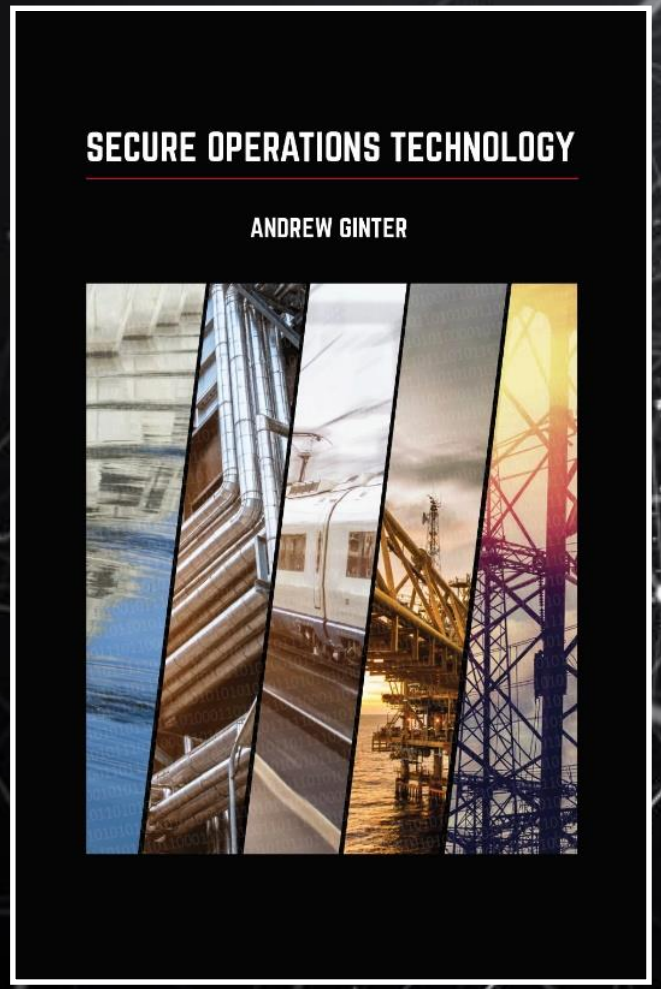
WATERFALL®
Stronger Than Firewalls

Advanced Cyber Security

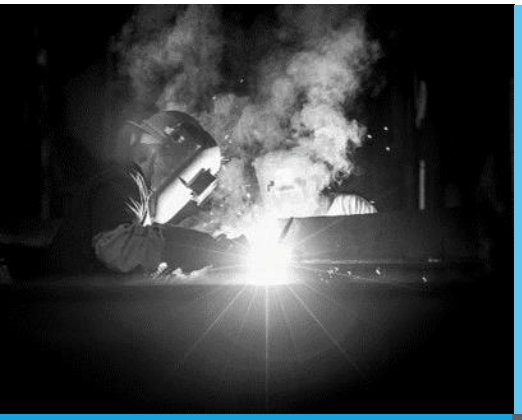
Andrew Ginter

VP Industrial Security
Waterfall Security Solutions



About Waterfall

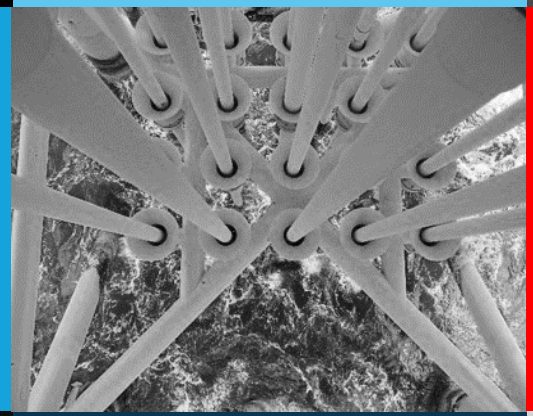
WATERFALL®
Stronger Than Firewalls



Founded in 2007

1000+ sites worldwide

Headquarters in Israel



Deployed in all critical infrastructure sectors

Sales & operations in the USA, EU & APAC

Multiple registered US patents

Technology & sales collaboration with global partners

Industrial Cybersecurity

WATERFALL®
Stronger Than Firewalls

Priorities:

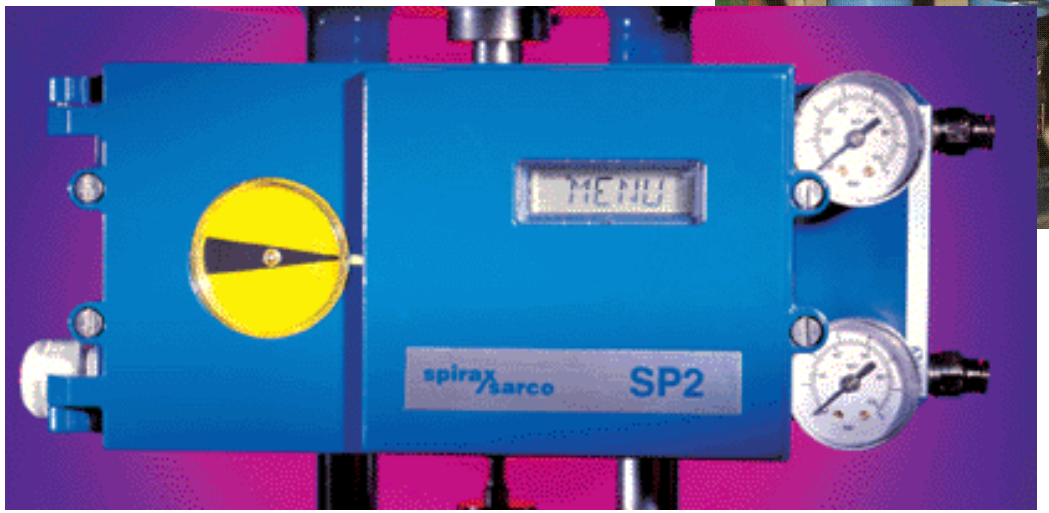
- Safe physical operations
- Reliable operations
  - Continuous
  - Correct
  - No equipment damage

At many sites, security programs are part of safety programs

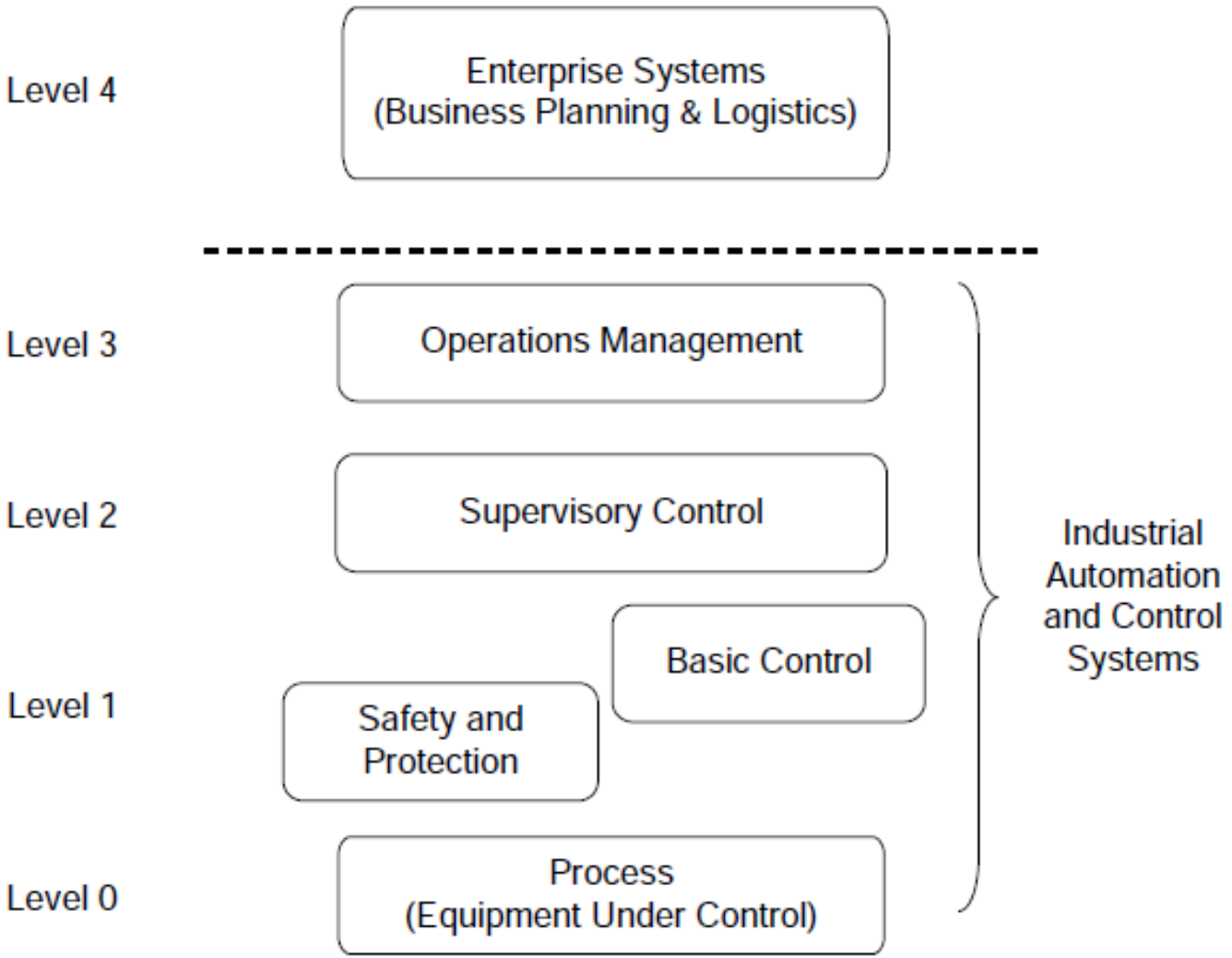
Human-Machine Interface (HMI)

WATERFALL®
Stronger Than Firewalls

Controllers & Sensors



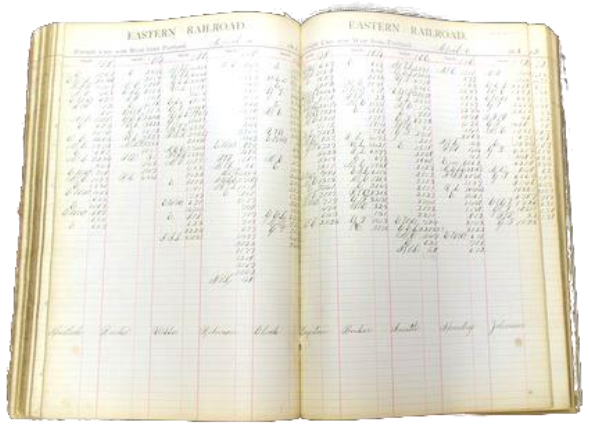
ISA SP99 (Purdue) Model



Data vs Monitoring vs Control

- 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

The First Three Laws

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

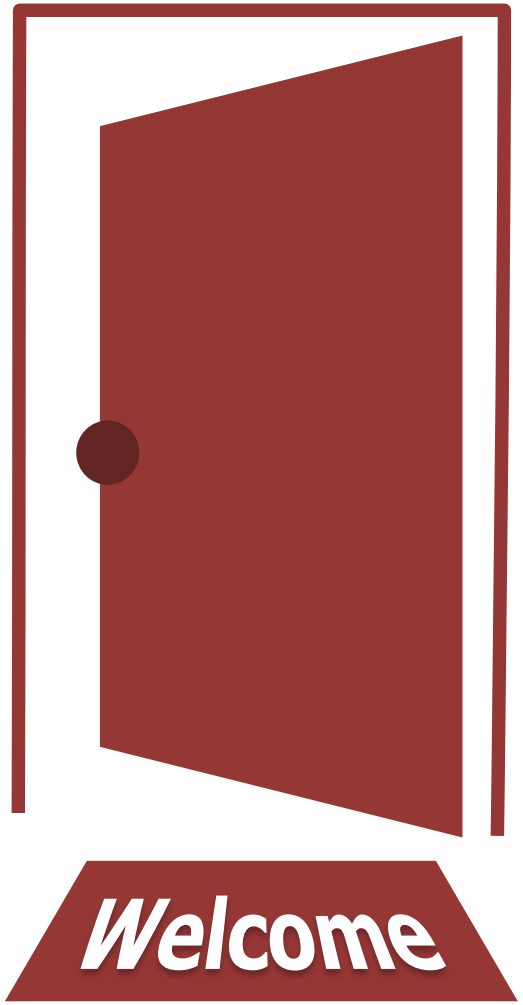
In the worst case a compromised CPU will issue every unsafe instruction to the physical process that the CPU is physically able to issue

Modern Attacks - Permissions

WATERFALL
Stronger Than Firewalls

- 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?



Threat Actors

Threat	Resources	Methods	Examples
Nation-states – military grade	Nearly unlimited	Autonomous, Targeted Malware	Stuxnet, Shamoon(?)
Intelligence Agencies	Professional	Remote control, exploit vulnerabilities	Triton, BlackEnergy
Hacktivists	Skilled Amateur	Remote control, exploit permissions	Anonymous, Ukraine(?)
Disgruntled ICS Insiders	Amateur	Exploit permissions	Maroochy
Organized Crime	Professional	Indiscriminate malware exploits vulns	Zeus, ransomware
Corporate insiders	Amateur	Exploit permissions	Fake vendor fraud

Defense In Depth

WATERFALL
Stronger Than Firewalls

- Start with HFLI attacks – firewalls, AV, patch programs
- Insiders: background checks, detailed auditing - deterrence
- IDS cost: false alarms
- IDS takes average 2-3 months while attacker has remote control
- Data exfiltration prevention does not detect sabotage

Can't restore equipment & human lives "from backups"

Threat	Defense	Cost	Eff
Nation-State Military	Escalate to national agencies	n/a	
Intelligence Agencies	IDS / Exfiltration prevention	$$$$	Poor
Hacktivists	Intrusion detection systems	$$$$	Fair
ICS Insiders	Physical security, detailed auditing	$$	Good
Organized Crime	Encryption, AV, security updates	$$$	Good
Corporate Insiders	Firewalls, role-based permissions	$	Fair

SECURE OPERATIONS TECHNOLOGY

IT-SEC:

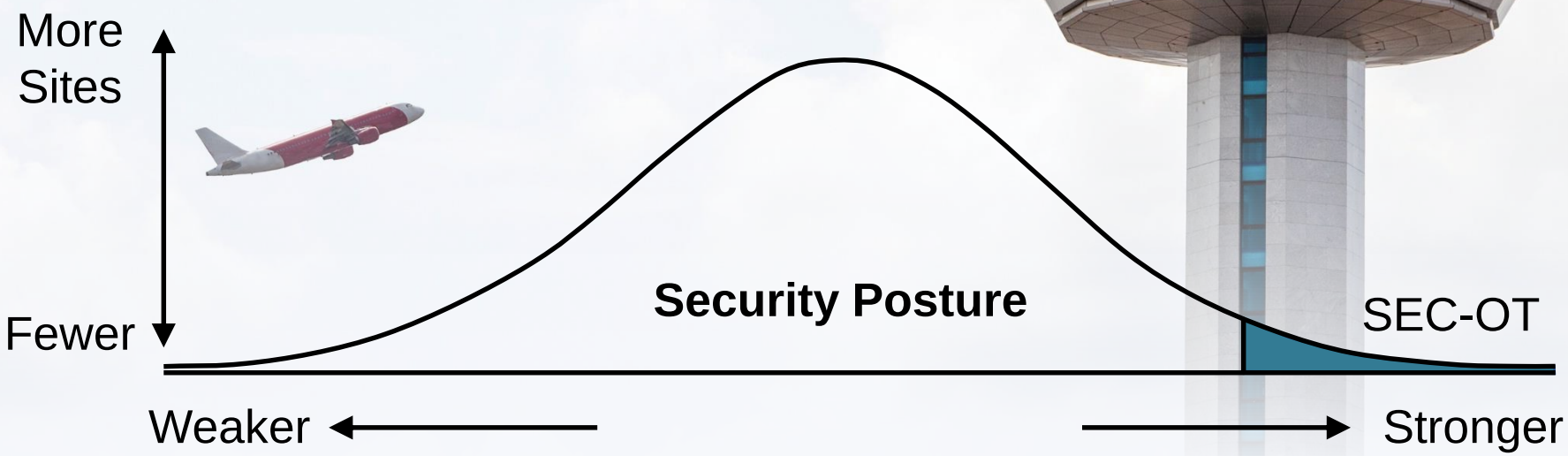
protect the information

SEC-OT :

protect physical operations *from* the information

CONTROVERSIAL?

SEC-OT describes what thoroughly-secured sites *already do*



Classifying Networks

- NERC CIP examples:
  - Low Impact: compromise impairs < 1500 MW supply
  - Medium Impact: impairs >= 1500 MW power plant
  - High Impact: grid control centers & balancing authorities
- French ANSSI examples:
  - Class 1 – IT, washing machine factory
    Class 2 – water plant for ½ million
    Class 3 – railway switching system
- German BSI – critical = impacts ½ million

Criticality is determined by worst-case consequences of compromise

ALL SOFTWARE CAN BE HACKED

- All information flows are attack vectors
- Focus on physical, not software protection, against cyber attacks

Control-Critical Networks

- Industrial networks ***important*** to business – not to society – eg: washing machine manufacturer
- Networks capable of ***controlling*** physical operations, or influencing the control of such operations
- Networks where worst-case physical ***consequences*** of compromise are unacceptable
- Most common focus: lost production

Most commonly – networks vital to continuous, correct and efficient control of physical operations

Photo credit: shannonpatrick17 / CC BY-SA 2.0

WATERFALL
Stronger Than Firewalls

ONLINE & OFFLINE PERIMETERS

- Critical network = a set of ICS networks
- There are always perimeters around important industrial sites and networks

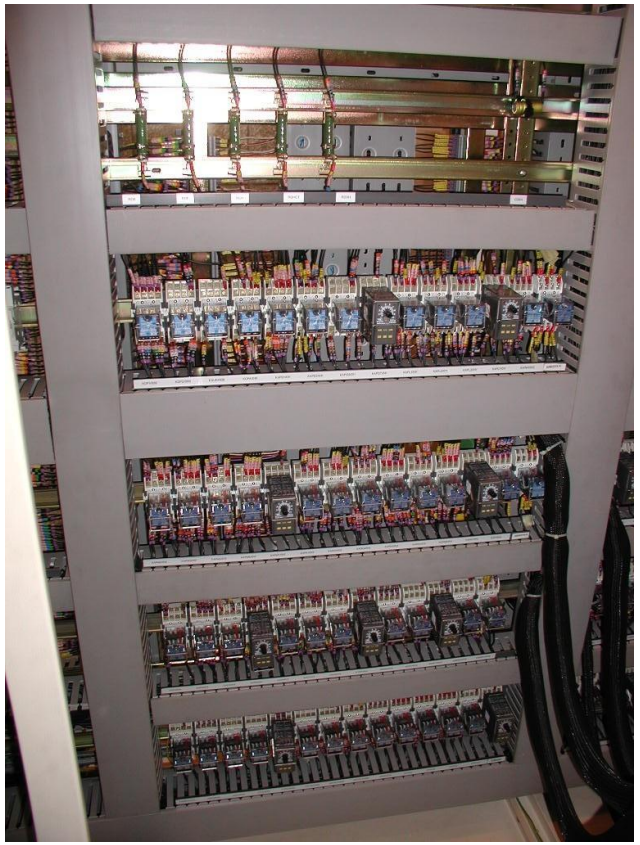
OFFLINE CONTROLS

- 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

WHAT'S NEW

Near-miss protocol for information incidents

Photo credit: Tony Hisgett / CC BY-SA 2.0

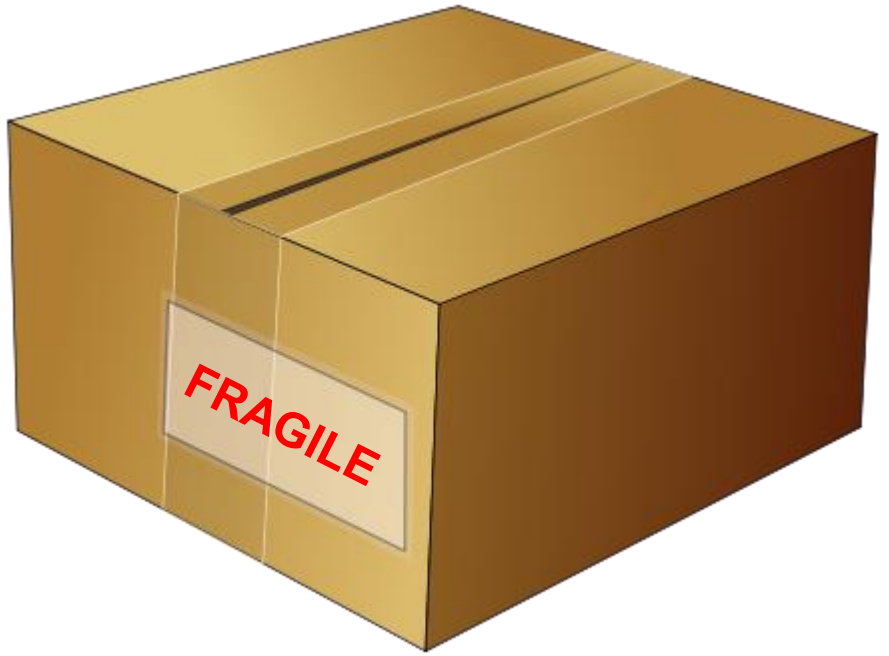
Removable Devices

- 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

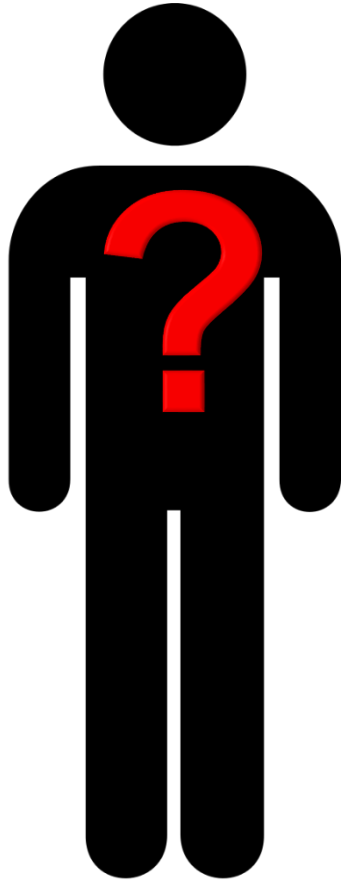
- Brand new cyber assets contain information/attacks as well
- Deploy first on test bed and test for security and other threats
- Buy “consumables” at random – reduces risk of targeted attacks
- Inspect where practical
- Contracts include penalties if unexpected hardware is included in shipments
- Label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

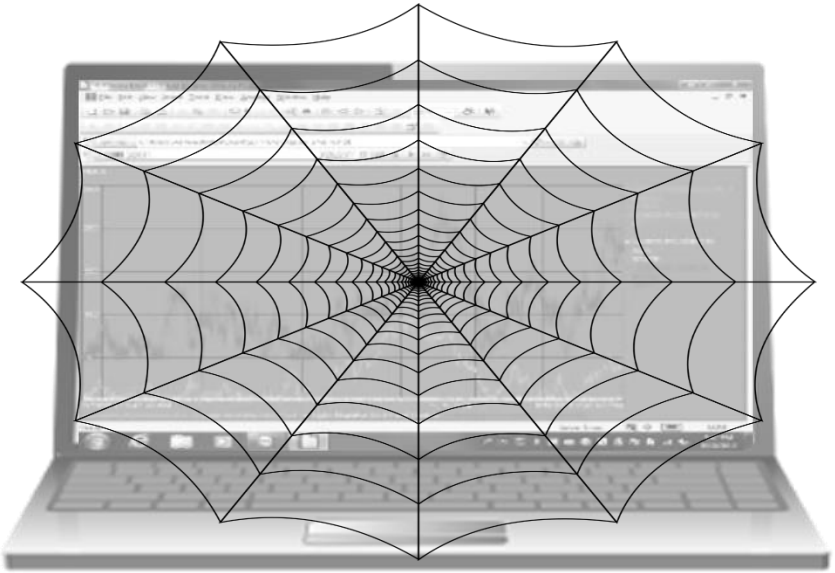
Deceived Insiders

- 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 priviledge
- 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

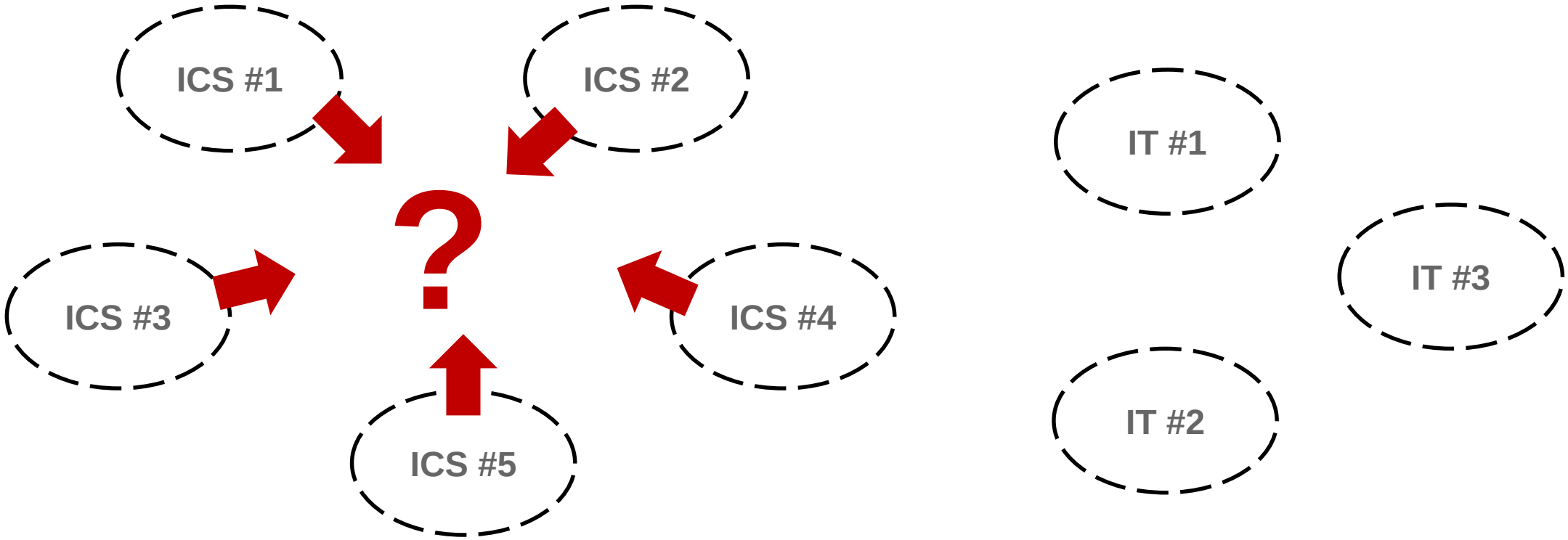
ONLINE CONTROLS

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

Use firewalls for internal ICS segmentation

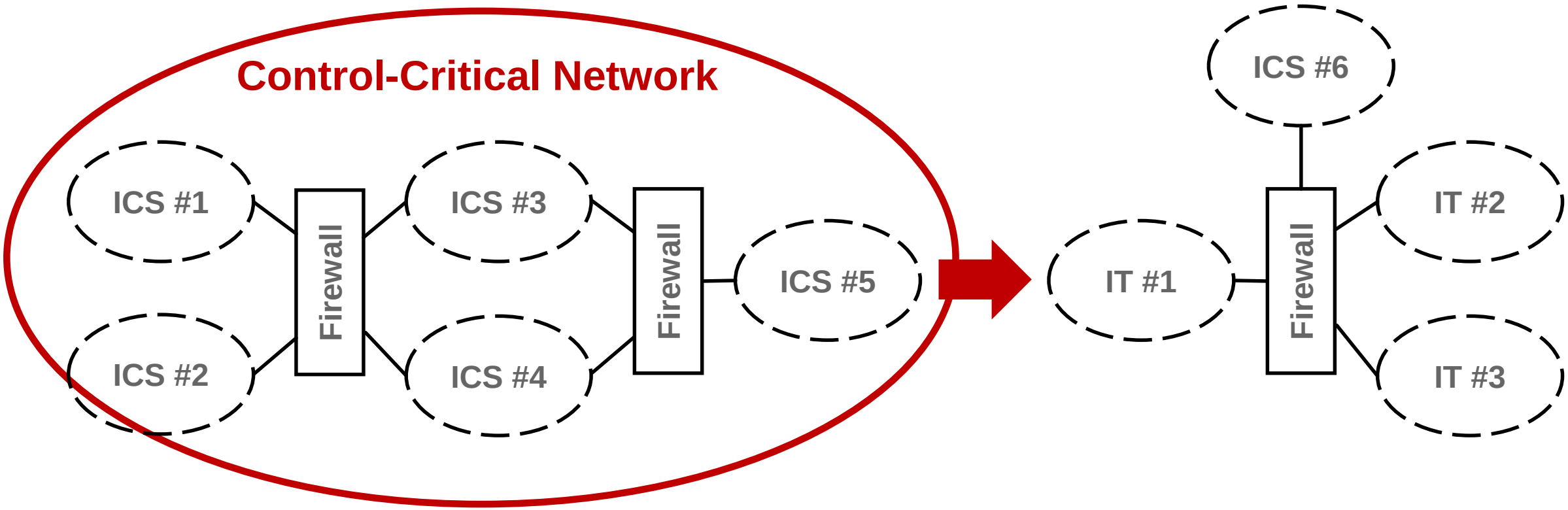
WHAT'S NEW: two dozen unidirectional network reference architectures

How Is This Practical?



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

Control-Critical Network Sets



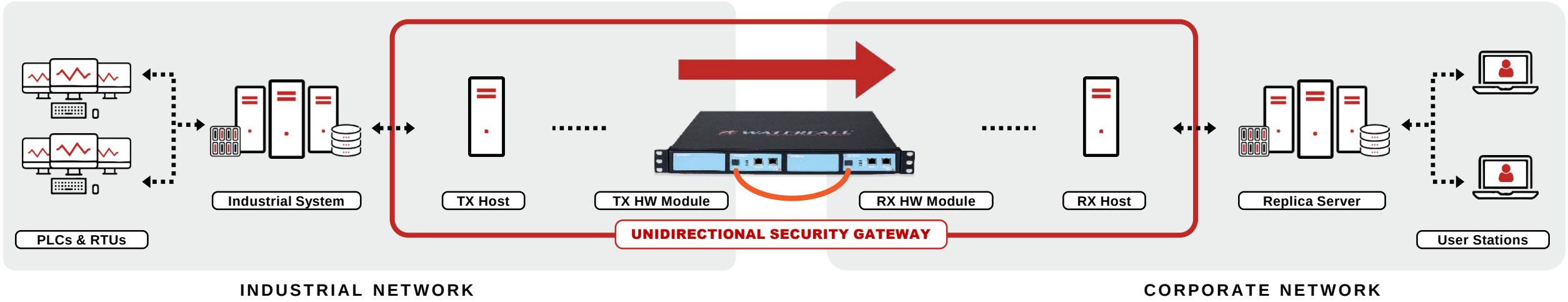
Control-critical networks are sets of ICS networks. Firewalls are used routinely within the set, but not across network criticality boundaries

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



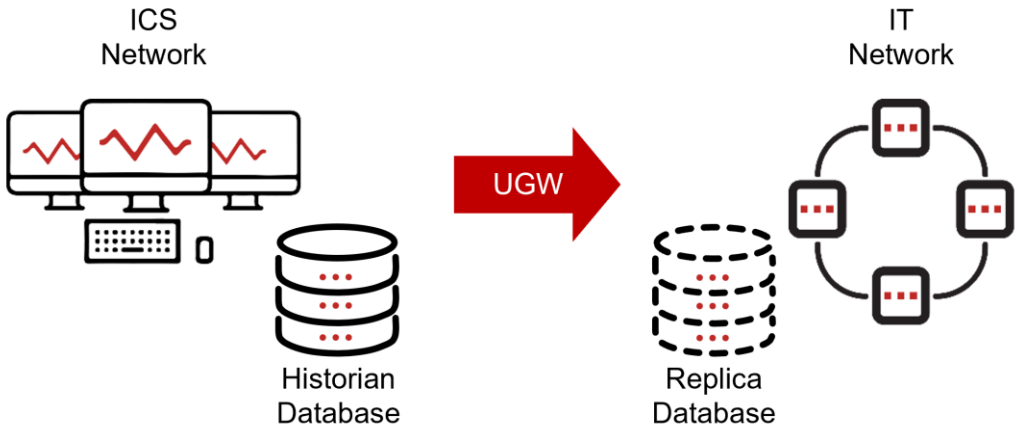
Unidirectional Security Gateways are a combination of hardware and software

- 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

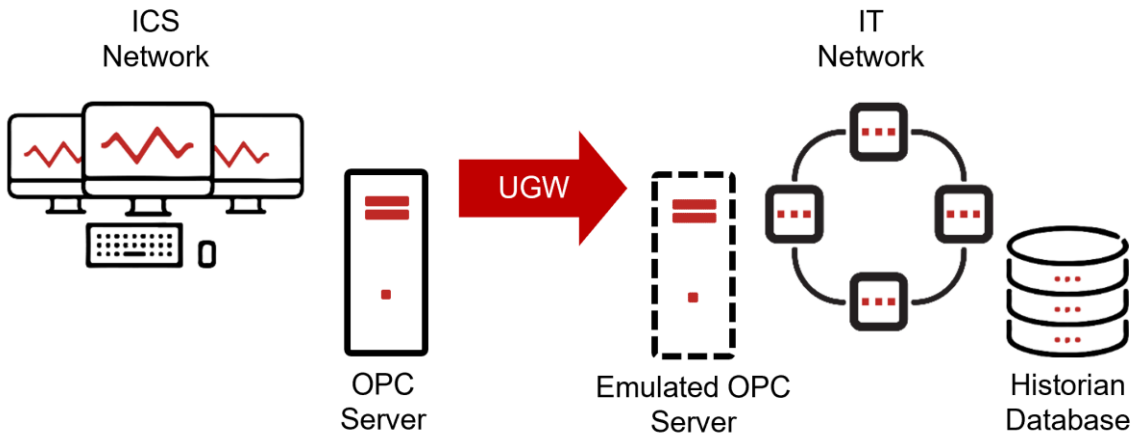
Database queries are sent by the gateway’s TX host to the ICS database & by the IT client to the IT replica



#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

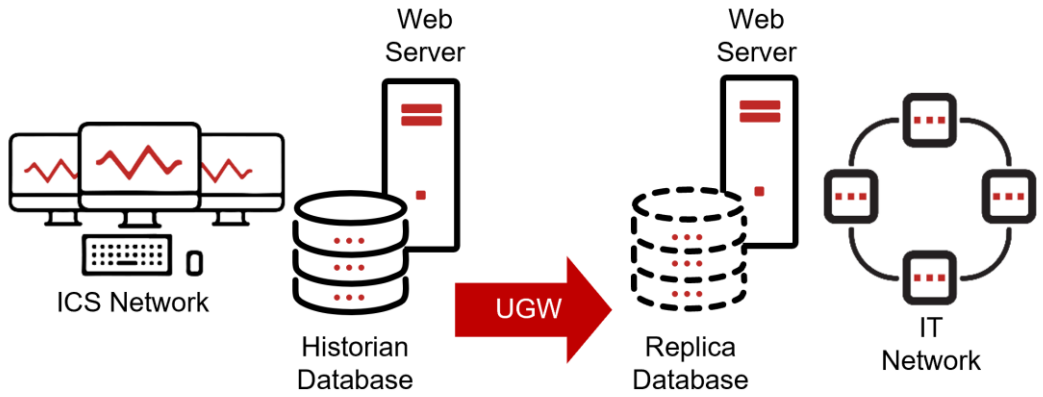
Unidirectional gateways send device state snapshots to external networks for use by emulators / replicas



#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

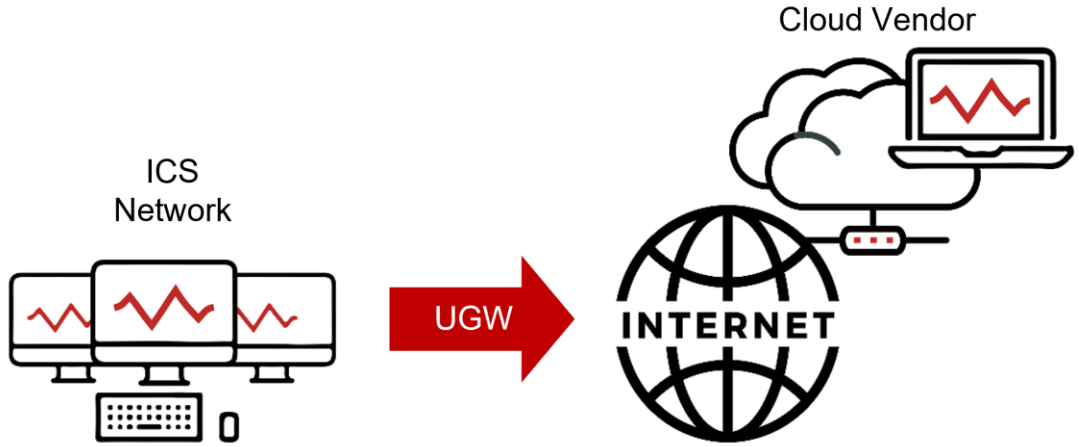
A second copy of web servers & other complex applications can easily be deployed when data sources can be replicated



#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

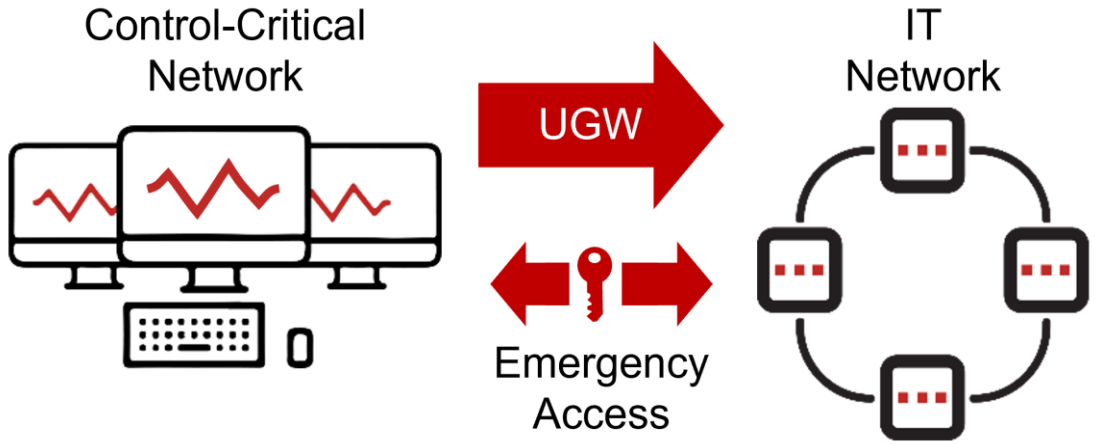
Both sets of needs are met



#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

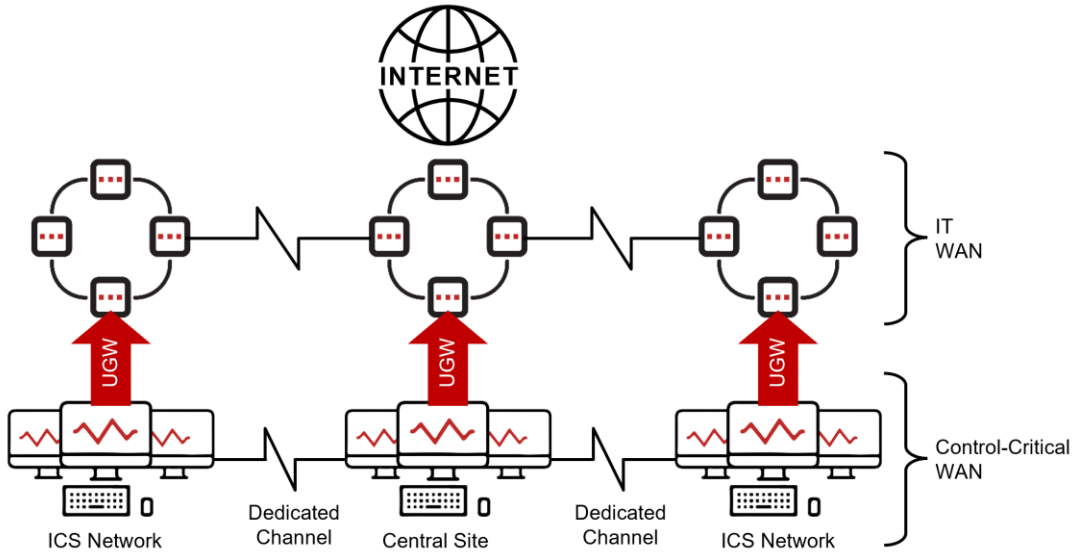
Full bi-directional remote access can be available temporarily, on a timer, in emergencies



#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

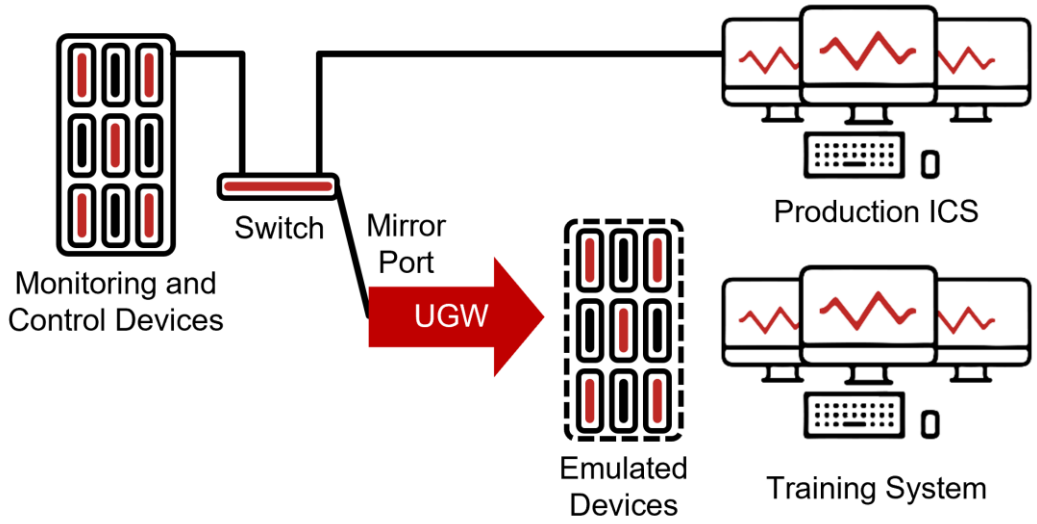
All sites must be secured as thoroughly as the most-critical site



#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

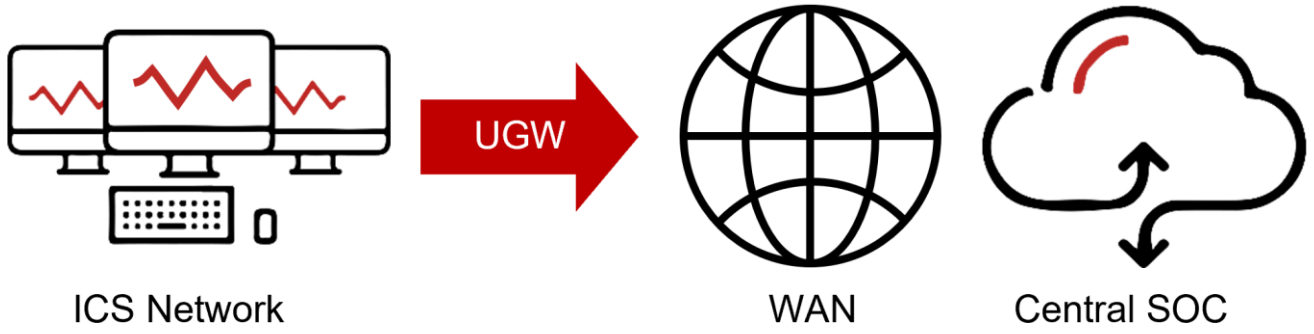
Unusual, but observed in production in a high-voltage transmission grid



#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

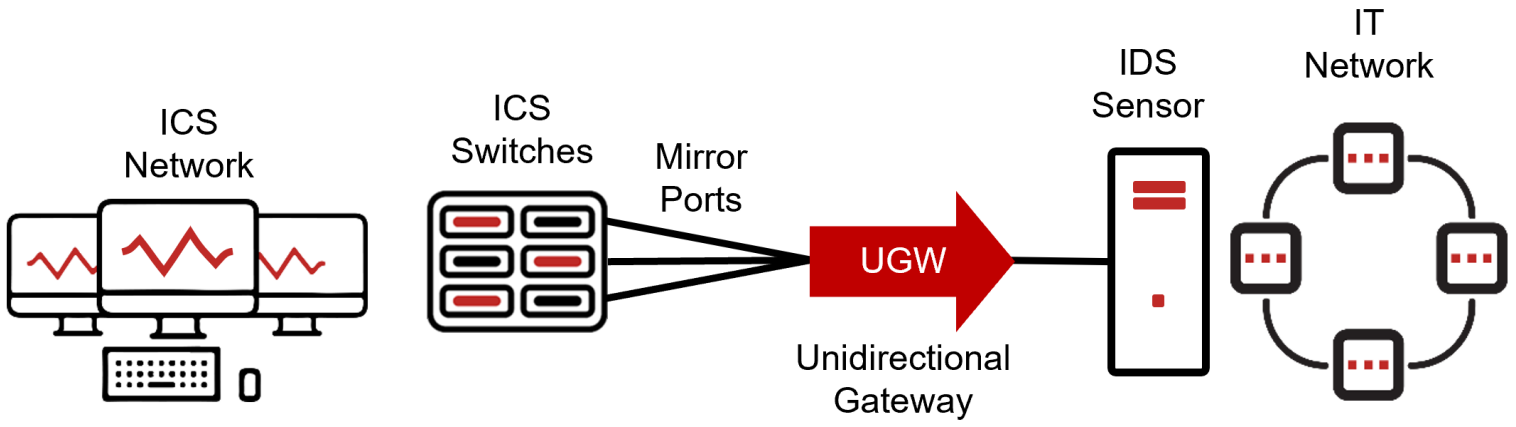


#9 Network Intrusion Detection

WATERFALL
Stronger Than Firewalls

- 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

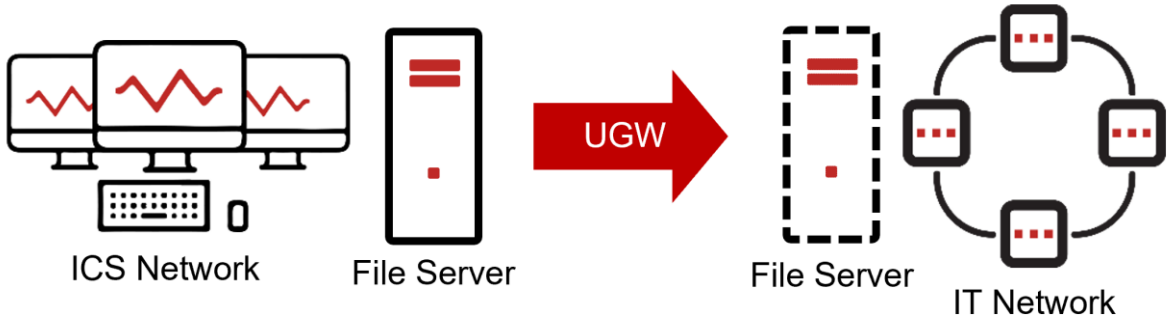
Most mirror ports are bi-directional, and those that are not, are only software unidirectional



#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

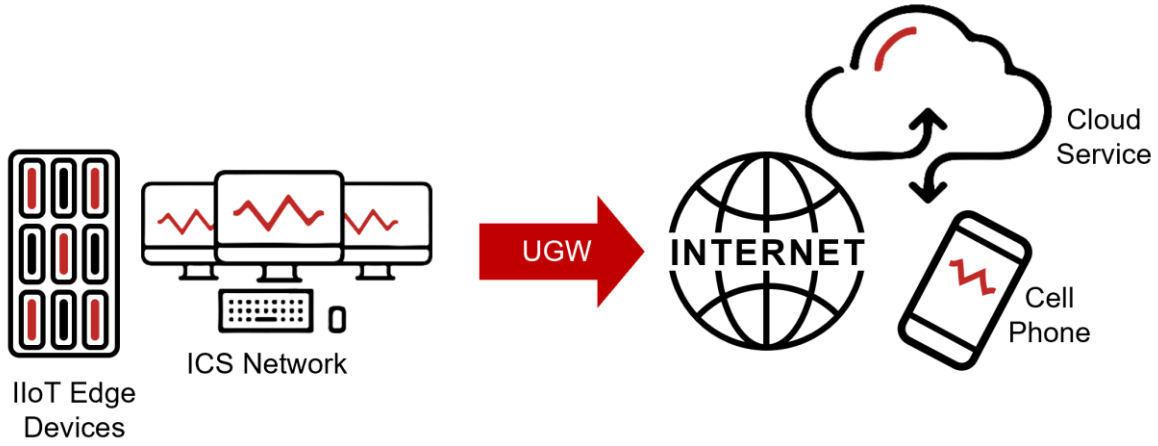
Convenient file server replication to an IT network dramatically reduces the need for removable media



#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

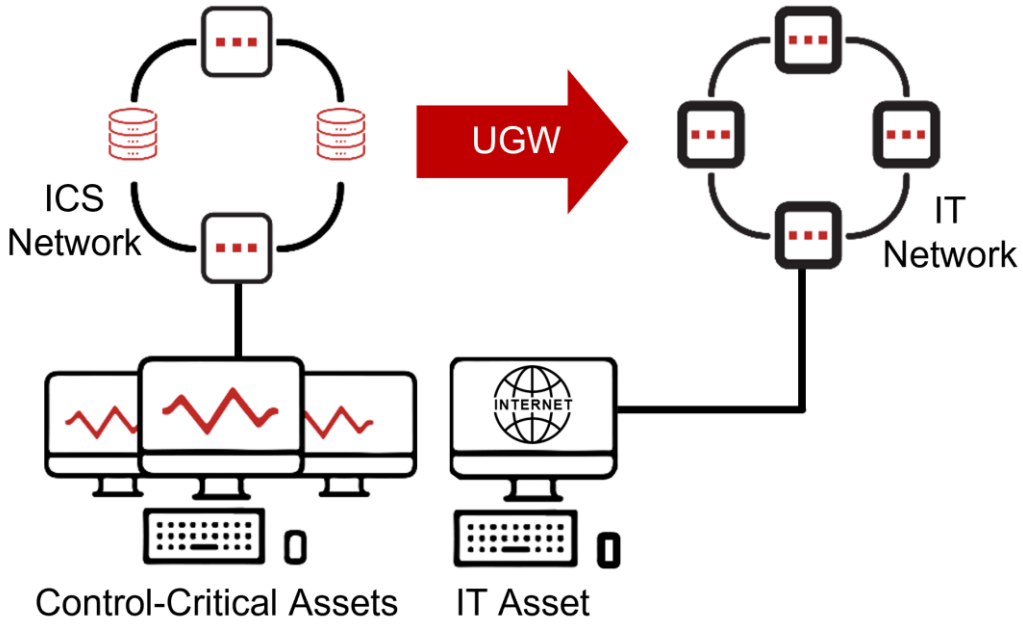
Eg: Pump #37 is about to fail – send a work crew in the next 3 days.



#12 Email & Web Browsing

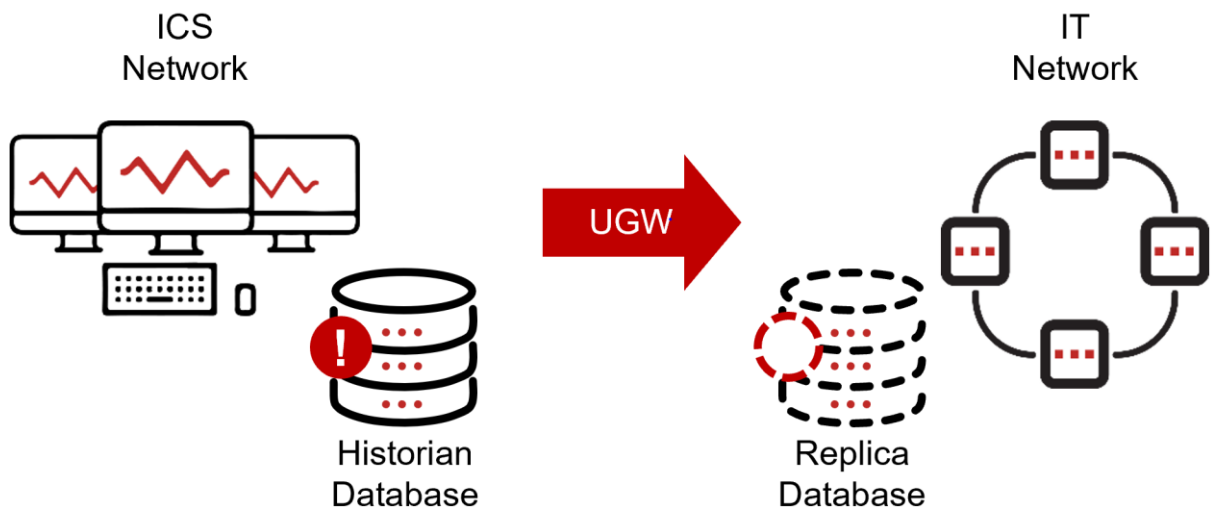
- Plant operators need email and web browsing abilities too
- SEC-OT sites enable these dangerous activities for operators and other plant personnel by deploying IT network endpoints on physical operator workstations
- Some sites deploy site-wide IT Wi-Fi networks

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

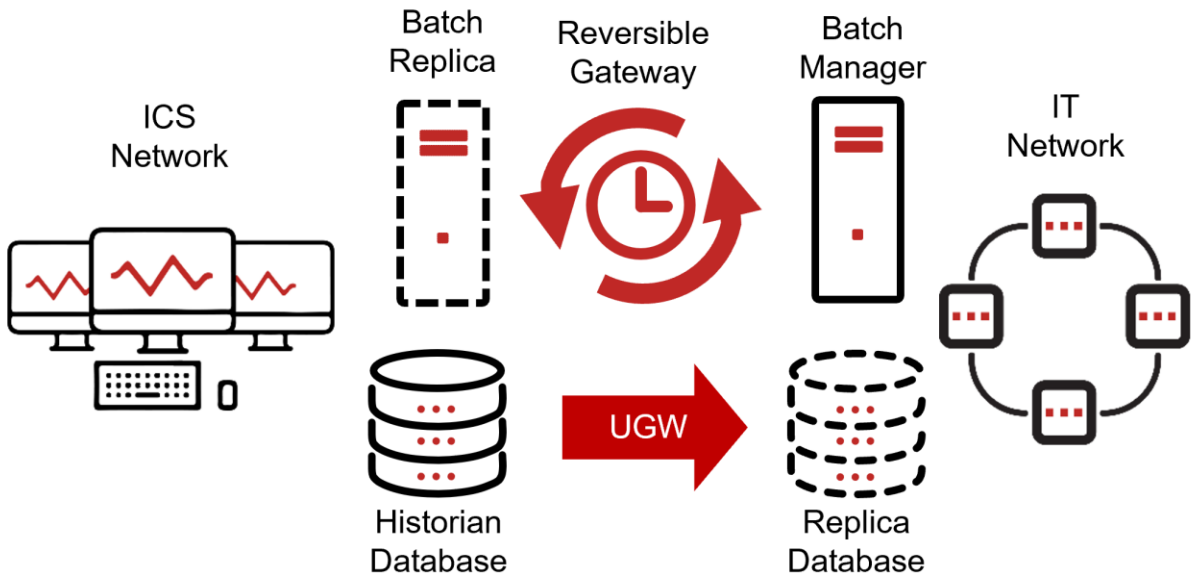


Leave trade secrets on OT networks

#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

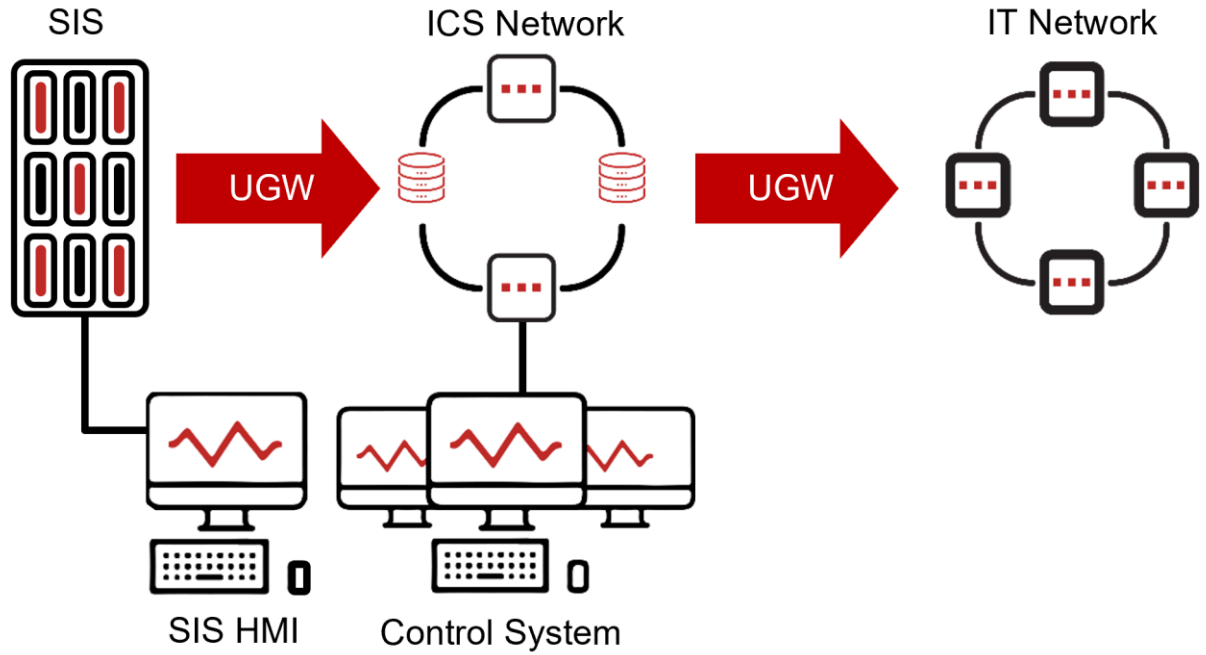
Reversible gateways provide disciplined, scheduled updates of OT systems



#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

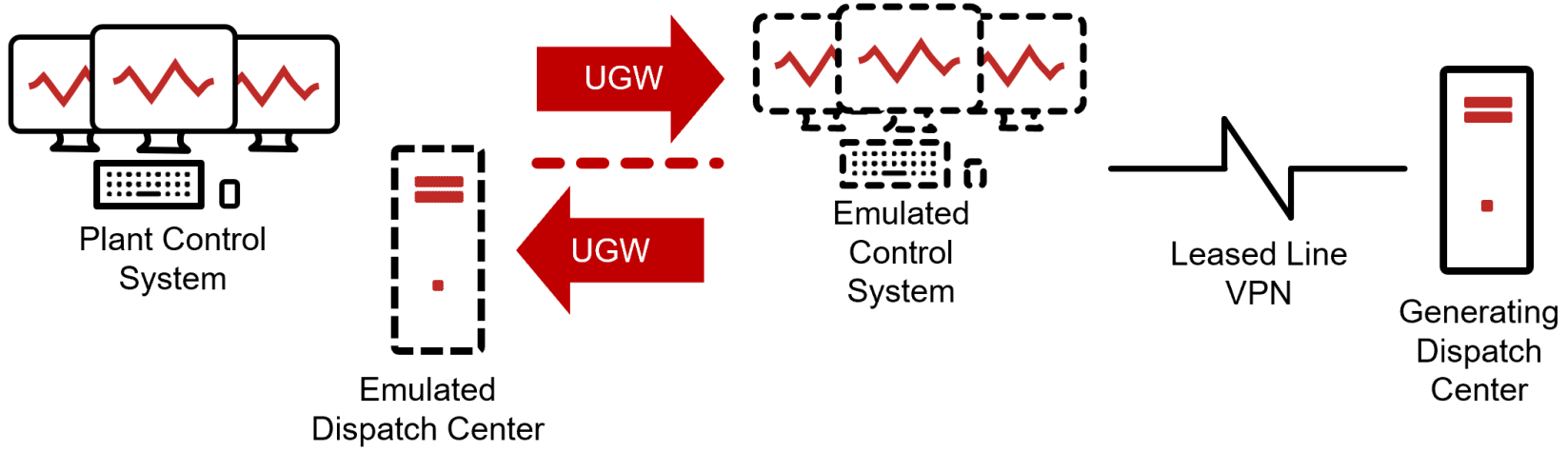
There is no safety without security



#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"

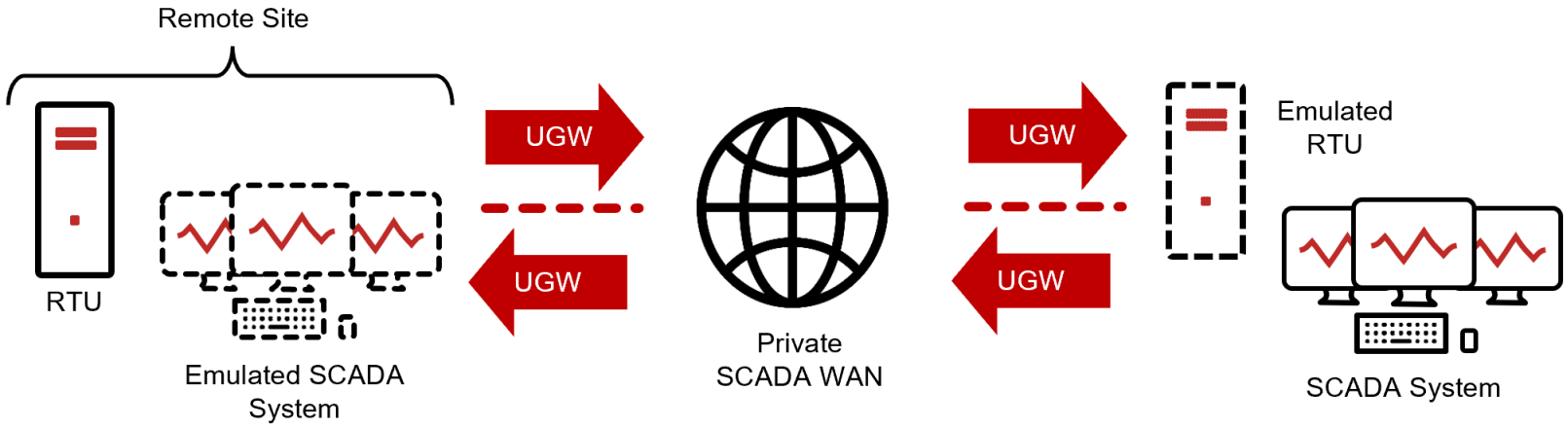
Compromise is only practical with insider help



#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

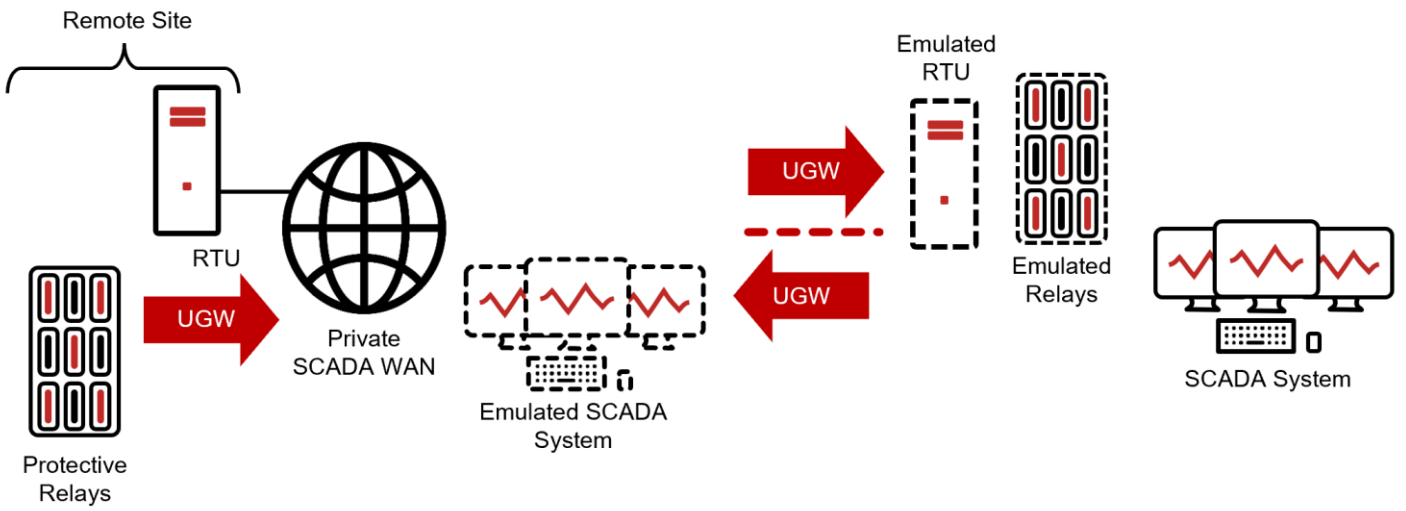
WAN visibility with disciplined control



#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

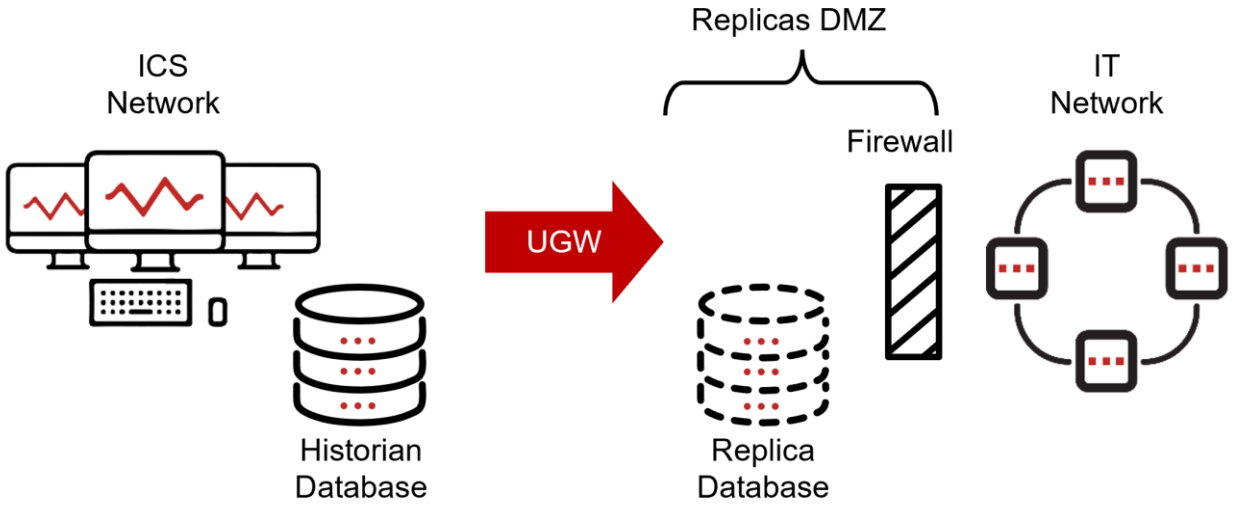
Protecting the protection equipment can be higher priority than protecting the process



#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

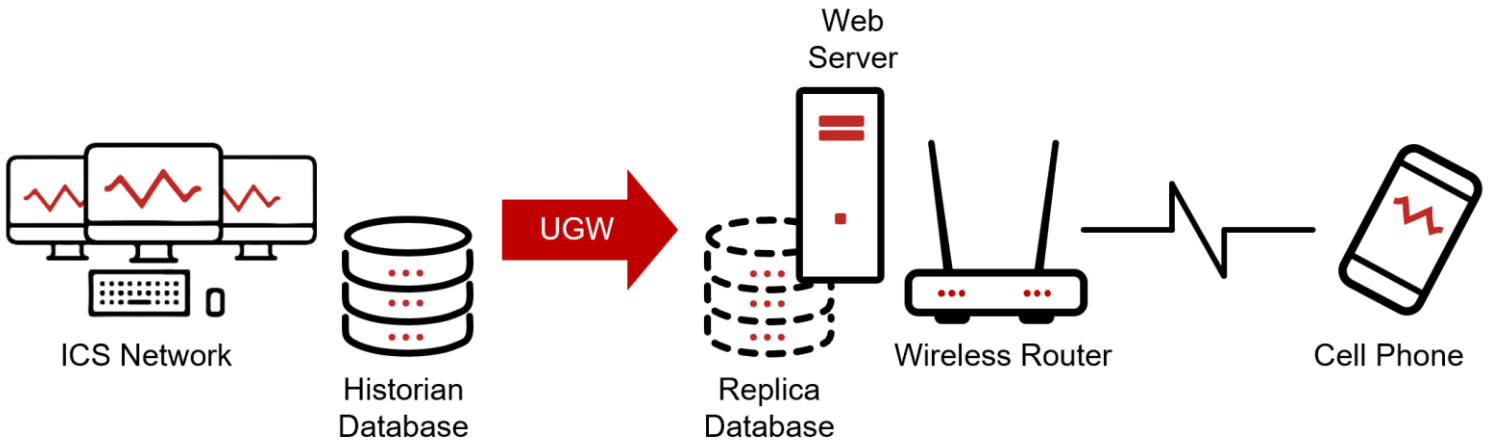
SEC-OT experts protect operations while IT-SEC exports protect information that reaches IT networks



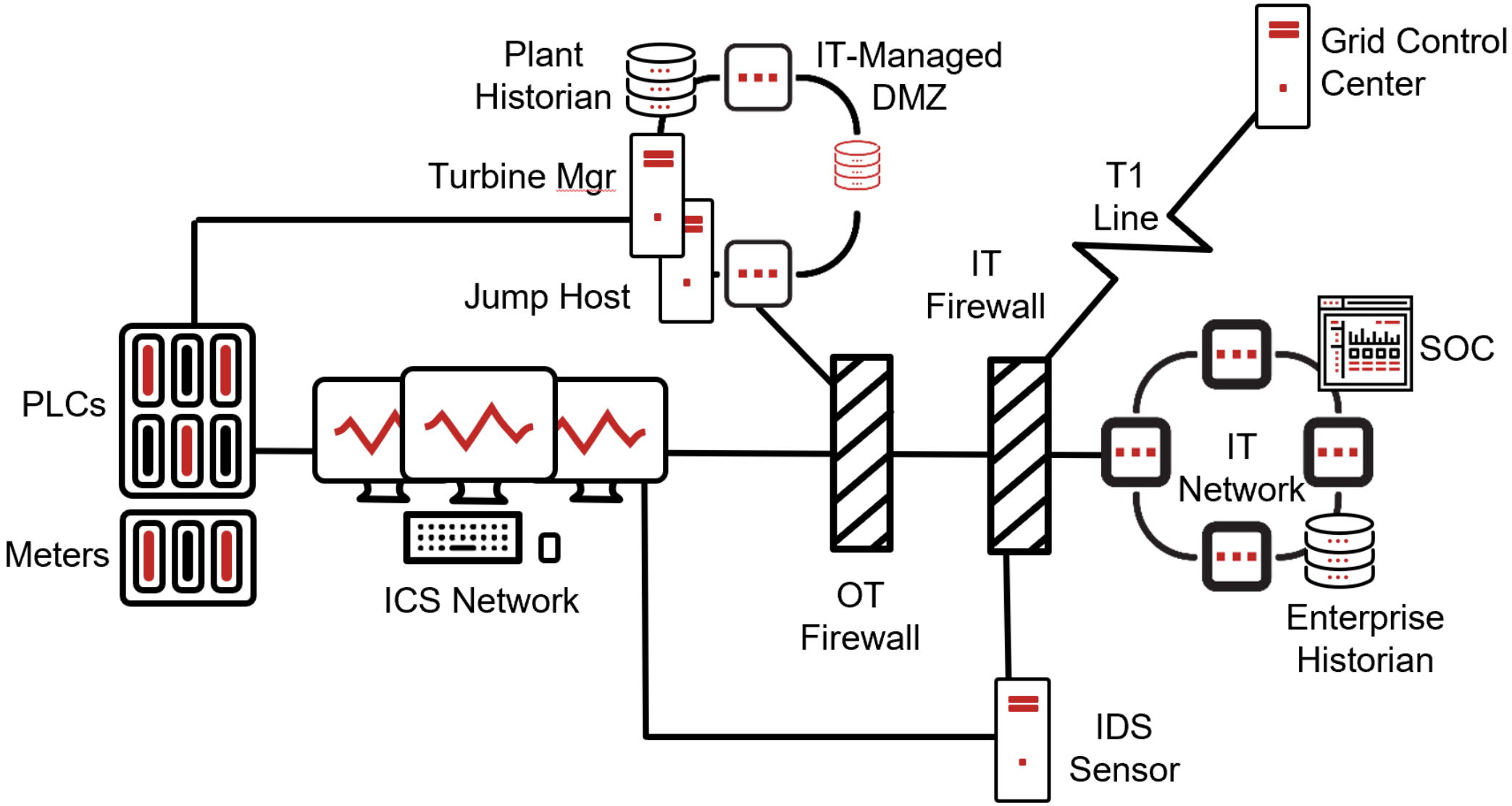
#20 Wireless Networks

- 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



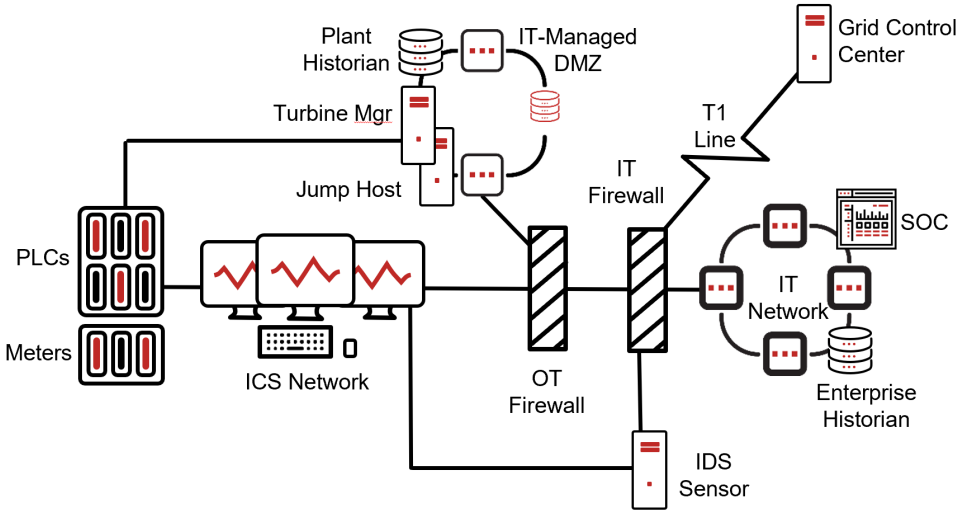
Power Plant Example - Original



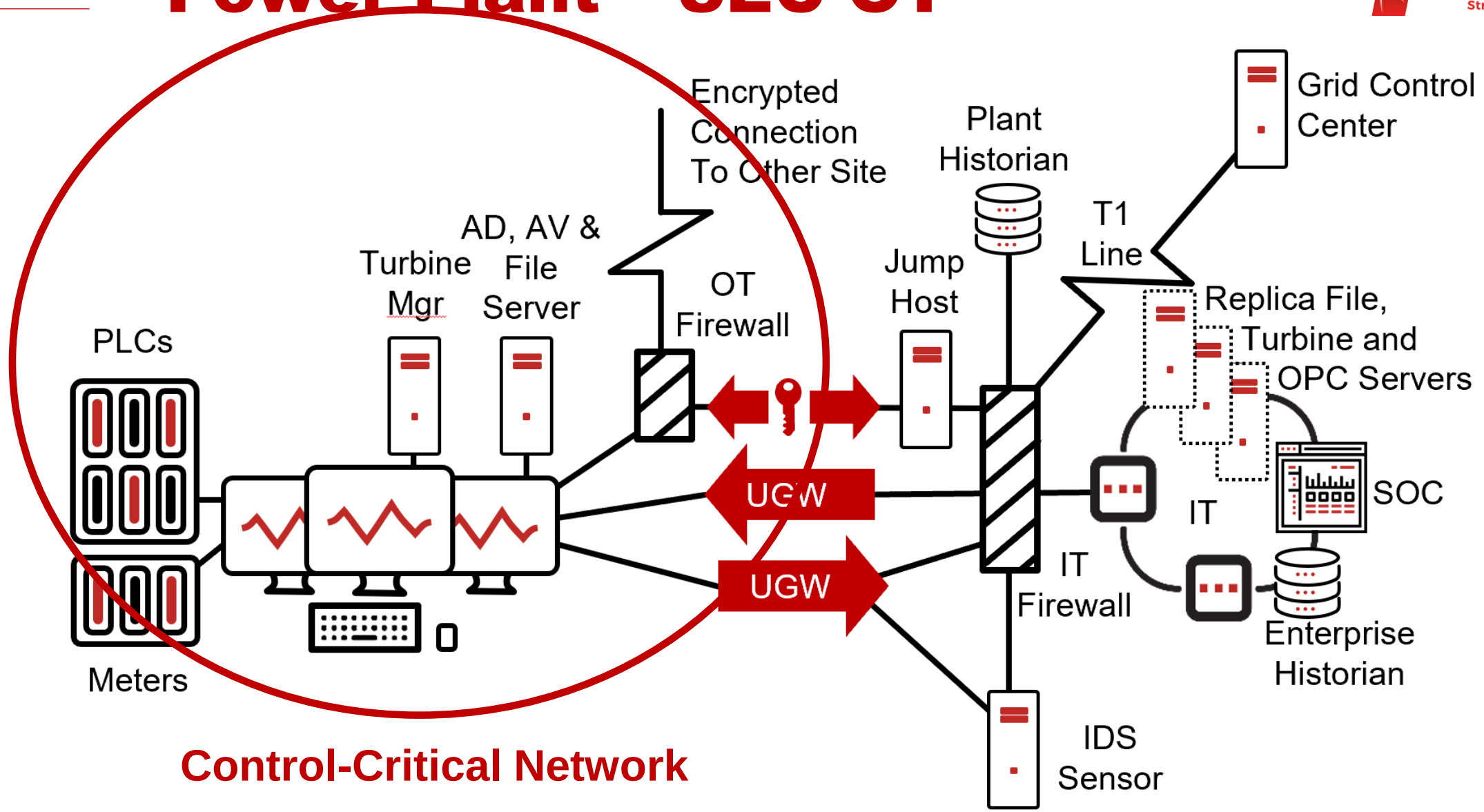
Power Plant Example – Original

- 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

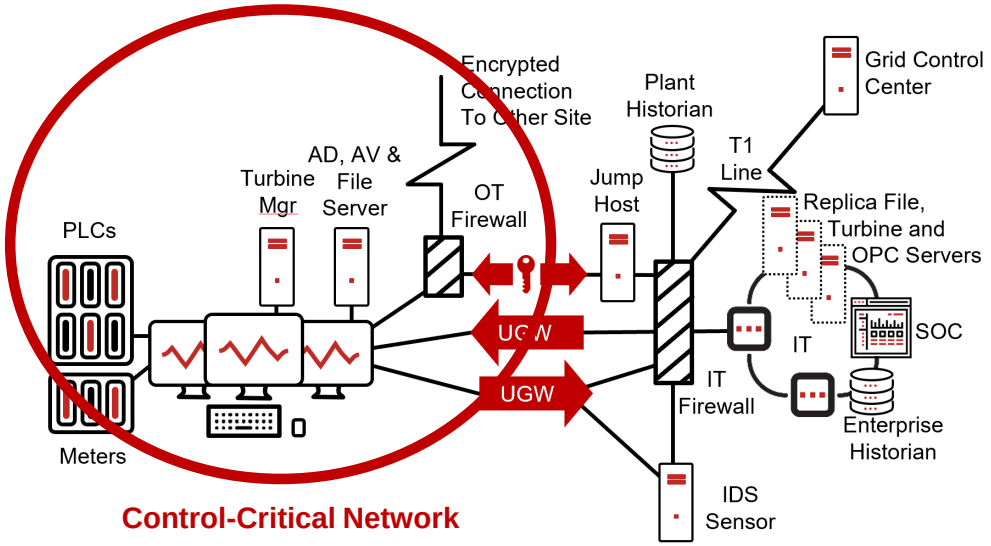


Control-Critical Network

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

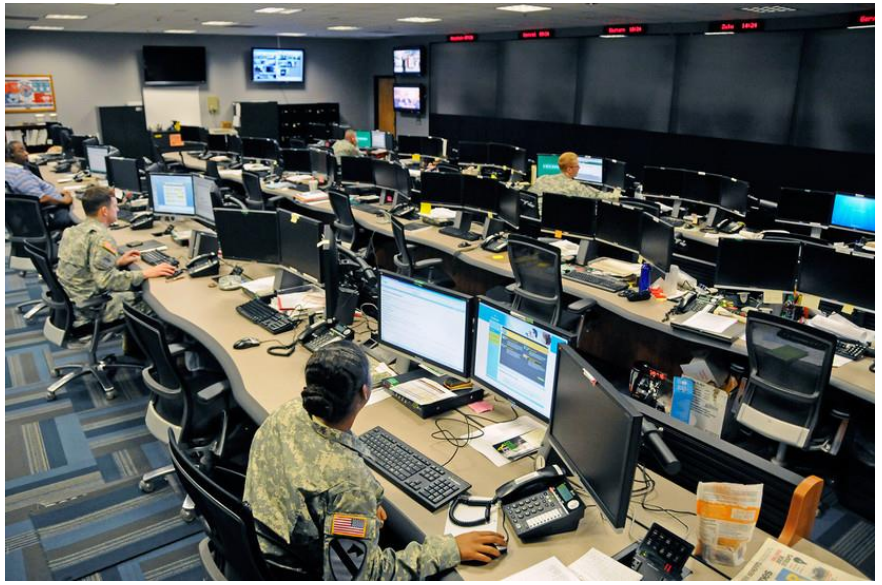
- In spite of the limitations of anti-malware systems, SEC-OT sites deploy such systems as universally as possible.
- Anti-malware systems are particularly important on any equipment whose removable media ports could not be physically disabled

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

- 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.



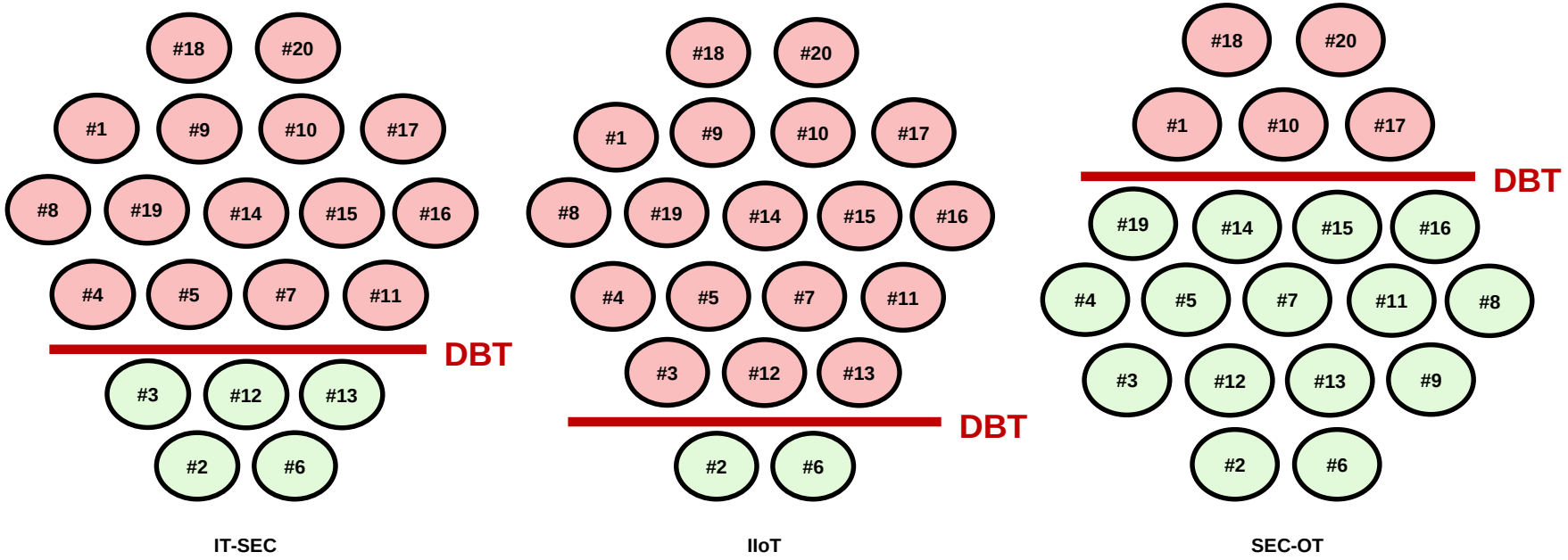
TOP 20 ICS CYBER ATTACKS

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

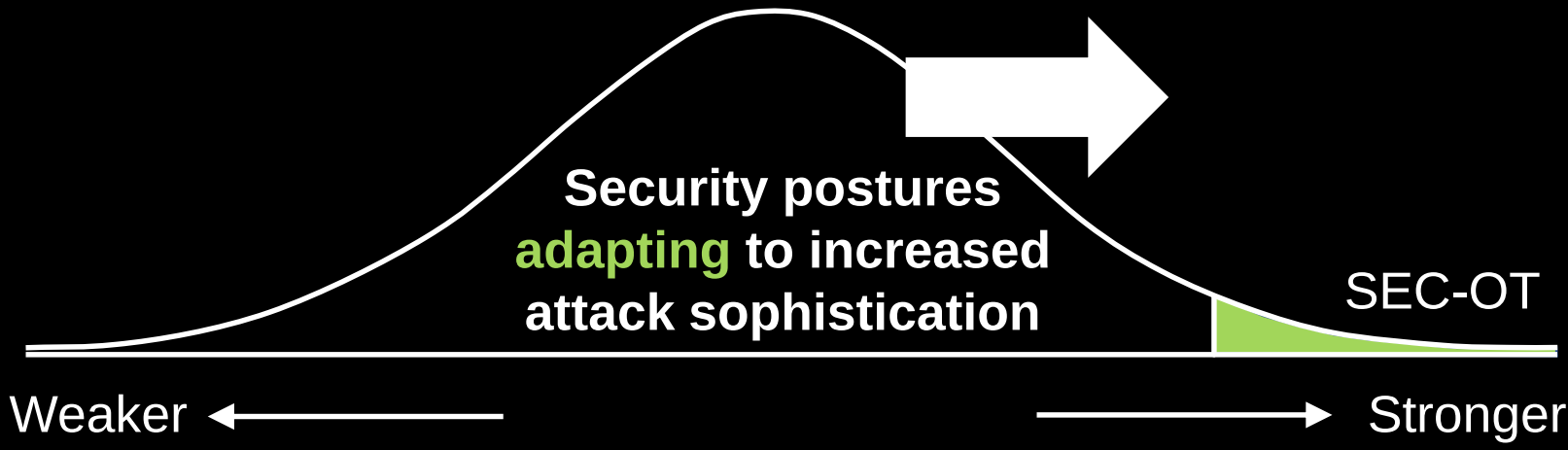
- Cyber DBT = line between set of attacks defeated reliably and those not so defeated
- There are always attacks not defeated & there is always a simplest such attack



SECURE OPERATIONS TECHNOLOGY

WATERFALL®
Stronger Than Firewalls

- **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