MASTER CLASS
Cybersecurity for Power Systems

Andrew Ginter

VP Industrial Security
Waterfall Security Solutions

2023

OT VS IT DIFFERENCE: CONSEQUENCE

PATCHING, AV, PASSWORDS, CRYPTO
Superficial – recognized since 62443-1-1

AIC VS SAFETY
NIST 800-82 - 2016

CONSEQUENCES
CIP, ANSSI, TS50701, Israeli standards

ISA SP99 / 62443 DEBATING THIS TODAY What factors determine system criticality?

Fundamental difference is consequence – even if we could wave a "magic patching" wand, we cannot restore human lives "from backups"

WATERFALL® Stronger Than Firewalls

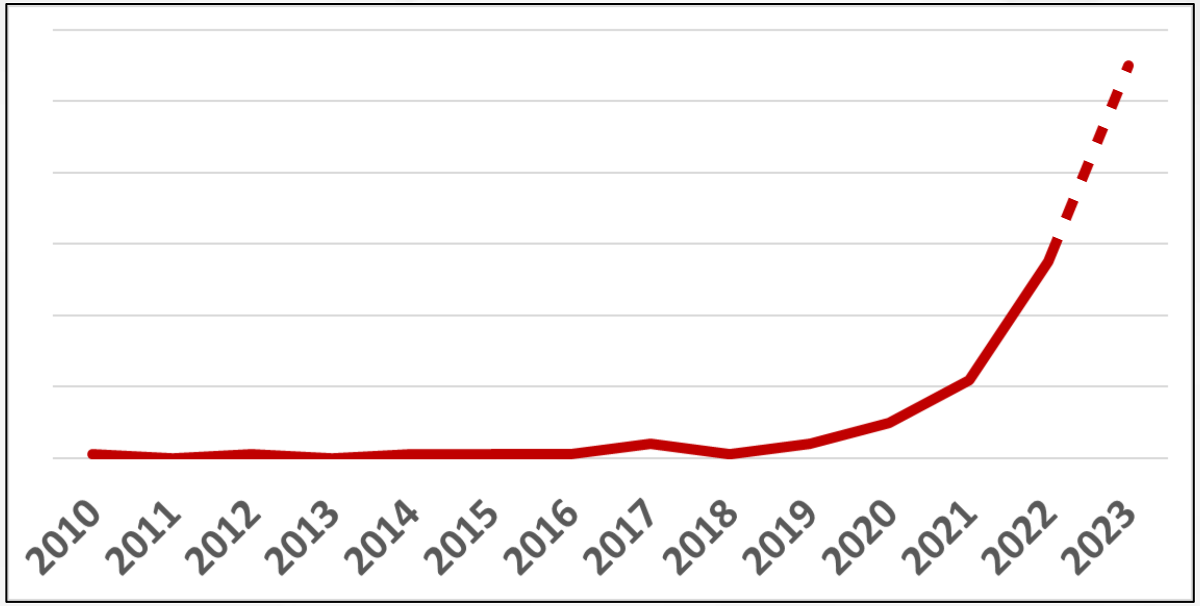
HIGHLIGHT: 2021 THREAT REPORT (MAY 2022)

CHANGED FOREVER: Cyber attacks with physical impacts were once a theoretical risk – today real

EXPONENTIAL: More than doubling every year

NATION STATE: Ransomware groups trailing nation state attack tools & techniques by only 3-5 years

ATTACKS WITH PHYSICAL IMPACTS

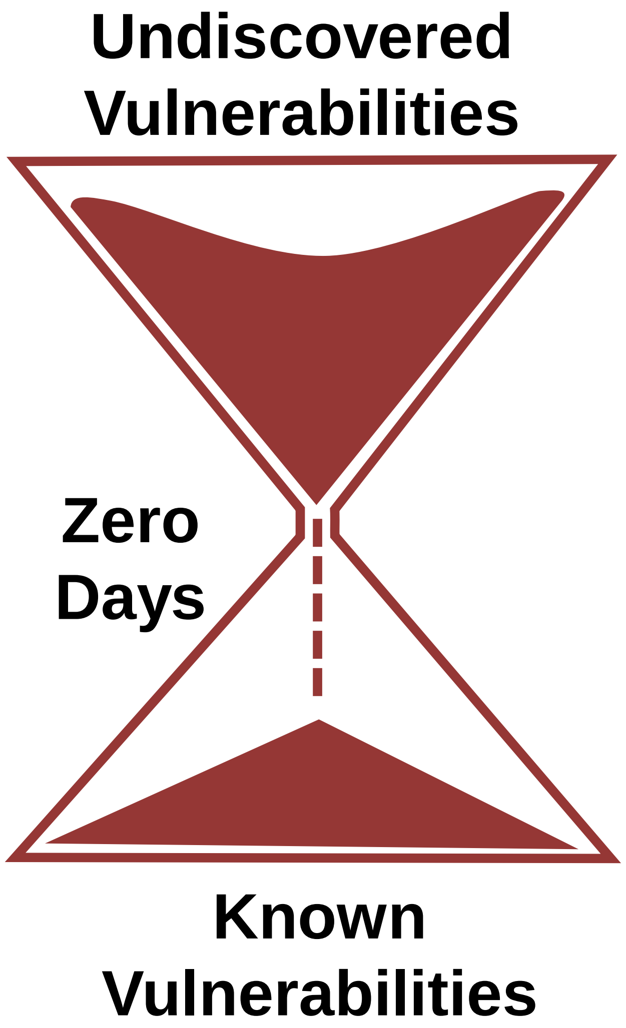


What we see nation states doing to each other today, ransomware will do to everyone with money in 3-5 years

Too Much Focus On Vulnerabilities

- If we could only get rid of our vulnerabilities, then we would be *invulnerable!*
- "Vulnerabilities" are quickly confused with "known vulnerabilities"
- And the security program turns into "quick – patch everything!"

This is of course nonsense, and costly as well



First Three Laws of SCADA Security

- Nothing is secure
- All software can be hacked
- All cyber attacks are information, and every bit of information can be an attack

In the worst case a compromised CPU will issue every unsafe instruction to the physical process that the CPU is physically able to issue

Firewalls Will Save Us

WATERFALL
Stronger Than Firewalls

- Many attacks: steal password, attack servers through the firewall with buffer overflows & sql injection, piggy-back on VPN, etc.
- Signature-based IPS is blind to new attacks – invent one with a fuzzer
- Hide exfiltrated data in legitimate web app NG firewall thinks it understands
- Attack servers outside firewall that are trusted by equipment inside firewall

Firewalls are porous. All firewalls forward messages from less-trusted networks to more-trusted ones

Photo credit: Red Tiger Security

Encryption Will Save Us

- Same key in each device is easily stolen
- Encryption protocols are frequently broken
- Encryption algorithms age and are broken
- Encryption software has bugs and are compromised
- Operating systems are software and are compromised, without compromising encryption
- Cryptosystems encrypt attacks just as happily as they encrypt legitimate comms

To defeat encryption, compromise an endpoint

Anti-Virus Will Save Us

- Signature-based defense – only effective against known attacks
- No signatures for “new” malware – no matter how simple or how sophisticated the malware
- No signatures for low-volume / targeted malware
- Have your malware turn off the AV tool

To defeat AV write your own bits of malware, and deploy them sparingly

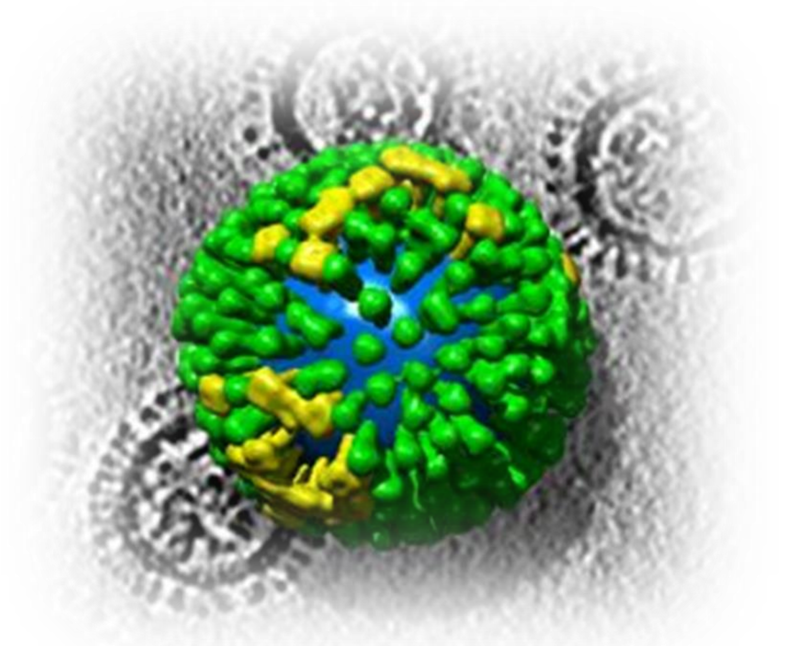


Photo credit: National Institutes of Health

Security Updates Will Save Us

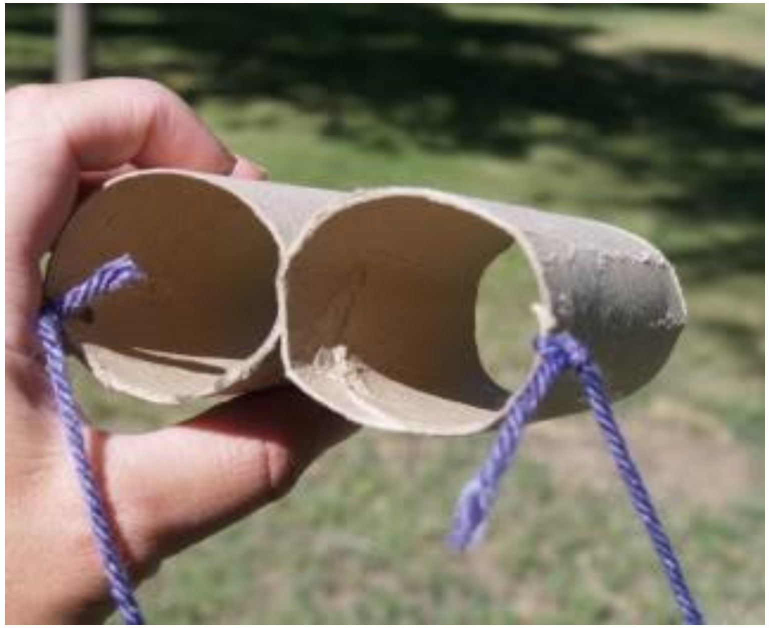
- All software has bugs, and some bugs are vulnerabilities, so all software can be hacked
- Security updates address known vulnerabilities, not zero-days
- Delay between vulnerability disclosure and update is opportunity to attack
- Security updates cannot defeat stolen or shared passwords or other permissions exploits

To defeat software updates, steal or create a password, then just log in

Intrusion Detection Will Save Us

WATERFALL
Stronger Than Firewalls

- Signature-based detection is blind to new attacks – invent one with a fuzzer
- Anomaly detection is defeated by low-and-slow attacks
- False alarm investigations cost time and talent
- Successful detection and remediation of real intrusions, assuming they are investigated to begin with,
  take time



How long can we let an intruder "stir the pot" in our power grid?

Information Sharing Will Save Us

- Information sharing shares futures: threat actor tracking, black-market tools capabilities, indications of immanent targeting. Eg: Ukrainian utilities: Russians are likely to target you
- Shares past – indicators of compromise when compromise is discovered in an organization. Eg: 3 Ukrainian utilities were compromised and 225,000 people were without power, with these indicators of compromise…

When a sophisticated ransomware or other attack simultaneously compromises assets throughout a grid, information sharing is too slow

The Government Will Save Us

WATERFALL
Stronger Than Firewalls

	Script Kiddies	Corp Insiders	Ransom ware	ICS Insiders	Hack-tivists	Targeted Rans-wre	Intel Agencies	Military Grade
Resources	Tools	Trust	Pros, $$	Trust	Amateur	Pros, $$	Pros, $$$	Pros, $$$, physical
Consequence	Low per incident	Med per incident	High	High	High	High	Very High	Very High
Frequency	High	Med	Med	Low	Low	Low	Low	Very Low
Corp Focus	High	High	High	Some	Some	Poor	Poor	Very Poor

Most organizations focus on High Frequency / Low Impact (HFLI) events, and expect the government to save them from HFLI events

But: the government cannot save industrial sites from nation-state-grade attacks – information sharing & incident response is too slow

Classic AMI Security Advice

- Encryption
- Security Updates
- Firewalls
- Anti-virus & IPS – in back office
- Intrusion Detection / Security Monitoring
- Power / Billing Anomaly Detection
- Auditing & Surveillance

Problem: classic advice addresses low-impact power theft, but does not prevent sophisticated attacks, but may detect attacks after attackers have been in the system for some time

High-Impact Consequences

WATERFALL Stronger Than Firewalls

- Public safety: toxic releases, explosions near population centers, contaminated human consumables (water, food, medication), lack of access to essential services – electricity, water, fuel, transportation
- Environmental: damage, disasters, catastrophes
- Worker safety: toxins, explosions, asphyxiation
- Equipment damage: turbines, pipelines, HV transformers
- Downtime: lost production & revenues, restart delays & costs
- Reputation damage: due to all of above

There was a time when only "accidents" could cause high impact consequences – nowadays, generally all these consequences can have cyber causes as well

RISK: LIKELIHOOD

RISK = CONSEQUENCE x LIKELIHOOD – classic equation

BUT LIKELIHOOD != PROBABILITY – for deliberate attacks, vs random events like equipment failures & hurricanes

Consequence			
High	Medium	High	High
Medium	Low	Medium	High
Low	Low	Low	Medium
Likelihood	Low	Medium	High

WATERFALL® Stronger Than Firewalls

RISK: CAPABILITY

RISK = CONSEQUENCE x THREAT – for threats with intent

THREAT = INTENT x CAPABILITY (x) OPPORTUNITY – more modern formulation

OPPORTUNITY != VULNERABILITY – modern attacks exploit permissions more often than software vulnerabilities

TOLERANCE DIRECTIVE – consequence + capability

WIDESPREAD CAPABILITIES – defenses must reliably defeat widely-available attack capabilities with unacceptable consequences

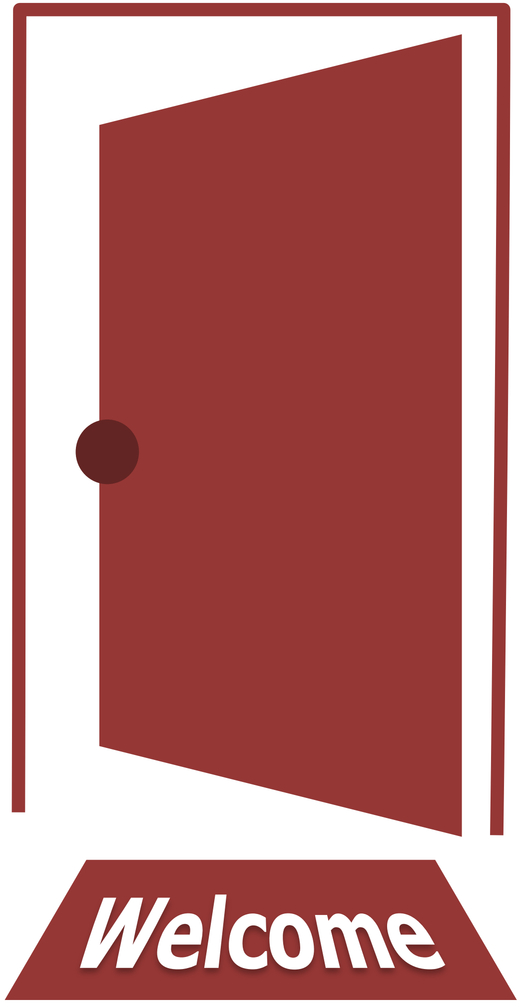
Twenty Standard Attacks	SEC-OT	IT Style
Common Ransomware	1	1
OT-Targeted Ransomware	2	2
Abundance of Caution	3	3
IT Dependences	4	4
Broken 2FA Ransomware	5	5
Cloud-Seeded Ransomware	6	6
ICS Insider	7	7
IT Insider	8	8
Cloud Insider	9	9
Hacktivist	10	10
Sophisticated Hacktivist	11	11
Nation State – Destruction	12	12
Nation State – Safety	13	13
Leave Behind	14	14
Cell Phone WiFi	15	15
Software Supply Chain	16	16
Hardware Supply Chain	17	17
Autonomous Malware	18	18
Nation State Crypto Hack	19	19
Nation State ICS Insider	20	20

WATERFALL®
Stronger Than Firewalls

Attackers Exploit Permissions

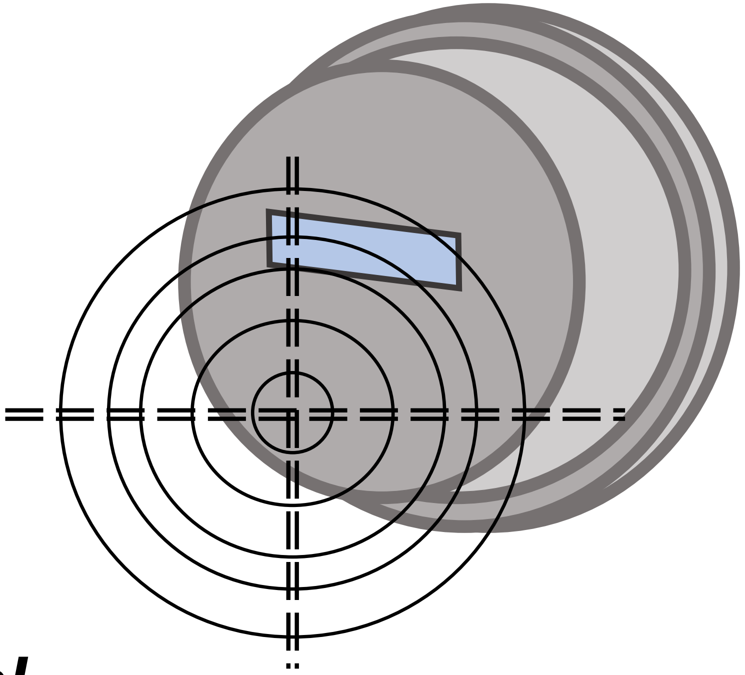
- Remote access attacks piggy-back on legitimate sessions / permissions, such as remote access sessions
- Phishing attacks steal credentials
- Pass-the-hash attacks re-use existing credentials
- Databases & other servers permit remote execution
- Remote Access Trojans (RATs) provide remote control to understand target, steal credentials & make next move

Why write code to exploit vulnerabilities when attackers can log in and execute what they want?



Use Case: Damaging AMI

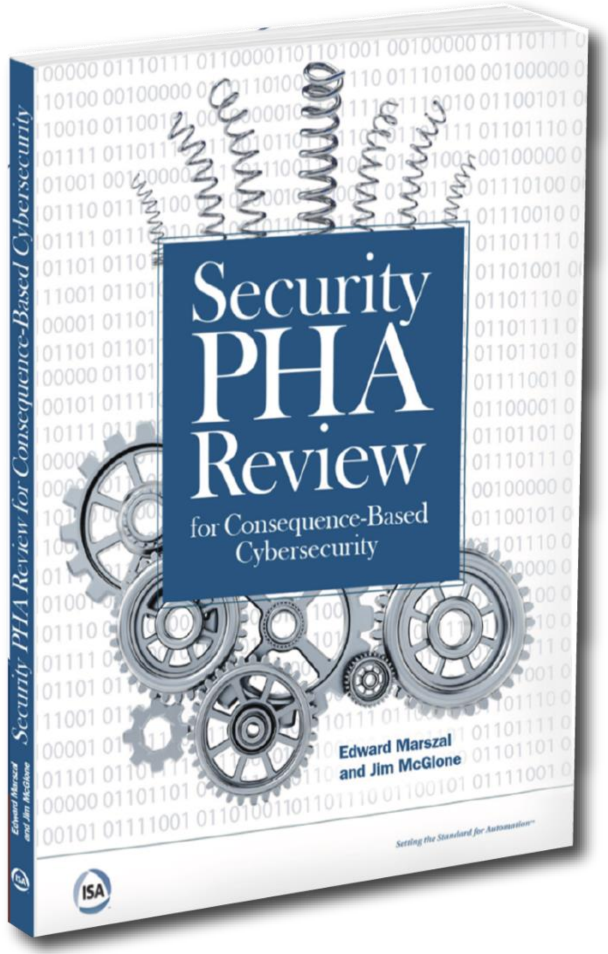
- Scenario:
  - Worm propagates automatically to most meters in a geography
  - Turns off consumer power
  - Damages meter, or erases firmware
  - 3M meters must be replaced
- Physical mitigations:
  - Design/modify meter to prevent damage
  - Design/modify meter to permit manual firmware restoration



Service should always be restorable via physical access or proximity, no matter what the compromise

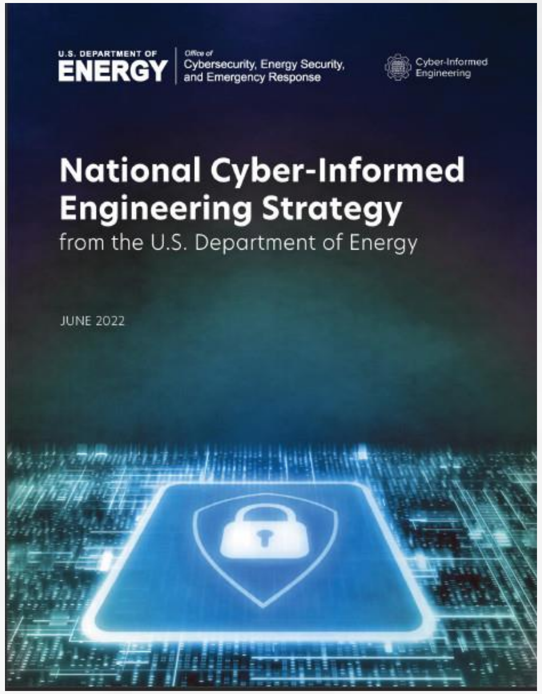
Security PHA Review

- PHA = Process Hazard Analysis = safety analysis
- Focus: preventing safety incidents
- All cyber systems with direct or indirect access to a routable network are deemed “hackable”
- If safety system is hackable, deploy physical mitigations – over-speed governors, over-pressure valves



With physical mitigations in place, no cyber attack can compromise safety

US DOE STRATEGY – “SECURITY ENGINEERING”



IF YOUR LIFE DEPENDS ON A BOILER NOT EXPLODING

Would you prefer spring-loaded valve, or longer PLC password? Where is the valve in IEC 62443 or NIST CSF?

ENGINEERING PROFESSION

Managed physical risk for a century – new threat, same risk

WOULD YOU TRUST A BRIDGE

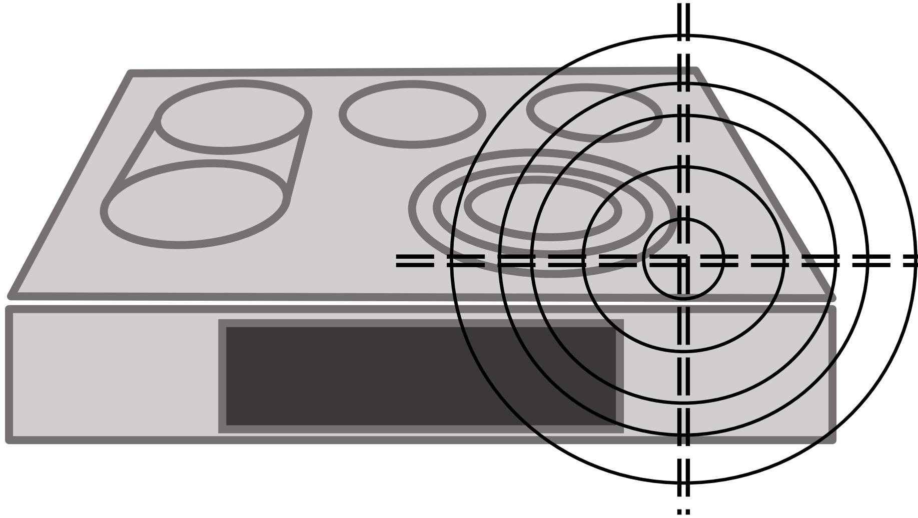
Whose design engineer “hopes” it will carry a specified load, for a specified number of decades?

Engineering-grade solutions work predictably and deterministically

WATERFALL®
Stronger Than Firewalls

Use Case: Smart Home/Stove

- Scenario:
  - Targeted attack reaches into smart meter network
  - Compromises meters with memory-resident remote-control malware
  - Malware uses home network to target “smart” touch-screen stovetops
  - Uses one vendor’s stovetop vulnerability to take over 10,000 stovetops
  - Turns on all burners at 2 AM – fires, casualties
- Physical mitigations:
  - 2 CPUs in stovetop – one able to sense & report, other able to control
  - Unidirectional connection between home network and smart meter



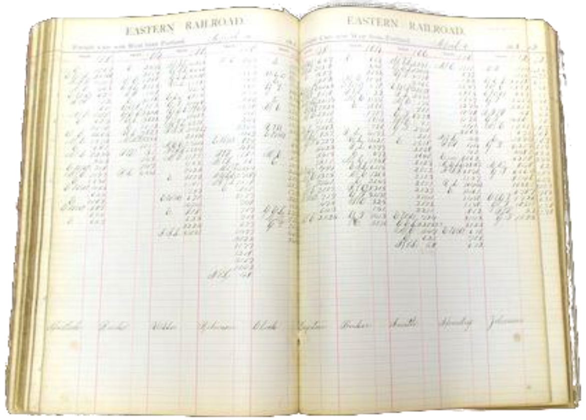
But – neither mitigation exists at this time

Data vs Monitoring vs Control

WATERFALL
Stronger Than Firewalls

- IT history: leger books / accounting data / transactions
- Industrial network history
  - Gauges = monitoring = IT data
  - Switches & dials = control = safety/reliability critical
- IT experts say “it’s all data,” but this blinds us to crucial difference between monitoring and control
- Correct control is vital to physical safety and physical reliability

Control is not AIC, CIA or “IT data” – control is really important



VS

Secure Operations Technology

WATERFALL
Stronger Than Firewalls

- Describes what the world's most secure sites do differently
- Ask different questions – get different answers
- Different way of looking at security

https://waterfall-security.com/sec-ot

SECURE OPERATIONS TECHNOLOGY

IT-SEC:

protect the information

SEC-OT :

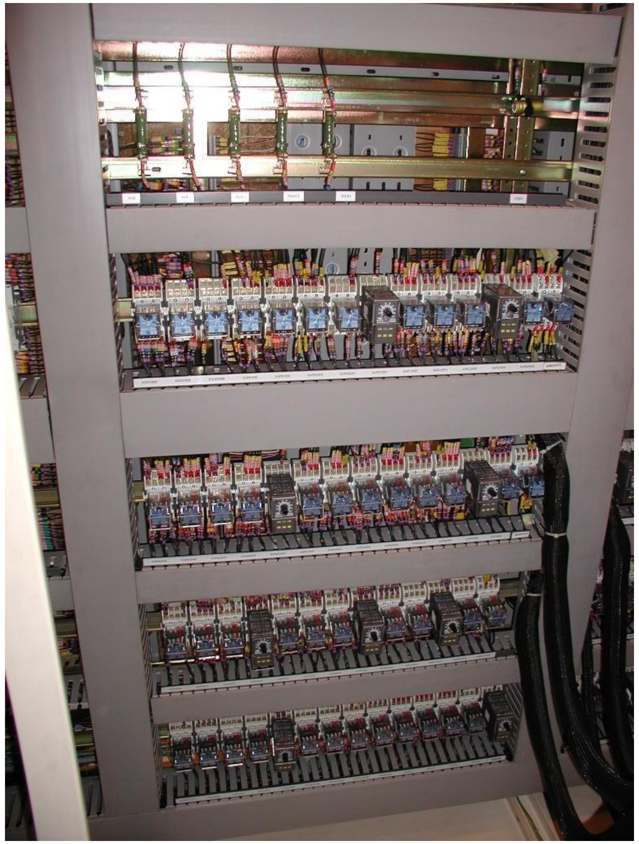
protect physical operations
from the information

OFFLINE CONTROLS

Offline Survey
Test Beds
Removable Media
Removable Devices
New Cyber Assets
Insider Attacks
Deceived Insiders
Nonessential Equipment

Test Beds

- Provide as accurate a copy of the industrial control system as possible for testing purposes
- Instrument the test bed heavily to search for safety, reliability and security problems
- Test all non-trivial information artifacts before trusting those artifacts for deployment on the control-critical network



Test beds should not be connected to ICS networks – malware and adversaries must not be given the opportunity to pivot

Removable Media

- Media = information storage without an embedded CPU – CDs, DVDs, floppies
- Software policies preventing media from mounting
- Multi-AV-scanning kiosks at physical perimeters
- Physically blocking or removing devices on all equipment except kiosks
- Publish scanned files to test bed or control-critical network

Removable media is the most frequent source of common malware on industrial networks

WATERFALL®
Stronger Than Firewalls

WHAT'S NEW

Near-miss protocol for information incidents

Photo credit: Tony Hisgett / CC BY-SA 2.0

Removable Devices

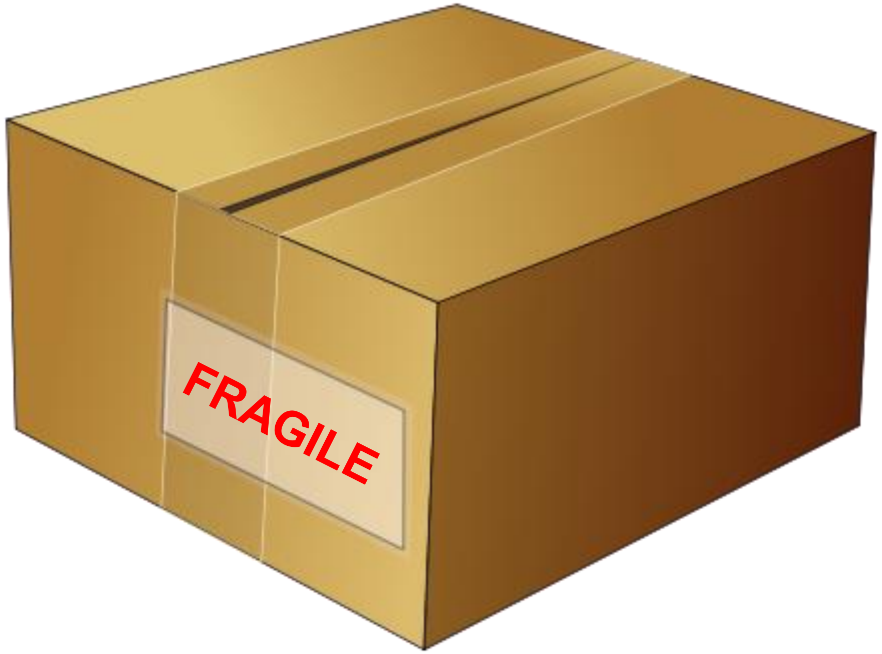
- Vendor laptop program
- Network Access Control
- Alerts
- Contracts forbidding devices
- Labelling control-critical devices
- USB charger program – reduces temptation

SEC-OT sites report that these programs essentially eliminate the use of IT-exposed removable devices

New Cyber Assets

- Brand new cyber assets contain information/attacks as well
- Deploy first on test bed and test for security and other threats
- Buy “consumables” at random – reduces risk of targeted attacks
- Inspect where practical
- Contracts include penalties if unexpected hardware is included in shipments
- Label control-critical assets clearly

Supply-chain integrity is a topic of on-going research in the SEC-OT community



Insider Attacks

- SEC-OT sites routinely draw on best practices from IT-SEC and physical security disciplines for addressing insider threats
- Enable detailed auditing as a deterrent
- Unidirectionally forward audit and other data into a tamper-proof forensic repository
- Deploy video monitoring
- Use video & forensic records routinely in cyber near-miss investigations

Monitoring is only a deterrent when potential perpetrators know that they are being monitored

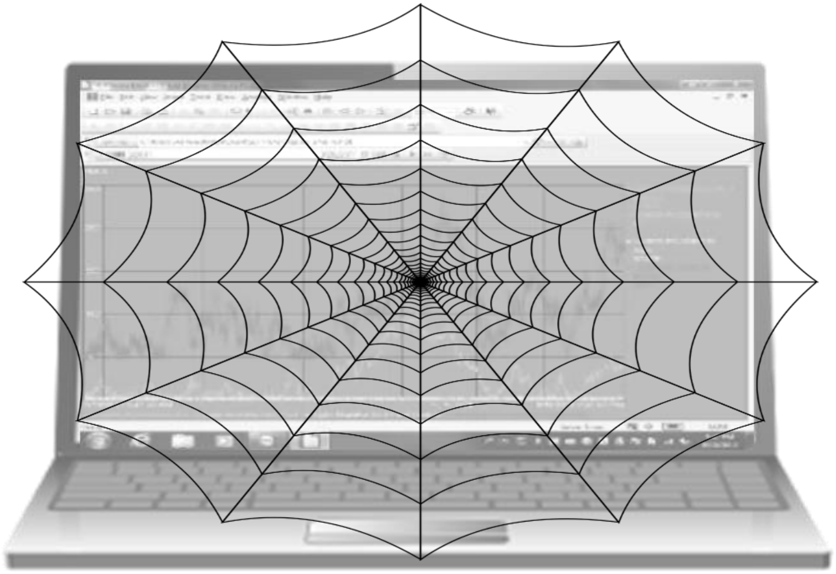
Deceived Insiders

- Well-meaning insiders can be deceived into acting on false information with physical consequences
- Insiders must be trained to be suspicious of and seek verification of externally-sourced information and information that has traversed a non-critical network

Emailed information and instructions should be verified verbally before taking action

Non-Essential Equipment

- Some equipment on control-critical networks does not need to run continuously – and some of this equipment has enormous privilege
- Engineering workstations can reprogram the control system
- PLC workstations can reprogram PLCs
- Administrative workstations can change permissions remotely



Power off the most trusted equipment until it is needed

Forbid firewalls as connection from ICS to IT networks – permit only unidirectional gateways

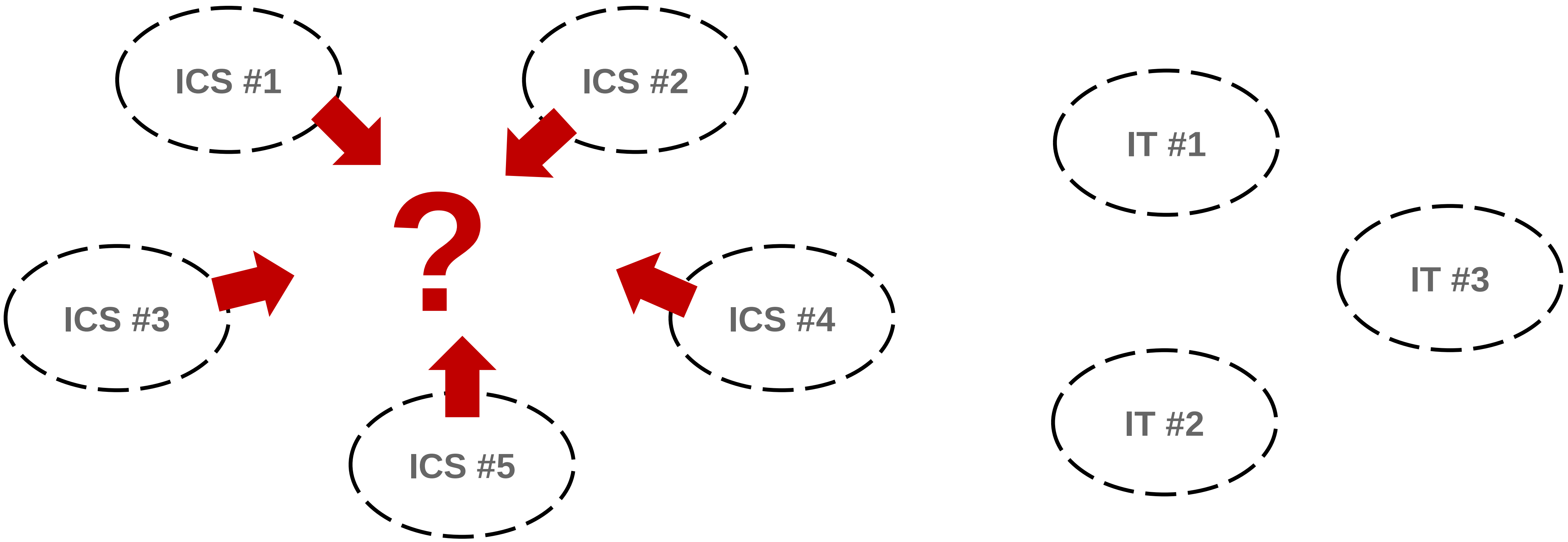
ONLINE CONTROLS

SEC-OT practice: one layer of unidirectional gateways in a defense-in-depth architecture

Use firewalls for internal ICS segmentation

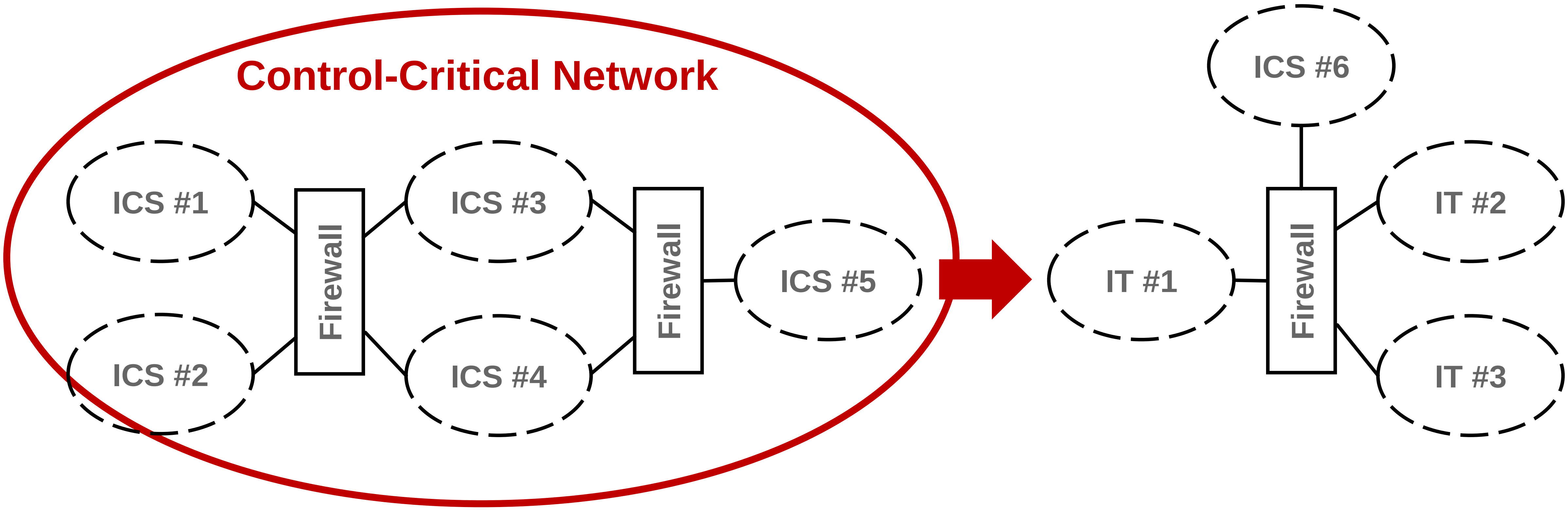
WHAT'S NEW: two dozen unidirectional network reference architectures

How Is This Practical?



Industrial Control Systems (ICS) at a site almost always need to cooperate and coordinate

Control-Critical Network Sets



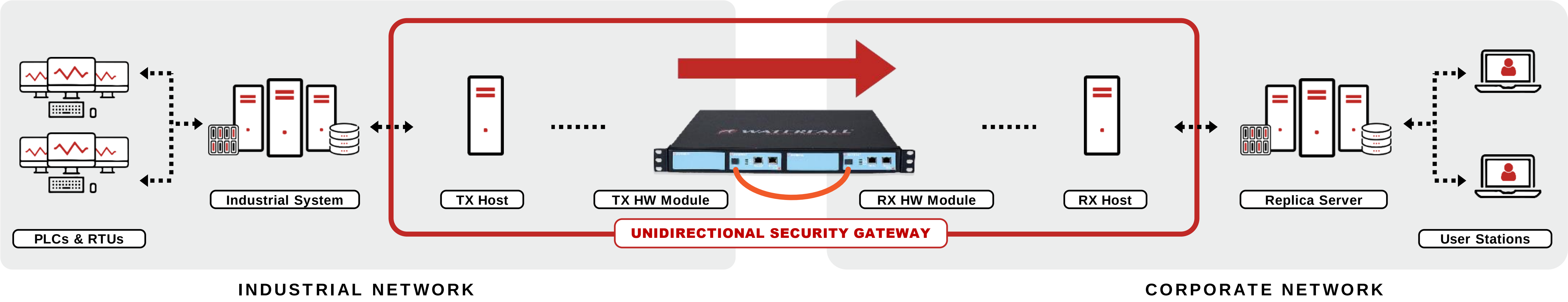
Control-critical networks are sets of ICS networks. Firewalls are used routinely within the set, but not across network criticality boundaries

TWENTY NETWORKS

#1 Database Replication	#8 Central or Cloud SOC	#15 Safety Systems
#2 Device Emulation	#9 Network Intrusion Detection Systems	#16 Continuous High-Level Control
#3 Application Replication	#10 Convenient File Transfer	#17 SCADA WAN
#4 Remote Diagnostics & Maintenance	#11 IIoT And Cloud Communications	#18 Protective Relays
#5 Emergency Maintenance	#12 Electronic Mail and Web Browsing	#19 Replicas DMZ
#6 Continuous Remote Operation	#13 Partial Replication Protecting Trade Secrets	#20 Wireless Networks
#7 Device Data Sniffing	#14 Scheduled Updates	

MOST COMMON GOAL: ENTERPRISE-WIDE VISIBILITY WITH DISCIPLINED CONTROL

Unidirectional Gateway



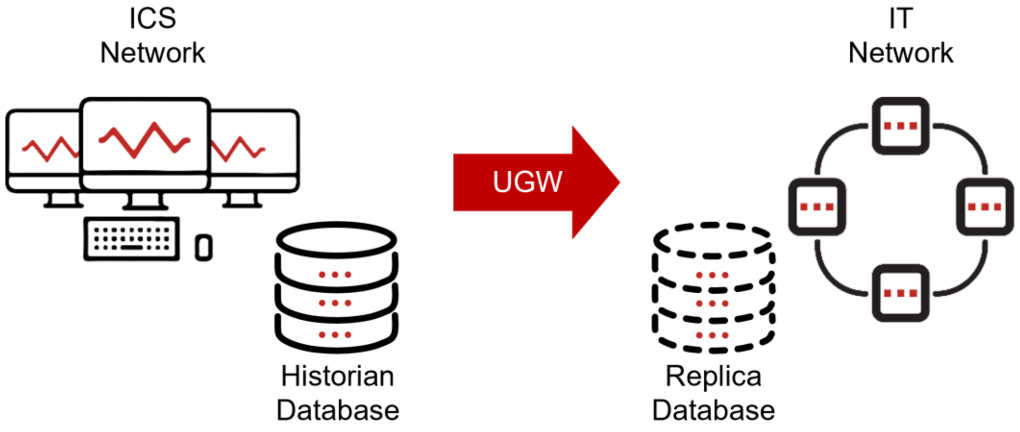
Unidirectional Security Gateways are a combination of hardware and software

- The hardware is physically able to send information in only one direction
- The software replicates servers & emulates devices from the OT network to the IT network
- IT replicas are normal participants in IT networks
- All cyber attacks are information – no attack, no matter how sophisticated, can propagate back to the industrial network through the gateway

#1 Database Replication

- SQL or historian databases are often the focus of IT/OT integration
- When replica databases develop gaps, those gaps can often be filled by a process called 'backfilling' the database. That process must be triggered manually on the ICS network, or on a timer.
- Meta-data replication is an added feature of some implementations – eliminating double data-entry

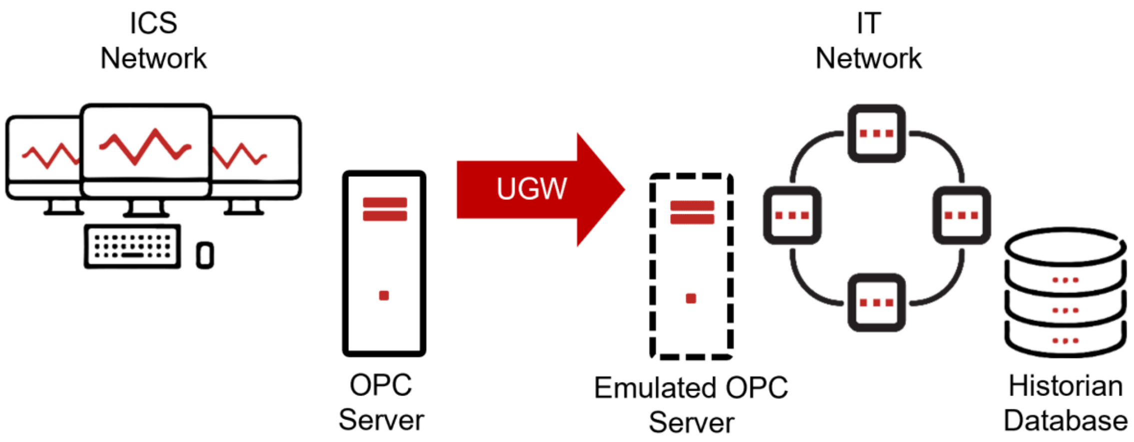
Database queries are sent by the gateway's TX host to the ICS database & by the IT client to the IT replica



#2 Device Emulation

- Replicates industrial devices such as OPC servers to IT networks – most commonly for use by enterprise historians
- Generally no ‘backfill’ function available – can only ask most industrial devices for current values, not old ones – so there is no way for the historian to ask the replica for old data
- High availability / no single point of failure designs are supported by some vendors to eliminate IT database gaps

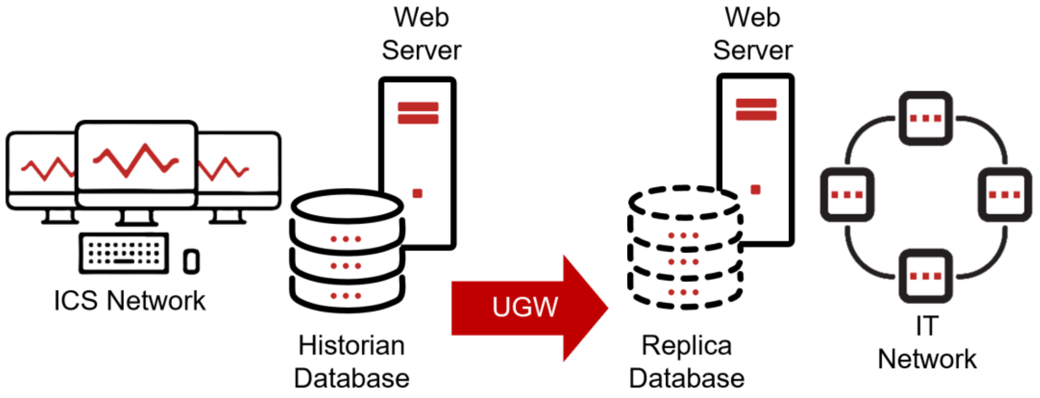
Unidirectional gateways send device state snapshots to external networks for use by emulators / replicas



#3 Application Replication

- Web applications, HMIs and other applications can be difficult to emulate
- Instead, unidirectional gateways replicate the underlying databases, devices or other data sources
- A second copy of the application on the external network uses the replica data sources and presents information to the external network as if it were the original

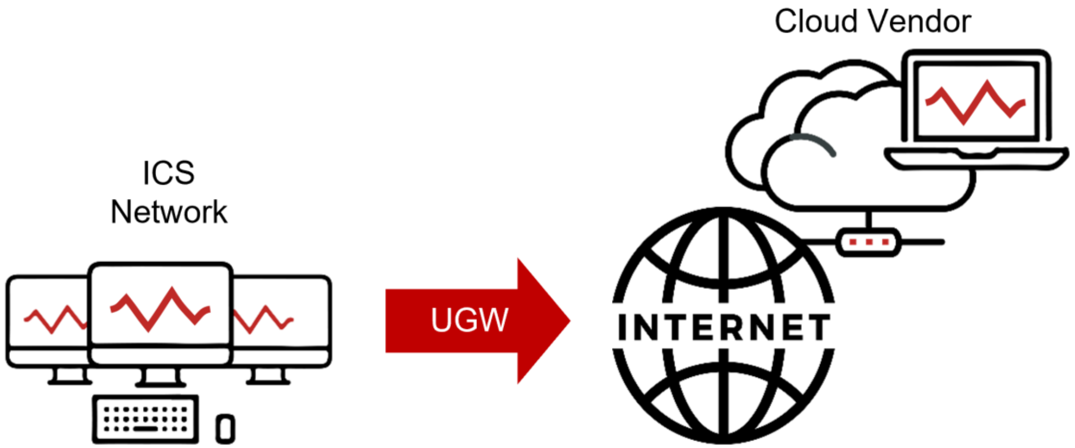
A second copy of web servers & other complex applications can easily be deployed when data sources can be replicated



#4 Remote Screen View

- Remote vendors can see the screens of workstations in control-critical networks and provide real-time advice over the phone
- Engineers at control-critical sites evaluate the advice and decide whether to apply the advice to critical equipment
- Vendors see the process as supervising the site
- Site engineers see the process as supervising the vendors

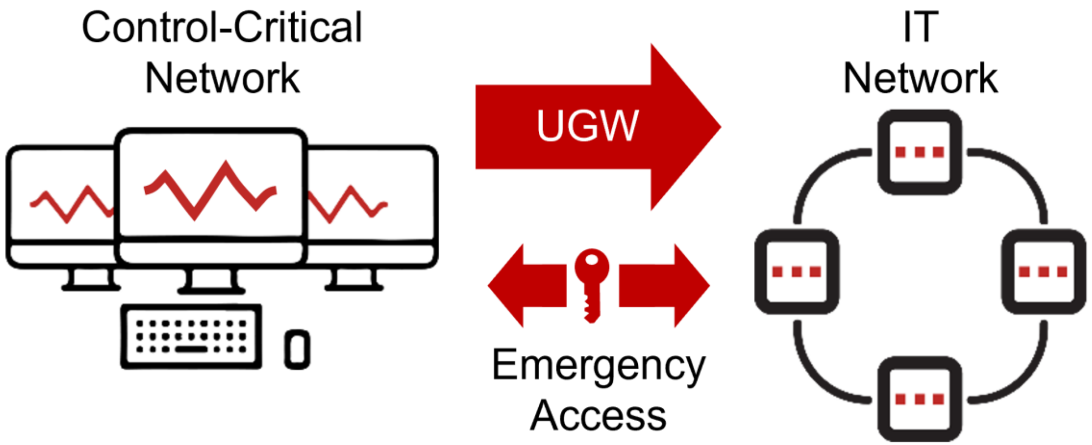
Both sets of needs are met



#5 Emergency Maintenance

- Emergency access hardware physical connects a pair of twisted-pair copper wires
- Access hardware is typically deployed in parallel with a unidirectional gateway
- A timer automatically disconnects bi-directional connectivity after a preset interval

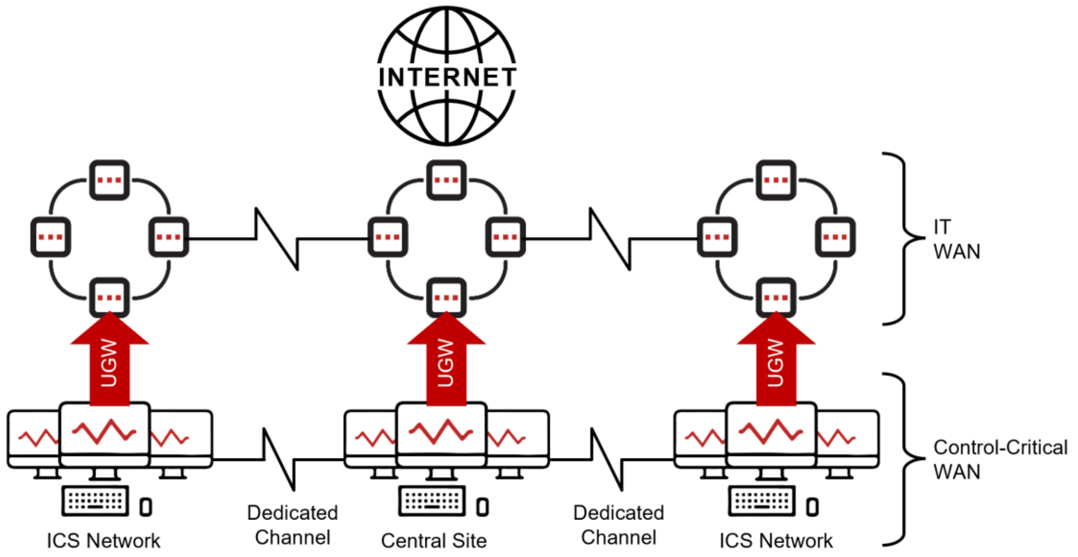
Full bi-directional remote access can be available temporarily, on a timer, in emergencies



#6 Continuous Remote Ops

- Remote operators or central support teams may need access to a control-critical network routinely, and for long periods of time
- Define a control-critical WAN, using dedicated telecommunications infrastructure such as T1, T4 or MPLS
- Models the entire WAN as control-critical, with internal, encrypting firewalls and unidirectional external connectivity

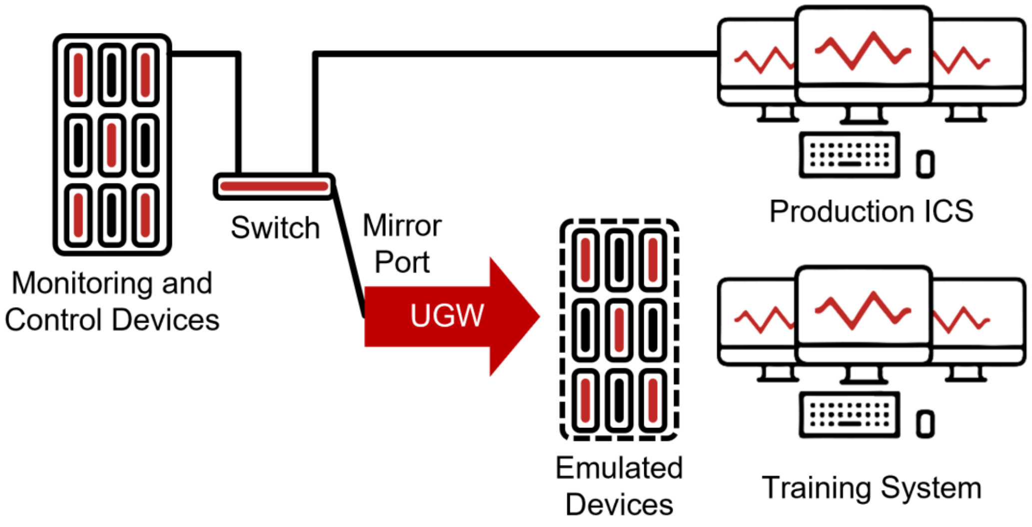
All sites must be secured as thoroughly as the most-critical site



#7 Device Data Sniffing

- Development and test networks benefit from access to live data
- Slow/costly WAN infrastructure can make dual monitoring of remote devices very costly
- Device data sniffing uses mirror port traffic – no new communications on the critical network
- The original devices are emulated to the external network based on data observed in device packets

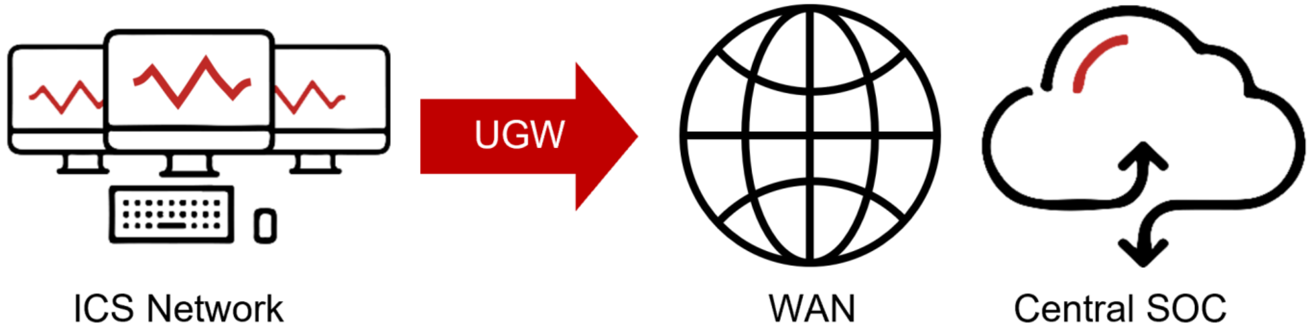
Unusual, but observed in production in a high-voltage transmission grid



#8 Cloud / Central SOC

- Most industrial enterprises have a central Security Operations Center hosted either on their IT network or in a vendor cloud
- Unidirectional gateways routinely gather data for Security Information and Event Management (SIEM) systems by replicating Syslog, SNMP and/or Windows logging

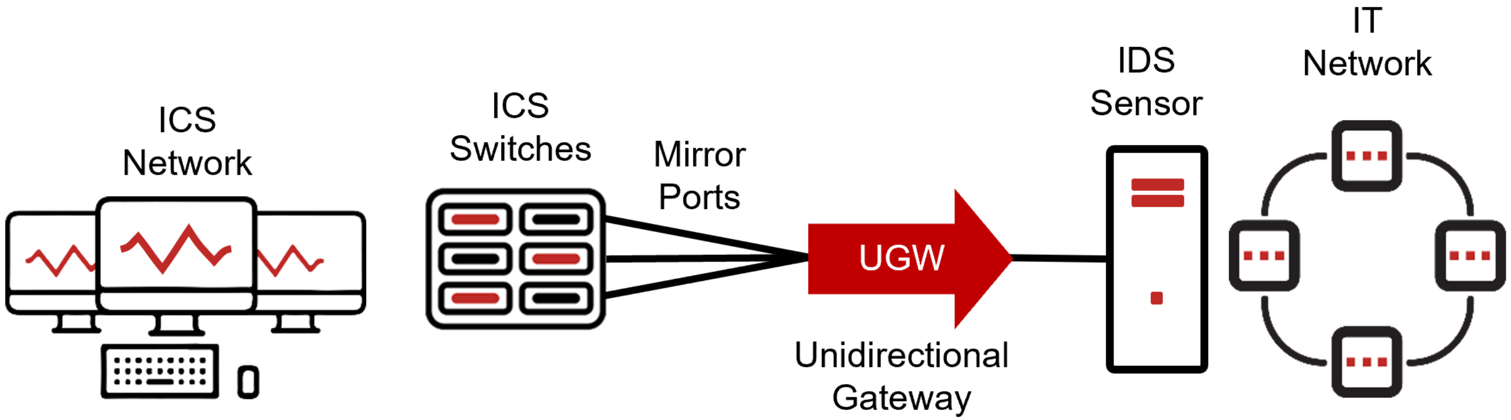
Safe, central monitoring allows enterprises to monitor and optimize industrial security



#9 Network Intrusion Detection

- Unidirectional gateways can emulate ICS SPAN and mirror ports to network intrusion detection system (IDS) sensors
- Most IDS sensors need frequent updates and adjustments to maximize sensitivity while minimizing false positives
- Unidirectional gateways permit sensors to be hosted safely on IT networks where SOC analysts can easily reach the sensors

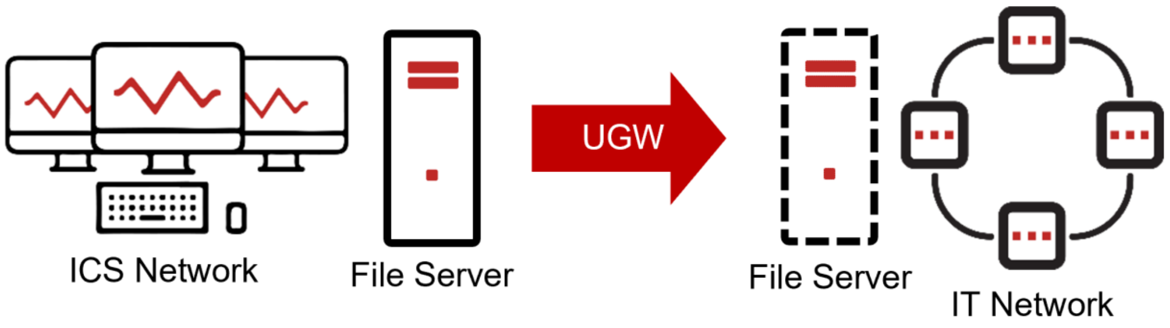
Most mirror ports are bi-directional, and those that are not, are only software unidirectional



#10 Convenient File Transfer

- Providing a mechanism for convenient file transfer is an important part of controlling removable media use
- Unidirectionally replicating file servers from critical to IT networks addresses the vast majority of ad-hoc file transfer needs

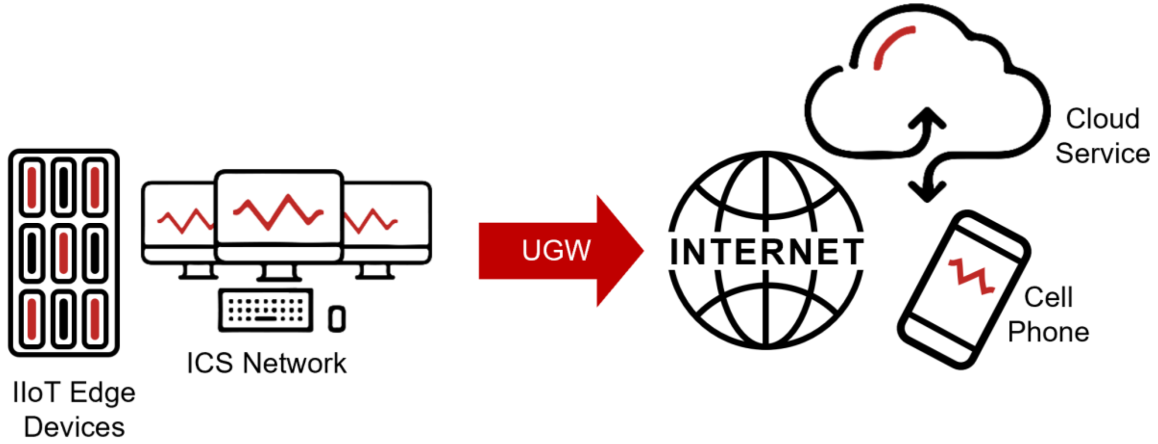
Convenient file server replication to an IT network dramatically reduces the need for removable media



#11 IIoT & Cloud Connections

- Monitor-only edge devices can be directly Internet-connected
- Unidirectional gateways can gather and translate industrial / edge device data and send it safely to cloud systems
- Edge device software updates must be via a local server
- Information/attack flows coming back from cloud services are ideally abstract enough for manual inspection for safety

Eg: Pump #37 is about to fail – send a work crew in the next 3 days.

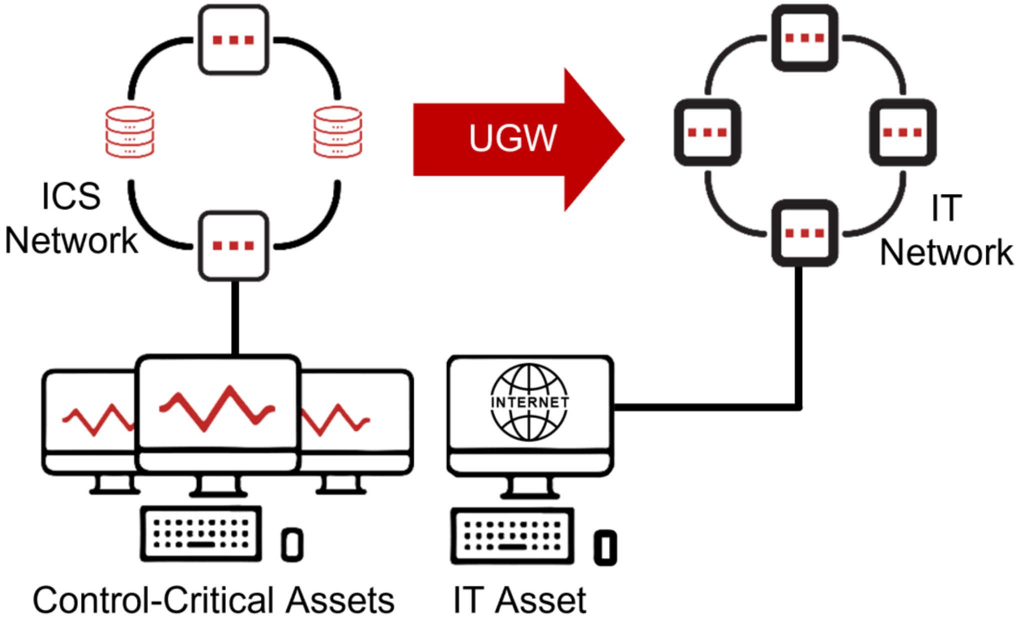


#12 Email & Web Browsing

WATERFALL
Stronger Than Firewalls

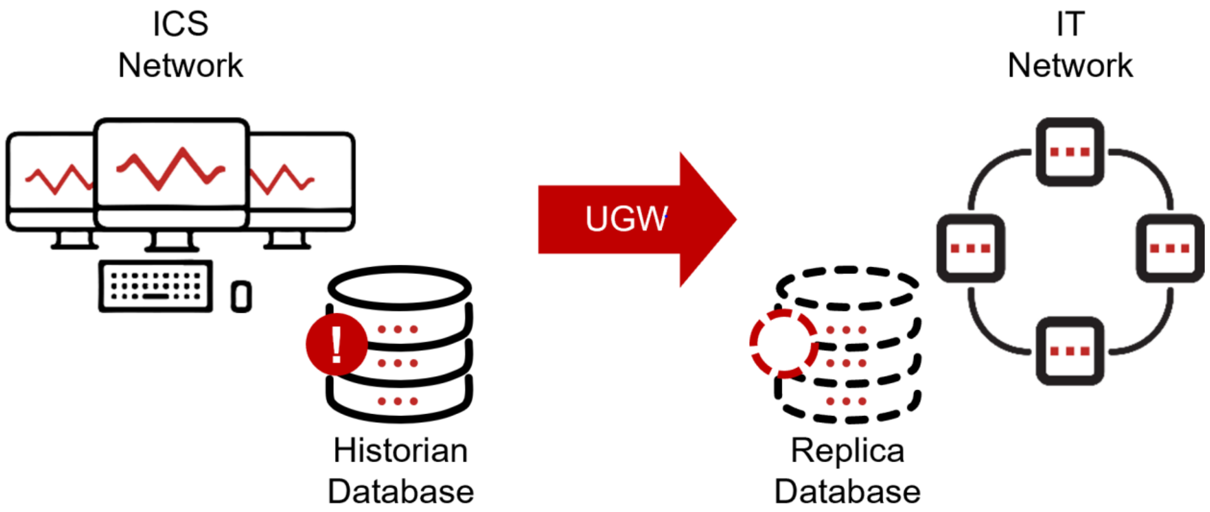
- Plant operators need email and web browsing abilities too
- SEC-OT sites enable these dangerous activities for operators and other plant personnel by deploying IT network endpoints on physical operator workstations
- Some sites deploy site-wide IT Wi-Fi networks

All equipment connecting wired or wirelessly to these extensions of IT networks are managed as IT devices – they must never connect to a critical network



#13 Partial Replication

- Industrial systems may encode trade secrets that are not to be shared with IT systems or the Internet
- Some unidirectional gateways support partial replication of databases and partial emulation of serves
- Configure the unidirectional equipment to “leave behind” trade secrets – either specify the data that can be shared, or specify what is to be left behind

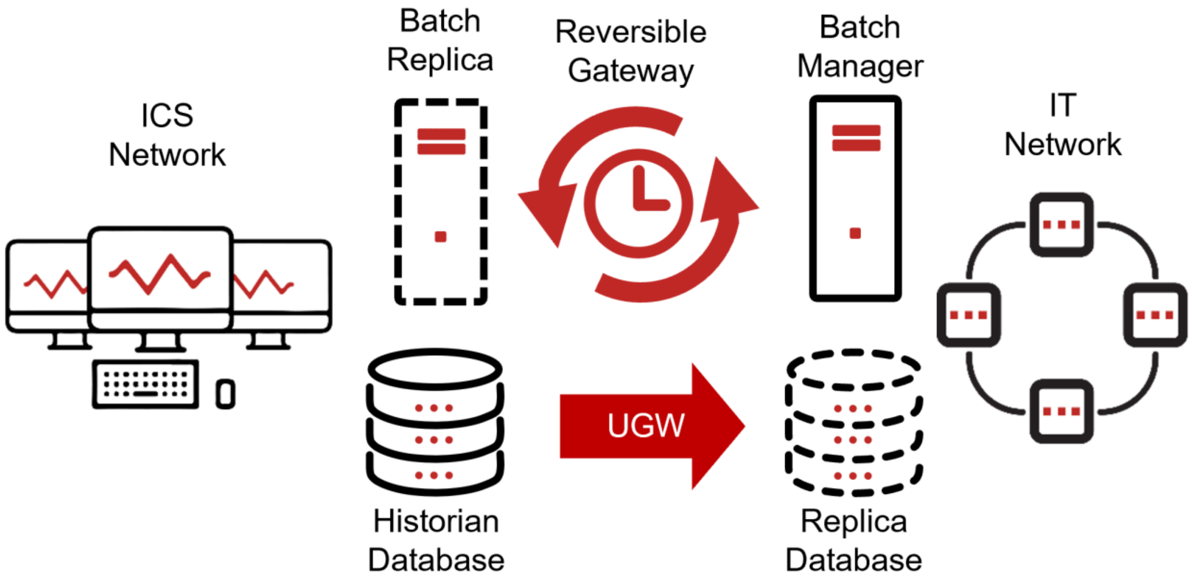


Leave trade secrets on OT networks

#14 Scheduled Updates

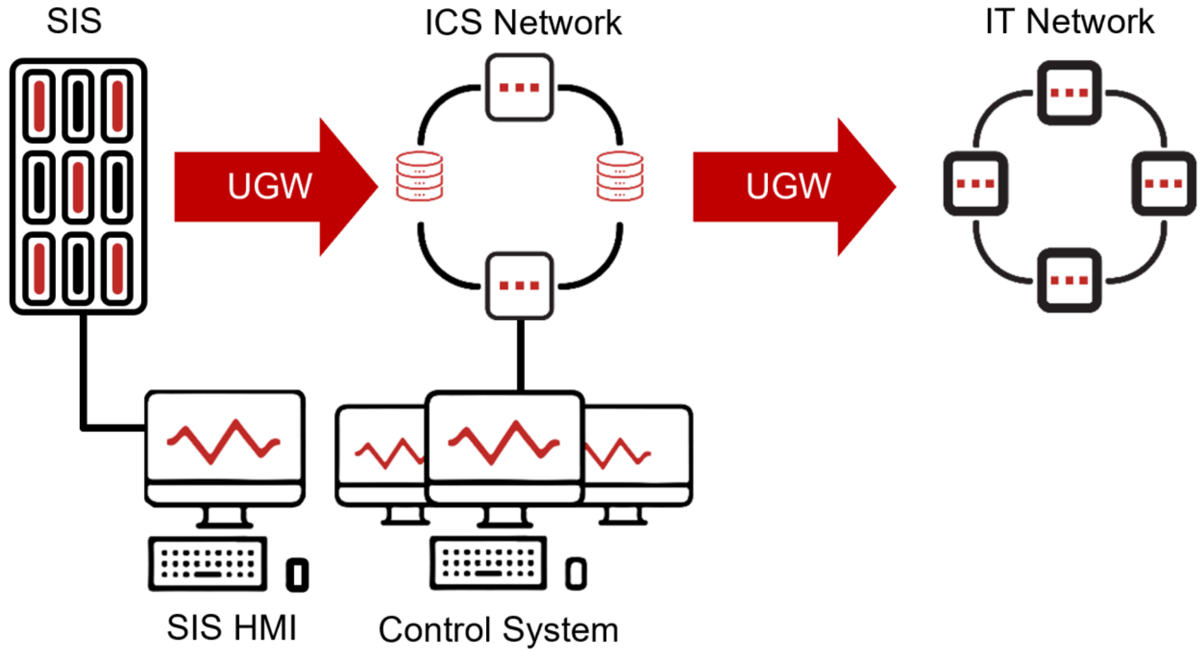
- Reversible unidirectional gateways can only send in one direction at a time and can reverse orientation periodically
- Replicate servers in either direction
- Independent replications are best – different protocols, different sub-networks
- Eg: historian out, AV back in
- Can be deployed in parallel to or instead of UGW

Reversible gateways provide disciplined, scheduled updates of OT systems



#15 Safety Systems

- Safety Instrumented Systems (SIS) are sometimes unidirectionally replicated
- Unidirectional replication allows safety system information to be integrated into the primary operator HMI
- Separately-wired safety screens give operators the ability to control or reset SIS when necessary

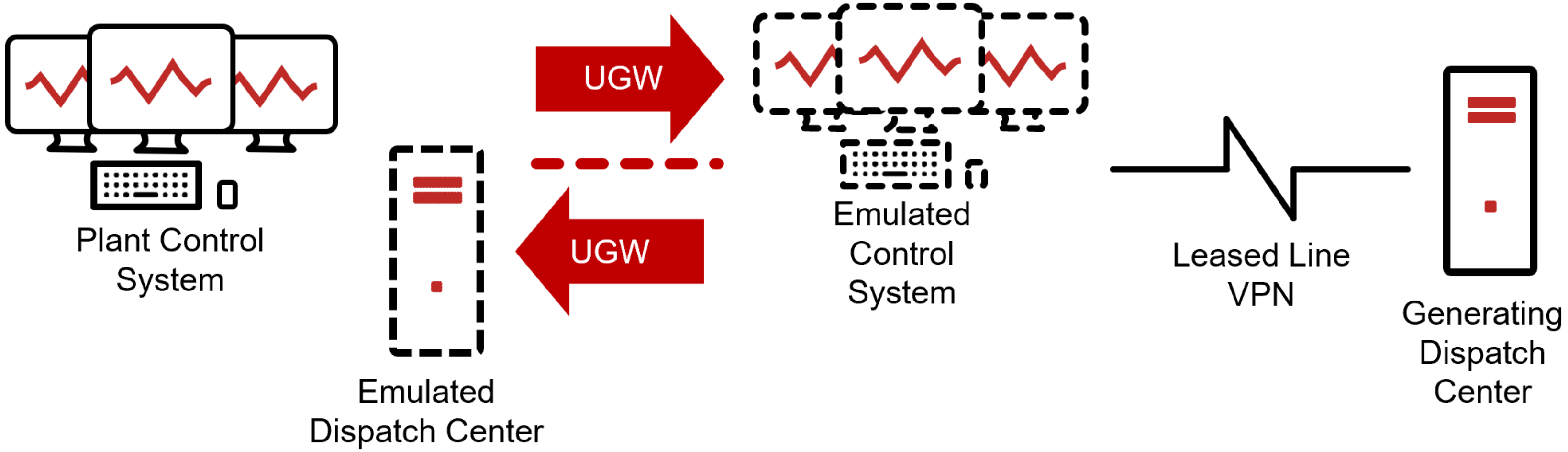


There is no safety without security

#16 Continuous Control

- Some sites require continuous, high-level control from an external authority, such as a power grid operator
- Inbound unidirectional gateways replicate those external authorities to internal systems
- Two gateways are stronger than firewalls – compromise through a firewall is one step, through an inbound gateway is 3 steps minimum, the last two of which are "blind"

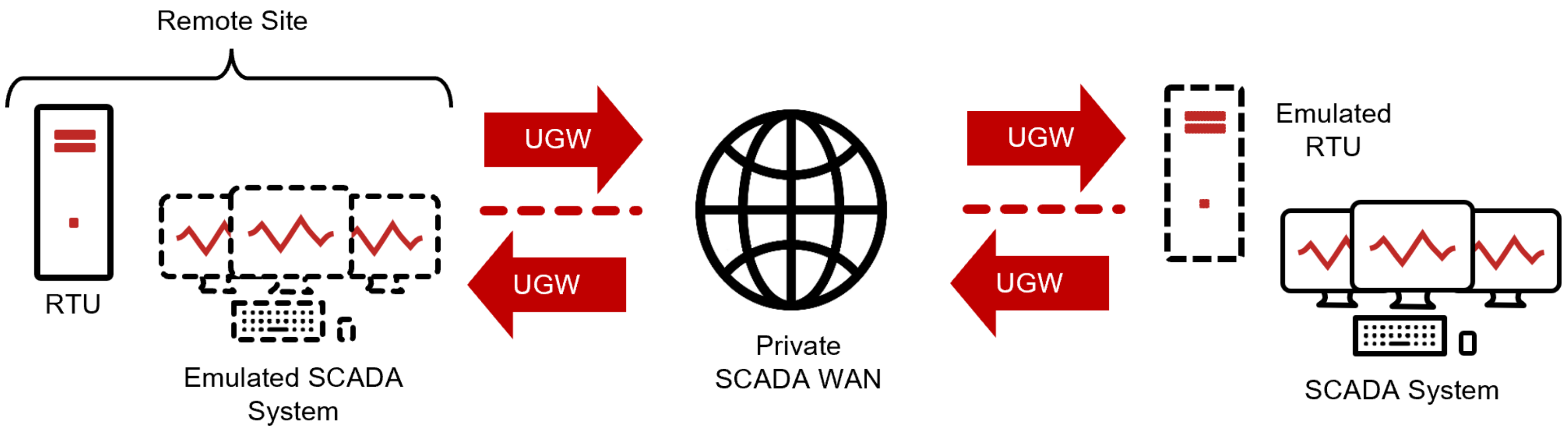
Compromise is only practical with insider help



#17 SCADA WAN

- Wide Area Networks (WAN) are intrinsic to power grids, water systems and pipelines
- WAN connections are often seen as high risk because elements of the WAN exist outside of any physical security perimeter
- Unidirectional gateways protect the central SCADA perimeter, as well as the perimeter of remote substations & pumping stns

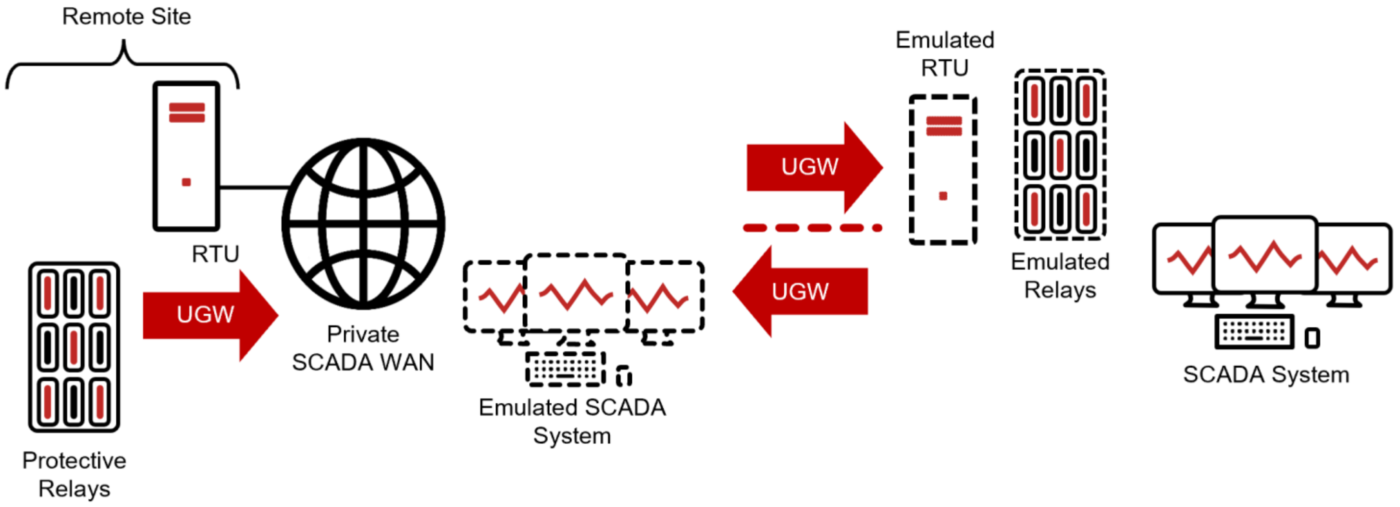
WAN visibility with disciplined control



#18 Protective Relays

- Protective relays improve “resilience” by preventing damage to physical equipment
- Protecting the relays is often seen as a higher priority than preventing shutdowns – shutdowns impair production for hours, equipment damage for weeks or months
- Unidirectional protection for relays lets engineers see what caused “trip” conditions without risk to relays

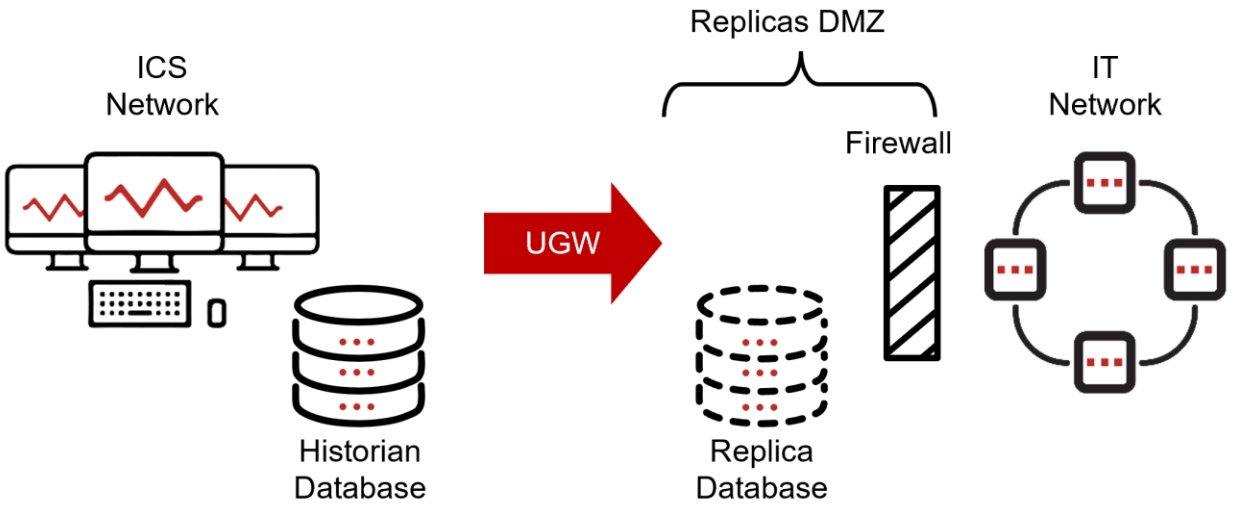
Protecting the protection equipment can be higher priority than protecting the process



#19 Replicas DMZ

- SEC-OT protects continuous, correct and efficient operations, while IT-SEC protects the information
- OT information is sent to IT networks because the information has value – often a lot of value
- Replica servers are often deployed on an IT-SEC DMZ to protect OT information being shared with IT

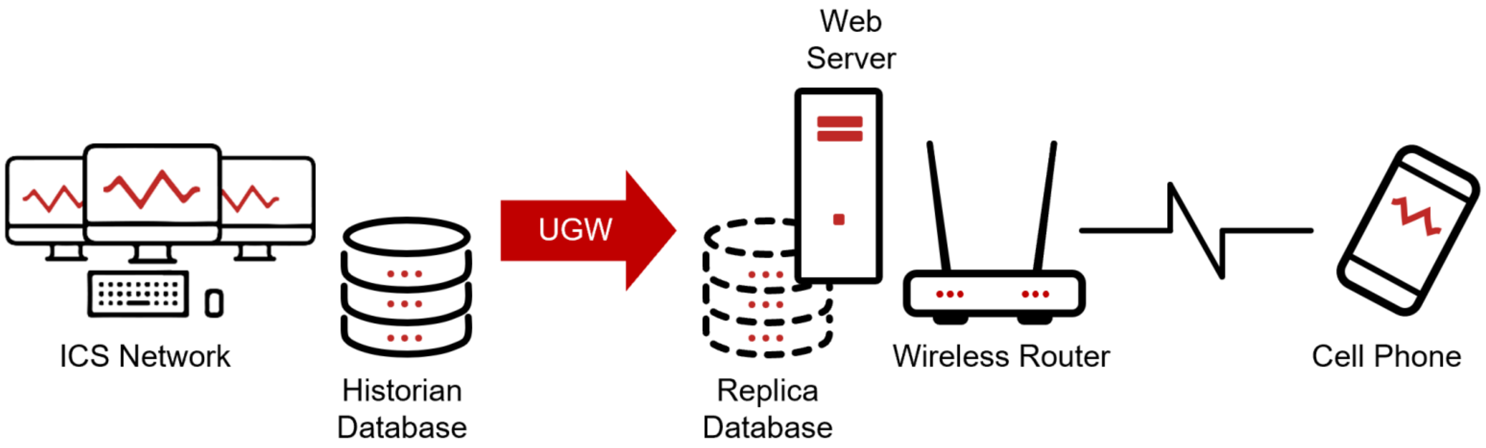
SEC-OT experts protect operations while IT-SEC exports protect information that reaches IT networks



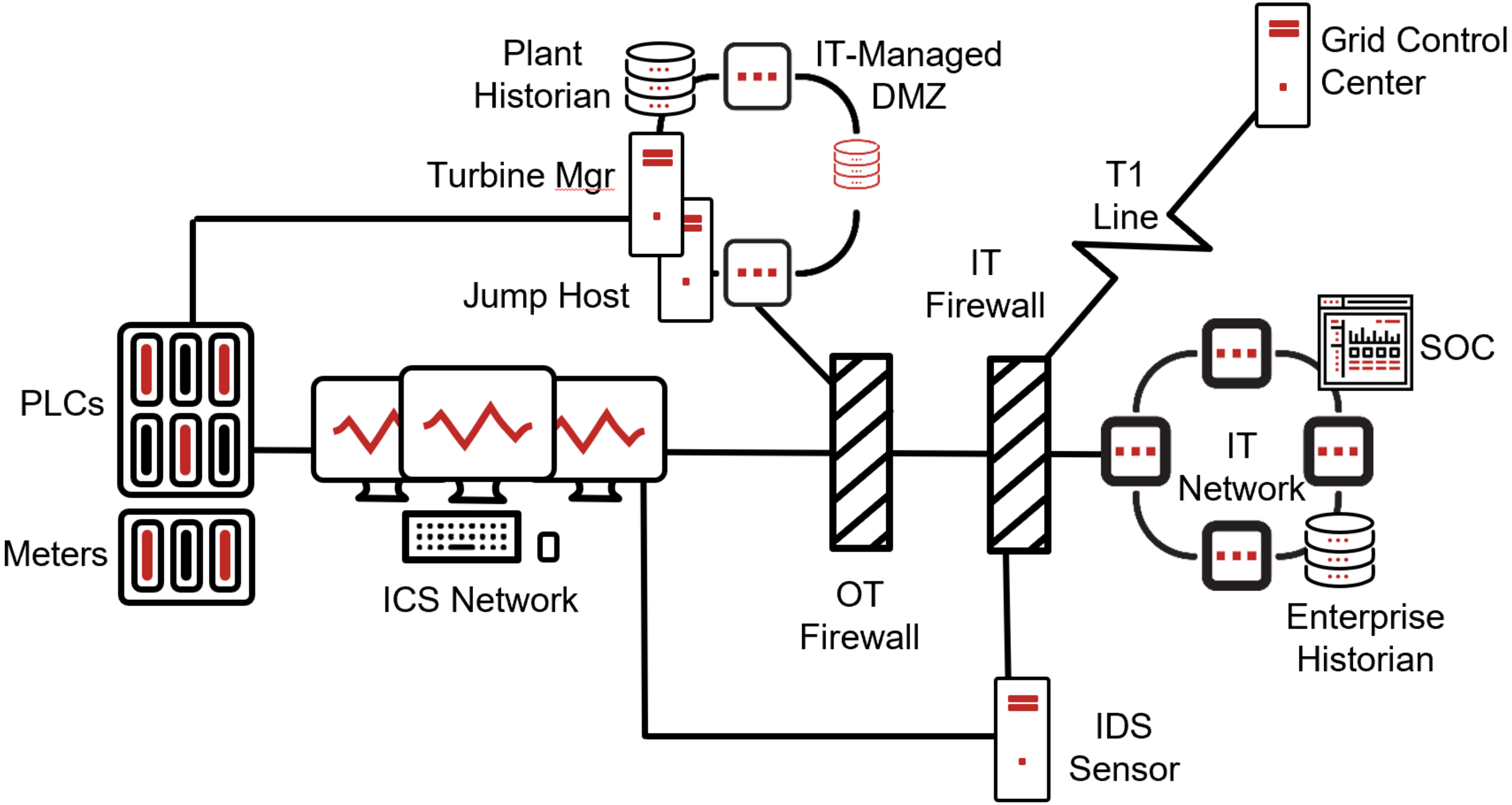
#20 Wireless Networks

- Wireless networks are intrinsically vulnerable to attacks from outside of physical perimeters
- Cell phones are walking wireless attack vectors
- Unidirectional replication of information to wireless networks helps to protect industrial networks
- Sophisticated attackers can still tamper with physical operations “through the brains” of ICS insiders

SEC-OT people are deeply suspicious of wireless networks



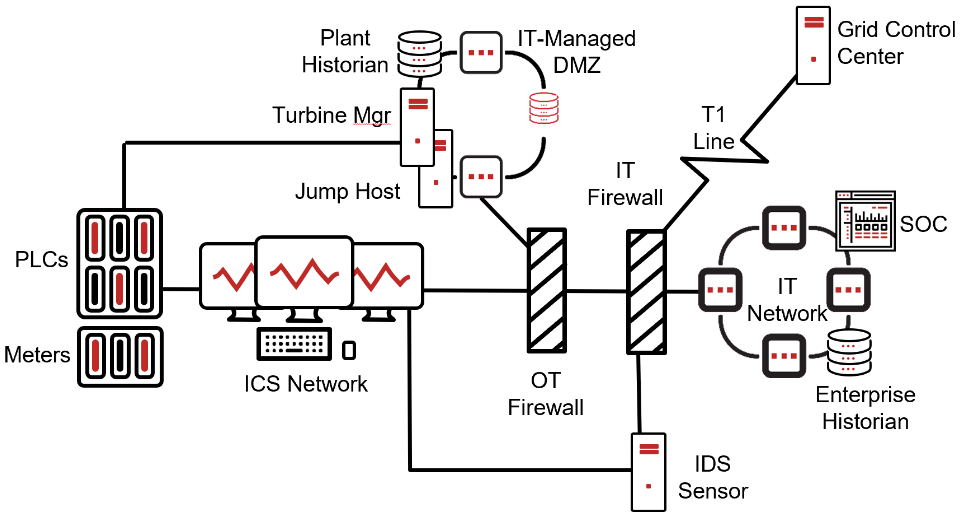
Power Plant Example - Original



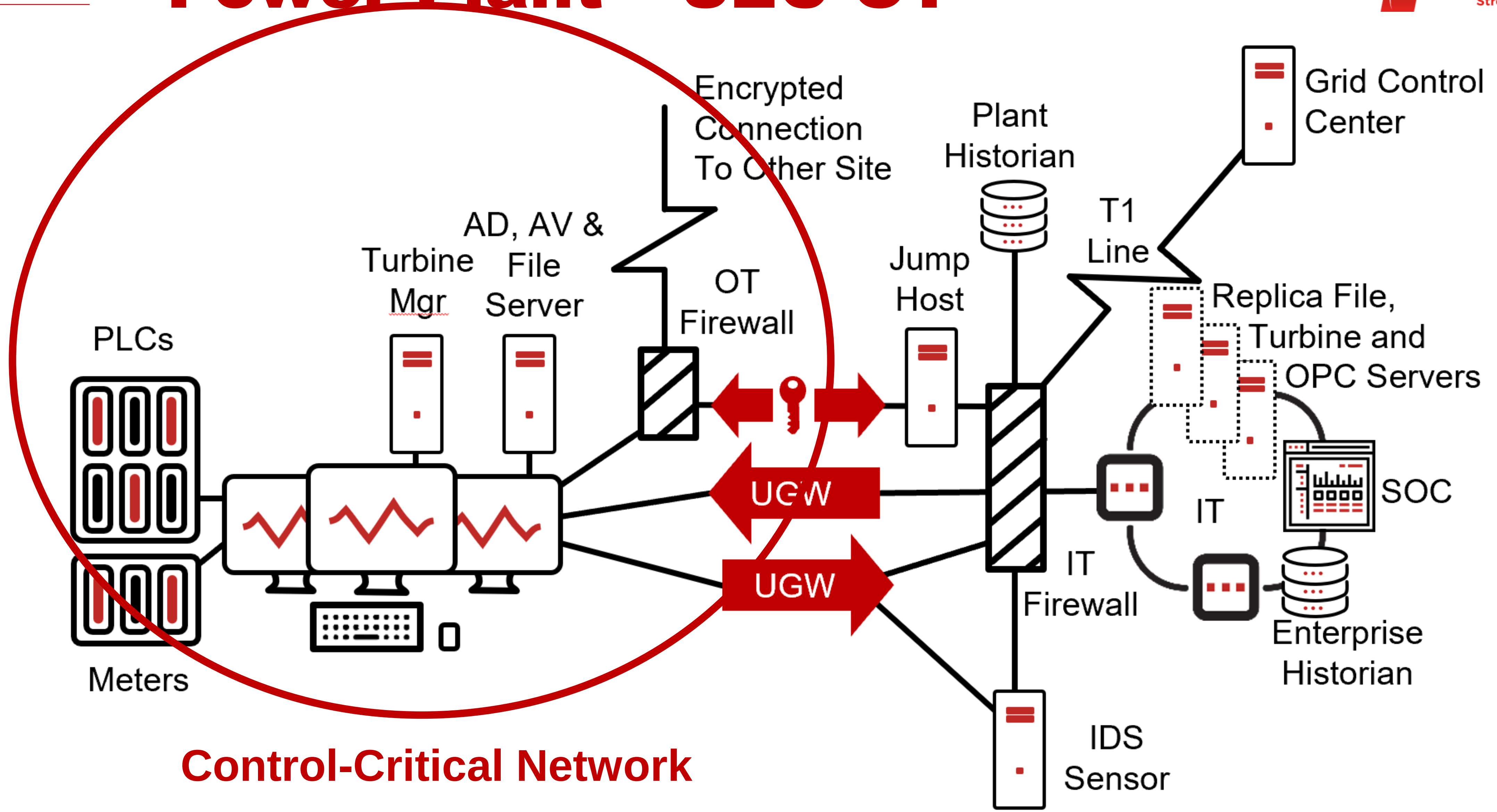
Power Plant Example – Original

- Two plants – large one & small one – operator at large plant operates small plant off-hours - remote control routed via IT WAN
- OT group responsible for ICS & OT firewall
- IT group responsible for IT & ICS DMZ - coordination issues
- Dual-ported hosts bypass one or more layers of firewalls
- Inconsistent application of security updates, AV, AD & other common security controls

Security program update focus: online attack threats



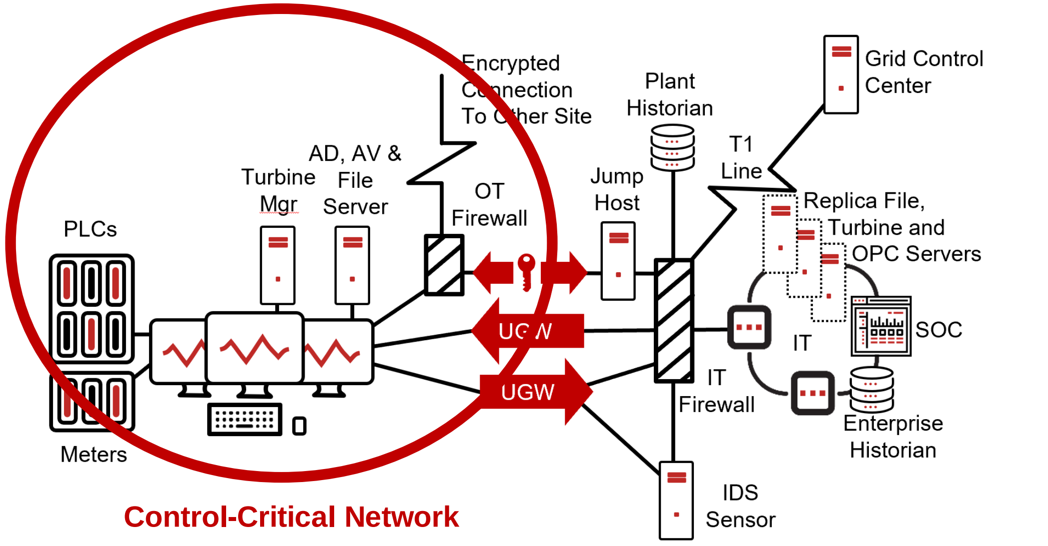
Power Plant – SEC-OT



Power Plant – SEC-OT

- Control-critical WAN includes private comms to small plant
- All control-critical equipment is managed as SEC-OT – unidirectional gateway replicates OPC, turbine servers & others to IT network
- Bypass unit enables remote access – temporarily bi-directional
- Inbound gateway replicates AV & grid control center to ICS
- Mirror / SPAN ports replicated to IT-resident IDS

All segments of control-critical WAN are managed as SEC-OT



SEC-OT Security Updates

- All SEC-OT sites have security update programs
- SEC-OT sites update equipment more frequently if the equipment is not critical to second-by-second control
- Sites with mature SEC-OT programs can afford to update critical equipment less frequently

The desire to simultaneously reduce security update program risks and costs is a strong driver towards deploying comprehensive SEC-OT practices.

SEC-OT Anti-Malware Programs

- In spite of the limitations of anti-malware systems, SEC-OT sites deploy such systems as universally as possible.
- Anti-malware systems are particularly important on any equipment whose removable media ports could not be physically disabled

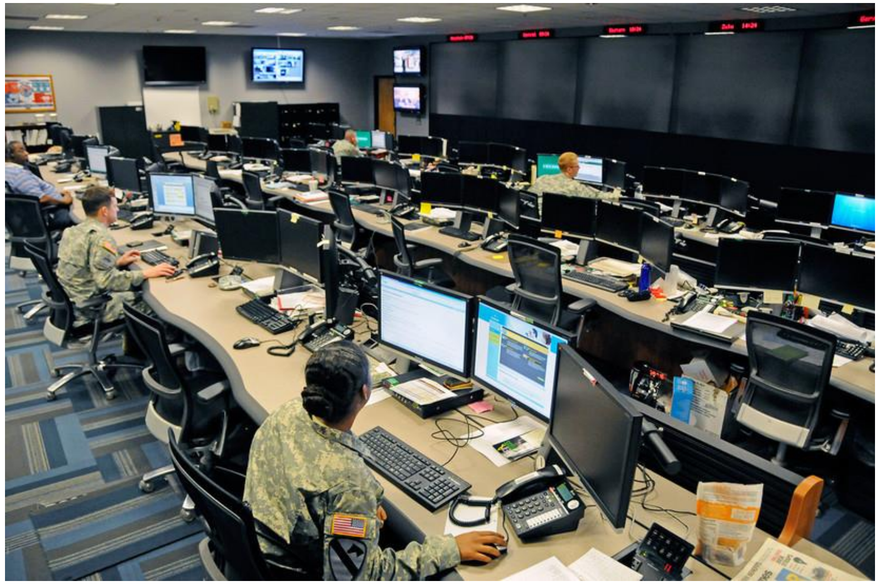
Exemptions to this policy are generally granted only for the most sensitive real-time components and components whose vendors do not yet support any kind of anti-malware

SEC-OT Security Monitoring

WATERFALL
Stronger Than Firewalls

- Security monitoring is an important addition to the strong preventive posture of the SEC-OT discipline
- Mature SEC-OT sites unidirectionally monitor their control-critical networks from central or cloud SOCs
- Security monitoring is fundamental to SEC-OT test beds and near-miss programs

We can only optimize what we measure. We must monitor and measure the security of our industrial sites.



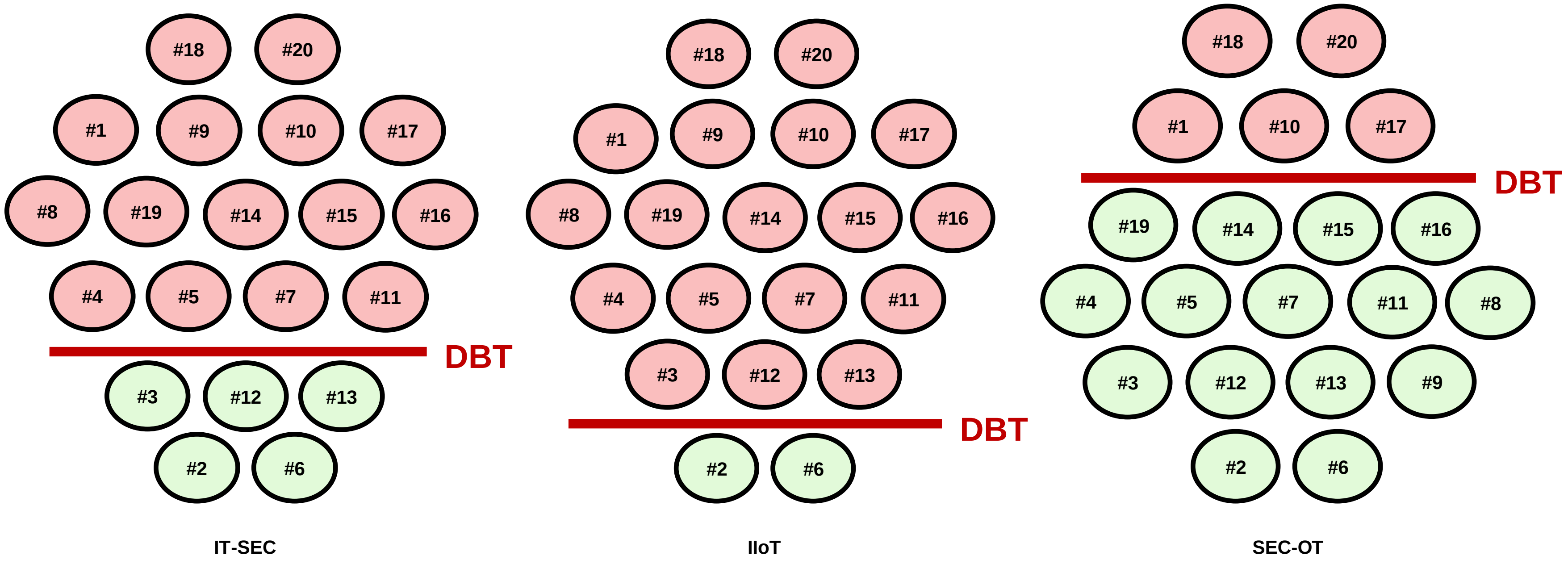
TOP 20 ICS CYBER ATTACKS

The Top 20 Cyberattacks on Industrial Control Systems			
ICS Insider	Ukrainian Attack	Hijacked Two-Factor	Vendor Back Door
IT Insider	Sophisticated Ukrainian Attack	IIoT Pivot	Stuxnet
Common Ransomware	Market Manipulation	Malicious Outsourcing	Hardware Supply Chain
Targeted Ransomware	Sophisticated Market Manipulation	Compromised Vendor Website	Nation-State Crypto Compromise
Zero-Day Ransomware	Cell Phone Wi-Fi	Compromised Remote Site	Sophisticated ICS Insider

Risk assessments focus on attack capabilities, not vulnerabilities

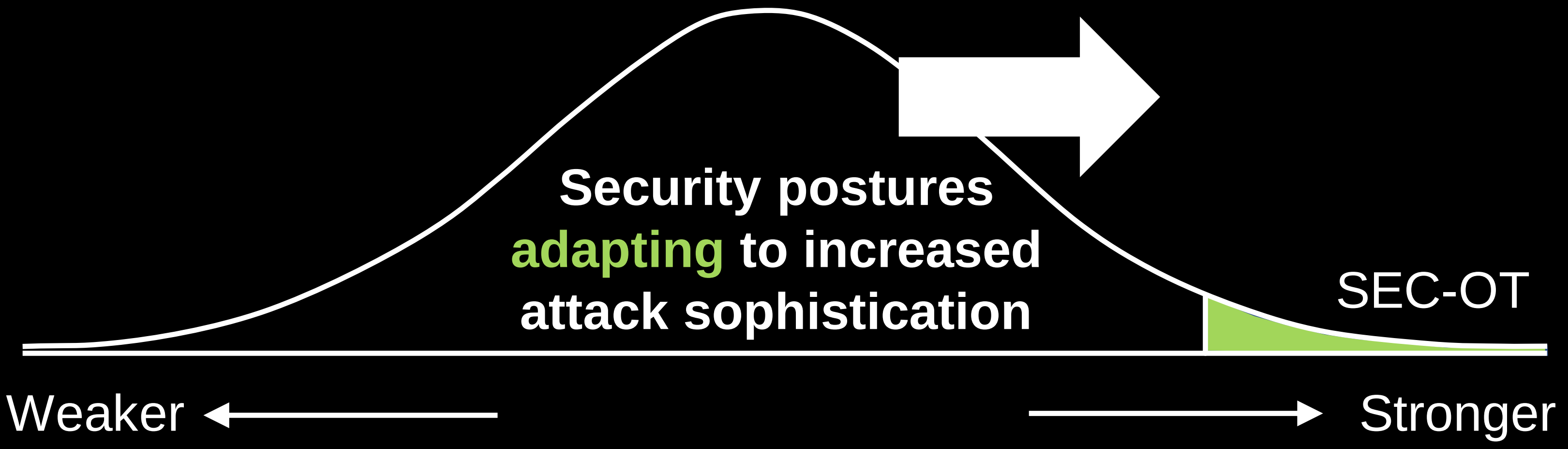
Cyber Design Basis Threat

- Cyber DBT = line between set of attacks defeated reliably and those not so defeated
- There are always attacks not defeated & there is always a simplest such attack



SECURE OPERATIONS TECHNOLOGY

- **Thorough** – address all attack vectors – offline and online
- **Robust** – physical & hardware protections, not just software
- **Disciplined** – not waiting on “edge of seat” for actionable intel
- **Futureproof** – cyber attacks will always be information



andrew.ginter@waterfall-security.com

Summary

- Sophisticated LFHI attacks are most likely to pose existential threats to electric utilities
- Physical protections are the most robust – governments cannot respond quickly enough to sophisticated attacks
- Preventing attacks is important to assure reliable infrastructure, recovering is important for resilience

More information: Industrial Security Podcast, visit WF booth for free book, follow us on Twitter, LinkedIn & Facebook & sign up for our newsletter:

WATERFALL® Stronger Than Firewalls

waterfall-security.com

Industrial Security Podcast

Secure Operations Technology