Setting the Standard for Automation™

Hot Topics in Control System Security

Will-DuPage Section
January 2014 Technical Meeting

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Presenter

Andrew Ginter is the VP Industrial Security for Waterfall Security Solutions. Andrew spent two decades developing control system software products and most of a decade developing control system software products. Today, Andrew speaks and writes frequently on the topic of industrial control system security, and represents Waterfall to regulatory authorities and standards groups. Andrew is the co-chair of ISA SP-99 Working Group 1, updating the 2007 Technical Report on Industrial Control System Security Technologies

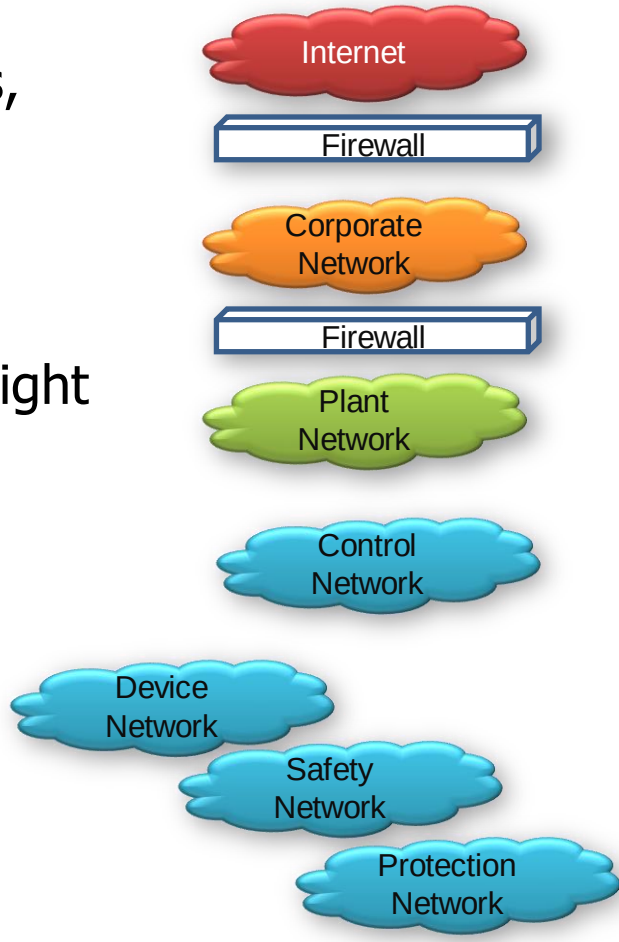
SCADA / Industrial Control System Security

Industrial Control System / SCADA System / DCS

Small Refinery

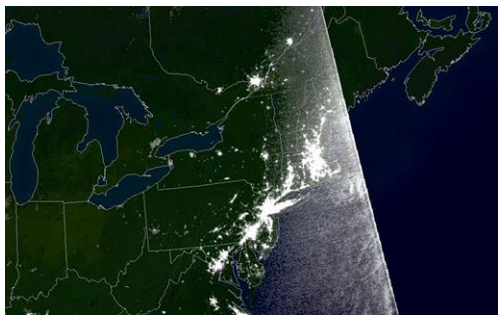
Control System Security = Safety + Reliability

- Security = Safety at many plants
- Safety Instrumented Systems = protect workers, public and environment
- Protection Systems = protect equipment
- Control Systems = operate the equipment
- HMI / Human-Machine Interface – human oversight
- Plant Historian – batch records



Why Are We Worried?

Operation "aurora" demonstration



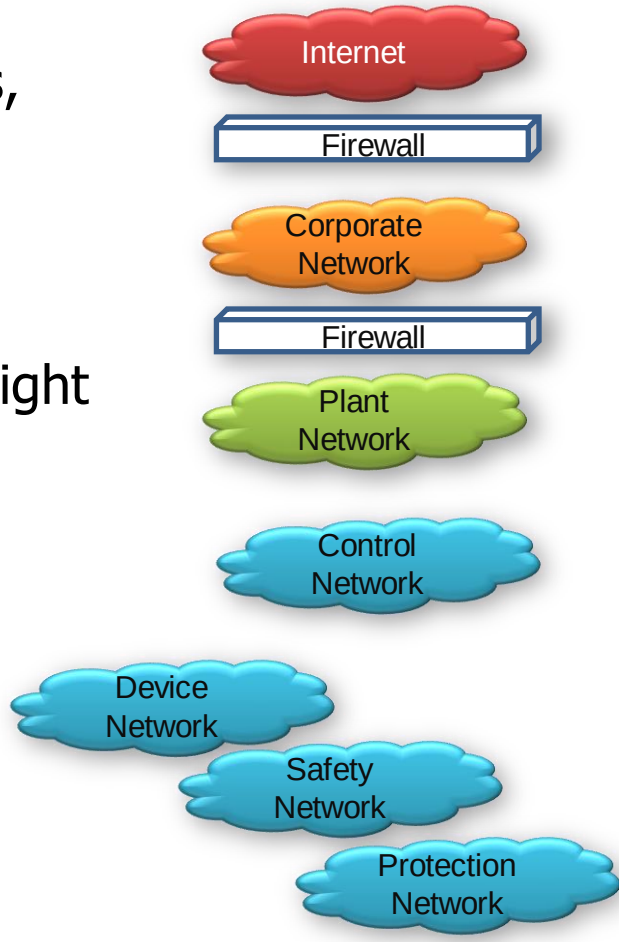
National Oceanic and Atmospheric Administration / Defense Meteorological Satellite Program image

Control System Security = Safety + Reliability

- Security = Safety at many plants
- Safety Instrumented Systems = protect workers, public and environment
- Protection Systems = protect equipment
- Control Systems = operate the equipment
- HMI / Human-Machine Interface – human oversight
- Plant Historian – batch records

Risk: mis-operation of HMI can cause disaster. Cyber-sabotage can cause mis-operation of HMI and worse

Risk: mis-operation or malfunction can cause "safety shutdown."



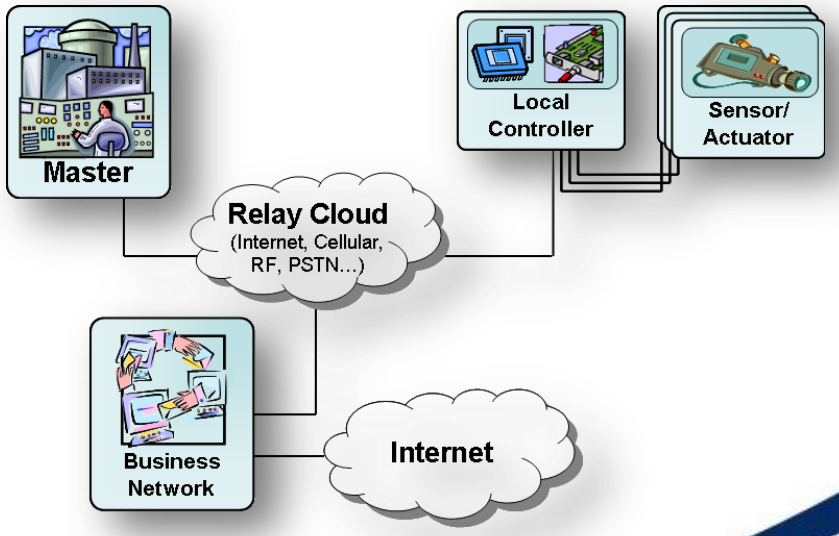
Security Basics

- You are never perfectly safe. You are never perfectly secure.
- Corollary: for every defense there is an offense
- Security problems fundamentally stem from errors
- Security problems stem from misplaced/breaches of trust
- The only secure computer is one that is disconnected and powered off in a closet with an armed guard in front of the door
  - Even then not perfectly secure
  - And not very useful either
- All software can be compromised

The Internet makes it easy: attackers in their living rooms on the other side of the planet

Industrial Network Connectivity: Drivers and Risks

- Predictive maintenance: crew scheduling, HR integration, spare parts inventories and ordering
- Just-in-time manufacturing, real-time inventories, batch records, LIMS integration, production planning, SAP/ERP integration
- Centralized support: more effective use of skilled personnel, critical mass of current experts next decade's experts
- ***But*** industrial network connects to business network, which connects to Internet & other networks



These connections let attackers target critical network with remote, online attacks

The "Internet of Things" – Is It Safe?

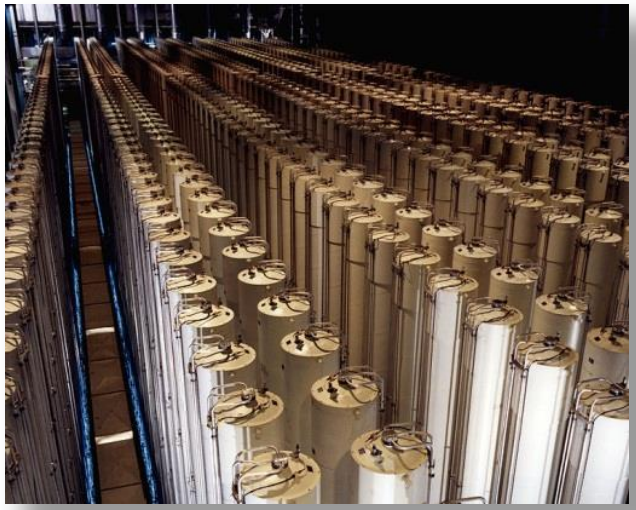
- Zigbee focus: encryption, authentication, privacy
- PC's legitimately participate in Zigbee network, even if compromised
- Safety / security axioms:
  - *Every CPU which can be compromised, will be compromised*
  - *Any unsafe command which a compromised CPU can issue, will be issued*

What happens when a virus on thousands of PC's turns on all the burners on thousands of stoves at 2 AM?

SCADA security focus: safety, reliability, hardware-protected

Stuxnet

- Artifact: autonomous, targeted, sabotage-oriented worm
- Adversary: Nation-state military / intelligence agency
- Propagates via USB and across LAN connections –compromised insider?
- Evaded firewalls, AV, security updates, host hardening
- 100,000 - 300,000 infected machines
- Compromised safety systems



You can protect against the artifact, but not the adversary

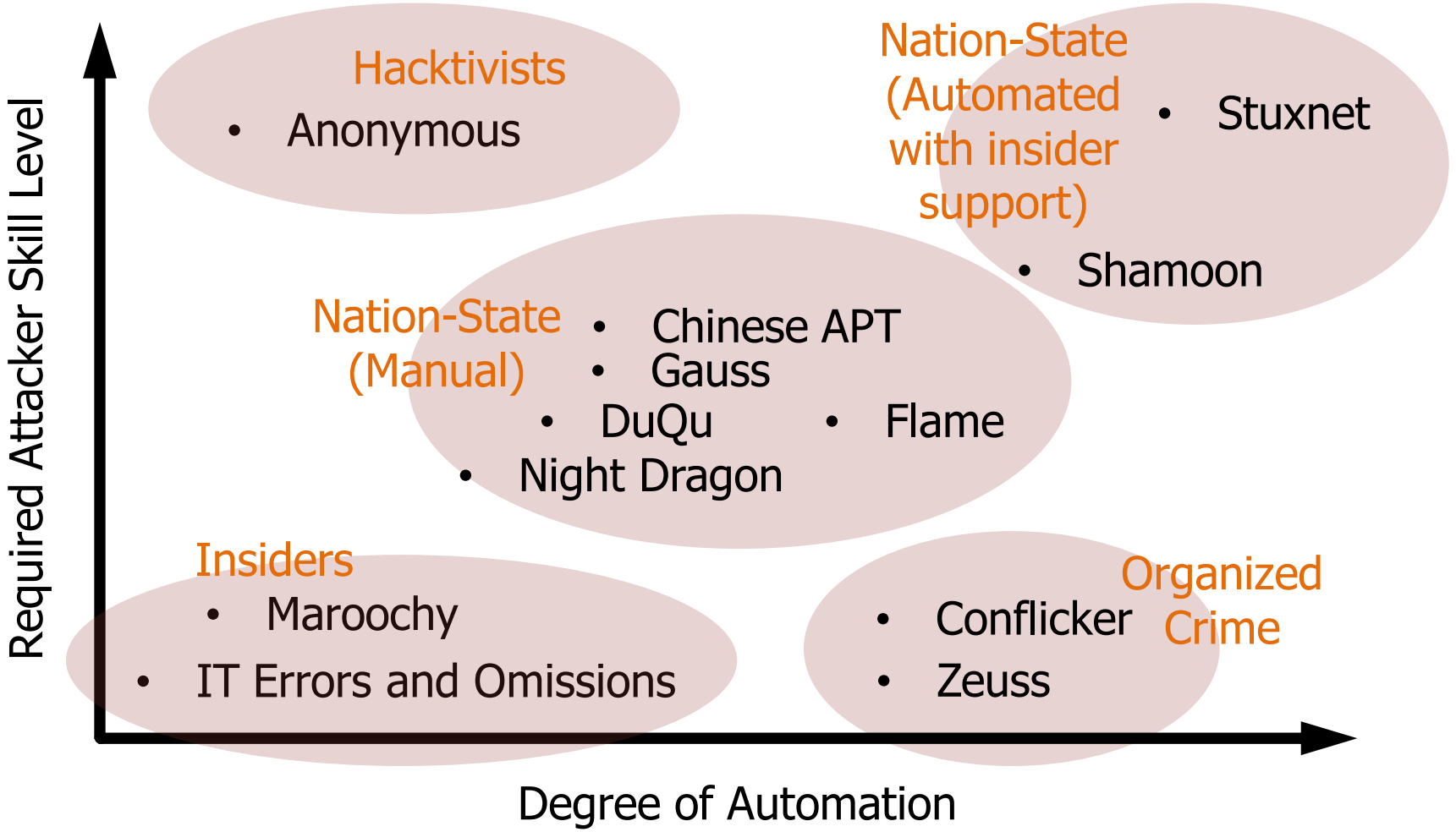
"Most Sophisticated Worm Ever"

- Targets Siemens S7 WinCC products, compromises S7 PLC's to sabotage physical process
- Exploited 4 Windows zero-day vulnerabilities
- Spreads via:
  - USB/removable media
  - 3 network techniques
  - S7 project files
  - S7 database connections
- Signed with legitimate (stolen) RealTek and JMicron certificates
- Installs clean on W2K through Win 7
- Conventional OS rootkit
- Detects and avoids major anti-virus products

Threat Spectrum

Threat	Resources	Methods	Existing Protection	Examples
Nation-state, sleeper insiders	High	Highly targeted, autonomous	Counter-espionage	Stuxnet, Shamoon(?)
Advanced threat	High	Targeted, manual remote control	NEI, CIP V5	Aurora, Ghostnet
Targeted threat	Medium	Targeted, manual remote control	NEI, CIP V5	Night Dragon, Shady RAT
Disgruntled insider with access to ICS	Low	Targeted: social engineering	NEI, ISA, NERC-CIP	Maroochy
Insider with access to IT network	Low	Targeted: social engineering	NIST	IT examples
Organized crime	Medium	Highly volume, automated	NEI, ISA, NERC-CIP	Zeus, Conflicker

Threat Spectrum: Skill vs Automation



Targeted Attacks

- Flame, DuQu, Night Dragon, Mandiant APT. Shamoon?
- Trick users into providing passwords, installing malware
- Custom malware, tested to evade anti-virus
- Remote control: steal credentials, propagate, escalate, create own passwords / accounts
- Security updates, firewalls: no need for vulnerabilities if you have passwords

Conventional ICS security guidance does not address targeted attacks

Safety, Reliability, Confidentiality

Attribute	Enterprise / IT	Control System
Scale	Huge – 100,000's of devices	100-500 devices per DCS
Priority	Confidentiality	Safety and reliability
Objective	Data Theft	Sabotage
Exposure	Constant exposure to Internet content	Exposed to business network, not Internet
Equipment lifecycle	3-5 years	10-20 years
Security discipline:	**Speed / aggressive change – stay ahead of the threats**	**Security is an aspect of safety - Engineering Change Control (ECC)**

Most IT controls are not appropriate. You manage IT and ICS networks differently

"Nobody" Really Uses Anti-Virus

- Every signature update is a threat of "false positive" failure – mistakenly diagnosing legitimate control system components as malware and quarantining them
- Constant testing for safety of new signatures is costly
- ICS vendors estimate 90% of customers never update ICS signatures
- Corporate AV servers are attack channels into every ICS host
- NERC-CIP & other standards mandate AV & signature updates but not frequency. Sites use very long frequency

Bottom line: at best AV signatures in ICS networks lag IT networks by several days. More often, AV is not effective in ICS

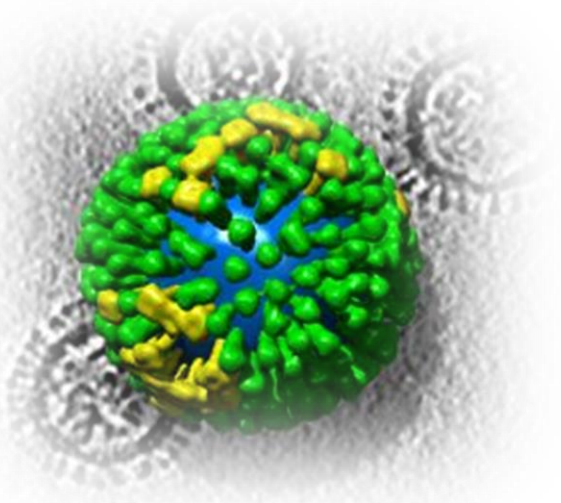


Photo: National Institutes of Health

"Nobody" Really Does Security Updates

- Every update is new code. Sometimes a ***lot*** of new code. Is it safe?
- Constant testing for safety of new code is extremely costly
- Corporate WSUS servers arhe attack channels into every ICS host
- Security update programs may be rolled out to plant-wide network
- Occasional spectacular failures effectively stall these programs at the DCS/SCADA perimeter
- NERC-CIP & other standards mandate security update programs but not frequency. Sites use very long frequency.

Bottom line: the closer you get to safety systems, the less effective security update programs become

Photo: Nivet Dilmen

Plain Text Device Communications

- The vast majority of PLC & RTU communications are not encrypted
- Owners and operators hold a deep suspicion of encryption: risk of impairing emergency diagnostics & response
- Encryption is worthless without key distribution / management
- Connections to Internet PKI infrastructure are dangerous. No standard ***safe*** key management has been proven, even in research settings

Bottom line: the closer you get to safety systems, the less likely it is that encryption will be used

100,000 Vulnerabilities

- Back of the envelope calculation: more than 100,000 buffer-overflow vulnerabilities alone are waiting to be discovered in ICS products

  50,000 * 2% * 10 * 3 * 5 * 0.75 = 112,500

- ICS security researchers confirm that they find 5-10 critical zero-days in the first few hours of examining every new ICS product
- ICS vendors are working on the problem, but it will be a long time before it is solved

Bottom line: ICS products are likely to be extremely vulnerable for the forseeable future

Old Equipment

- Hardware vendors go out of business, drop product lines, but costly physical equipment has not yet reached end of useful
- "Smart homes" making the quandry clear: will you throw out your refrigerator when its firmware is obsoleted?

Bottom line: every site has at least some equipment so old no AV vendor supports it, and no security updates are available for it.

Wireless Communications

- Wireless communications are already used for safety-critical functions: emergencies on land and at sea
- WEP is broken. WPA is stronger, but rainbow / dictionary attacks work surprisingly well
- Rogue access points:
  - Well-meaning insiders: awareness
  - Malicious – scanning
  - Nasty: cellular access
- All wireless communications should be modeled as WAN communications and encrypted

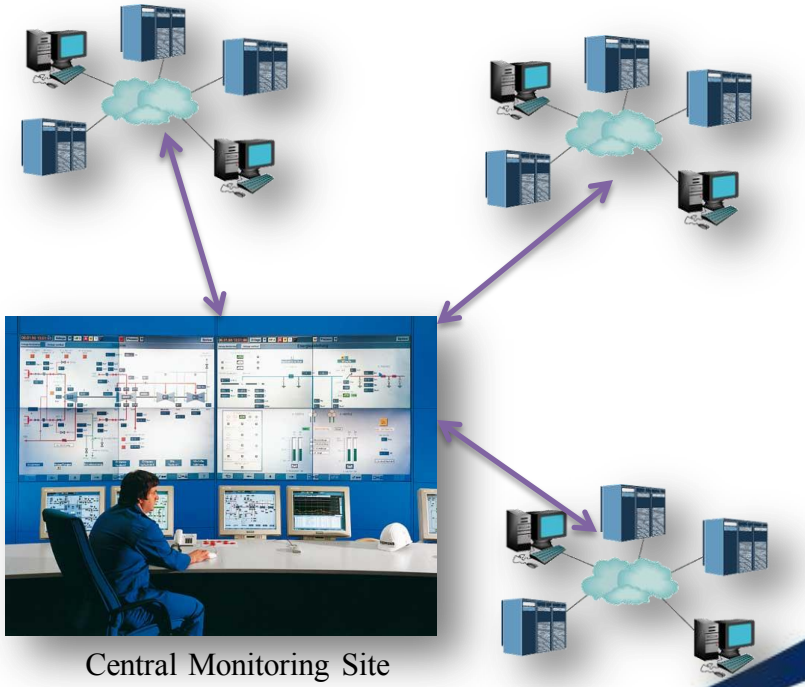
Least-appreciated wireless threat: directional antenna + noise generator = denial-of-service

Control Systems in the Cloud

- Control system / equipment / turbine vendor site "monitors" many customer sites, in many countries
- Central vendor site configured for "occasional" remote control
- Industrial network exposed to attack from central site and from other customers / countries
- Remote control attacks, virus propagation

Vendor connection bypasses corporate security protections

Industrial network is completely dependent on vendor security



13 Ways Through a Firewall

Attack Type	2FACT	ENC	RULES	HOST	NET	SUPD	UGW
1) Phishing / trojan / drive-by-download – victim pulls attack through firewall	0	0	2	1	1	1	2
2) Social engineering – steal a passwd/ keystroke logger / shoulder surf	2	0	0	0	0	0	2
3) Compromise domain controller – create control system or firewall account	1	0	2	0	0	0	2
4) Attack exposed servers – SQL injection/DOS/buf-overfl/default passwords	0	1	1	1	1	1	2
5) Attack exposed clients – compromised web svrs/ file svrs/ data svrs	0	0	2	1	1	1	2
6) Session hijacking – MIM / steal HTTP cookies / command injection	0	2	1	0	1	0	2
7) Piggy-back on VPN – split tunneling / malware propagation	1	1	2	1	1	1	2
8) Firewall vulnerabilities – bugs / zero-days / default password / design vulns	0	0	0	0	1	1	2
9) Errors and omissions – bad firewall configs / IT reaches through firewall	1	1	1	1	1	1	2
10) Forge an IP address – firewall rules are IP-based	1	1	0	1	1	1	2
11) Bypass network perimeter – rogue cables/wireless/cell phone / dial-up	1	1	0	1	1	1	0
12) Physical access to firewall – administrator ports / no pw / modify hw	0	0	0	0	0	0	0
13) Sneakernet – removable media / untrusted laptops	0	0	0	1	0	1	0
Total Score:	7	7	11	8	9	9	20

Photo: Red Tiger Security

Grade	Description
2	Blocks essentially all attacks in this class
1	Blocks some attacks in this class
0	Not effective at blocking this class of attacks

Firewalls are never deployed without compensating measures

Abbr.	Compensating Measure
2FACT	2-factor authentication
ENC	Encryption, cryptographic authentication
RULES	Better firewall rules
Host	Host intrusion detection / prevention systems & SIEMs
Network	Network intrusion detection / prevention systems & SIEMs
SECUPD	Security updates / patch programs
UGW	Unidirectional security gateways

Supply Chain Integrity

- Counterfeit equipment – not certified for safety-critical use at all
- USB components – embedded CPUs
  - Eg: Netragard pen test – gift mouse with CPU, flash, malware and keyboard emulator inside
- NSA accused of intercepting computer equipment shipments destined for unfriendly countries
- Truly paranoid are buying computer components "at random" – random computer stares, in person
- Flame malware successfully impersonated Microsoft security updates

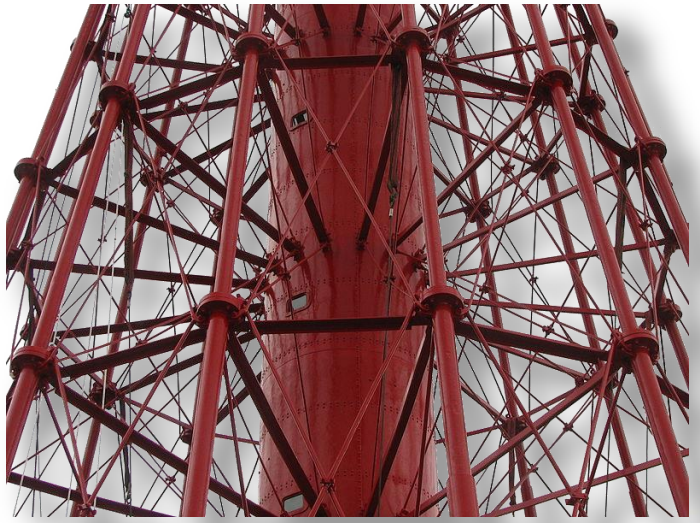
Photo: Netragard
www.netragard.com

ICS Security (NA): State of the Practice

- Nuclear generation: truly paranoid
- Truly paranoid: sharply limited network connectivity, deeply suspicious of removable media, parallel IT/ICS infrastructures
- Misguided: IT & ICS infrastructures merged, ICS infrastructure security managed as if it were IT infrastructure
- In denial: minimal protections, lawyers in charge of security programs, exposed
- Oblivious: "we are still air gapped"
- Entrenched: mature, old-school security program
- Emerging: security budgets increasing, looking to leapfrog old-school costs & approaches

Redundancy, Diversity, Complexity, Safety Systems

- Grid is massively redundant – top 100 generators produce less than 25% of North America's power
- Every ICS configured differently, connected to different devices, each device with different wiring to physical process
- Typical control system has tens of thousands of input and control points
- Safety & protection systems automatically shut down in unsafe conditions
- Information sharing will save us



Control rooms are too complex and too diverse to target credibly with autonomous malware. Serial attacks fall to information sharing

Compliance vs Security

- NERC Critical Infrastructure Protection (CIP) standards versions 1-4 are the "poster child" for compliance vs security
  - CIP is very prescriptive
  - Max fine: $1M /day of non-compliance
  - Lawyers put in charge of utility security programs
- Legislative initiatives to enforce greater security meet with stiff resistance from industry

Security is doing what you need to, in order to protect something.

Compliance is doing what somebody told you to do, whether it's useful or not

Information Sharing

- Redundancy, complexity & diversity
- If critical infrastructures are too complex and too diverse to attack simultaneously, then they must be attacked serially
- Prompt sharing of information about attacks – successful & failed – can prevent similar attacks – "actionable intelligence"
- Laws proposed to permit sharing of information from government bodies to private sector
- "Safe harbor" laws to encourage sharing

Really only works if sites can detect attacks promptly, and have forensics technology and expertise to analyze them

Risk Analysis: Different Approaches / Conclusions

- DHS/government/military: capability-based
  - American intelligence has demonstrated very sophisticated attack capabilities – Stuxnet, Flame, DuQu, Gauss were theirs
  - What they can do, presumably others can do
  - Assume an attack: compare offensive capabilities to defensive
- Industry: actuarial / insurance-style / case-based
  - Has never been a major cyber incident
  - Lawyers are put in charge of NERC-CIP *compliance programs*, not security programs

Infrastructure in the developed world is highly automated, and so highly vulnerable

Compensating Measure: Enhanced Safety Systems

- Expand process safety and equipment protection programs
- To the greatest extent practical, detect all unsafe conditions and trigger automatic return to safe state / process shutdown
- In theory: hacking ICS with robust, automatic process safety system results in plant outages at worst: reliability risk, not safety risk
- In practice: impossible to predict all failure modes – cyber-sabotage can cause simultaneous and subtle failures

Safety systems are an effective, partial compensating measure only if they are very secure

Compensating Measure: Physical Security

- Strictly control access to critical ICS computers
- Reduce risks due to USB, CD-ROMS, cell phone connections and other removable media / networking
- Reduce risks due to rogue laptops & other equipment plugged into ICS / safety networks
- Entire ICS network must lie within physical security perimeter

But: insider threat is still real, and distant adversaries can compromise equipment over the Internet by remote control

Compensating Measure: Device Control & Whitelisting

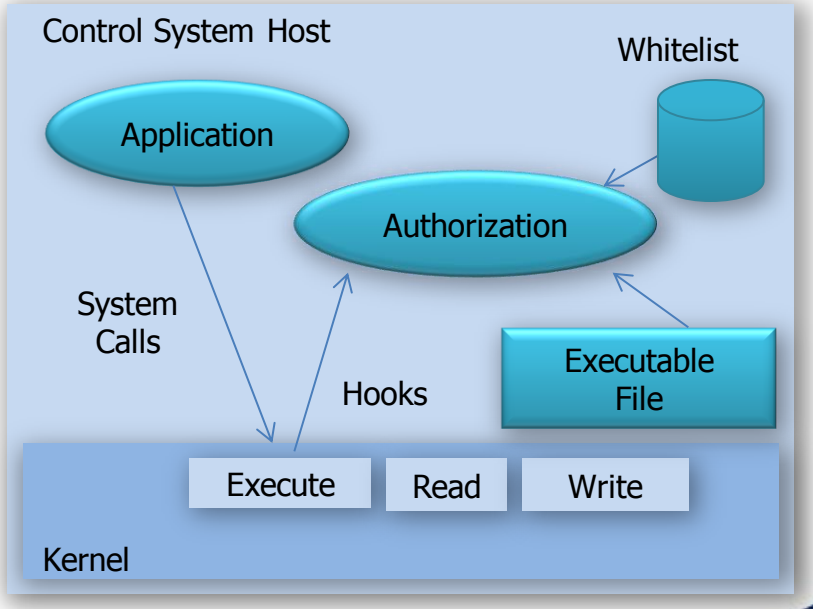
- Whitelisting: strictly control what software is allowed to run where
  - Currently used more for "devices" with complex embedded operating systems than for entire ICS systems
- Device control: forbid entirely the execution of software from removable media, control what kinds of USB devices (keyboards, mice) are allowed to be connected to which ports
  - Less intrusive than whitelisting, applied more commonly to larger parts of ICS systems

But: cannot prevent remote control of legitimate applications

Application Control / Whitelisting

- Automatically maintain list of all authorized executables and libraries
- Allow only recognized executable files to be executed, recognized libraries to be loaded
- Zero days: detects new viruses before signatures are issued
- Includes device control capabilities
- In-memory protections
- NERC CIP V5 allows instead of AV
- Good fit for ICS:
  - No signatures to update
  - Predictable execution costs

Better fit for ECC networks than anti-virus systems



Device Firewalls

- Specialized – fewer features, fewer possible connections, fewer mistakes
- Deep understanding of industrial protocols
- Allows only certain protocol commands through from certain machines
- Eg: Only certain hosts can change PLC programs, or change firmware, or write certain values
- Denial-of-Service protection

Anomaly-Based Network Intrusion Detection

- Comparatively small, uniform industrial networks support anomaly-based intrusion detection without floods of false-positive alerts
- Anomaly-based: learns what is "normal" – alerts on everything else
- Statistics based – new traffic flows or unusually big flows are suspicious
- Passive – mirror port on managed switch sends a copy of every message

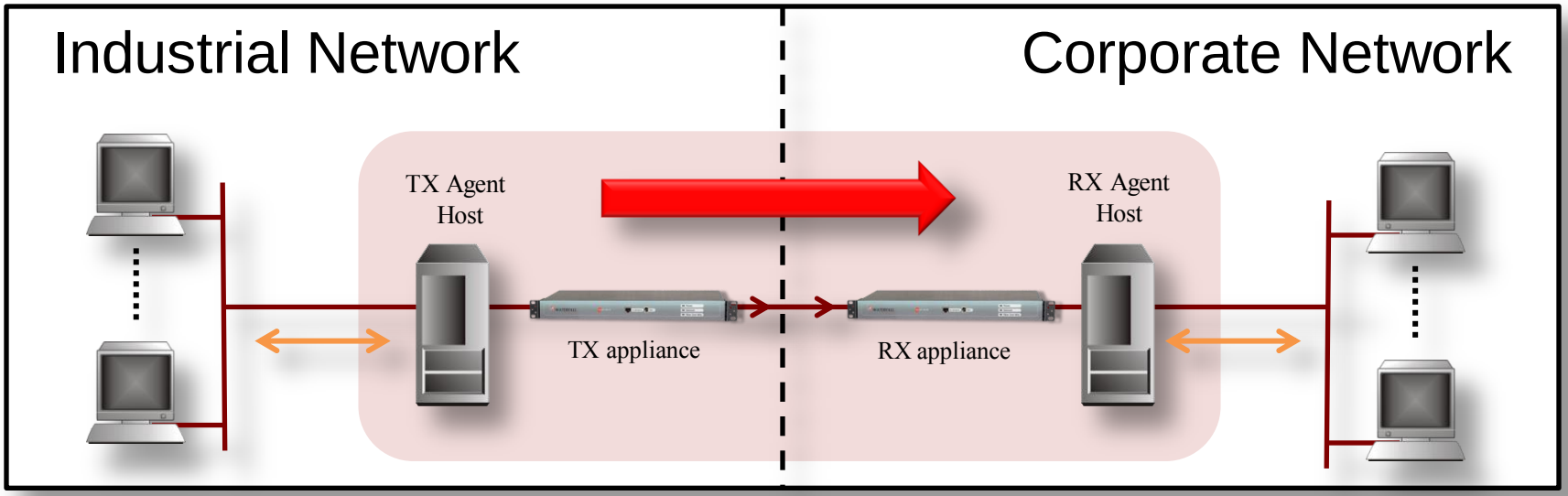
If you don't assume you have been breached and start looking for your attackers, you will never find them

SIEM and Intrusion Detection

- Security Information and Event Management (SIEM)
- Gathers security logs, security events, and compliance information into one pane of glass
- Gathers information from industrial systems, networks and devices
- Enterprise-wide scope: correlate alarms and conditions
- Integrate with cloud-based Global Threat Intelligence – correlate local conditions with global threats and conditions

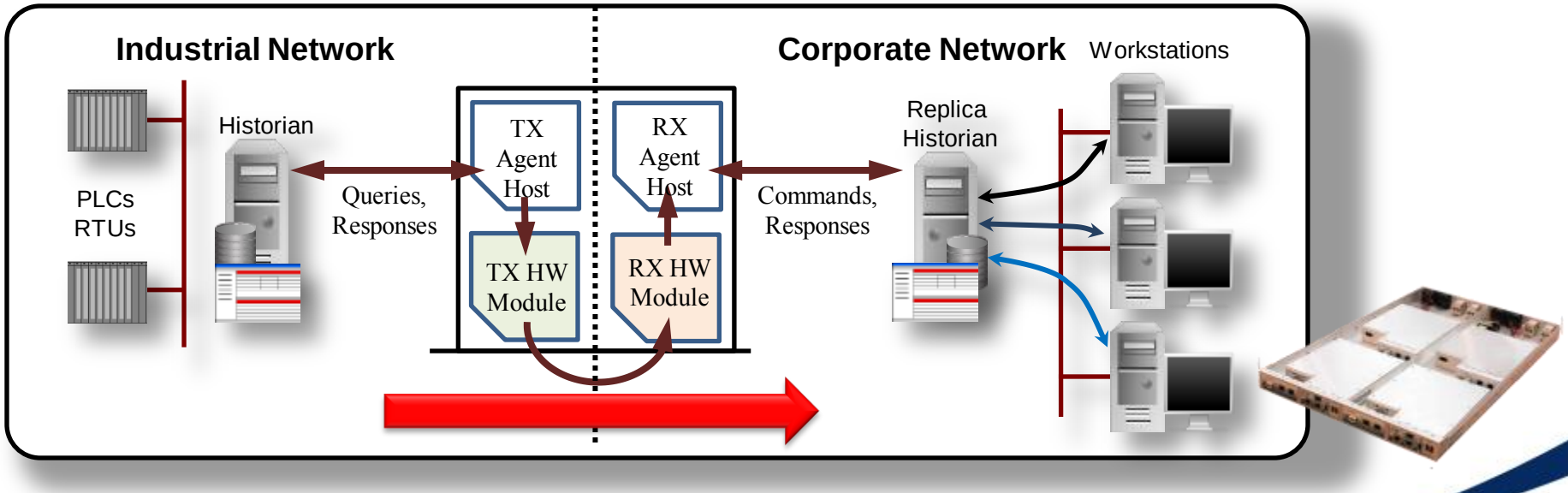
Unidirectional Security Gateways

- Laser in TX, photocell in RX, fibre-optic cable – you can send data out, but nothing can get back in to protected network
- TX uses 2-way protocols to gather data from protected network
- RX uses 2-way protocols to publish data to external network
- Absolute protection against online attacks from external networks



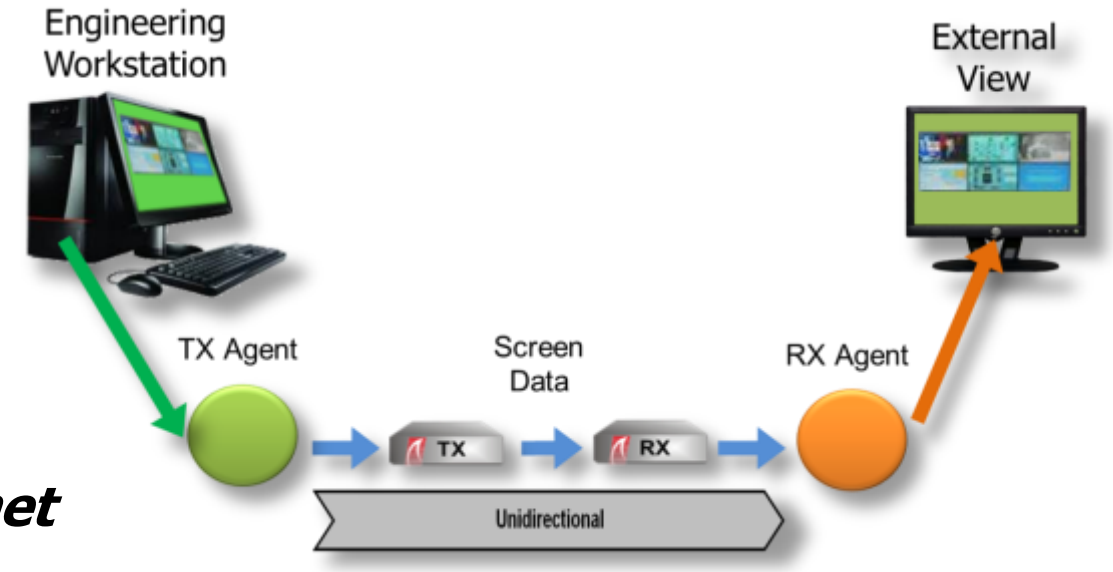
Unidirectional Gateway: Historian Server Replication

- Hardware-enforced unidirectional historian replication
- Replica historian contains all data and functionality of original
- Corporate workstations communicate only with replica historian
- Industrial network and critical assets are physically inaccessible from corporate network & 100% secure from any online attack



Remote Screen View

- Vendors can see control system screens in web browser
- Remote support is under control of on-site personnel
- Any changes to software or devices are carried out by on-site personnel, supervised by vendor personnel who can see site screens in real-time
- Vendors supervise site personnel
- Site people supervise the vendors

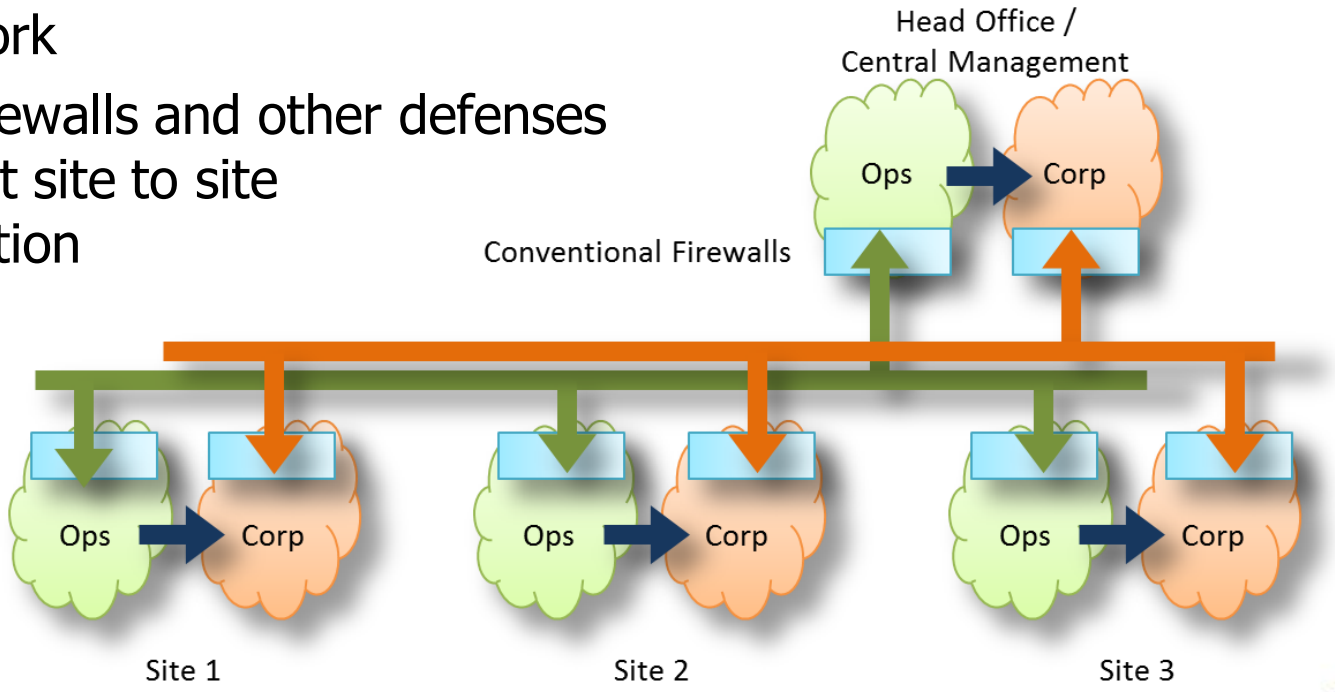


Both sets of needs are met

Central Management: Segregated Operations Network

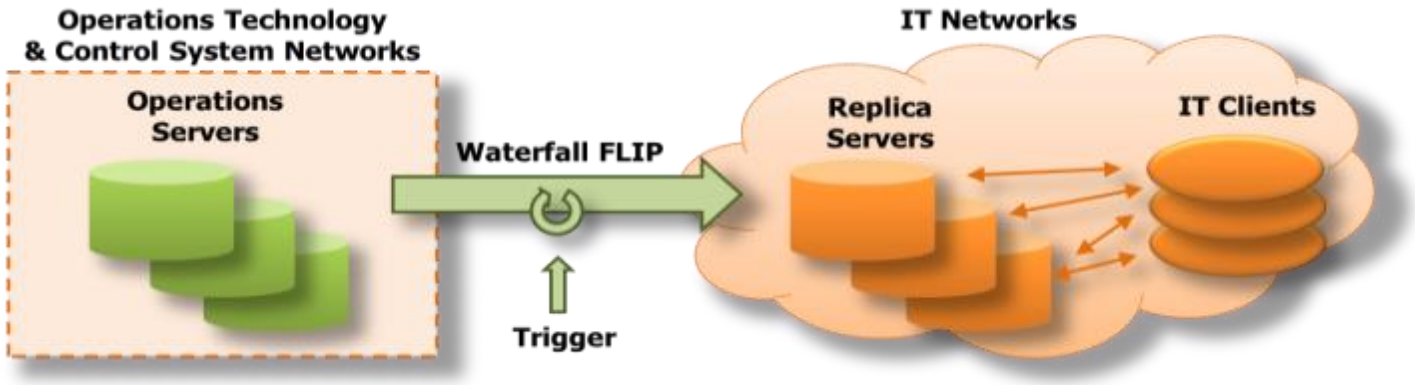
- Operations WAN (green) separate from corporate WAN
- Unidirectional Gateways are only path from operations to corporate – breaks infection / compromise path from corporate WAN / Internet
- Central operations staff have two workstations: one on operations network, and one on corporate network
- Conventional firewalls and other defenses deployed to limit site to site threat propagation

Isolated, yet still centrally managed

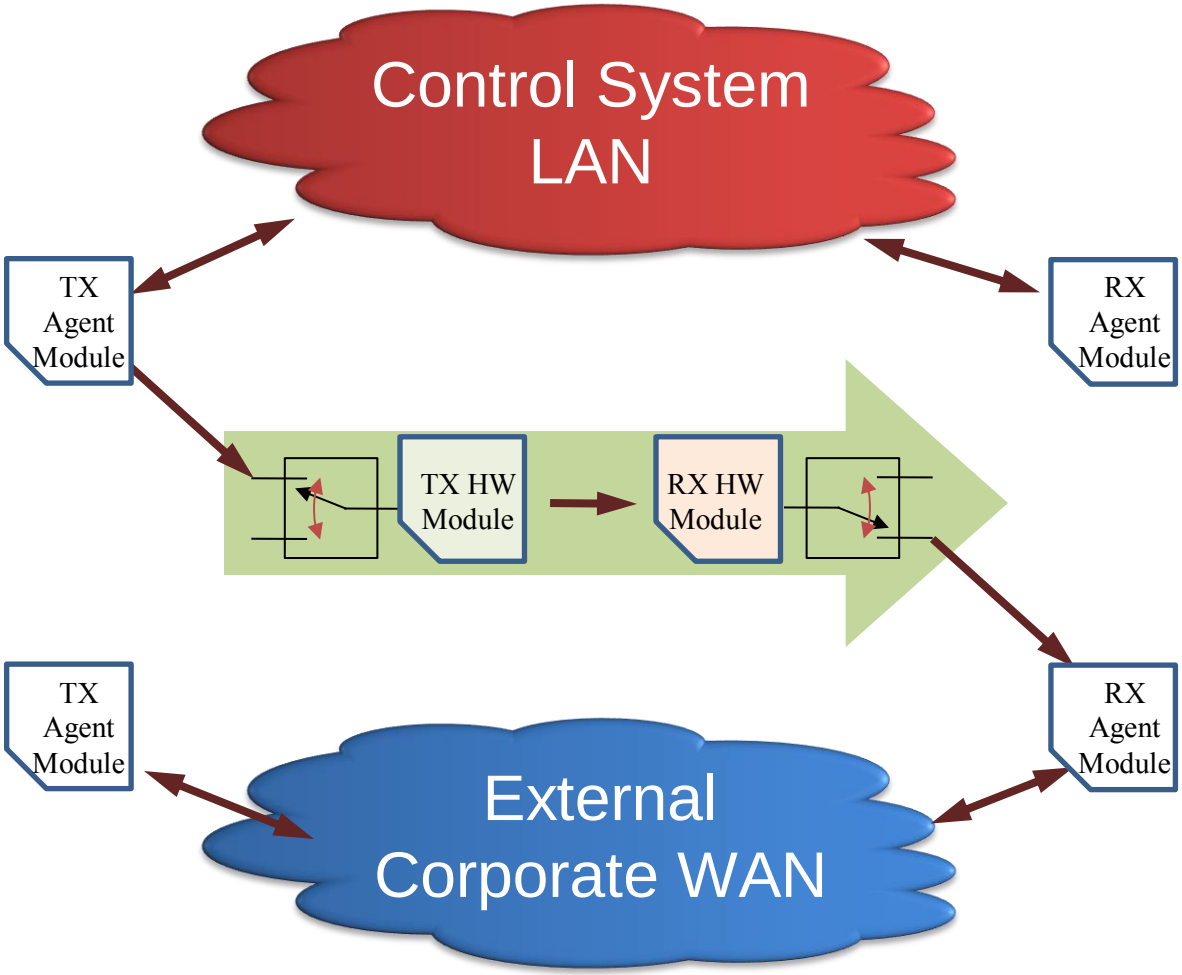


Waterfall FLIP™

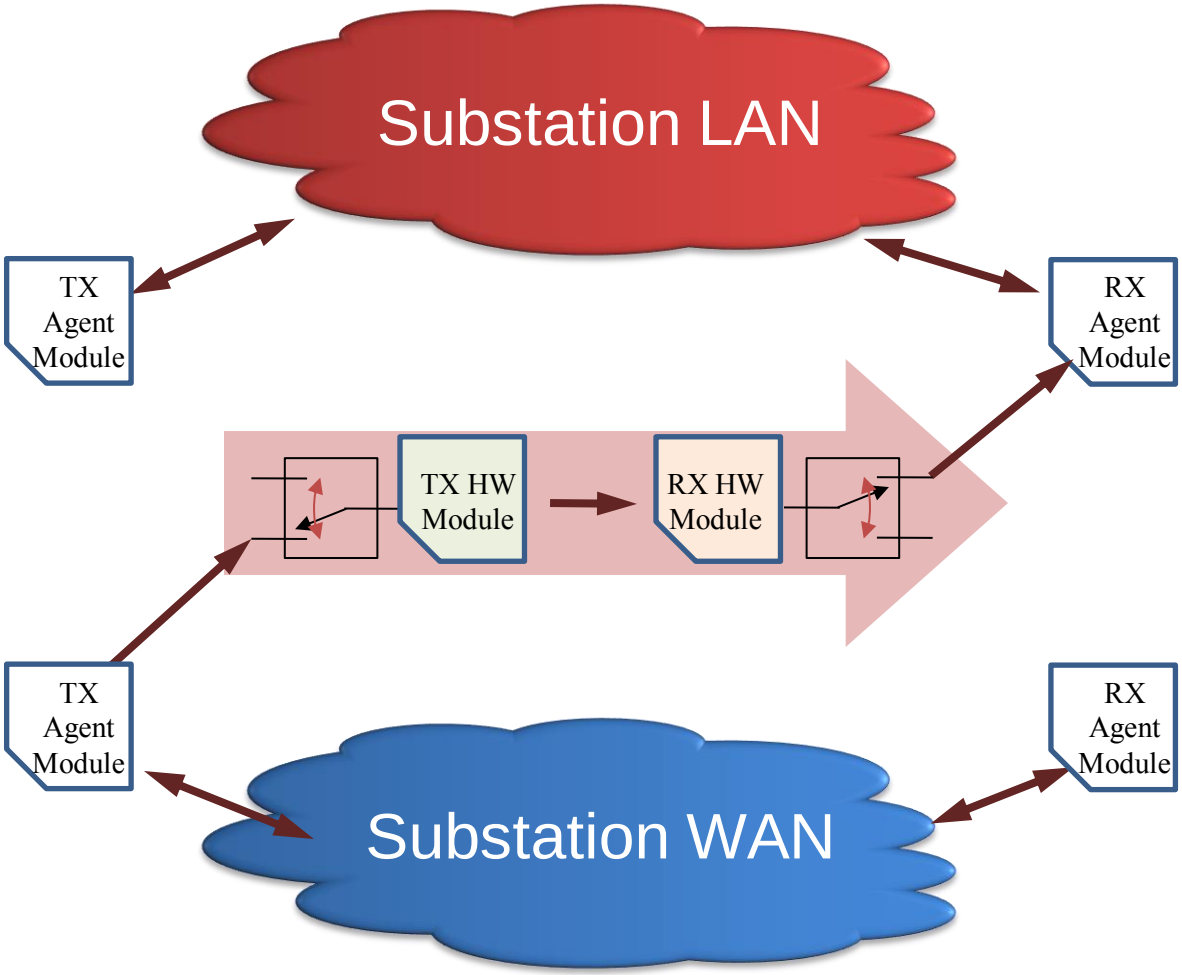
- Unidirectional Gateway whose direction can be reversed:
  - Regular and randomized security updates & AV signatures
  - Chemicals / refining / mining / pharmaceuticals: batch instructions
  - Substations, pumping stations, remote, unstaffed sites
- Variety of triggering options
- When 'flipped' – incoming unidirectional gateway replicates servers: no TCP/IP, no remote control attacks
- Stronger than firewalls, stronger than removable media



Normal Operation



Reversed



FLIP: Stronger than Firewalls

- Outbound data flows are absolutely secure – temporary in-bound flows are the concern
- Gateways replicate servers / terminate protocol sessions – no packets forwarded, no protocol-level attack passes through
- Interactive remote control is impossible – there are never in-bound and out-bound data flows simultaneously
  - Attackers "flying blind" – no feedback
- No TCP/IP sessions are possible

Stronger than firewalls: 100% secure 99% of the time. Stronger than a firewall the rest of the time

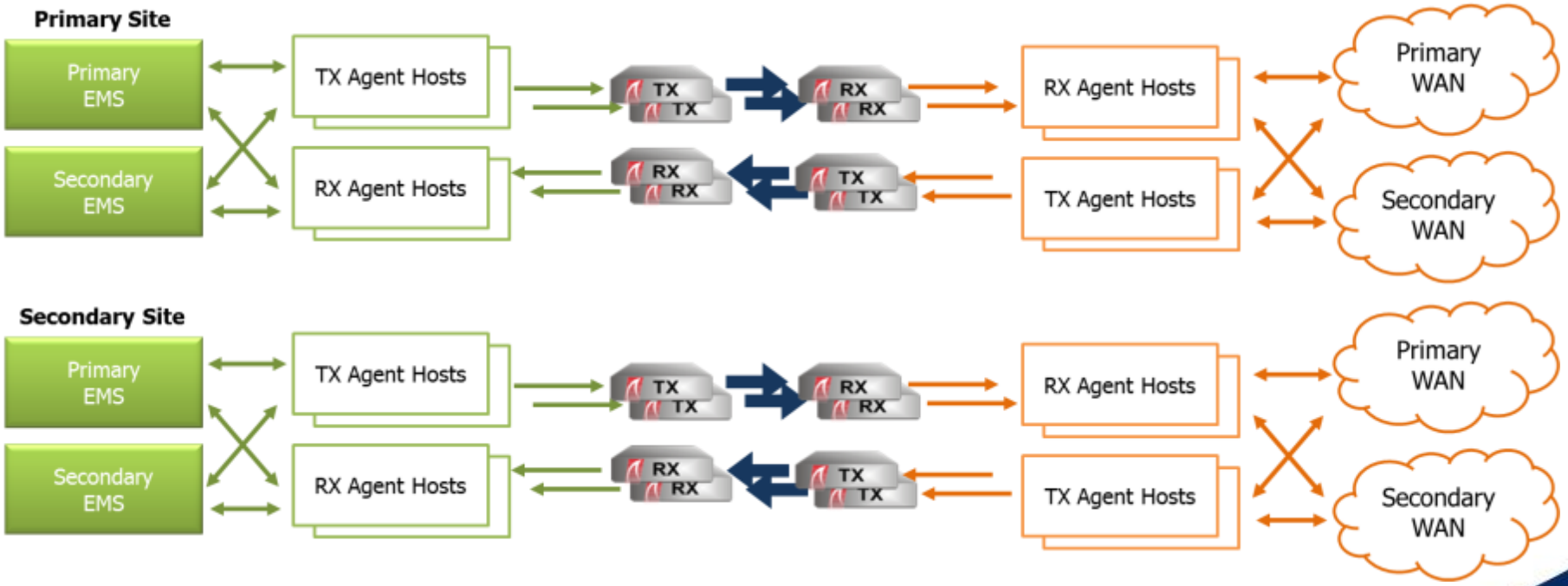
Perimeter Security Attack Tree Analysis

Attack Type	WF Soln	Fwall
1) Phishing / drive-by-download – victim pulls your attack through firewall	4	2
2) Social engineering – steal a password / keystroke logger / shoulder surf	4	1
3) Compromise domain controller – create ICS host or firewall account	4	2
4) Attack exposed servers – SQL injection / DOS / buffer-overflow	3	2
5) Attack exposed clients – compromised web svrs/ file svrs / buf-overflows	4	2
6) Session hijacking – MIM / steal HTTP cookies / command injection	3	2
7) Piggy-back on VPN – split tunneling / malware propagation	4	2
8) Firewall vulnerabilities – bugs / zero-days / default passwd/ design vulns	3	2
9) Errors and omissions – bad fwall rules/configs / IT reaches through fwalls	3	2
10) Forge an IP address – firewall rules are IP-based	4	2
11) Bypass network perimeter – cabling/ rogue wireless / dial-up	1	1
12) Physical access to firewall – local admin / no passwd / modify hardware	3	2
13) Sneakernet – removable media / untrusted laptops	1	1
Total Score:	41	23

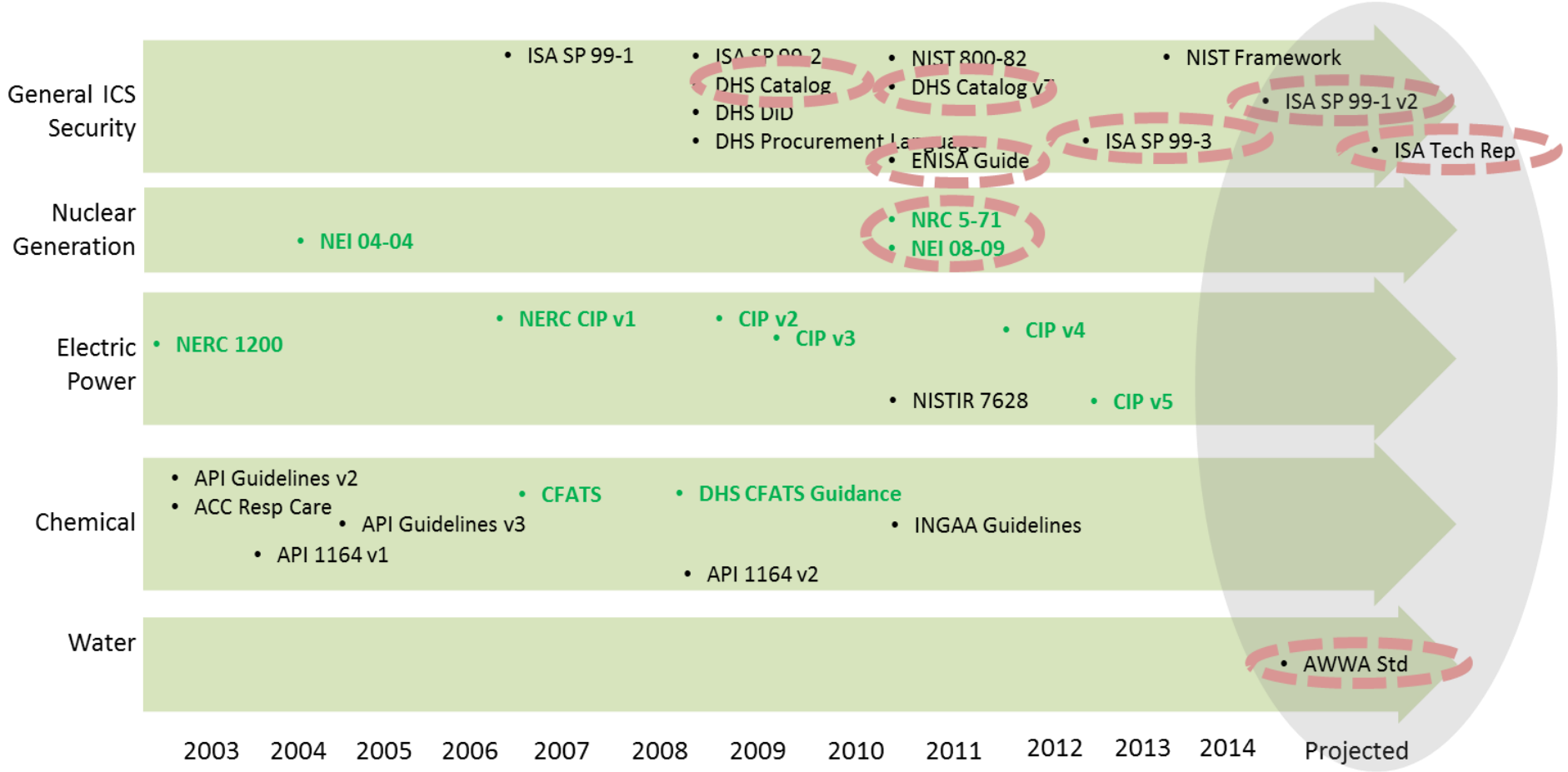
Attack Success Rate:	Impossible	Extremely Difficult	Difficult	Straight-Forward

Balancing Authority / Control Center Solution

- Gateways send commands "out" to partner utilities. Second channel polls/reports data "in"
- Multiply redundant – automatic at site, manual fail-over between sites
- Some ICCP reconfiguration needed – channels are independent



Current and Emerging Standards



NIST Framework - Disappointing

- Mandated by recent executive order
- Order talks about "SCADA Security" but framework is IT-centric
- Framework is extremely high level – no mention of technologies, not even firewalls
- NIST risk management framework is actuarial, not capabilities-based
- Framework elements:
  - Identify: inventory, security config mgmt, policy, governance
  - Protect: network & host protections, training, awareness
  - Detect: monitoring & intrusion detection
  - Respond: incident response teams, planning, escalation
  - Recover: backups, recovery, testing, business continuity

Waterfall Security Solutions

- Headquarters in Israel, sales and operations office in the USA
- Hundreds of sites deployed in all critical infrastructure sectors

FROST & SULLIVAN — Best Practice Award 2012, Industrial Network Security 2013 Oil & Gas Customer Value Enhancement Award

Gartner — IT and OT security architects should consider Waterfall for their operations networks

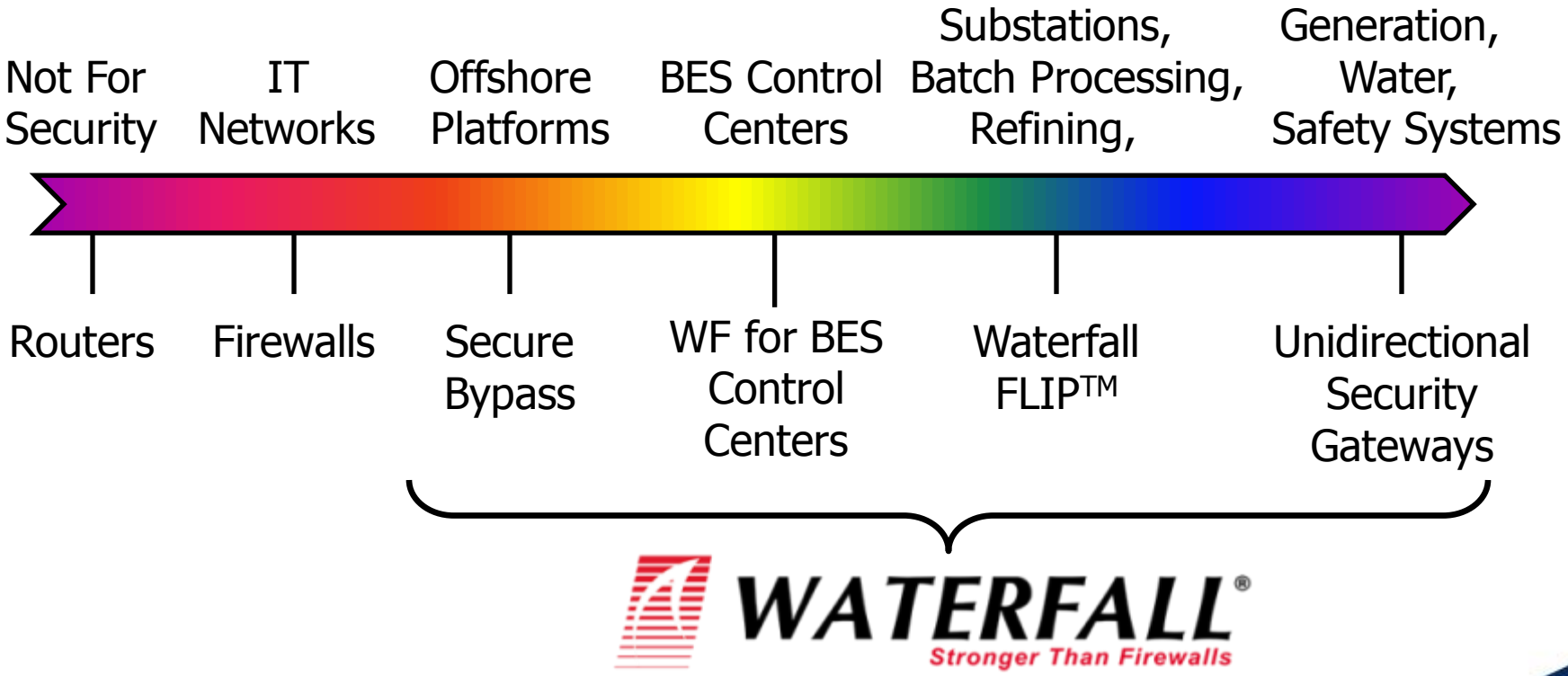
PikeResearch Cleantech Market Intelligence — Waterfall is key player in the cyber security market – 2010, 2011, & 2012

- Strategic partnership agreements / cooperation with: OSIsoft, GE, Siemens, and many other major industrial vendors

Market leader for Unidirectional Security Gateways

Waterfall's Mission: Replace ICS Firewalls

- Waterfall's new mission: revolutionize ICS perimeter security with technologies stronger than firewalls
- Look for additional product announcements over the next 12 months



Control System Security: State of the Practice

- ICS "soft interior" will never be as secure as IT
- ICS perimeter security will always be disproportionately important
- Cultivate deep suspicion of external inputs: comms, files, equipment
- Communicating risk is the key to management buy-in for cyber-security investments
- Industry leaders "get it"
- On average: much work yet to be done

Bottom line: modern threats defeat standard IT protections routinely.

Advanced IT/confidentiality protections do nothing to prevent cyber-sabotage.

Deploy ICS-specific protections.