

SECURE OPERATIONS TECHNOLOGY

WHAT DO THE WORLD'S MOST SECURE SITES
DO DIFFERENTLY?

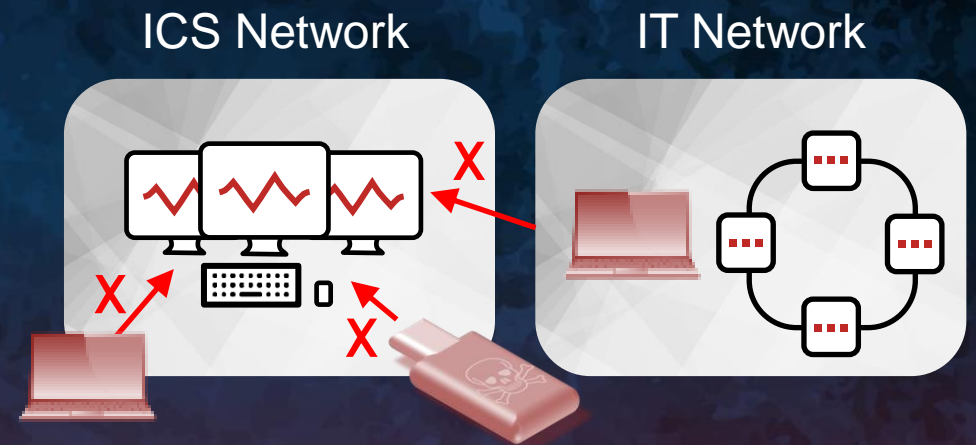
2020



CONVENTIONAL SECURITY

- Intrusion detection, security monitoring & incident response
- Passwords & permissions
- Anti-virus, security updates & host hardening
- Firewalls, encryption, VPNs, jump hosts, MFA
- Offline backups! (tested)

There are a lot of ways that attackers & malware can enter a control system



RESIDUAL RISK

RISK MANAGEMENT OPTIONS

MITIGATE – TAKE STEPS TO REDUCE FREQUENCY OR REDUCE CONSEQUENCES

TRANSFER – PAY AN INSURER TO ACCEPT THE RISK

ACCEPT – DO NOTHING / SUFFER CONSEQUENCES

Any risks we cannot transfer or mitigate, we accept

Consequence →

	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Med Low	Medium	Med Hi	High	High
Likely	Low	Med Low	Medium	Med High	High
Possible	Low	Med Low	Medium	Med Hi	Med Hi
Unlikely	Low	Med Low	Med Low	Medium	Med Hi
Very Unlikely	Low	Low	Med Low	Medium	Med Hi

↑ Frequency

SECURE OPERATIONS TECHNOLOGY



IT-SEC:

protect the information



SEC-OT :

protect physical operations
from the information



FIRST THREE LAWS OF SCADA SECURITY

1. Nothing is secure
2. All software can be hacked
3. All attacks are information, and every bit of information can be an attack

In the worst case, a compromised CPU will issue every unsafe instruction the CPU is electrically able to issue

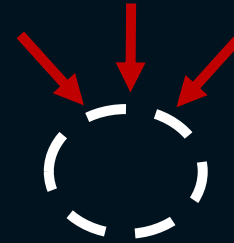




ONLINE & OFFLINE PERIMETERS



Critical network = a set of ICS networks



There are **always** perimeters for important sites & networks

Secure sites **physically** control information flows

OFFLINE CONTROLS

Offline Survey

Test Beds

Removable Media

Removable Devices

New Cyber Assets

Insider Attacks

Deceived Insiders

Nonessential Equipment

WHAT'S NEW

Near-miss protocol for information incidents



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

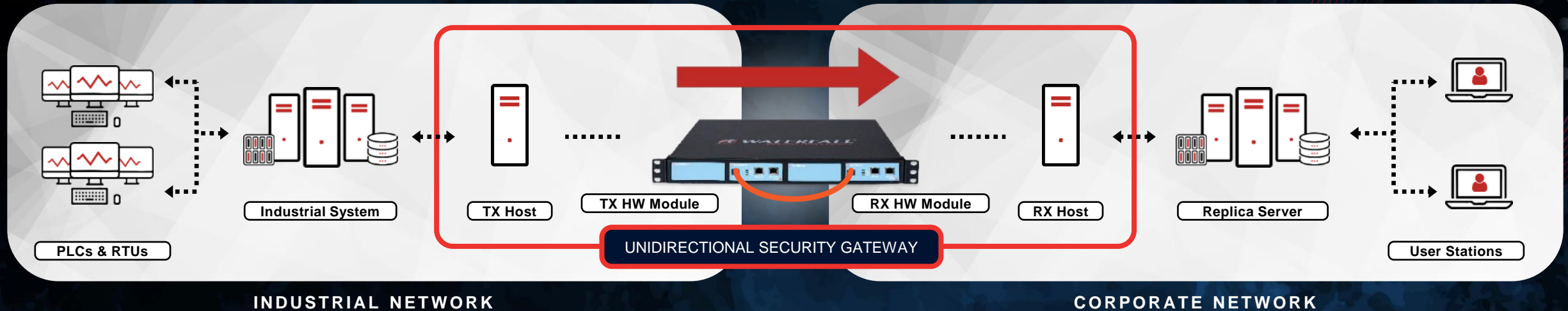
ONLINE CONTROLS

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

UNIDIRECTIONAL SECURITY GATEWAY

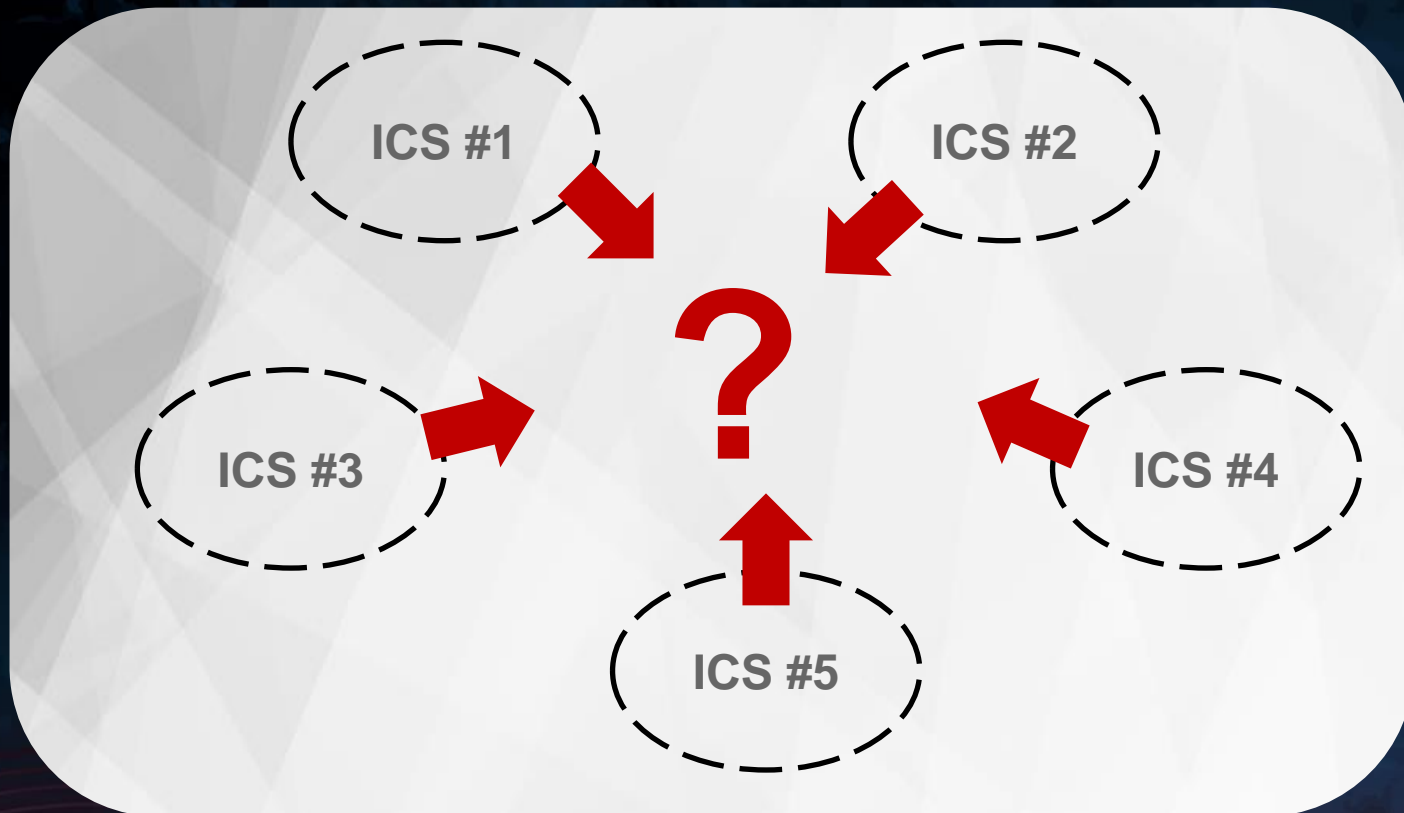


Unidirectional Security Gateways are a combination of hardware and software

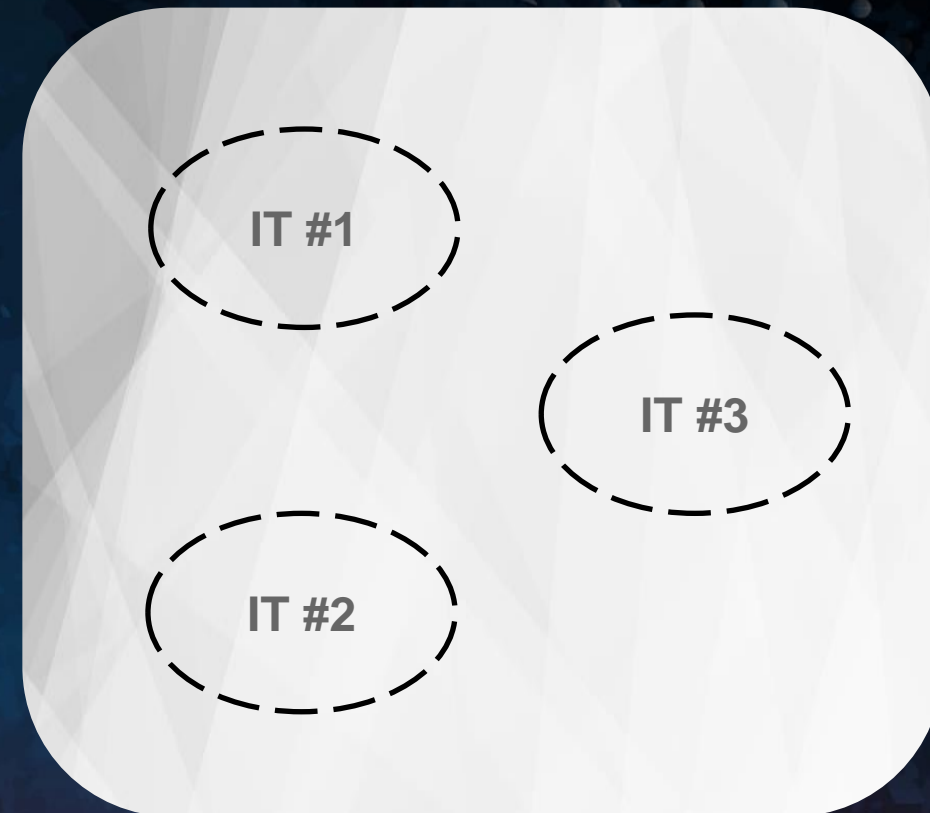
- The hardware sends information in only one direction
- The software replicates servers & emulates devices from the OT network to the IT network
- No attack, no matter how sophisticated, can propagate back to the industrial network through the gateway

HOW IS THIS PRACTICAL

Industrial Network



Enterprise Network



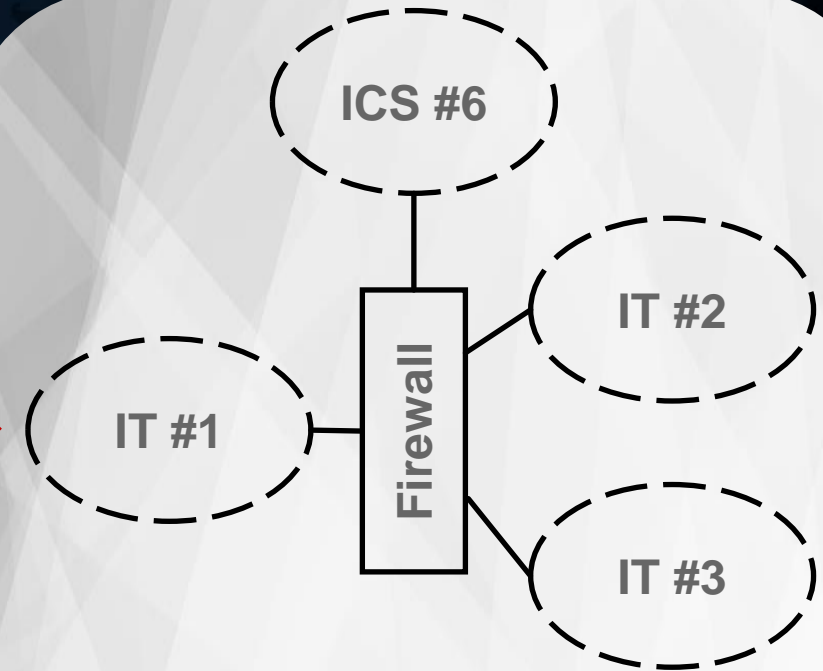
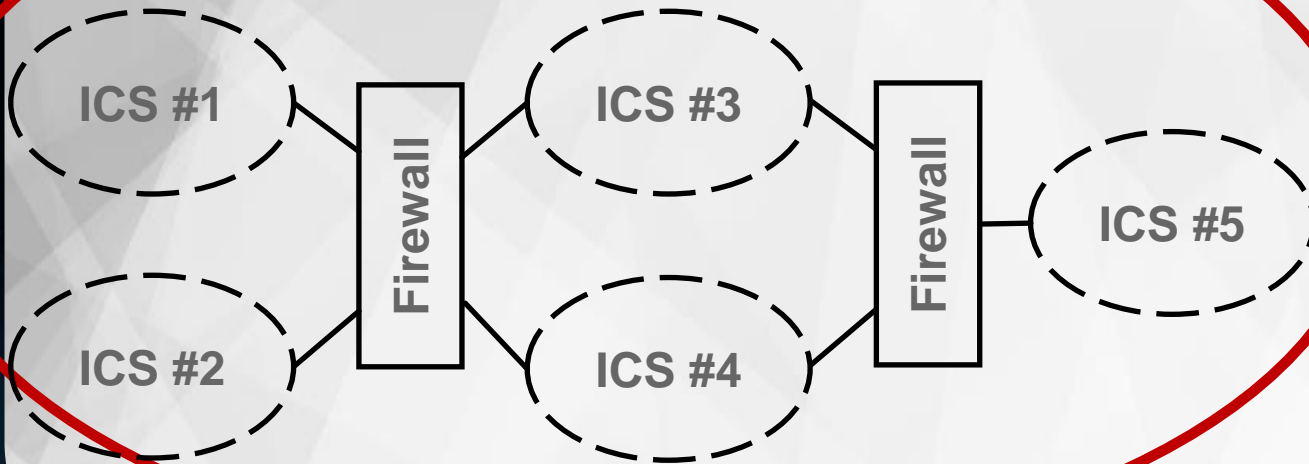
Industrial Control Systems (ICS) at a site almost always need to cooperate and coordinate

CONTROL-CRITICAL NETWORK SETS

Industrial Network

Enterprise Network

Control-Critical Network

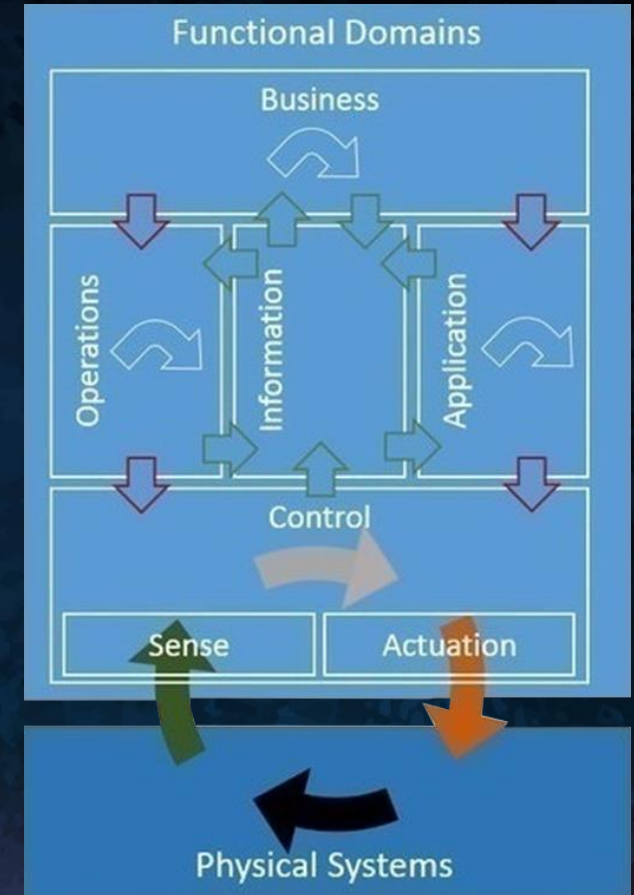


***Control-critical networks are sets of ICS networks.
Firewalls are used routinely within the set,
but not across network criticality boundaries***

DISCIPLINED CONTROL

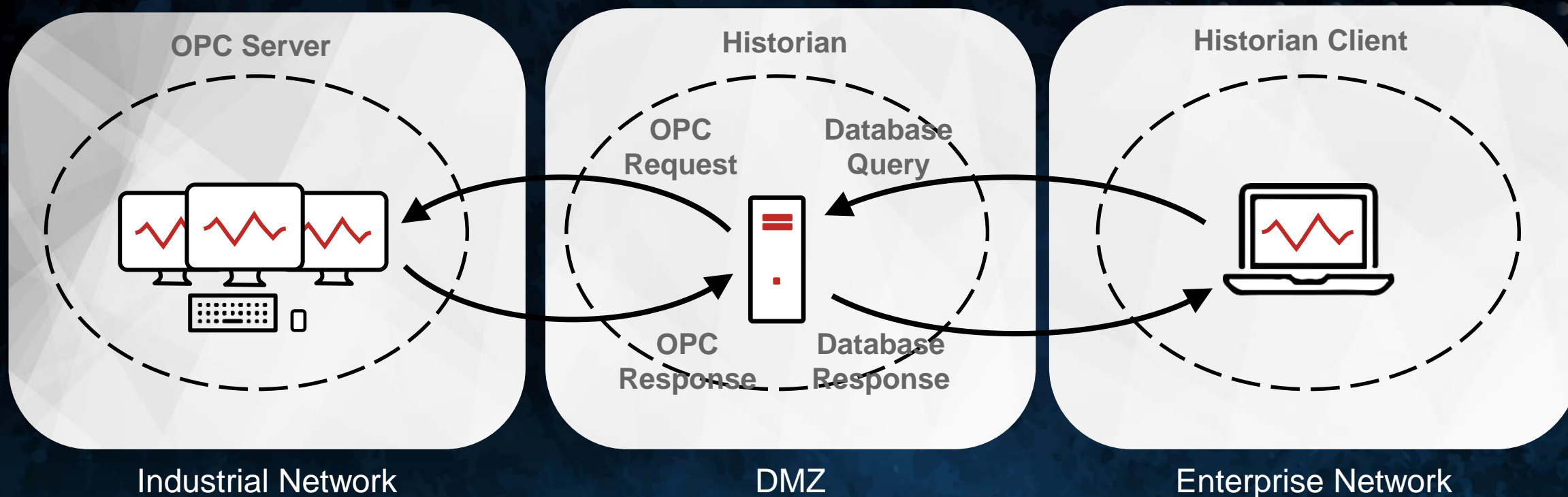
- Something always needs to get back in to control-critical networks
- Industrial Internet Consortium (IIC): Every information flow from “higher level” networks into control-critical networks is a kind of control
- Firewall – only one flow control hammer – “open another port”

Disciplined control – the safest mechanism to meet a business need efficiently



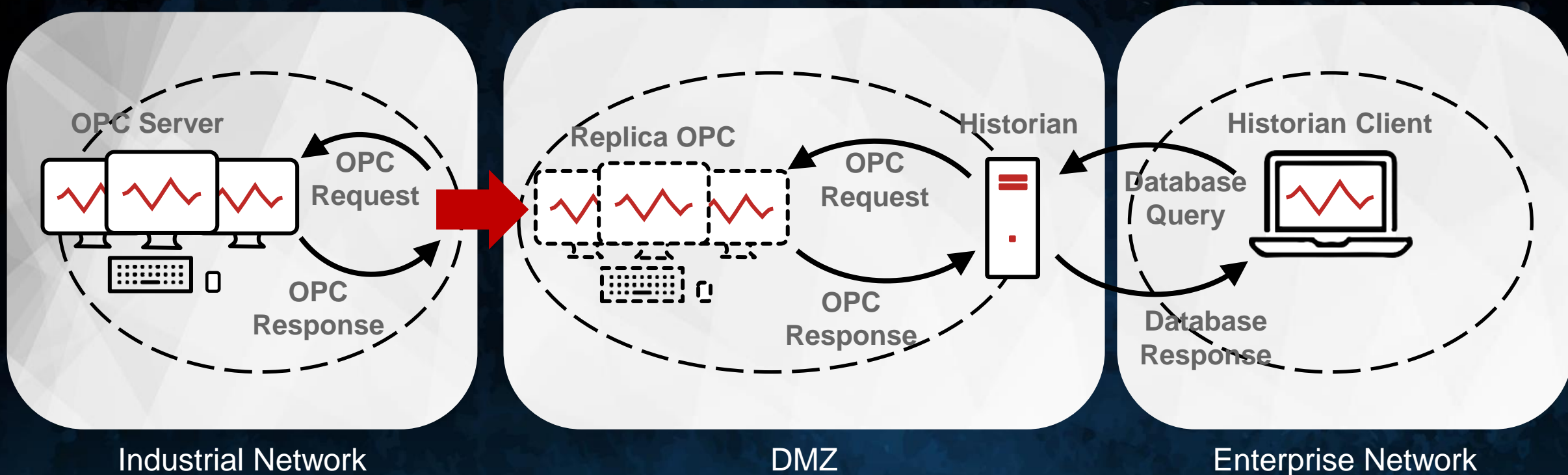
Industrial Internet Consortium
Reference Architecture

EXAMPLE: QUERY / RESPONSE



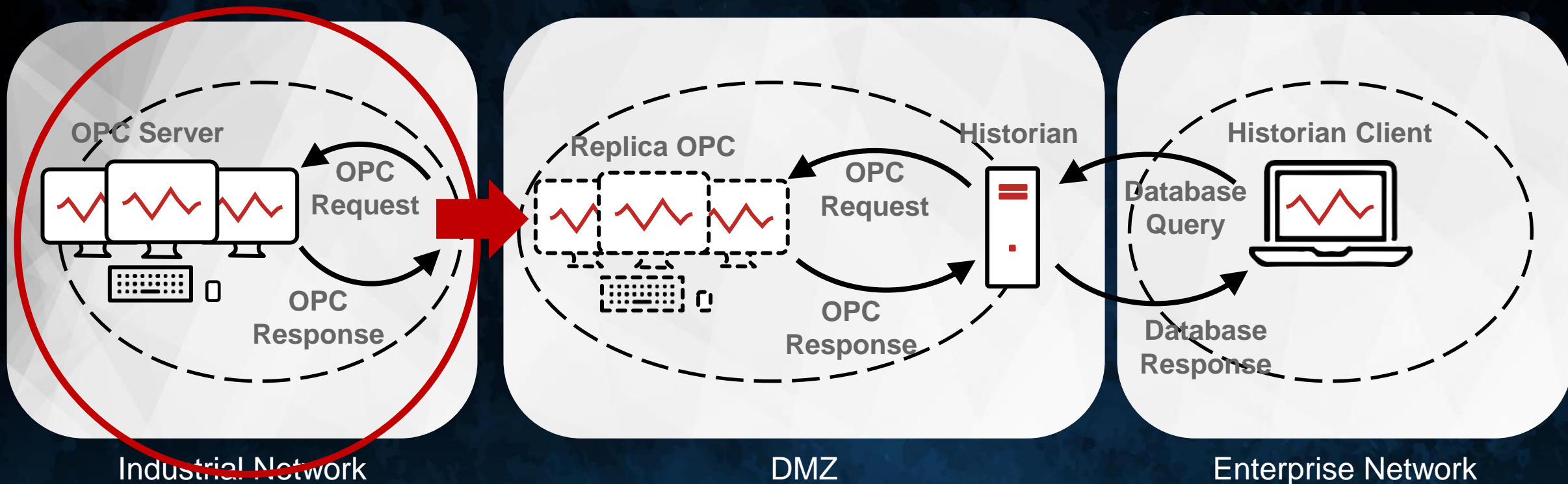
***All incoming communications are a kind of control
Eliminate what can be eliminated
Impose strict discipline on the remainder***

OPC SERVER REPLICATION



With the entire OPC Server replicated, there is no need for OPC requests to pass from the DMZ into the control network

OPC SERVER REPLICATION



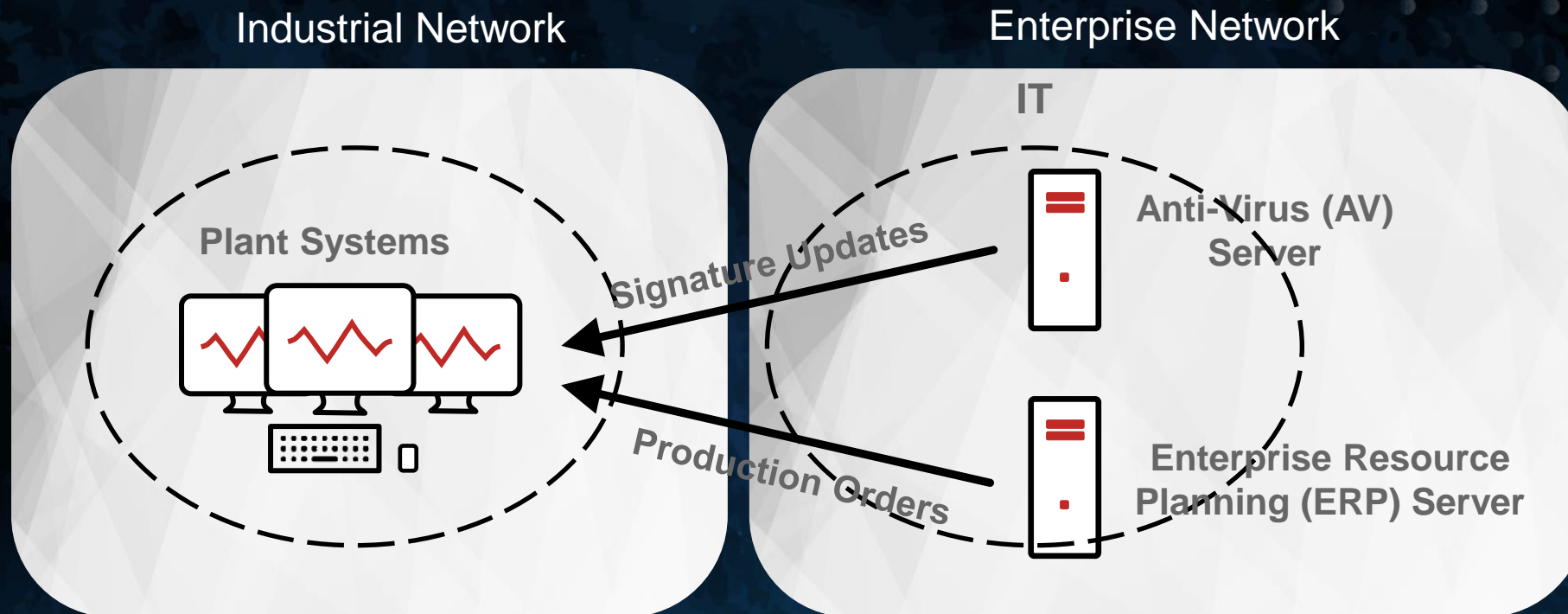
**Control-Critical
Network**

*The OT network in this example
is the control-critical network:
nothing gets in*

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	

#14 SCHEDULED UPDATES

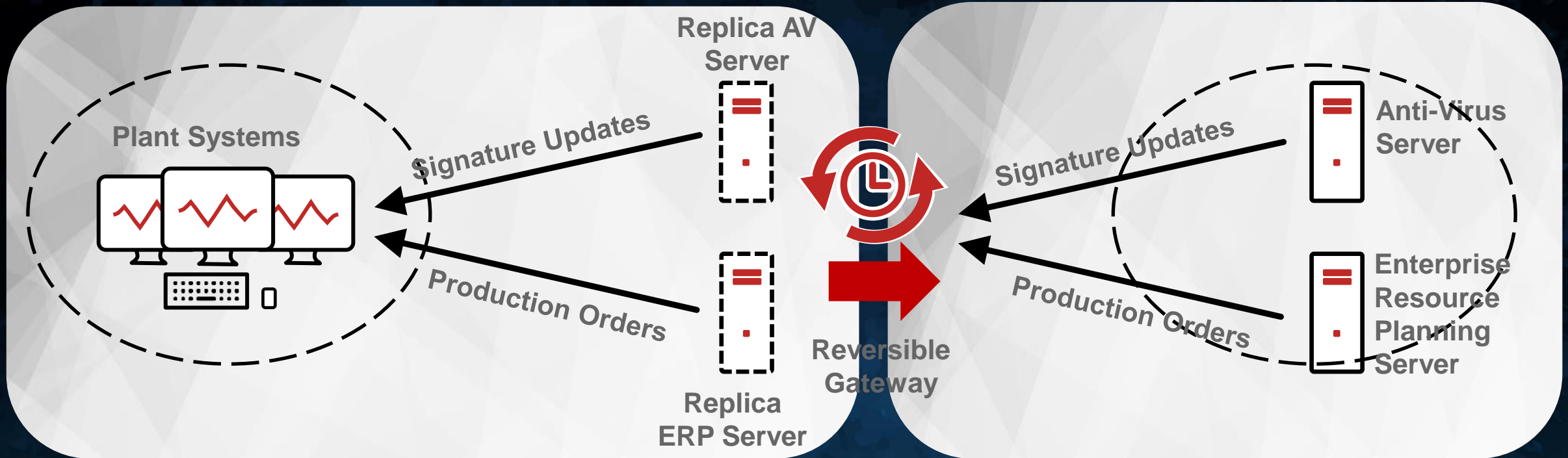


Anti-virus signatures are updated several times per day
7-10-day backlog of production orders from ERP
is updated once or twice per day

#14 DISCIPLINED SCHEDULED UPDATES

Industrial Network

Enterprise Network

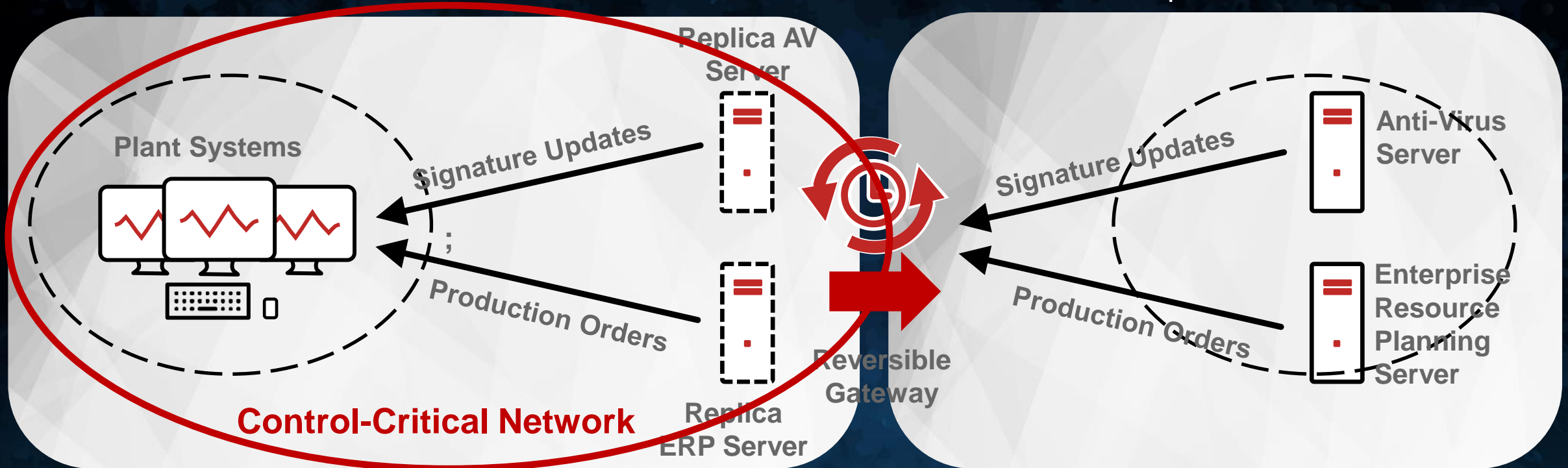


Reversible gateway replicates ICS servers “out” and Anti-Virus (AV) and Enterprise Resource Planning (ERP) servers “in” on a schedule – for disciplined, scheduled updates

#14 DISCIPLINED SCHEDULED UPDATES

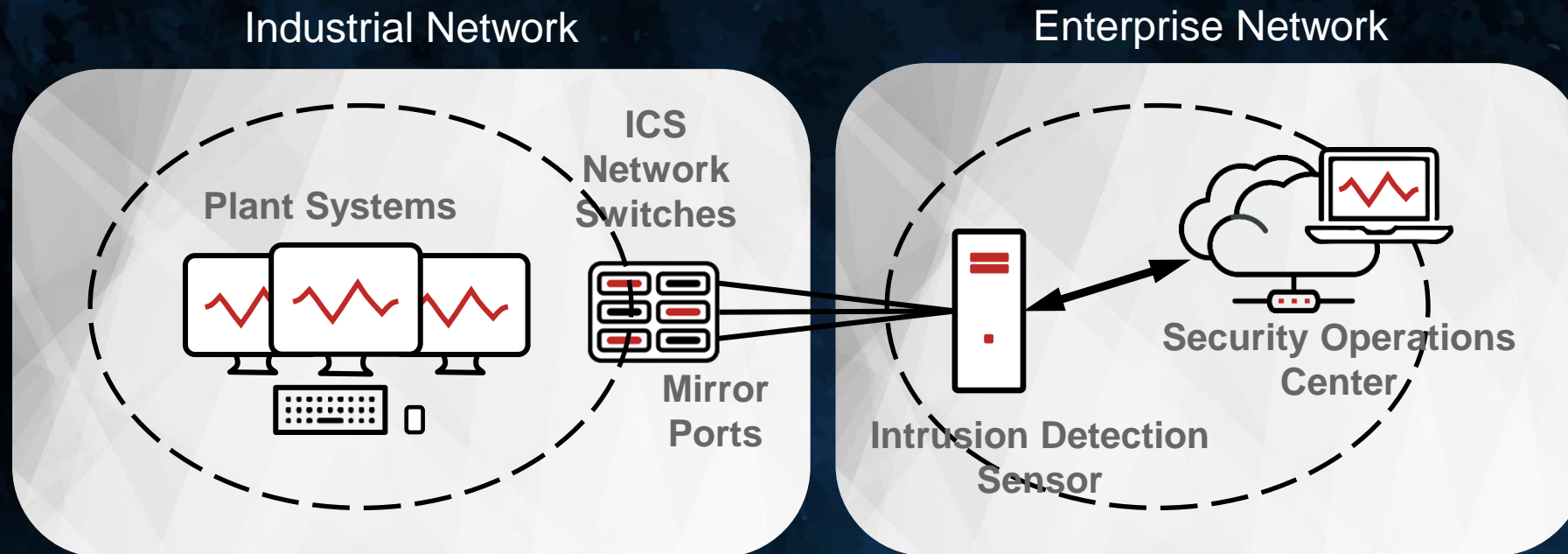
Industrial Network

Enterprise Network



The reversible gateway does not forward arbitrary files, but actively fetches and validates only those files and other updates needed by the control-critical network

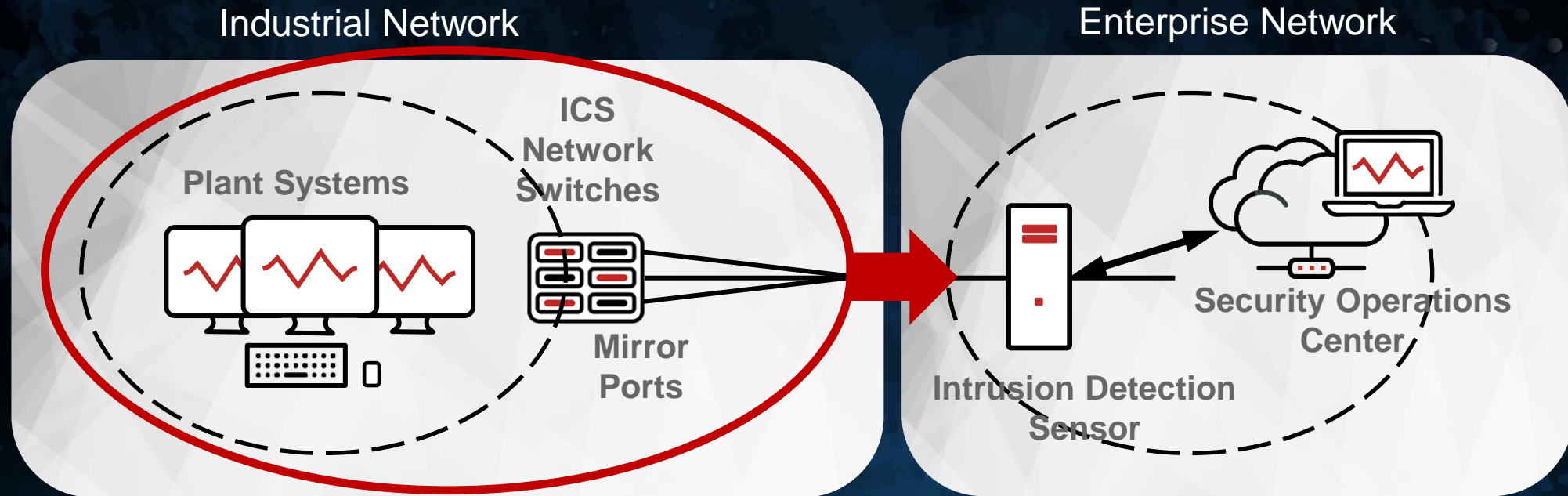
#9 NETWORK INTRUSION SENSORS



IDS sensors should be deployed on IT networks - they need frequent updates and adjustments by central SOC analysts

But – mirror ports are notorious for bi-directionality, and all switch unidirectionality is software-based, not physical

#9 NETWORK INTRUSION SENSORS




Control-Critical Network

Unidirectional gateway replicates mirror port traffic captures so that network IDS sensor can be deployed safely on IT network


WATERFALL – THE OT SECURITY COMPANY



Founded in 2007



1000+ sites
worldwide



Headquarters
in Israel



Deployed in all
critical infrastructure
sectors



Sales & operations
in NA, EU & APAC



Multiple registered
US patents



Technology & sales
collaboration with
global partners

INDUSTRIAL SECURITY PODCAST

- Guests from all over the industrial security space
- Vendors – issues, technology & approaches
- Government agencies – programs & resources
- Owners & operators – priorities & approaches
- Other – recruiters, educators & more

If you like it, please submit a review & spread the word on social media

<https://waterfall-security.com/podcasts>

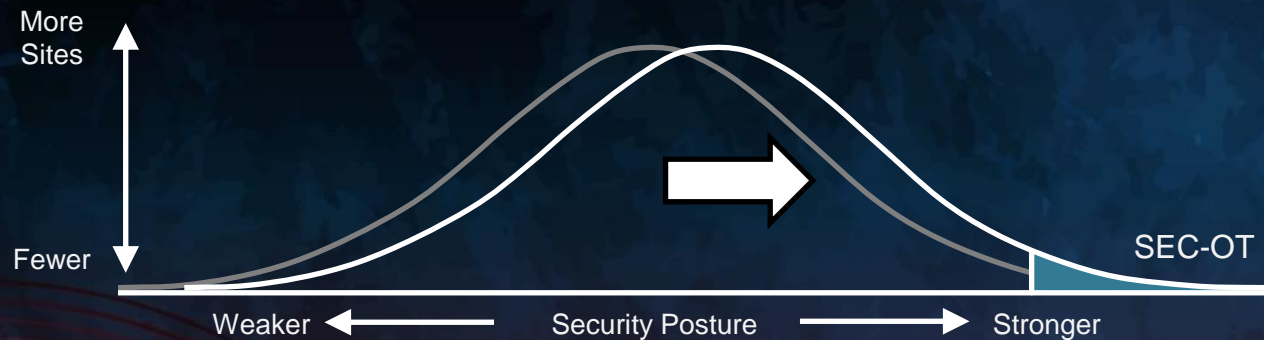


RAISING THE BAR

Attack capabilities only increase, so must our security posture

Identify & control information flows across physical and network perimeters

Control online flows unidirectionally
Physical protection from online attacks



andrew.ginter@waterfall-security.com
<https://waterfall-security.com/sec-ot>

