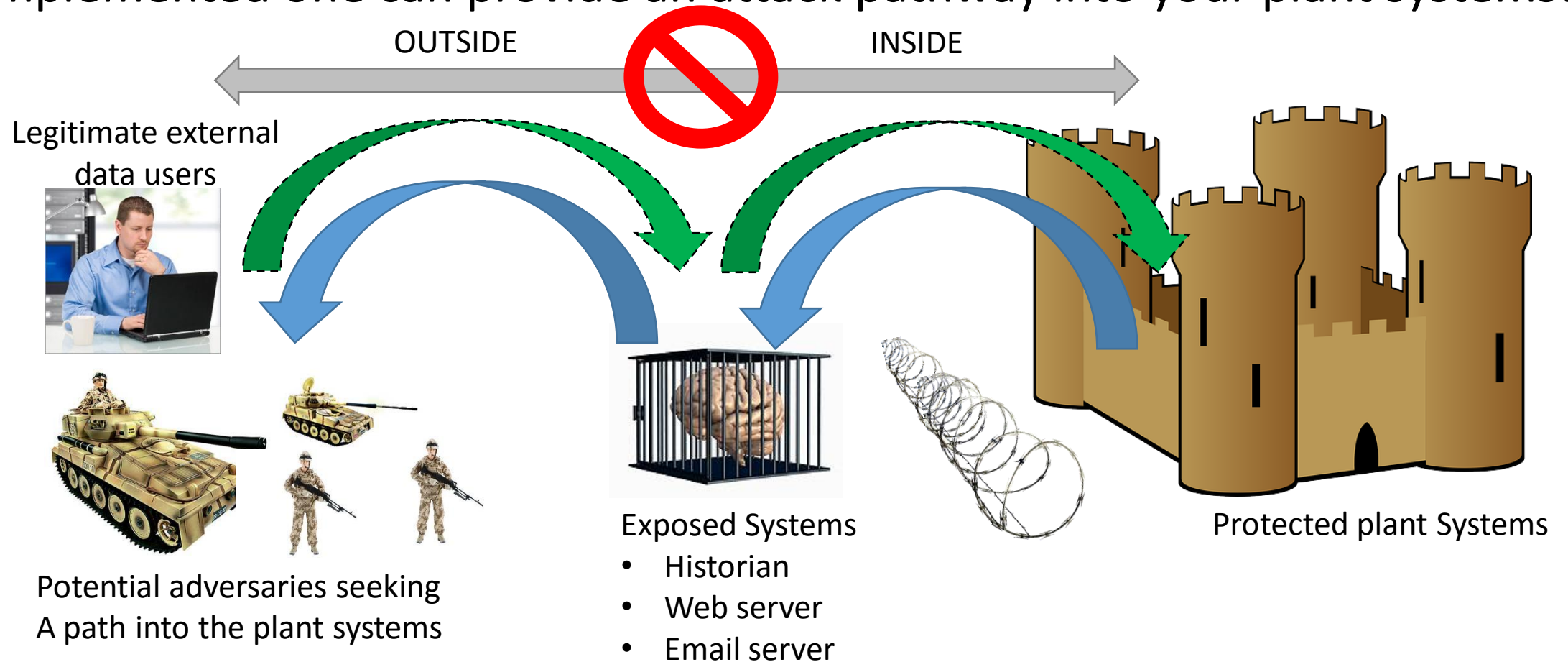
So a typical IT approach is to provide site support and administration of networks and cyber security countermeasures via remote access

Establishing a network/cyber DMZ (a term borrowed from the Korean War) is one way of providing remote access to systems and even recommended in the ISA SP-99 standard

In a DMZ strategy you place a minimum number of systems into a special, restricted LAN segment that is 'visible' from both the "inside" (other plant systems and users) and "outside" (corporate IT and hackers)

Some IT Best-Practices are Dangerous

Properly implemented DNZs can provide an effective cyber barrier. But a badly implemented one can provide an attack pathway into your plant systems!



Some IT Best-Practices are Dangerous

You plan on the fact that systems in the DMZ are visible to bad guys and will be attacked and you strip them down to the basics (something called “hardening”) and put cyberattack monitoring measures inside the DMZ with those systems

The DMZ provides an early warning system of sorts and delays an attacker thus giving the plant the chance to respond by taking actions ranging from totally shutting off the external connection or at least making changes to the plant’s external firewall

But I have been at plants where everything except the drinking fountain and their old DCS was placed into their DMZ, just so corporate IT could support them remotely.

Most of these systems in the DMZ were not even given any special protections against cyberattack as if just being in the DMZ was protection enough. The approach used seemed to be focused on making life convenient for the IT folks.

Some IT Best-Practices are Dangerous

The plant was wide open for a cyberattack because of this, but they actually thought they were being made cyber secure by corporate IT

Their only true cyber protection came from the fact that the plant DCS was somewhat old and obsolete and did not support TCP/IP networking

I understand why many corporations have had to resort to remote support, keeping IT folks at each plant is expensive and sending people to site takes time

But there are ways to make remote access secure; putting everything you have into a DMZ is not one of them.

Some IT Best-Practices are Dangerous

IT folks like to centrally manage things in other ways as well. With IT systems it is common to use a centralized user authentication server (like MS Active Directory) to control user logins. If poorly configured/implemented the inability to reach that server can block legitimate users from logging onto their systems.

I witnessed a SCADA system event where system operators lost access to system configuration functions (fortunately not control functions) due to a corporate WAN outage; after IT had modified their system to use the corporate AD server for engineering and administrative login authentication

What They Teach you in IT School

In the IT world that often use the acronym CIA (no, not THAT CIA) to help them remember their major objectives:

- CONFIDENTIALITY – Keep the information on the systems from being leaked
- INTEGRITY – Make sure the information on the systems is not altered/lost
- AVAILABILITY – Try to keep the systems running and available to users

Many of the cyber security actions they take are aimed at achieving those three objectives; with information confidentiality being their most important consideration

Most plants would consider the priority order to be backwards – availability is top followed by integrity and for some few applications, confidentiality

Keep this in mind when IT makes suggestions about implementing what is needed to achieve adequate cyber security

Where Have all the Spare Parts Gone....

Many of the digital assets and systems have no test/support environment on which changes can be tested

As has already been mentioned a lot of digital assets in an industrial facility are legacy systems years out of date with current technologies

The plant may have originally purchased enough spare parts to build a test and support environment for such a system, but by now, because the vendor either doesn't exist or no longer supports the system, that support environment has been cannibalized for spare parts or for parts to expand the original system

Where Have all the Spare Parts Gone....

This means that the only way to test a change, a patch, a new application is on the 'live' production system

Most plants would really, really resist the suggestion to put untested changes onto a running production system, especially if it seems to be working just fine (and a LOT of patches are not even important!)

This is less of a safety issue in a discrete manufacturing environment or even a BATCH production environment; but it is still not a practice I would personally recommend.

Industrial Protocols and Communications

IACS often use industrial protocols and vendor-proprietary protocols that are unknown to IT people and conventional IT security products

Most of the early local area industrial protocols devised prior to the widespread acceptance of Ethernet (and TCP/IP) have been ported as “ISO-Layer 7” protocols that can be transported using Ethernet-TCP/IP networking.

Most (all?) DCS systems have been converted to use Ethernet, and possibly TCP/IP, in place of their older, vendor-proprietary networking technologies.

But the protocols and message types used by IACS and I&C devices are not always supported by commonly-used IT protective and detective mechanisms such as firewalls and NIDS (network intrusion detection/protection systems)

Industrial Protocols and Communications

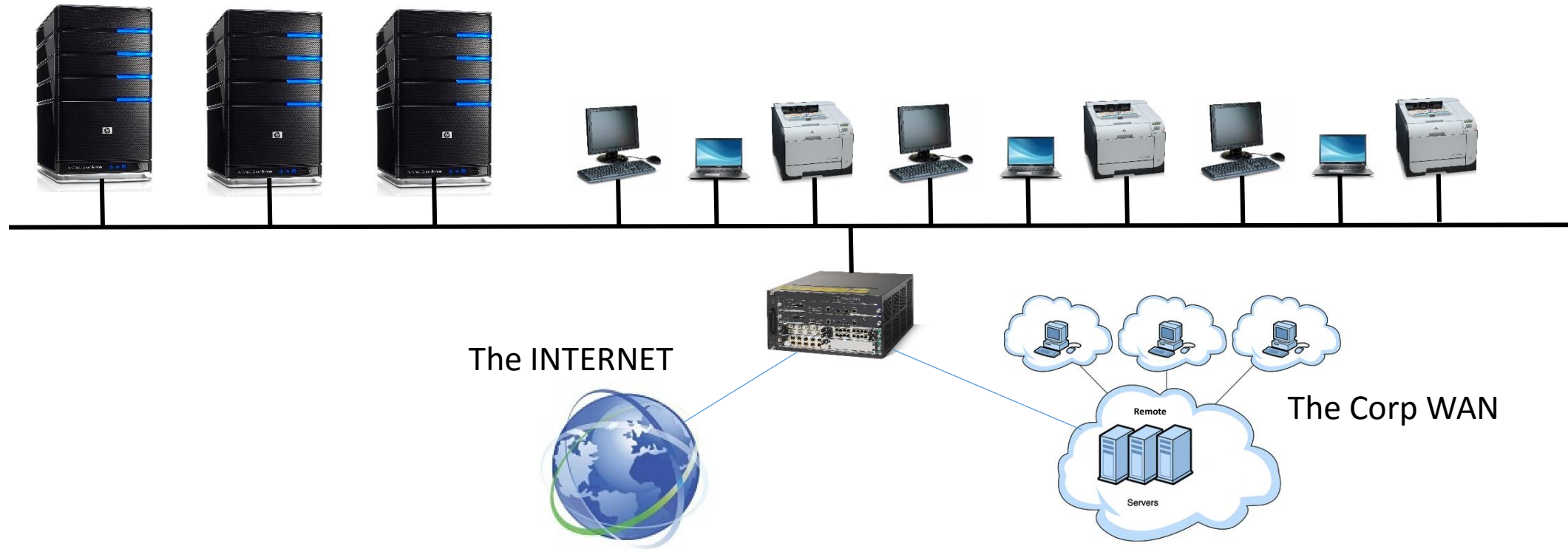
It's not that such mechanisms don't "see" such message traffic, after all it is carried in Ethernet frames and probably IP datagrams.

The problem is that those tools either can't interpret, or have a limited capability to interpret, and decode such message traffic and thus determine which of those messages are allowed and which might be malicious or unauthorized.

IT personnel usually know nothing about those "industrial protocols", and it might not be their fault; if it's a vendor's proprietary system messages they might not actually be documented anywhere.

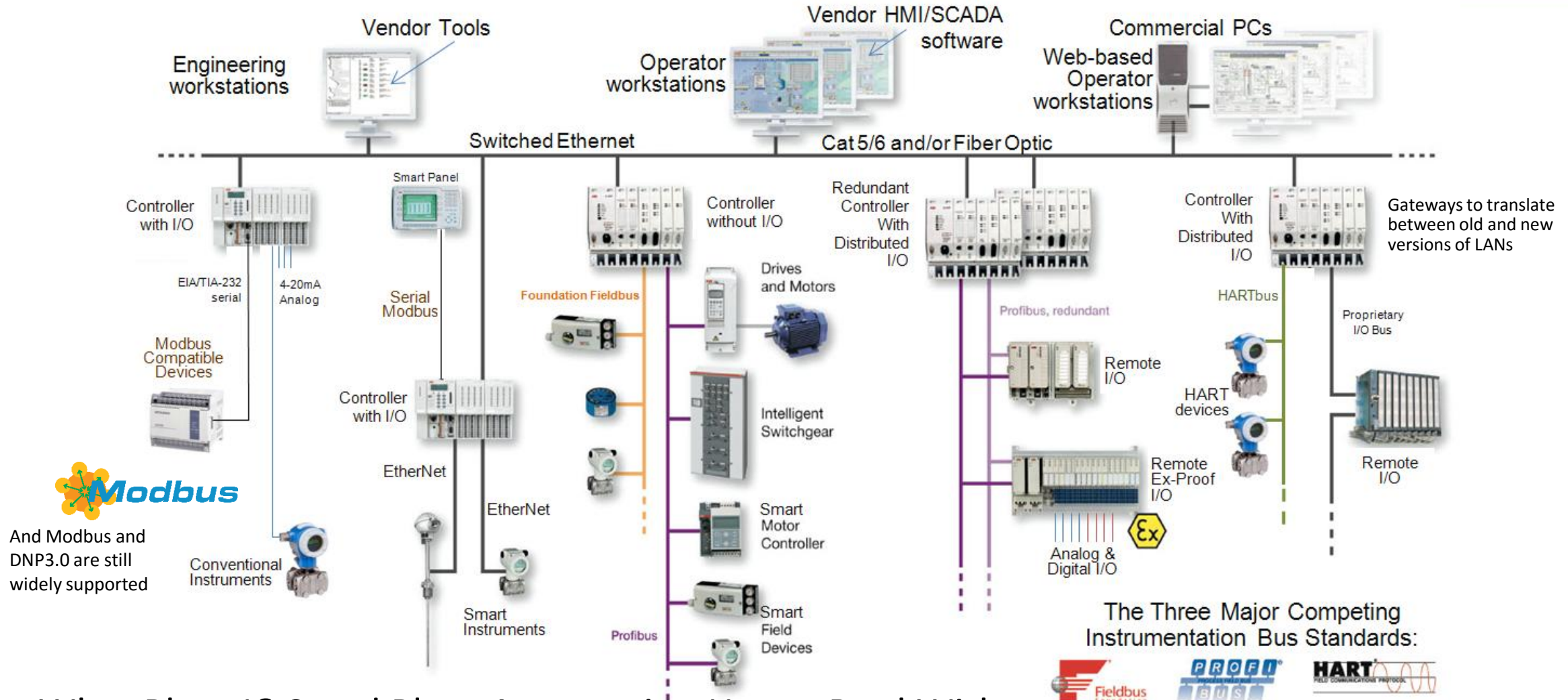
Industrial Networks are Very Different

What IT Deals With - A Typical Corporate IT Business Network



Why Cyber Security is Harder for Industrial Facilities

Industrial Networks are Very Different



And Modbus and DNP3.0 are still widely supported

What Plant I&C and Plant Automation Has to Deal With

Why Cyber Security is Harder for Industrial Facilities

IACS Predates Modern IT Technology

Older plant networks may still incorporate legacy communications and LAN technologies that pre-date Ethernet and TCP/IP.

First and even second generation DCS systems mostly used vendor-designed LAN hardware and software.

Early PLC based systems used vendor-designed LAN hardware and software. A lot of that stuff is still out there running in plants.

Also communications interconnectivity between digital systems and devices originally was established using low-speed, minimal-functionality, point-to-point (or multipoint) “serial” communication and “SCADA” protocols

IACS Predates Modern IT Technology

All SCADA system vendors in the 1970s and even 1980s devised their own communication protocols. An amazing amount of legacy RTU equipment still utilize those old protocols.

Some of those protocols, such as DNP3.0 (and Modbus-RTU) became standards and adopted by many product manufacturers

There are few if any products available to monitor or secure such communications (e.g. encrypting modems)

On the other hand it may be overkill to attempt to do so based on the consequences or difficulty involved in compromising such communications

“Serial” Industrial Communications

Many “smart” devices communicate using legacy “serial” protocols which have no intrinsic cyber security mechanisms and operate across RS-232/422/485 circuits or even analog phone lines or voice-grade radio connections. The need for cyber protections here depend on the difficulty of gaining access to the communication channel and the functionality of the device and protocol:



Increasing need for security

Read values and status from device

Read values and status and send parameters to device

All the above and download configuration/program changes to the device

All the above and send commands for remote control of device outputs (what process/plant equipment do they operate/control?)

The Russians are hacking! The Russians are hacking!

Some industrial facilities are highly unlikely to be the focus of a targeted cyberattack but still move forward on implementing excessive cyber security protections out of fear and ignorance.

The government, in the form of the department of homeland security, has tried to identify industry segments that are important to the nation and economy and thus are much more likely to be a target for cyber terrorists.

Facilities that make glass, dog food and shoes (ok, we don't have shoe plants ... so maybe toothpaste) are not going to be grabbing headlines if they are shut down, and probably no one would be killed in the process and the economy would be largely unaffected.

The Russians are hacking! ... No, Really!

This does not mean that an *ad hoc* cyberattack could not occur. Someone can always unknowingly bring an infected laptop into work and connected it to a plant network. (This actually happens surprisingly often!)



But protecting against that kind of attack does not require the levels of protection and detection as would say, a nuclear power plant or a large refinery, where an adversary would likely target them and be willing to expend significant resources in an effort to create a headline-catching catastrophe.

One of the challenges with industrial facilities is picking the appropriate level of cyber security based on cyberattack risk and likelihood

The Chinese & Koreans are hacking too!

Most IT organizations assume that ALL of their assets are important (after all the business couldn't keep running without them) and therefore they ALL need to be given equal/maximum protection

On the other hand individual industrial plants, and specific areas/units/trains within those plants, need to be assessed to determine how much (if any) protection is adequate and how much risk is tolerable

Cyber security has to be cost-justified in order to get funded. Usually that is done by showing risk (exposure) reduction and/or consequence mitigation based on cyber efforts undertaken (think insurance policy!)

The Chinese & Koreans are hacking too!

And unlike the IT world, when we do a consequence assessment, we often can include backup ESD, SIS and hard-wired safety shutdown logic designs that provide worst-case safe shutdown of critical processes in that assessment process (which often greatly reduces actual consequences)

Assets are important (after all) and therefore they ALL

specific

essed to determine

with risk is tolerable

Cyber security has to be cost-justified in order to get funded. Usually that is done by showing risk (exposure) reduction and/or consequence mitigation based on cyber efforts undertaken (think insurance policy!)

In Conclusion....

All industrial facilities need to implement adequate cyber security, but what that means can vary widely from plant to plant

The cyber threats are real and potentially dangerous so inaction is risky

Don't try to protect everything containing a microprocessor/computer; many smart devices don't need much/any protecting

Be realistic about protecting "industrial" communication channels

IT can be helpful; but remember that their objectives and best practices don't always align with the realities of operating a plant