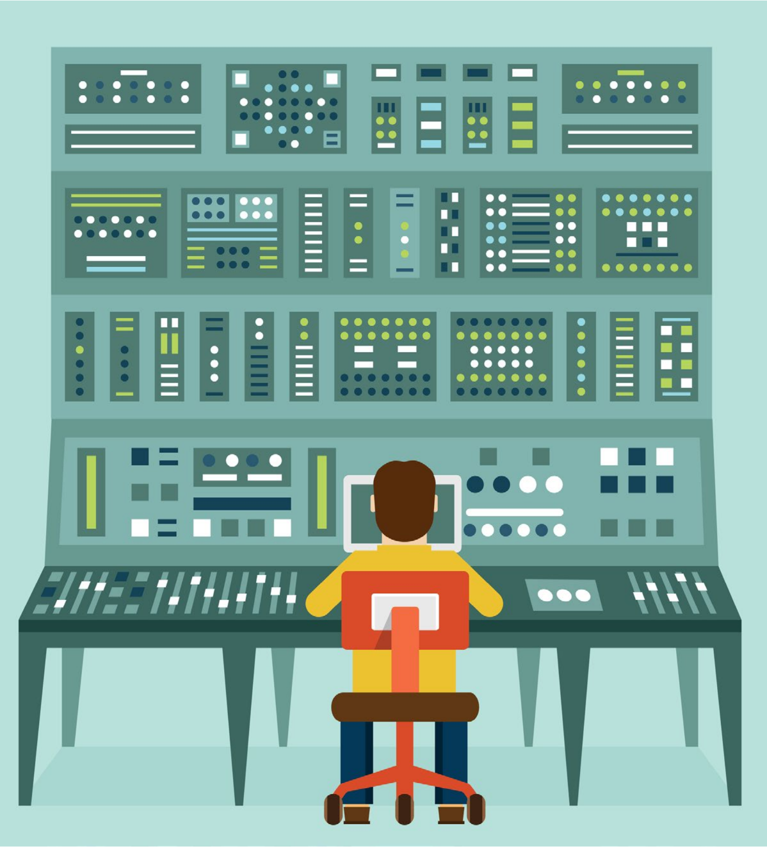
SANS | ICS SECURITY

Defending the Things that Make all the Things Work

Tim Conway - SANS

IT (Information Technology) and OT (Operational Technology)

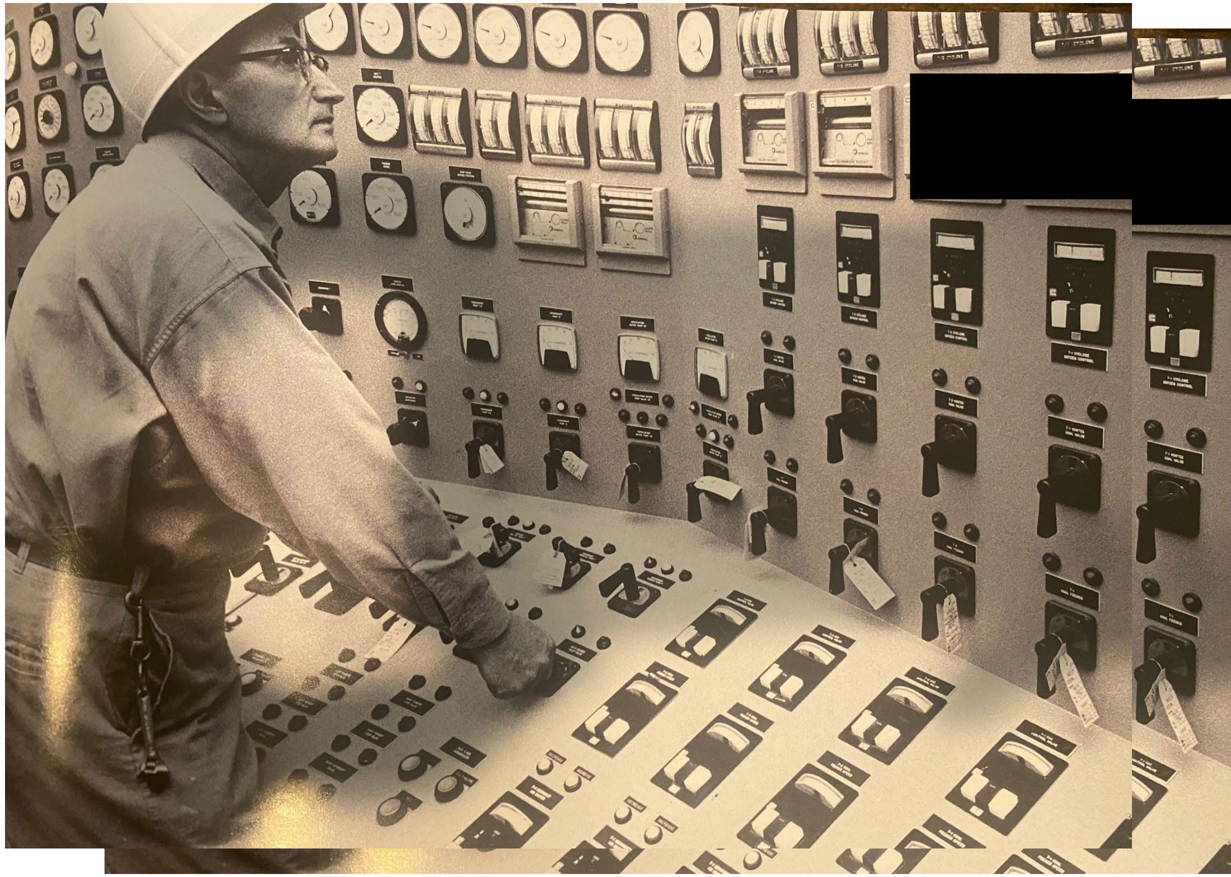
Data at rest, data in motion, and data in use



Data that does something in the physical world – kinetic component

Thinking About OT

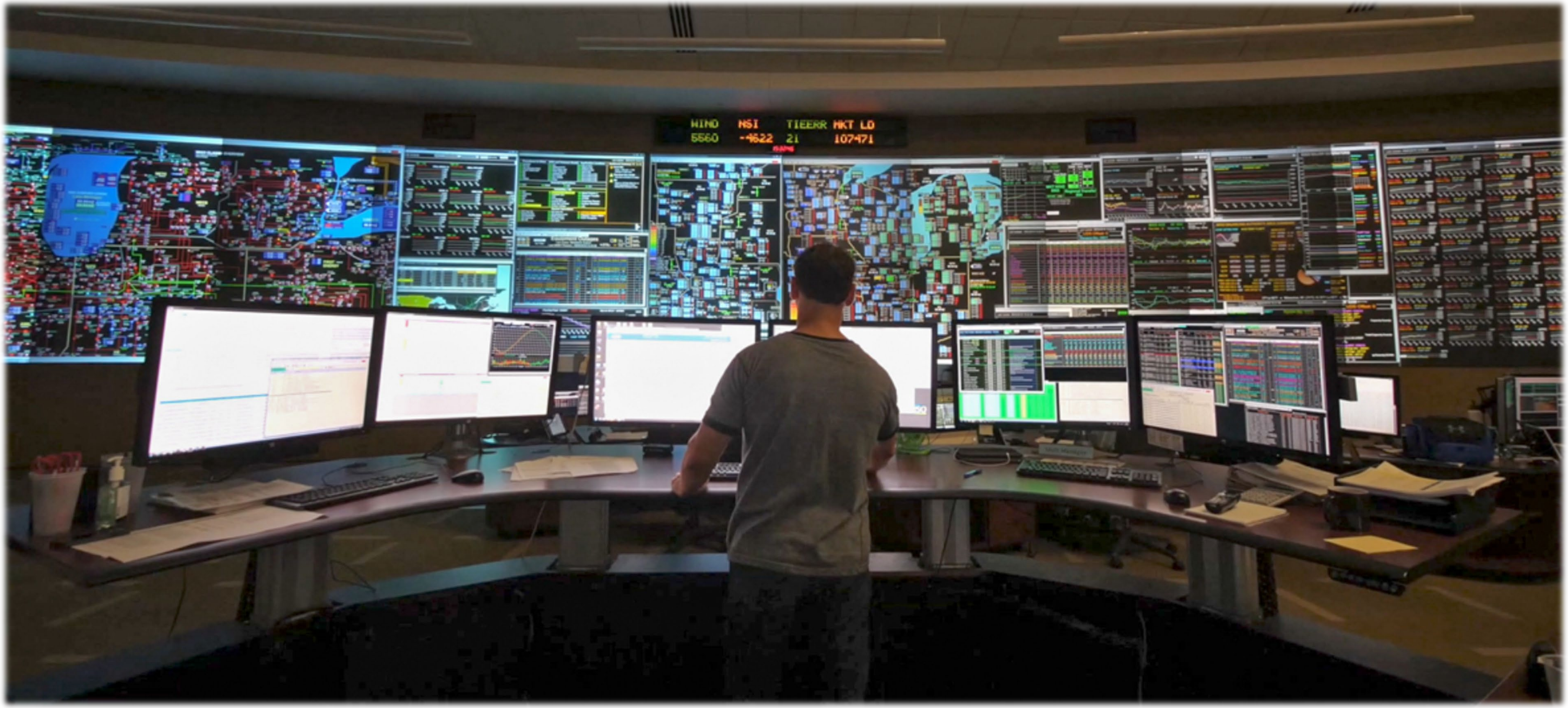
Dispatch operator manually tracking crews working in the field – 1940s



[redacted]

Generating station control room operator – 1960s

Cyber-Enabled Digital Controls



Changing Operational Environment

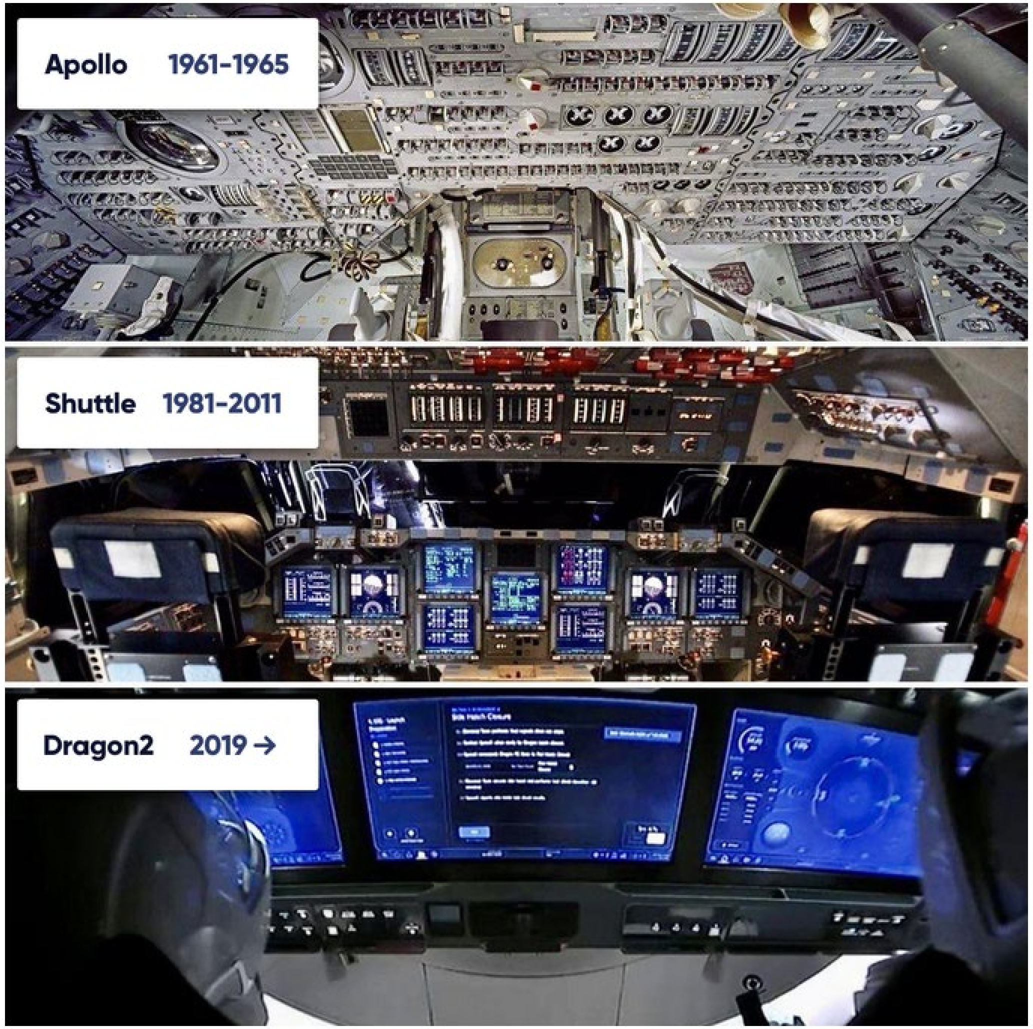


Image ref: https://uxdesign.cc/

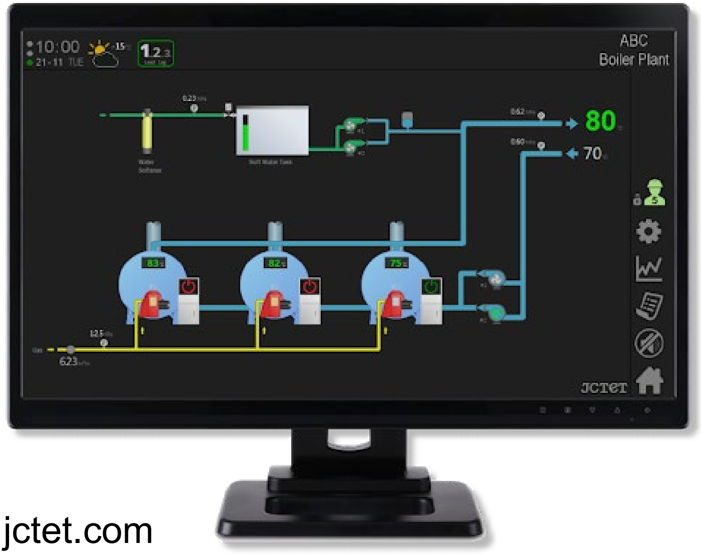


Image ref: http://www.jctet.com

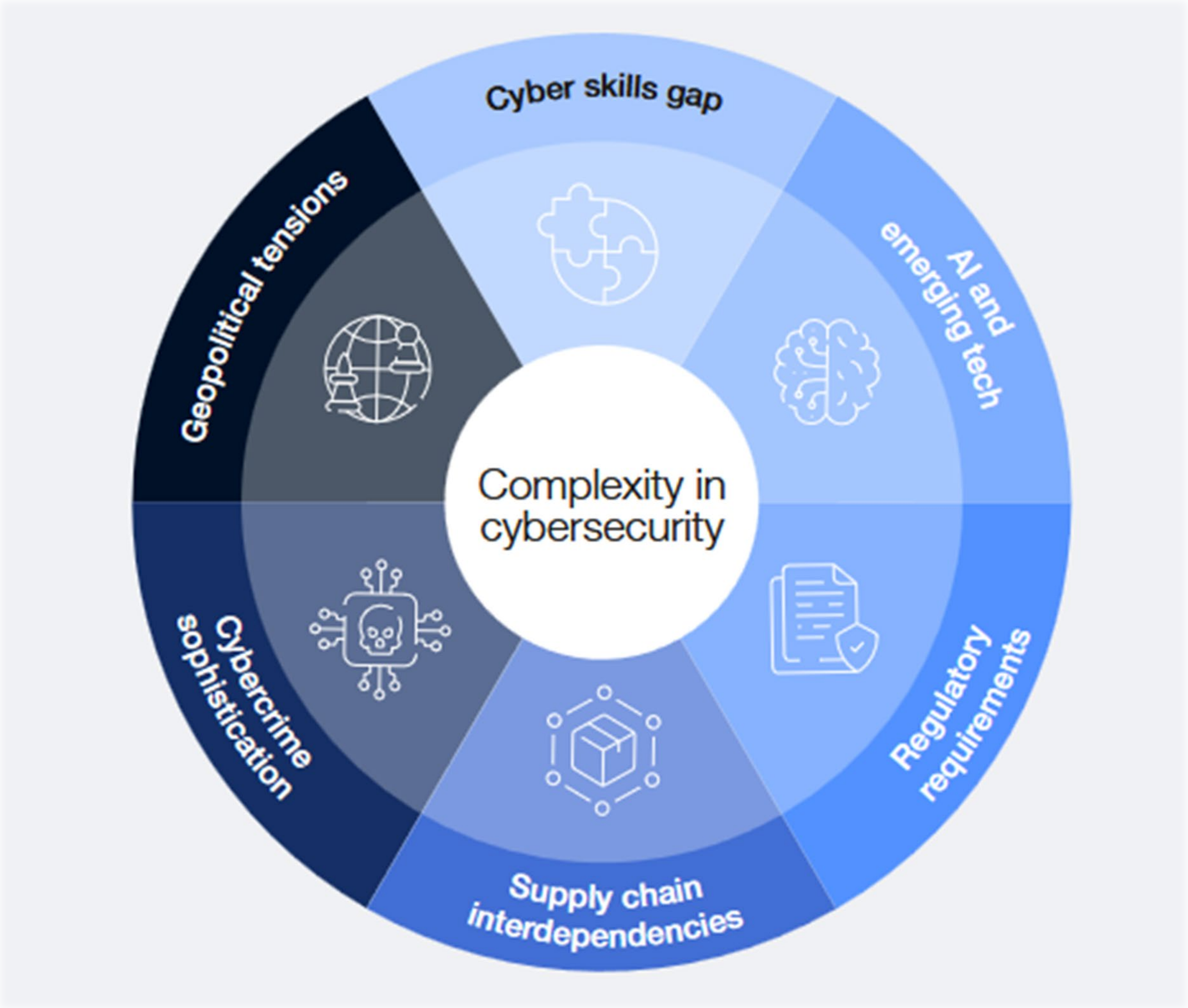
IT ←→ OT "its all just T"

"Critical Infrastructure organizations and Industrial Control Systems security practitioners cannot lose sight of what makes them special, there is a need for unique hybrid skill sets in this space that intersects operations, engineering, technology, security, and safety. It is crucial for an organization that these unique skill sets are developed and harnessed in a way that recognizes the operational drivers and constraints of the process environment and technology used to control it. IT and OT are different, the ICS community needs to focus on the unique demands that are represented by the first letter in those Acronyms and leverage the second letter in a manner that is informed by the risks to the organization and the overall mission."

#4 - Complexity

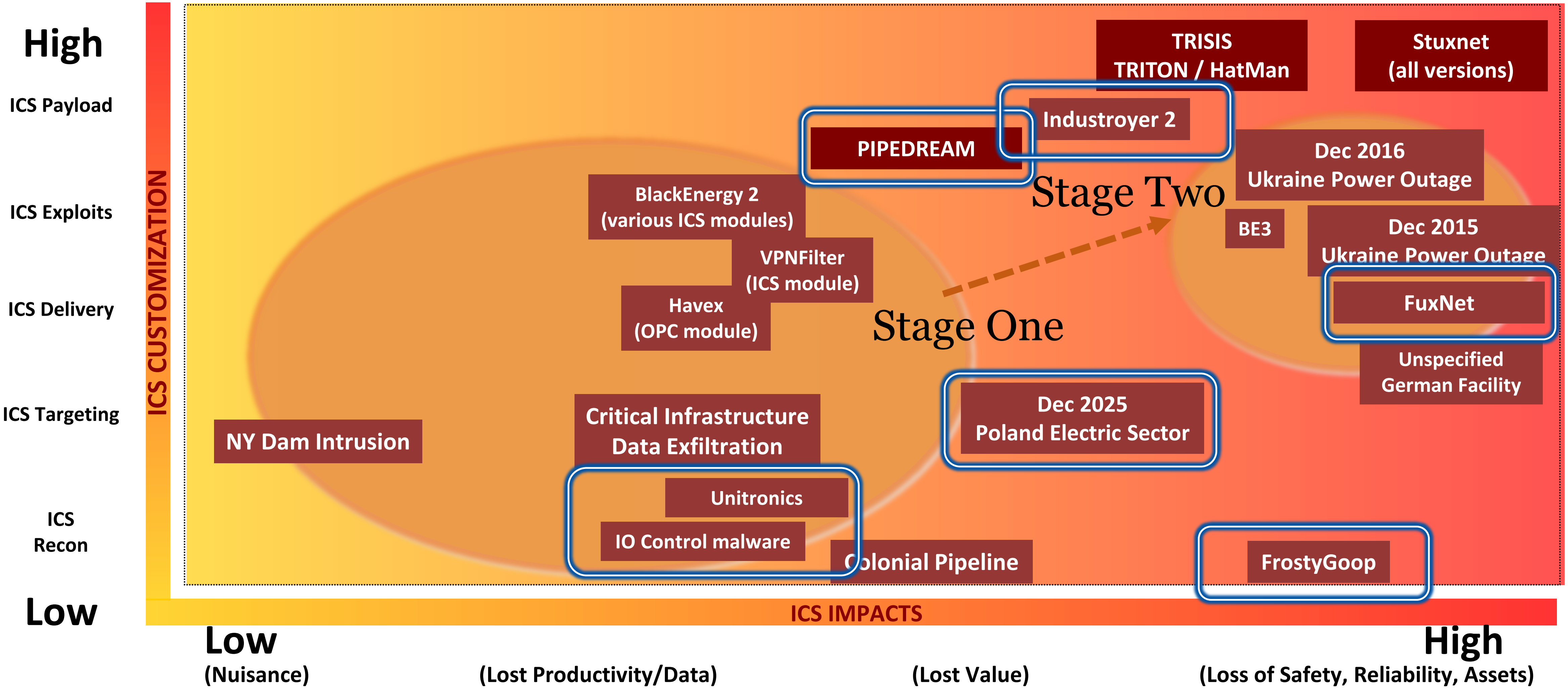
World Economic Forum – Global Cybersecurity Outlook 2025 Report

- Growing disparity between large and small organizations
- Regional variations are growing with perceived lack of critical infrastructure cyber resilience

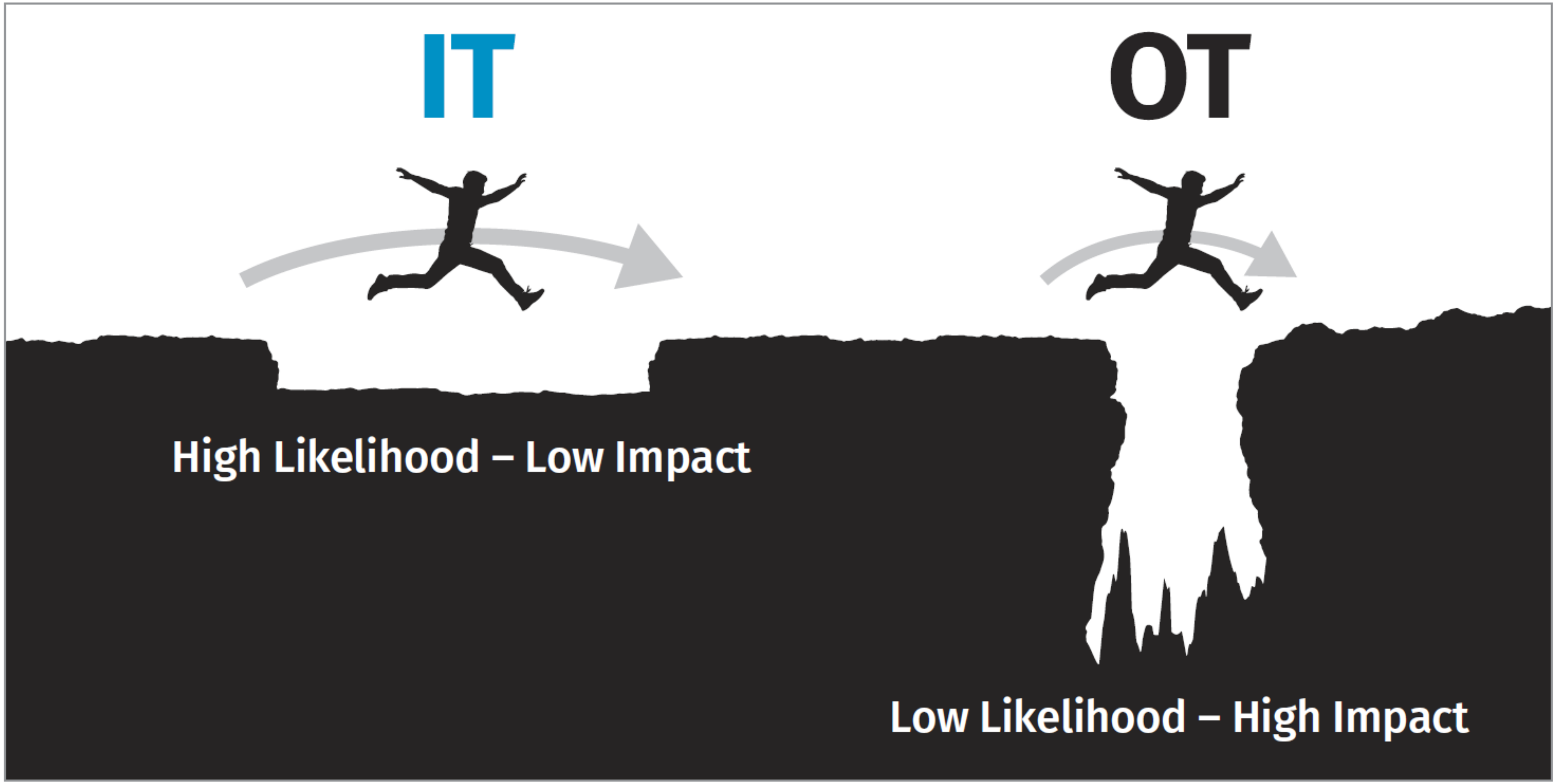

Complexity in cybersecurity
Cyber skills gap
AI and emerging tech
Regulatory requirements
Supply chain interdependencies
Cybercrime sophistication
Geopolitical tensions

Factors compounding the complex nature of cybersecurity

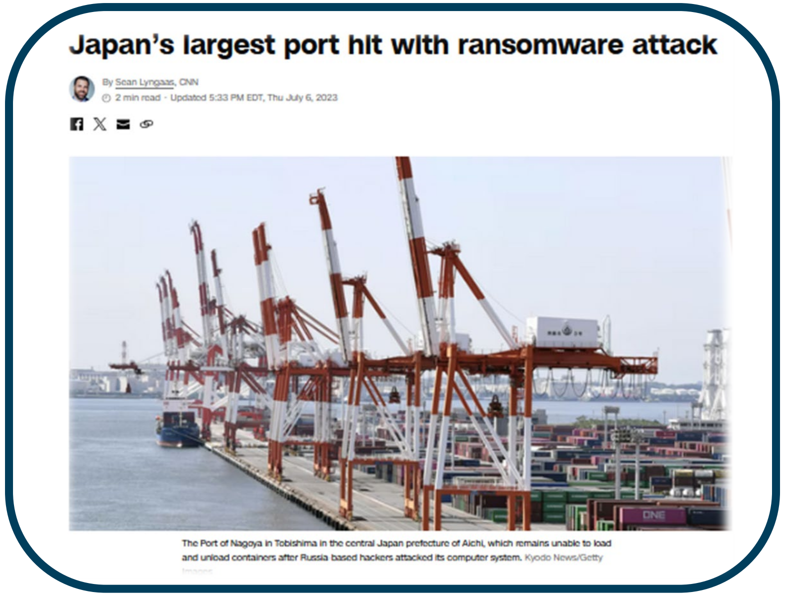
ICS Incidents & Access Campaigns



Impact to Organization



OT Impacting Ransomware & ICS Effects Based Targeting

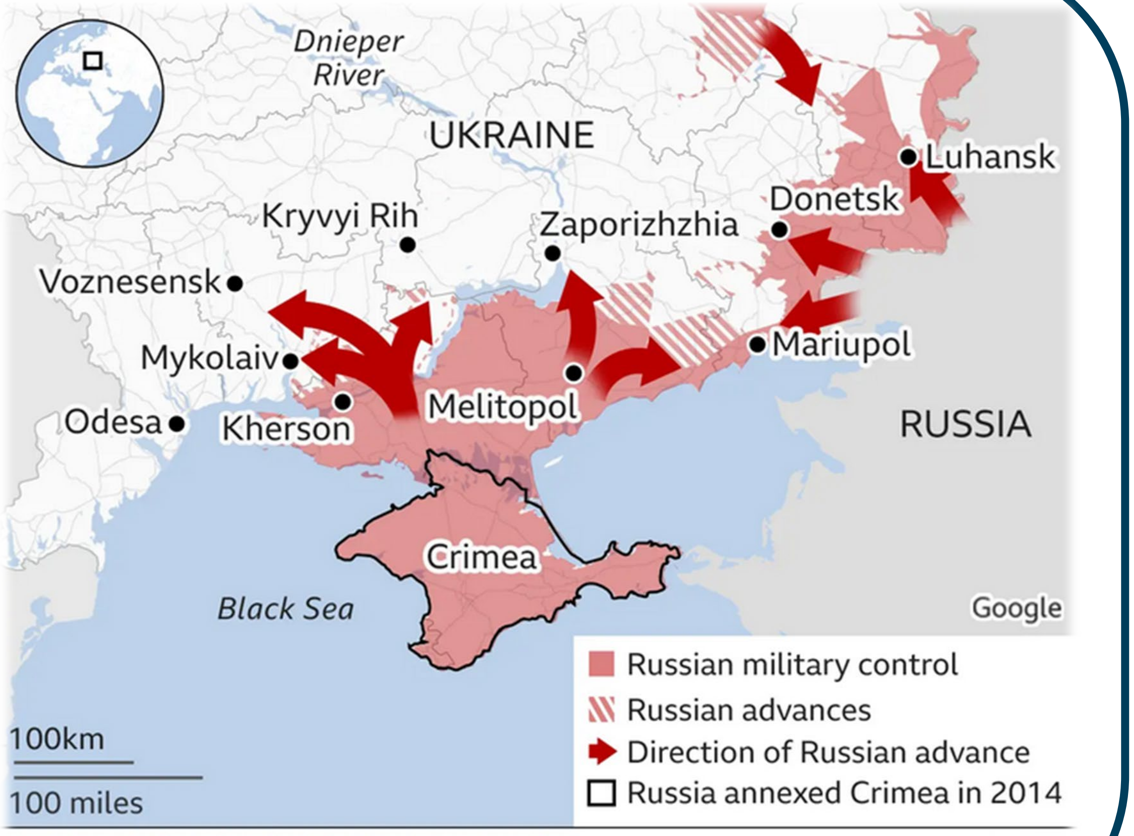


Japan's largest port hit with ransomware attack

By Sean Lyngaas, CNN

2 min read · Updated 5:33 PM EDT, Thu July 6, 2023

The Port of Nagoya in Tobishima in the central Japan prefecture of Aichi, which remains unable to load and unload containers after Russia based hackers attacked its computer system. Kyodo News/Getty Images



- 🟥 Russian military control
- ▨ Russian advances
- ➡ Direction of Russian advance
- □ Russia annexed Crimea in 2014

Source: UK MoD / Institute for the Study of War (21:00 GMT, 20 March) BBC

OT Impacting Ransomware

Criminal financially motivated adversary groups

- Well understood IT and business impacts

+ Impacts to operational environments

+ Impacts to delivery of product or service

+ Impacts to system integrity

Extreme growth in specific sectors (manufacturing, government, healthcare)

Lessons learned on:

- Recovery
- Ransom response planning
- User awareness
- End point protections
- Detection and active mitigations
- Role of cyber insurance

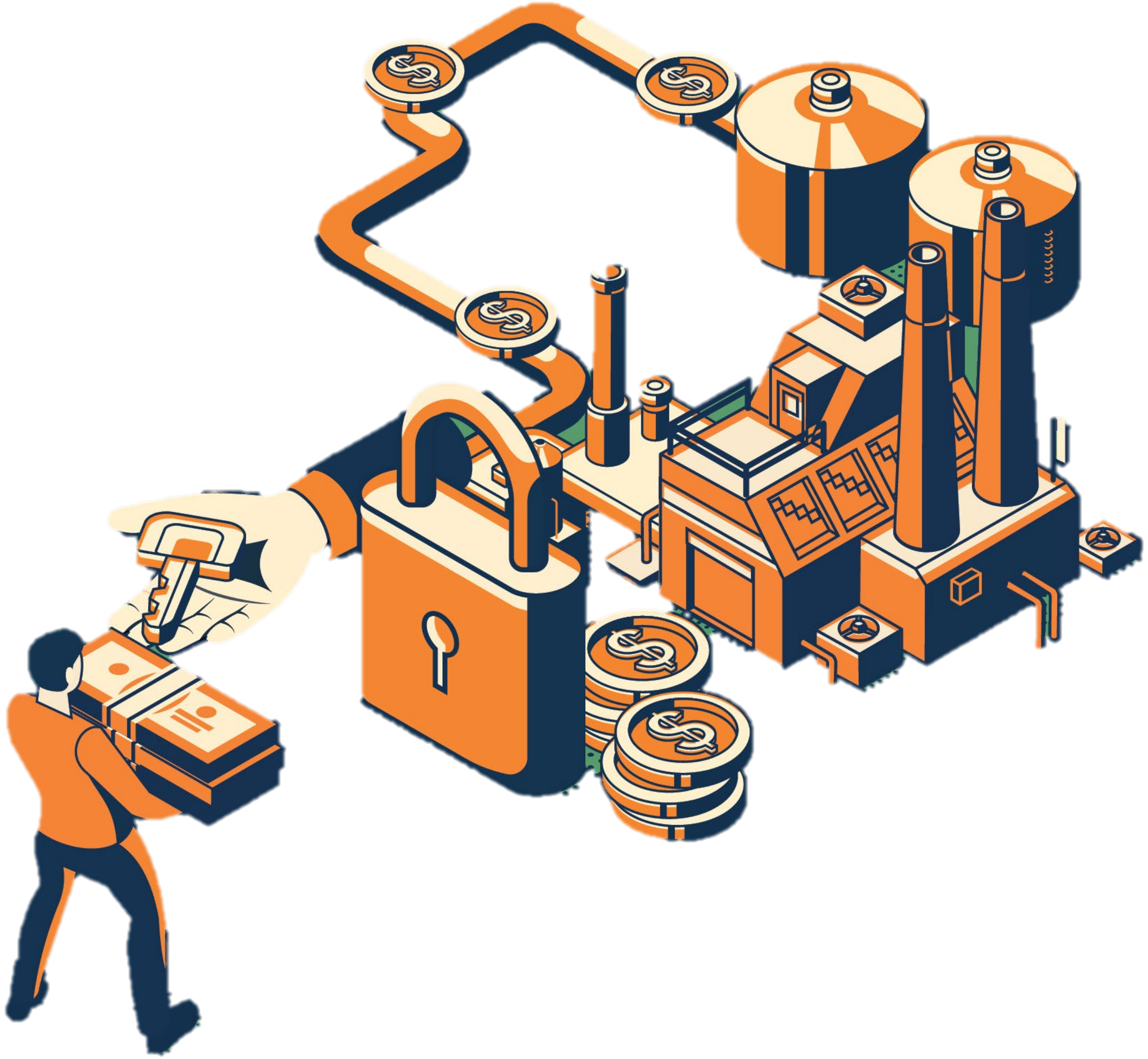
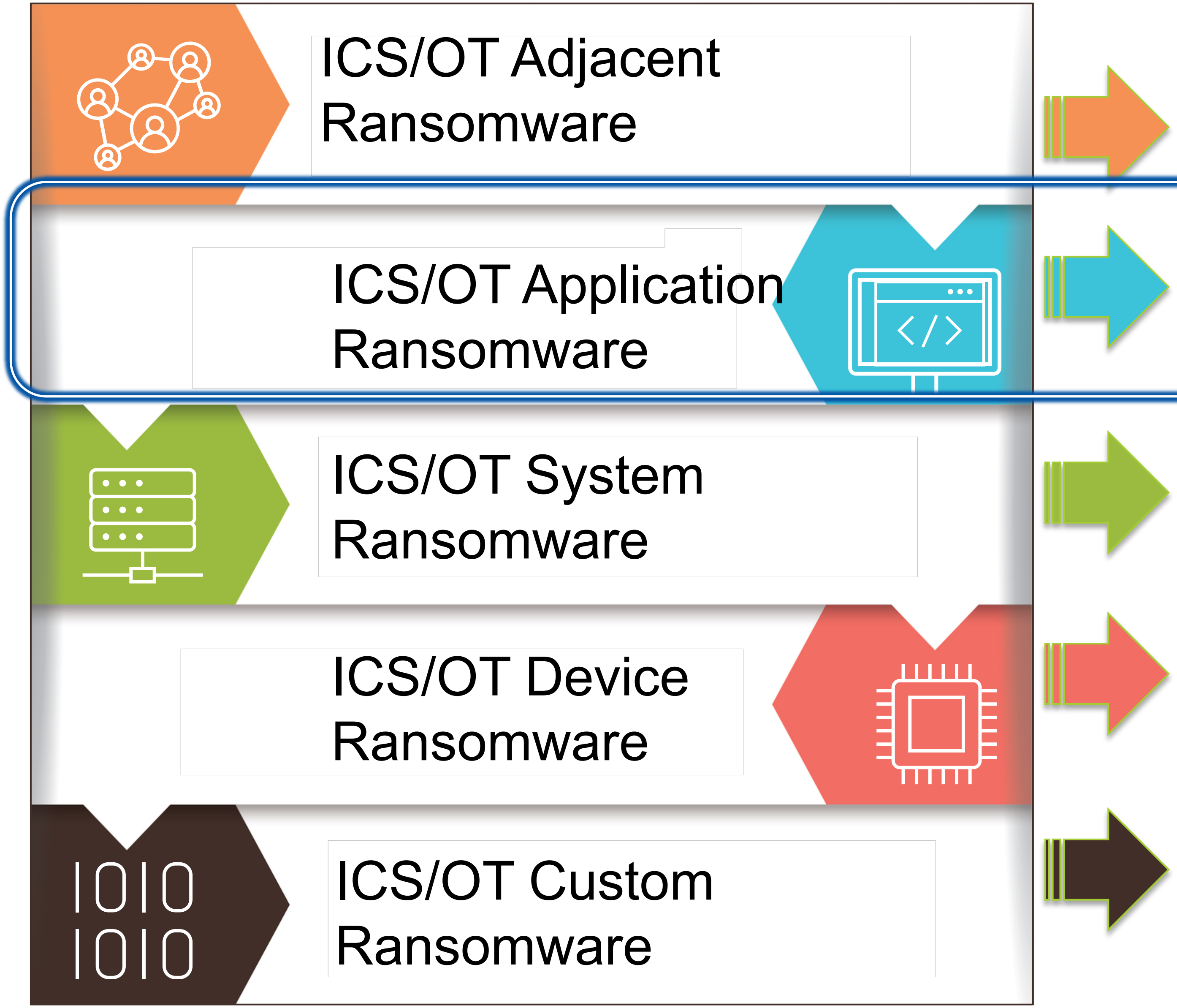


IMAGE USED WITH PERMISSION FROM SINGAPORE’S OT CYBERSECURITY MASTERPLAN 2024

Operations Impacting Ransomware



ICS/OT Adjacent Ransomware

ICS/OT Application Ransomware

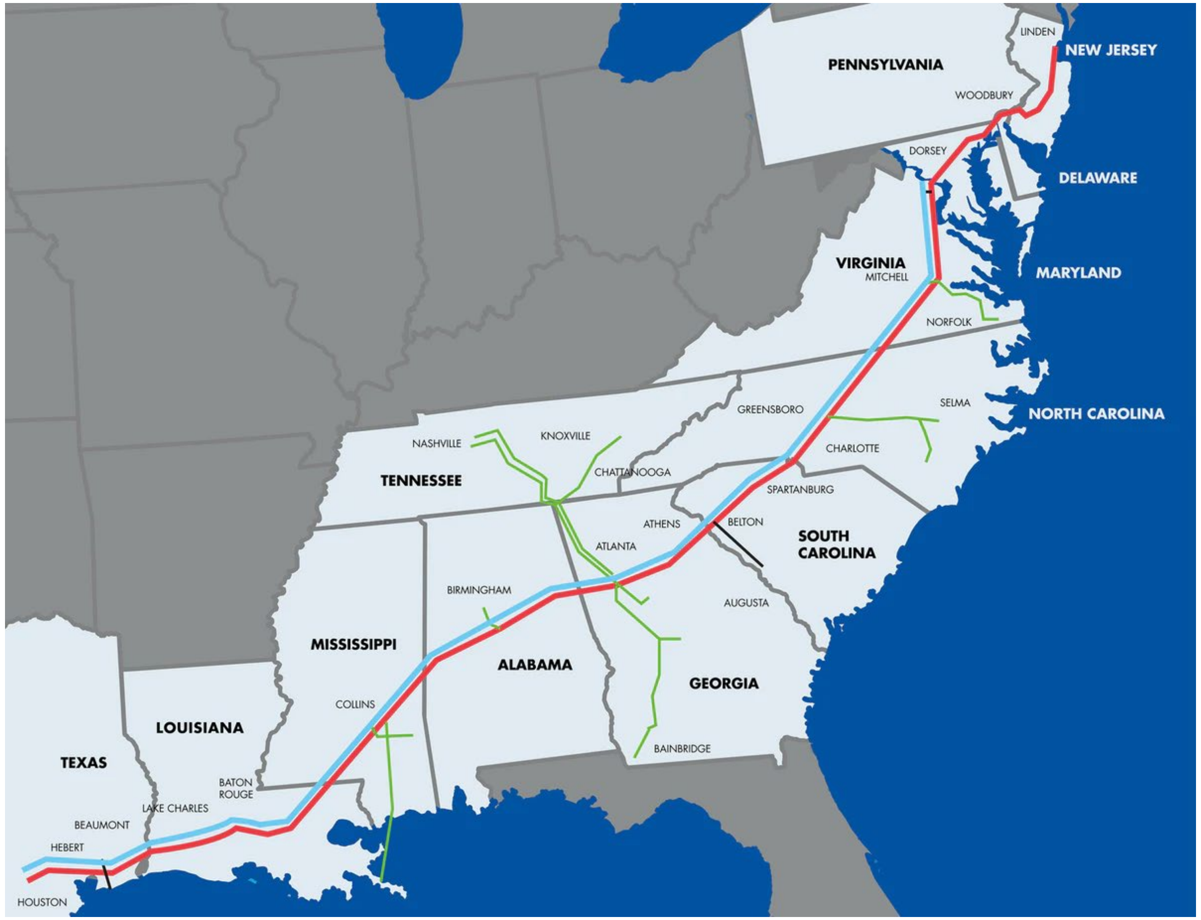
ICS/OT System Ransomware

ICS/OT Device Ransomware

ICS/OT Custom Ransomware

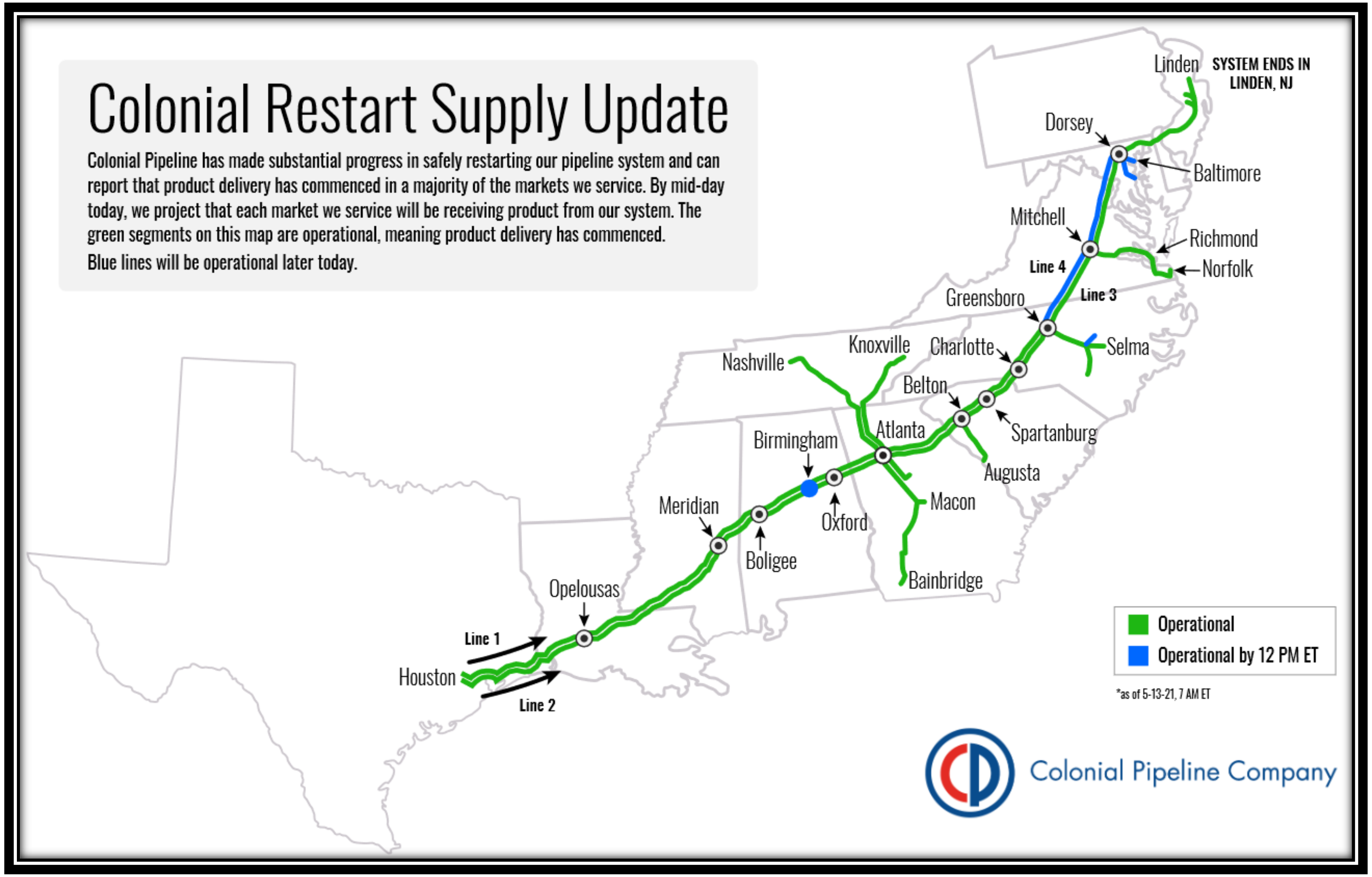
Target	Impact
IT systems	Integrity of adjacent ICS/OT systems
IT systems running key ICS/OT applications	Visibility into operations
ICS/OT systems performing operational tasks	Operational denial of service
ICS/OT device operational programming and configuration data	Visibility and reliable operation
ICS/OT devices or software	Impacting protocols, essential files, licensing, databases, critical tasks

Colonial Pipeline Details - 2021



- **Largest refined products pipeline in the US**
- **Moves 100 million gallons of fuel daily across 5,500 miles of pipeline**
- **Over 280 facilities and field terminals, transporting 45% of the fuel to the East Coast**
- **On Friday May 7th Colonial temporarily shut down all pipeline operations due to a ransomware attack on its IT business systems**

Restoration of Service



Colonial Restart Supply Update

Colonial Pipeline has made substantial progress in safely restarting our pipeline system and can report that product delivery has commenced in a majority of the markets we service. By mid-day today, we project that each market we service will be receiving product from our system. The green segments on this map are operational, meaning product delivery has commenced.

Blue lines will be operational later today.

🟩 Operational

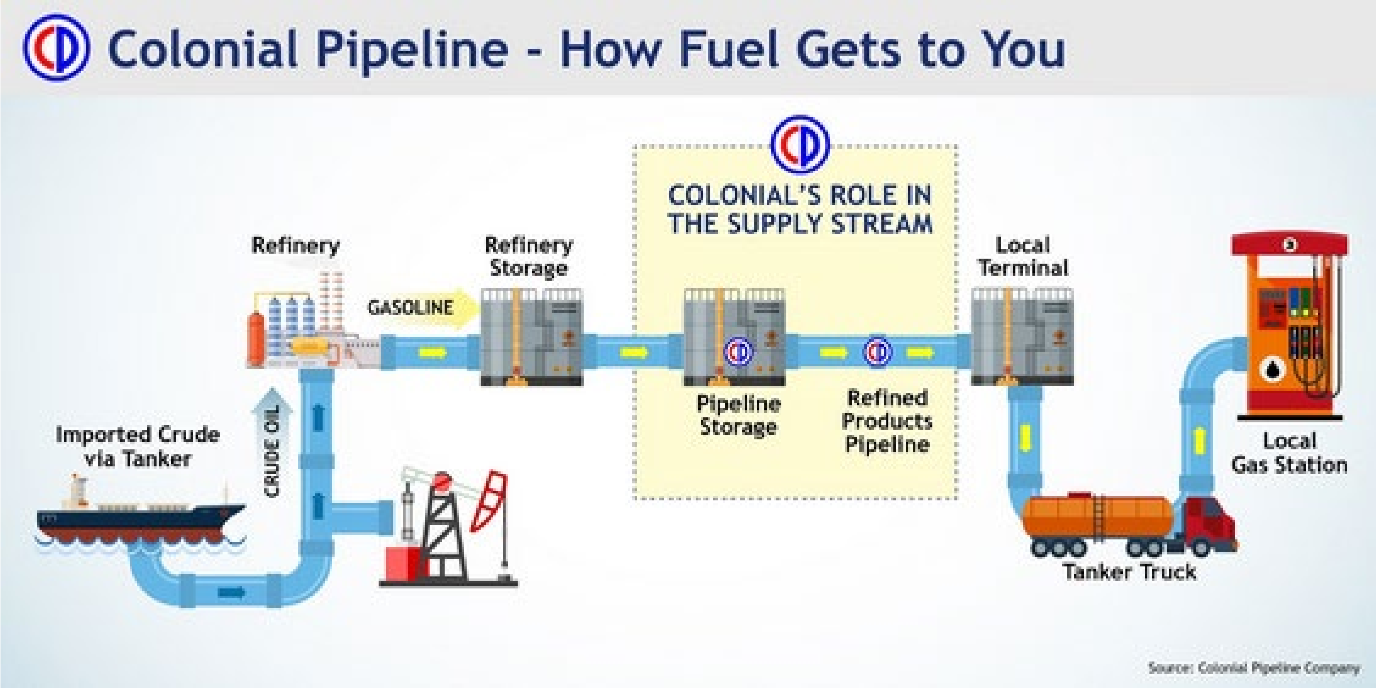
🟦 Operational by 12 PM ET

*as of 5-13-21, 7 AM ET

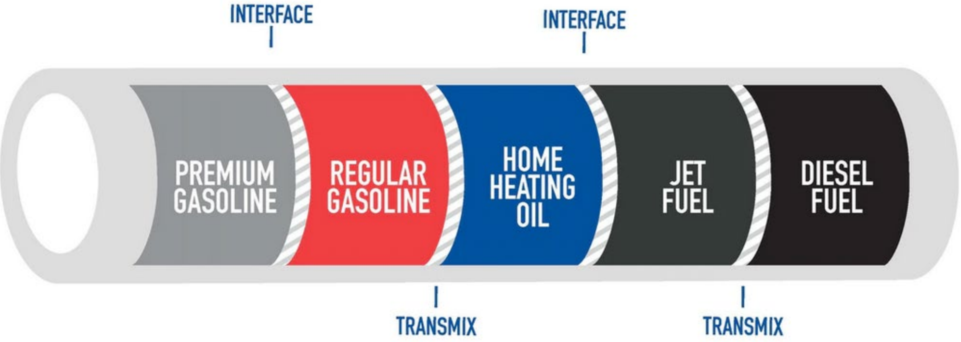
Colonial Pipeline Company

- 5 days after the operational impact – startup began at Wednesday May 12 at 5:11PM
- May 13th - product delivery commenced in most markets served
- All markets receiving product by mid-day

Numerous Products


Colonial Pipeline - How Fuel Gets to You
COLONIAL'S ROLE IN THE SUPPLY STREAM
Refinery
GASOLINE
Refinery Storage
Pipeline Storage
Refined Products Pipeline
Local Terminal
Local Gas Station
Tanker Truck
Imported Crude via Tanker
CRUDE OIL

Source: Colonial Pipeline Company

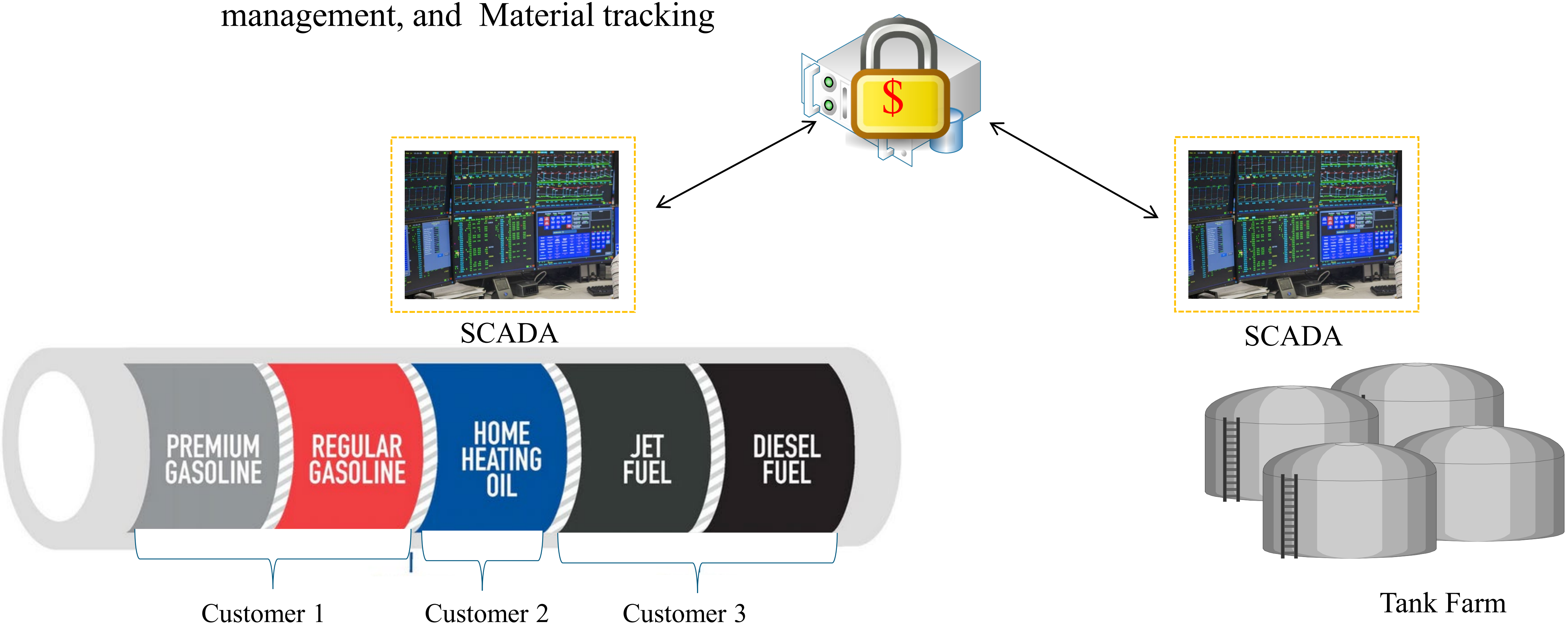


Product Sequencing

- Loaded in as batches
- Products blend with each other at interface points
- Interfaces are removed at destination sites
- Control Center SCADA system monitors flow, temperature, pressure, quality, and leak detection

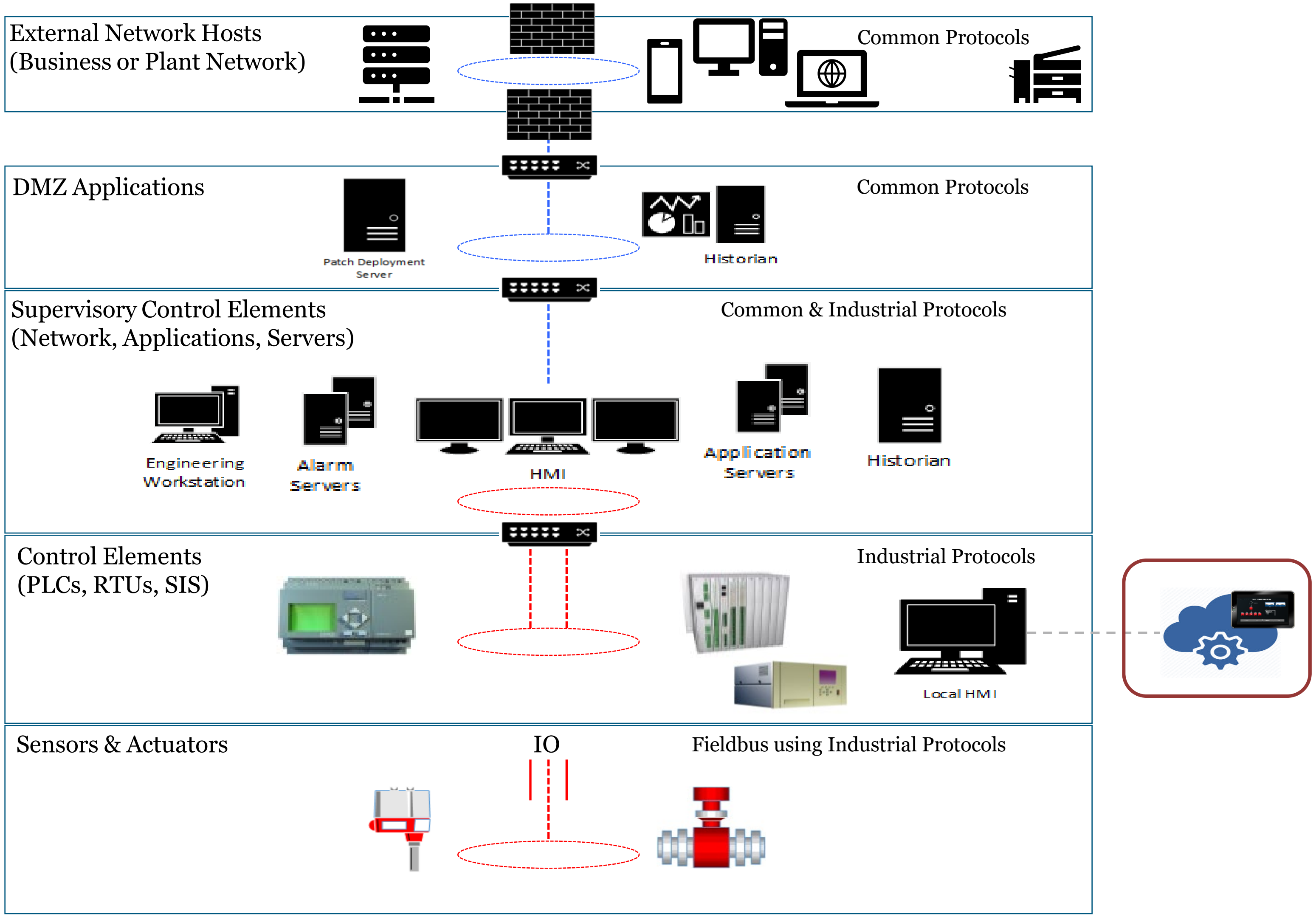
IT and OT Asset Critical Interdependencies

Critical Systems like Recipe management, Quality assurance, Work In Process (WIP) tracking, and genealogy, Performance management, and Material tracking



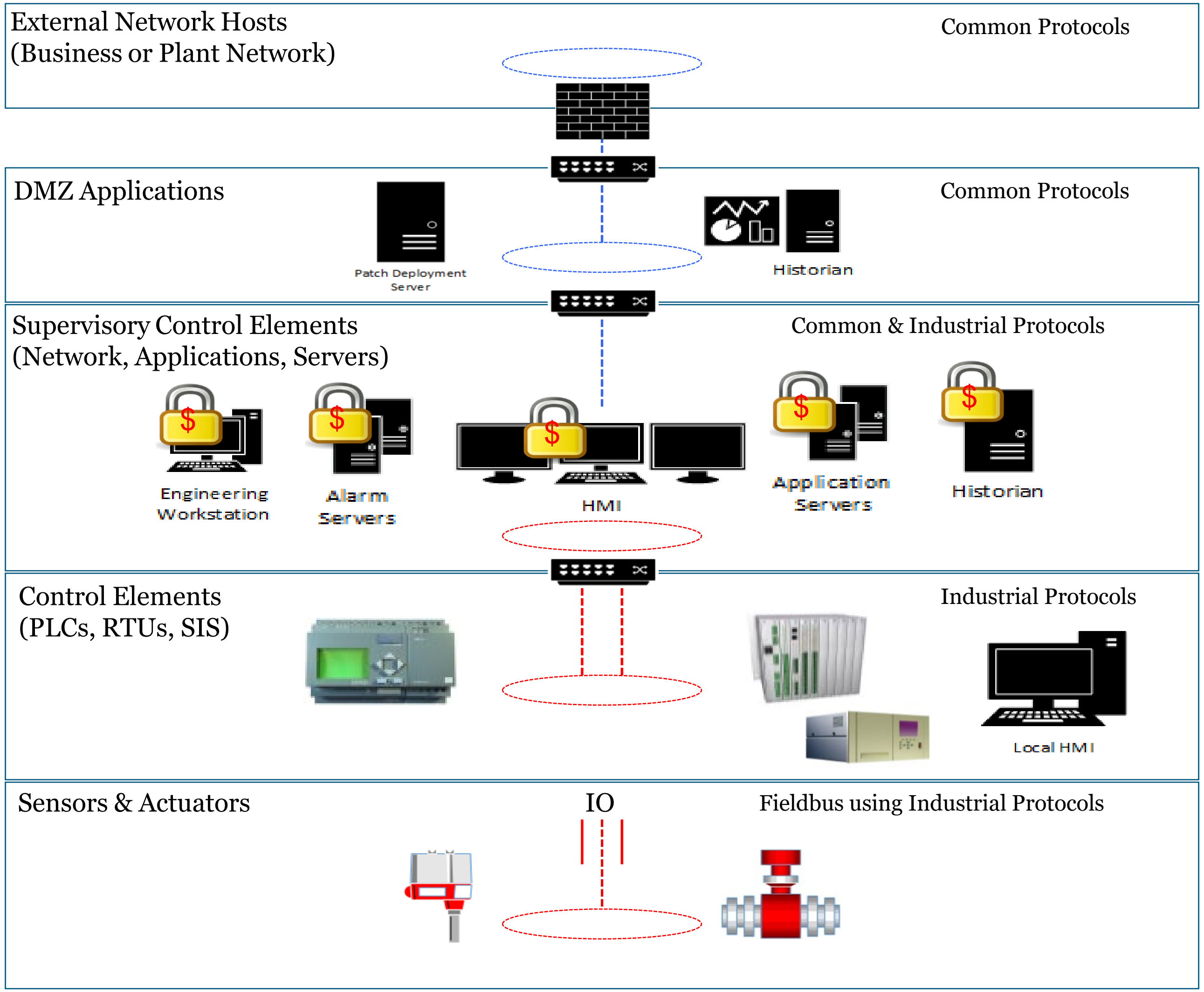
IT / OT and the “in between” aka bridges for business / badness

- Attacks on corporate IT networks that pivot over trusted communications to resources in industrial DMZs
- Impacts to systems with connectivity into both IT and OT environments, causing disruptions
- Connections to partner networks that could extend impacts beyond target



OT Assets – Ransomware Low Hanging Fruit

- Typical Ransomware targets computer systems, not embedded systems like PLC's
- Affects include but are not limited to:
  - No access to design tools on engineering workstations
  - Loss of process visibility (HMI) & alarm servers
  - Loss of historical data
  - Loss of quality assurance systems
  - Loss of analytics tools
  - Loss of SCADA functions
  - Inability to authenticate users



External Network Hosts
(Business or Plant Network)

Common Protocols

DMZ Applications

Common Protocols

Supervisory Control Elements
(Network, Applications, Servers)

Common & Industrial Protocols

Control Elements
(PLCs, RTUs, SIS)

Industrial Protocols

Sensors & Actuators

IO

Fieldbus using Industrial Protocols

ICS Effects Based Targeting

- Process Discovery
- Manipulating Protection
- Misuse to Destruction

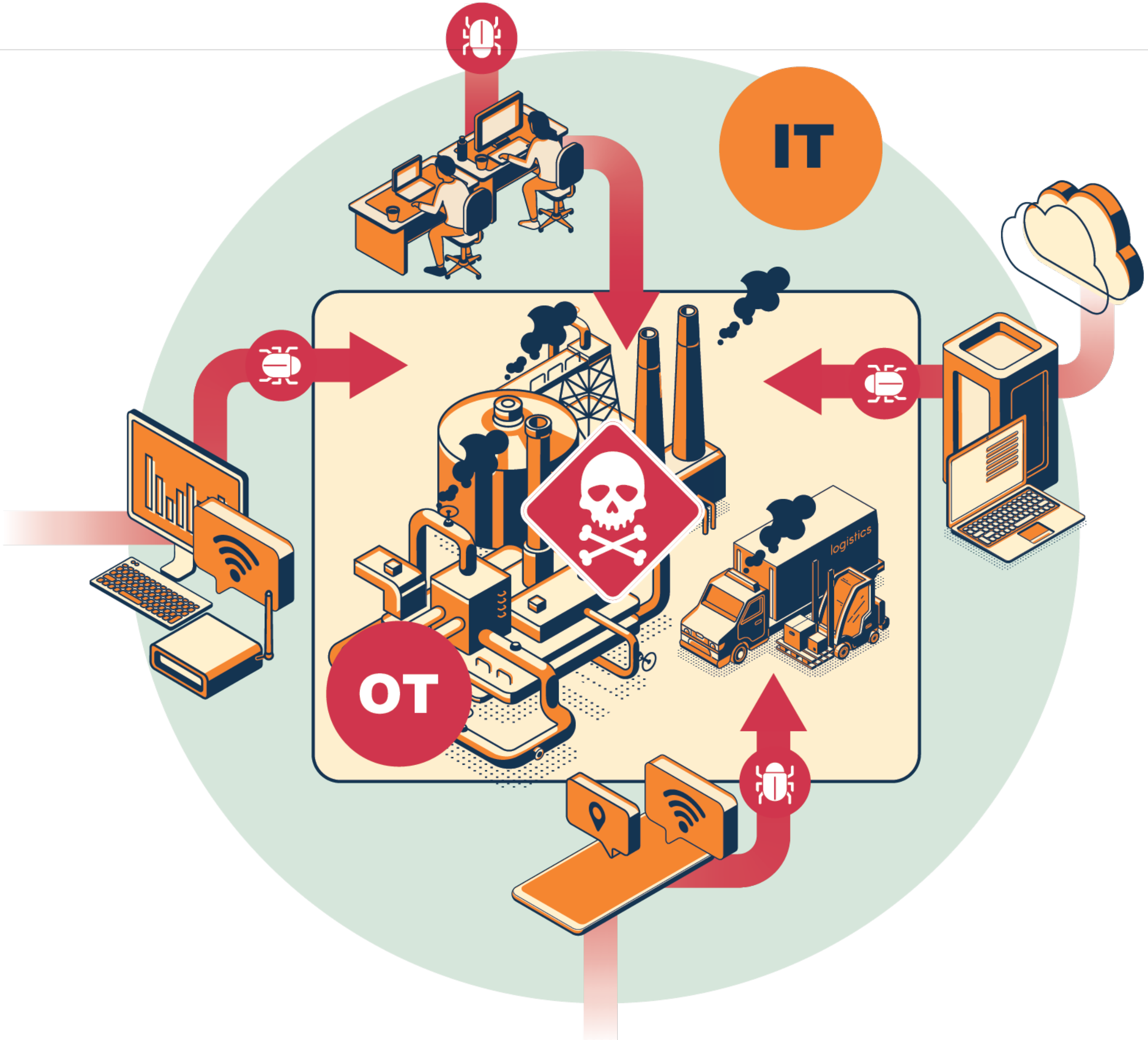
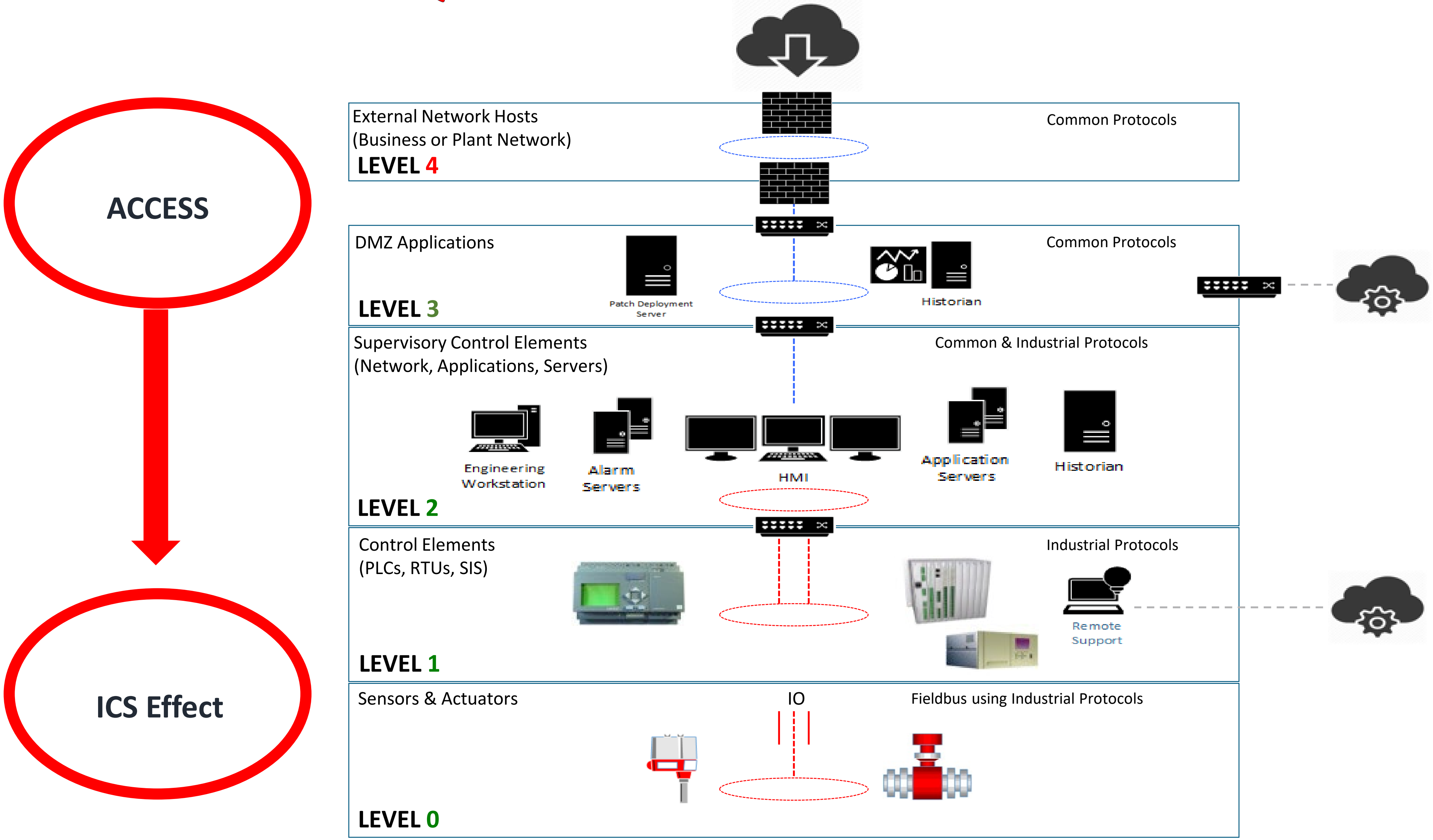


IMAGE USED WITH PERMISSION FROM SINGAPORE'S OT CYBERSECURITY MASTERPLAN 2024

REQUIRES MULTI-STAGED ATTACKS



ACCESS

ICS Effect

External Network Hosts
(Business or Plant Network)
LEVEL 4

Common Protocols

DMZ Applications

LEVEL 3

Patch Deployment Server

Historian

Common Protocols

Supervisory Control Elements
(Network, Applications, Servers)

Common & Industrial Protocols

Engineering Workstation

Alarm Servers

HMI

Application Servers

Historian

LEVEL 2

Control Elements
(PLCs, RTUs, SIS)

Industrial Protocols

Remote Support

LEVEL 1

Sensors & Actuators

IO

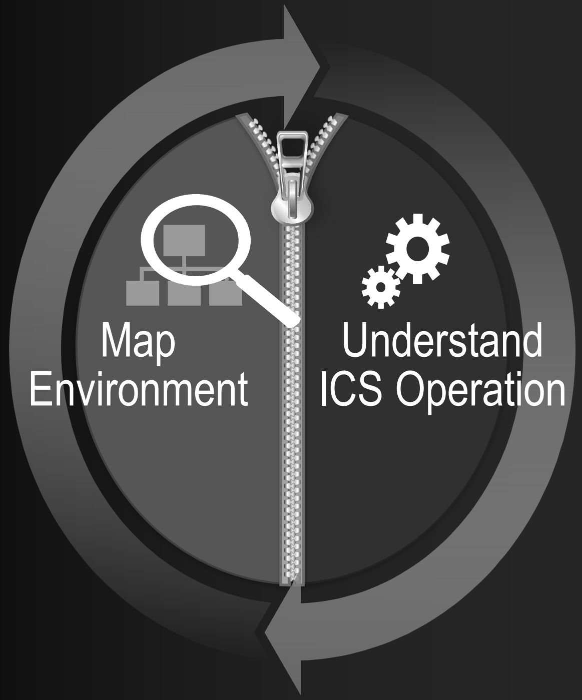
Fieldbus using Industrial Protocols

LEVEL 0

Building Bridges

Stage 1

- Adversary has successfully performed the necessary elements of the Stage 1 Kill chain
- To have an ICS effect the adversary needs to move into the elements of the Stage 2 ICS Kill Chain

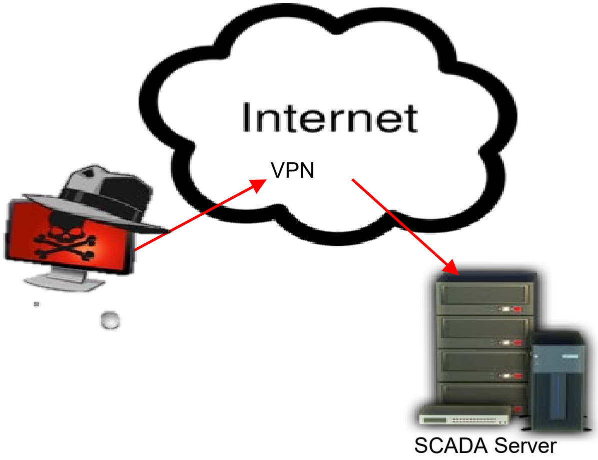


- Trusted connections
- Vendor access
- Support personnel remote access
- System backup or alternate site replication tasks
- System Mgmt. communications – patching, monitoring, alerting, configuration and change Mgmt.
- Data historians
- Direct access dial up
- Waterholing attacks
- Social Engineering

Stage 2

- When the adversary has identified a path into the ICS environment the Stage 2 ICS Kill Chain elements can be acted upon

Ukraine Electric Distribution System Attack

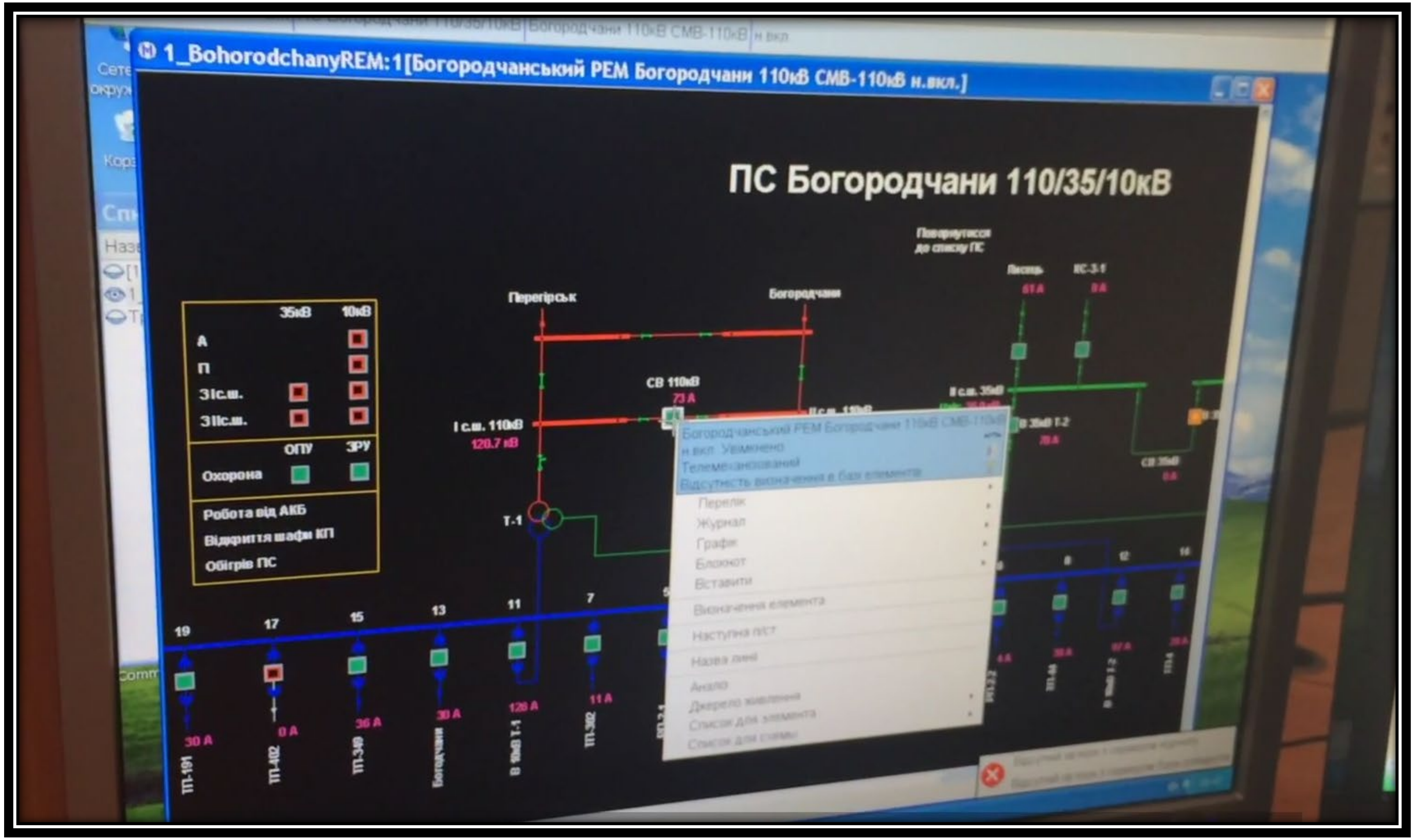


Rogue Client
Remote SCADA Client Software

Phantom Mouse
Remote Amin Tools at OS-level

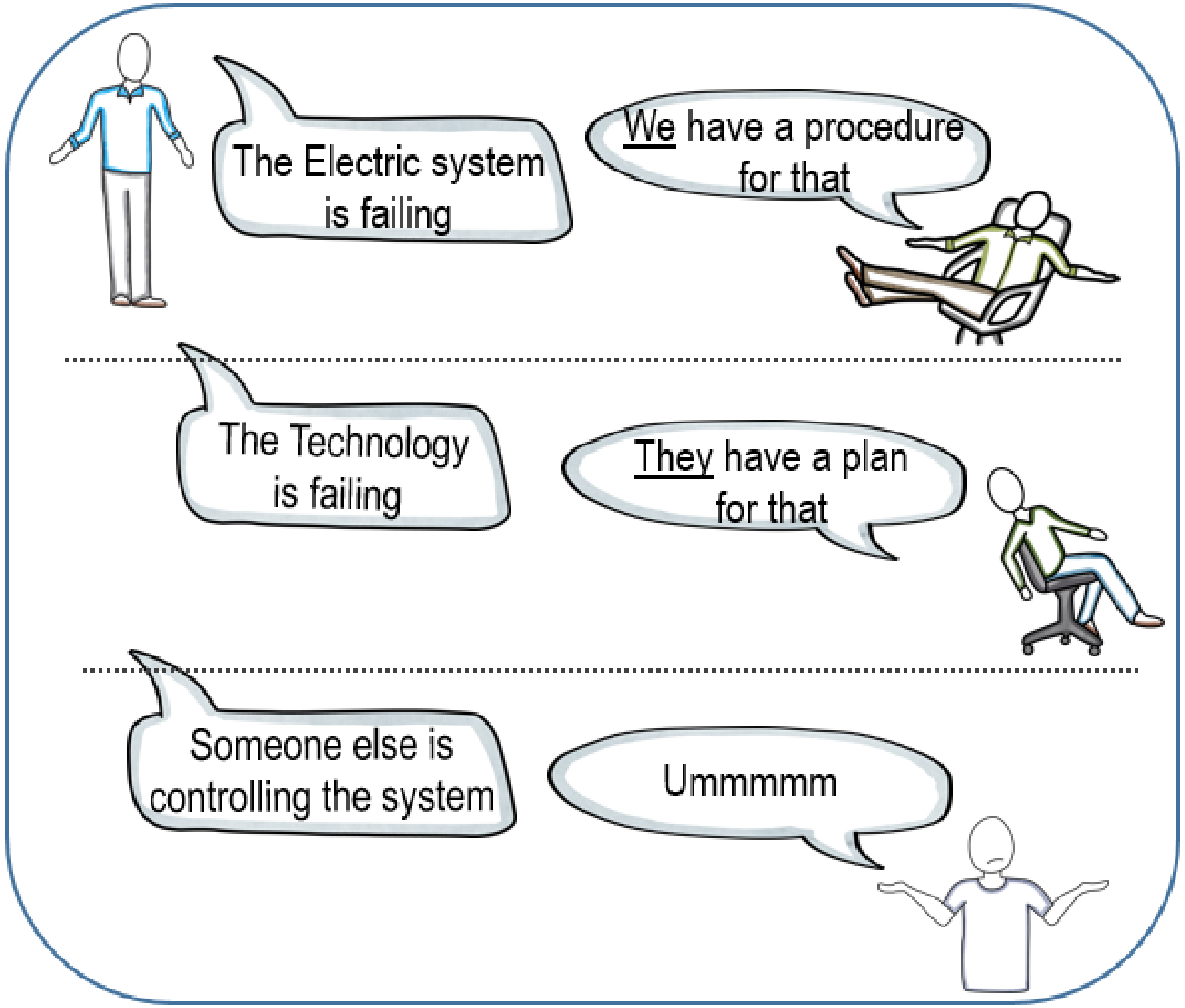
The attackers develop two SCADA Hijack approaches (one custom and one agnostic) and successfully used them across different types of SCADA/DMS implementations at three companies

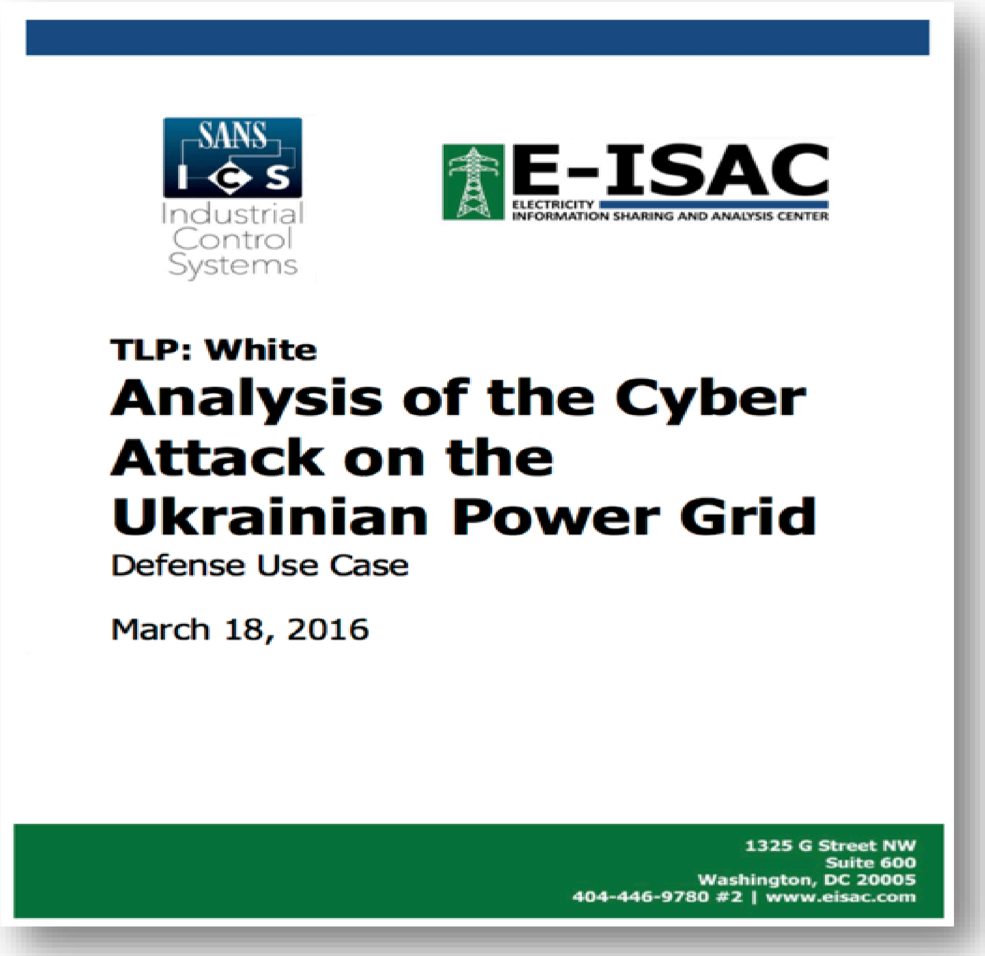
What Did They Do? What Have We Learned?



https://www.wired.com/story/russian-hackers-attack-ukraine/

2015 Lesson Learned


The Electric system is failing
We have a procedure for that
The Technology is failing
They have a plan for that
Someone else is controlling the system
Ummmmm



SANS ICS Industrial Control Systems

E-ISAC ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

TLP: White

Analysis of the Cyber Attack on the Ukrainian Power Grid

Defense Use Case

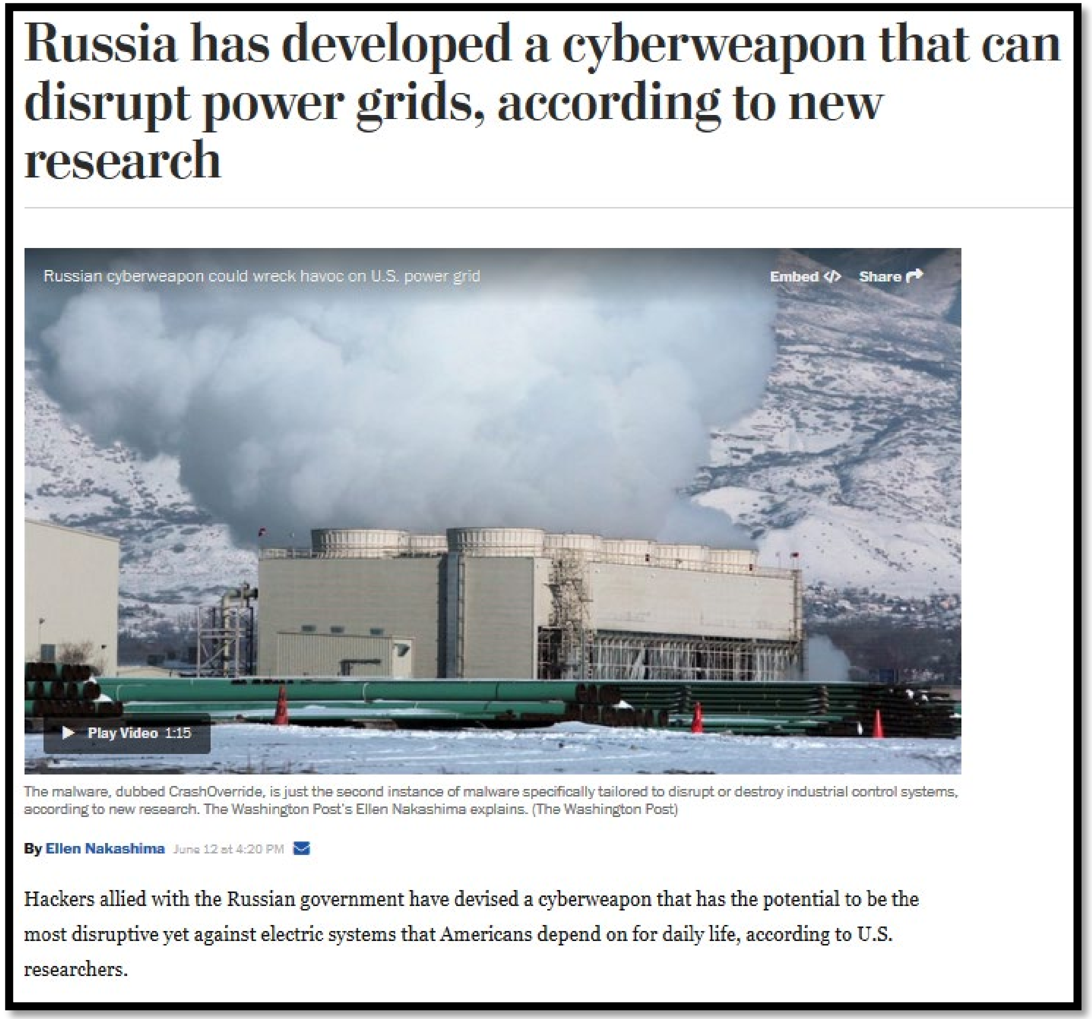
March 18, 2016

1325 G Street NW
Suite 600
Washington, DC 20005
404-446-9780 #2 | www.eisac.com

https://www.esisac.com http://ics.sans.org/ics-library

Ukraine Electric Transmission System Attack

Malware Discovery Associated with Electric Outages



Russia has developed a cyberweapon that can disrupt power grids, according to new research

The malware, dubbed CrashOverride, is just the second instance of malware specifically tailored to disrupt or destroy industrial control systems, according to new research. The Washington Post's Ellen Nakashima explains. (The Washington Post)

By Ellen Nakashima June 12 at 4:20 PM

Hackers allied with the Russian government have devised a cyberweapon that has the potential to be the most disruptive yet against electric systems that Americans depend on for daily life, according to U.S. researchers.

ANDY GREENBERG SECURITY 06.13.17 12:41 PM

'CRASH OVERRIDE': THE MALWARE THAT TOOK DOWN A POWER GRID

Cyber firms warn of malware that could cause power outages

INDUSTROYER

eset ENJOY SAFER TECHNOLOGY™

DRAGOS

CRASH OVERRIDE

Analysis of the Threat to Electric Grid Operations

Demonstrated Complexity is Escalating

ICS Attacks

225k

Ukraine 2015

Three electric utilities attacked through a cyber means resulting in 225k customers out of power

200 MW

Ukraine 2016

Electric transmission substation attacked through a cyber means

SIS

Middle East Facility 2017

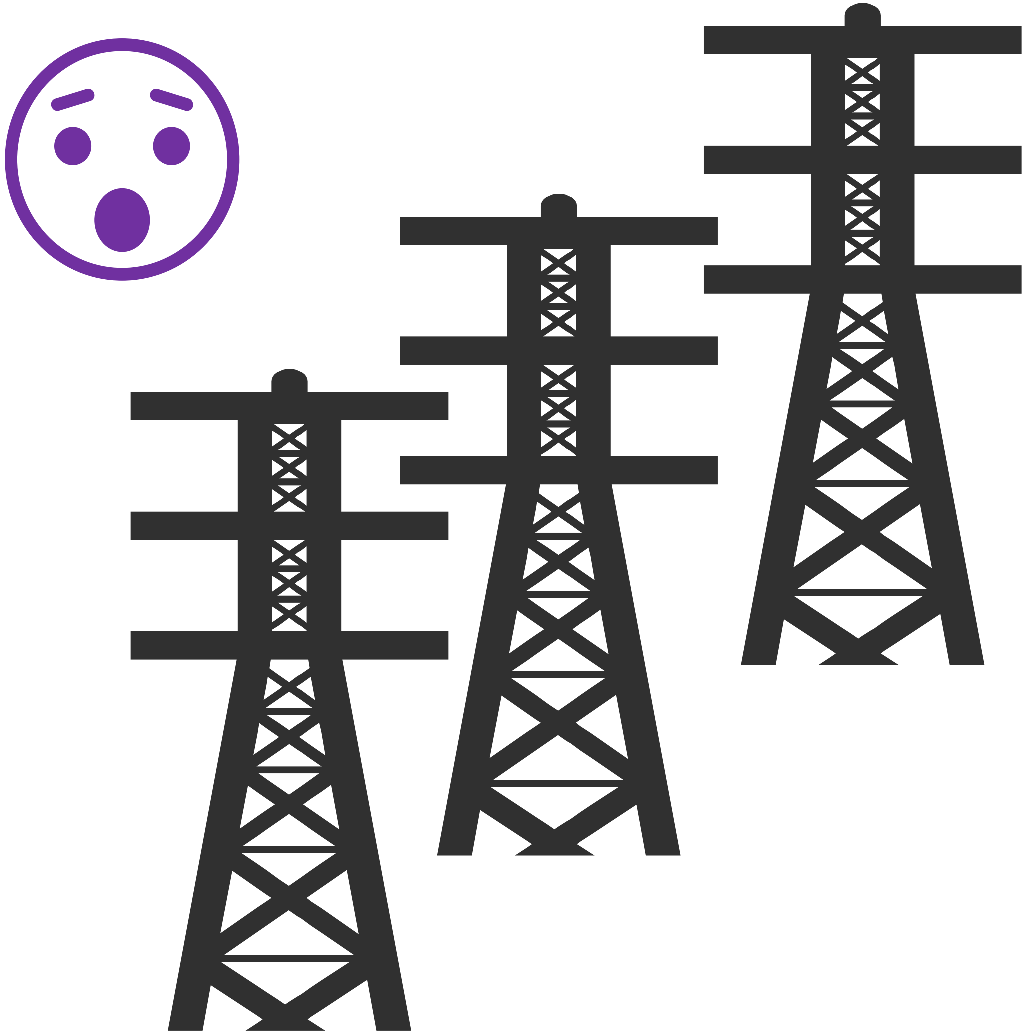
Safety Instrumented System, targeted and impacted

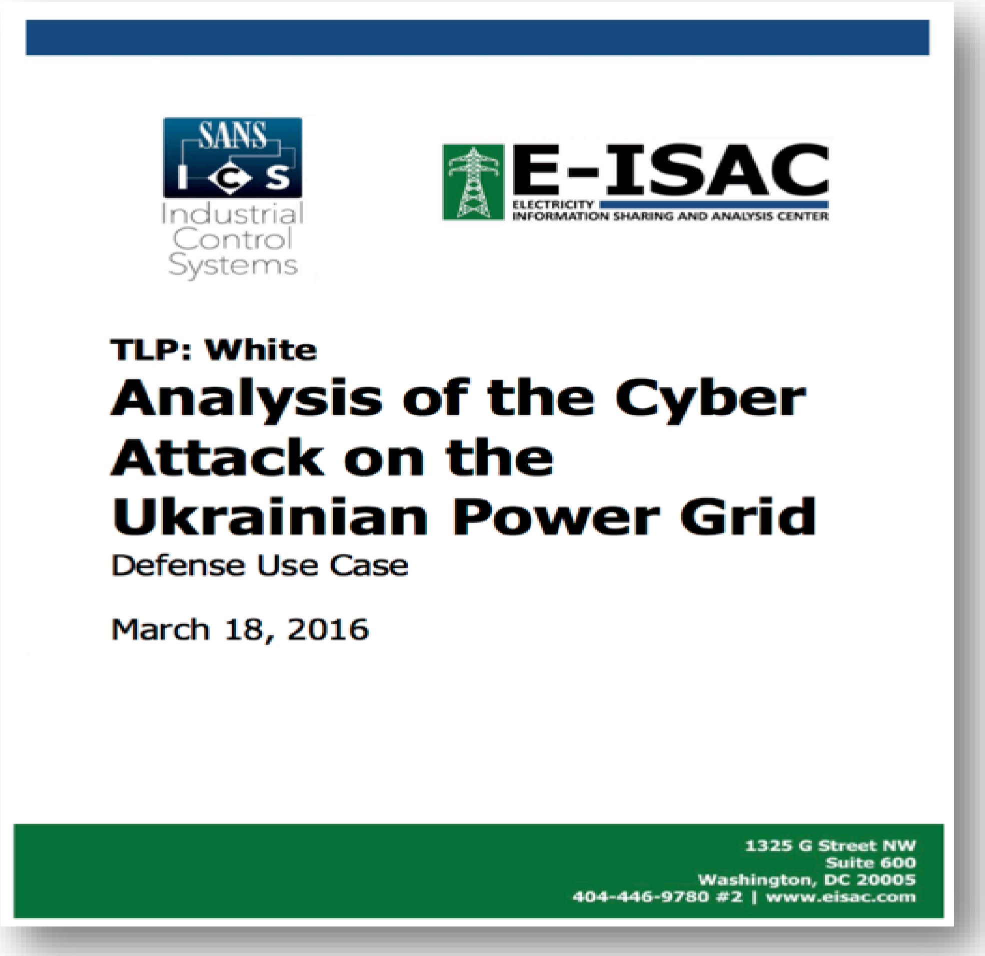
?

Combination

Safety or protection system manipulation followed by intentional control system misuse to cause equipment damage and human health and safety impact

2016 Lesson Learned





SANS ICS Industrial Control Systems

E-ISAC ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

TLP: White

Analysis of the Cyber Attack on the Ukrainian Power Grid

Defense Use Case

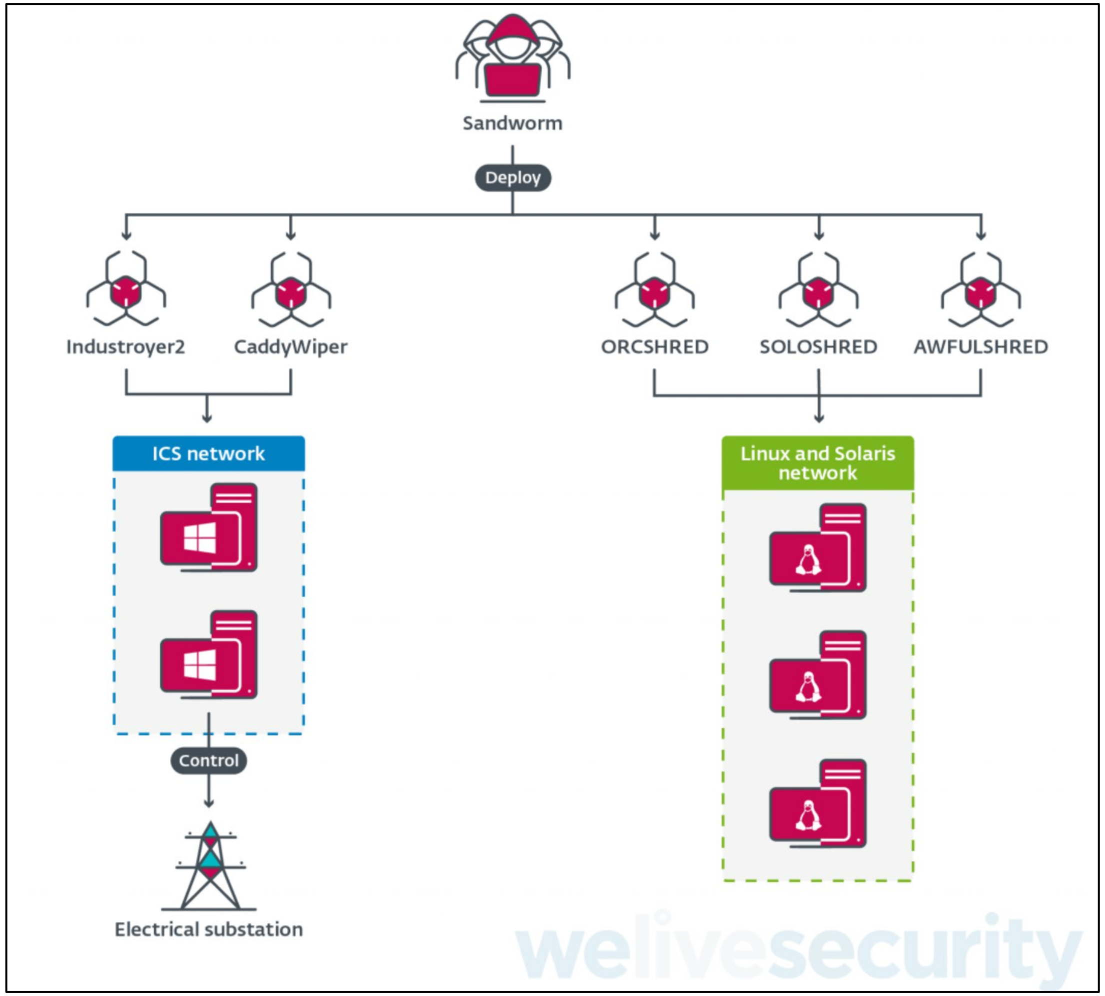
March 18, 2016

1325 G Street NW
Suite 600
Washington, DC 20005
404-446-9780 #2 | www.eisac.com

https://www.esisac.com

http://ics.sans.org/ics-library

Ongoing Ukrainian Electric System Attacks - Industroyer 2



Sample Details

- ❑ 4/8/2022 15:02:22 scheduled task to launch Industroyer2
- ❑ 4/8/2022 6:10 scheduled execution of Industroyer2
- ❑ 4/8/2022 16:20 scheduled execution of CaddyWiper
- ❑ Industroyer2 only implements IEC-104
- ❑ Industroyer2 is recompiled for each victim environment

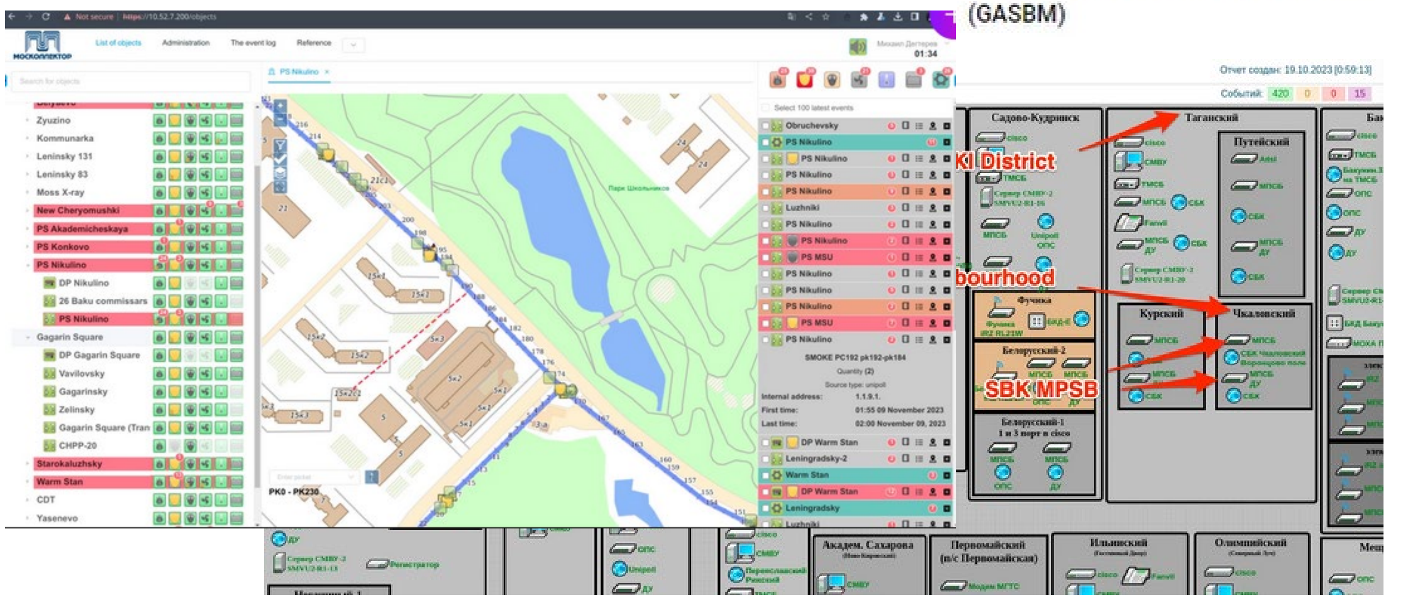
2024 Ukrainian Blackjack Group Attack

- Moscollector, a Moscow-based company, that is responsible for the construction and monitoring of underground water and sewage
- Impacts by FuxNet malware, as analyzed and claimed, would have remotely accessed the targeted devices over communications gateways and delivered destructive attack over serial RS-232 and RS-485
- Interesting technique of NAND Chip exhaustion with bit flip re-writes occurring until corruption is reached.
- Claims of tens of thousands of devices impacted, likely significantly less.

Temperature and humidity sensor (TVSB)

Fire and security system console (PPOSB)

Gas analyzer of the security system (GASBM)

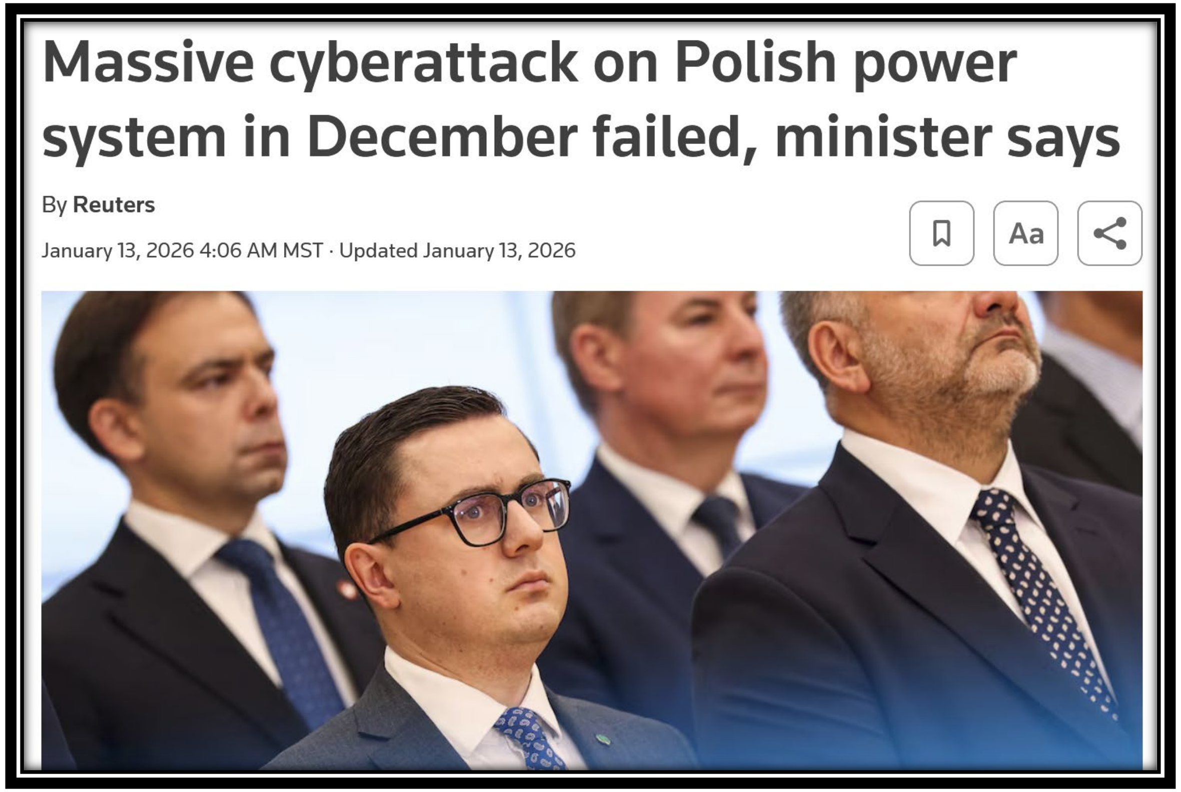


Past, Present, and Future

- Ongoing coordinated cyber and physical attacks
- Critical infrastructure impacts enabling invasion and entrenchment

- Positioning, capability validation, effects-based attacks
- Targeted service outages and equipment damaging attacks

Dec 29, 2025 Polish Electric Sector Incident



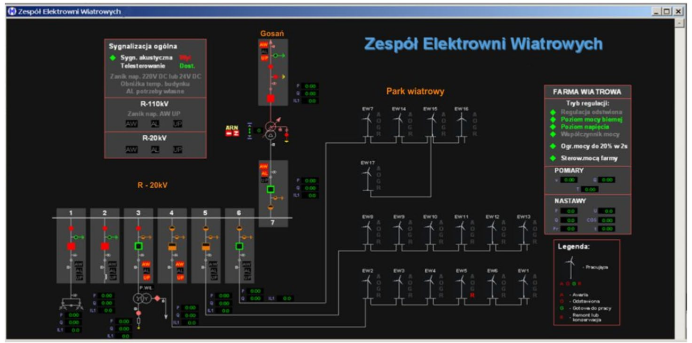
Massive cyberattack on Polish power system in December failed, minister says

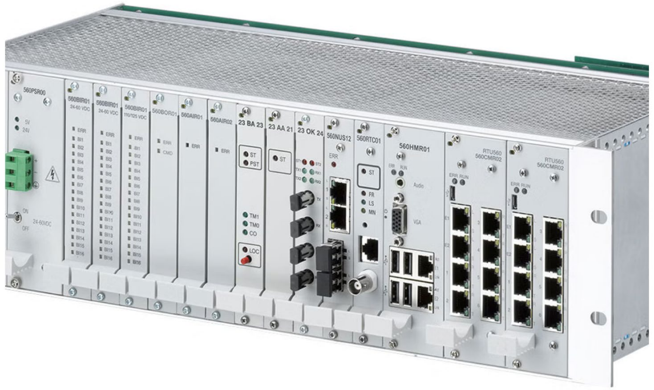
By Reuters

January 13, 2026 4:06 AM MST · Updated January 13, 2026

- ❑December 29th, 2025 a coordinated attack was conducted across the Polish electric system
- ❑Targeted 30 renewable energy sites, a combined heat and power (CHP) facility, and a manufacturing facility
- ❑Vulnerable Fortinet devices, no MFA, default credentials, or reused credentials
- ❑Impacted RTU’s, Local HMI’s, Protection Relays, serial communication servers, communication links to DSO’s
- ❑Impacted operational visibility, communications, and control capabilities
- ❑Did not result in Electric System Outages

ICS Impacts and Operational Effects



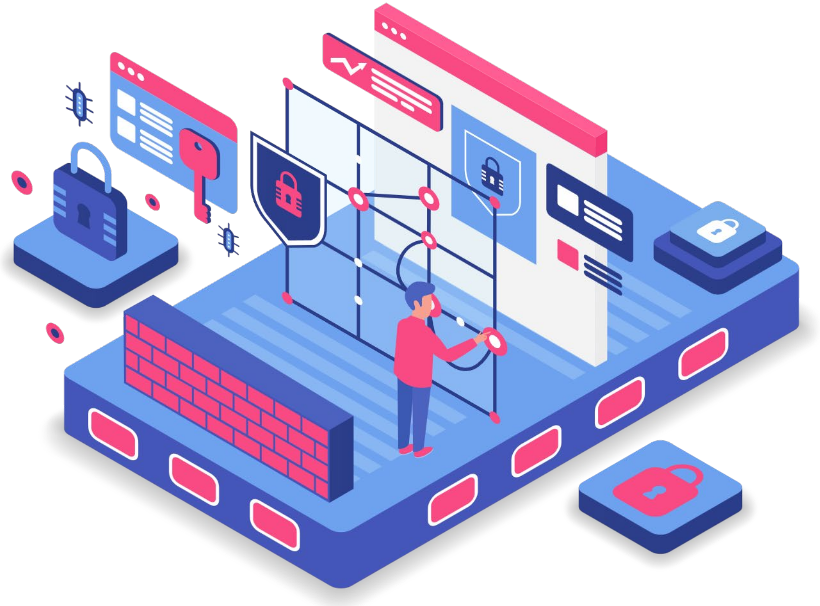


- ❑ Hitachi RTU560 – Attackers uploaded corrupt firmware causing a device fault and reboot loop
- ❑ Mikronika RTUs – Attackers executed commands to delete all system files resulting in device failure
- ❑ Hitachi Relion 650 Protection and Control Relays – Attackers deleted system files essential for device operation causing the device to fail and no longer startup
- ❑ Mikronika HMI Syndis Software – executed DynoWiper
- ❑ Moxa Nport 6xxx serial device servers – wiped config, changed pw, set net address to loopback

Good and Bad Demands

Authentication
Authorization
Accounting

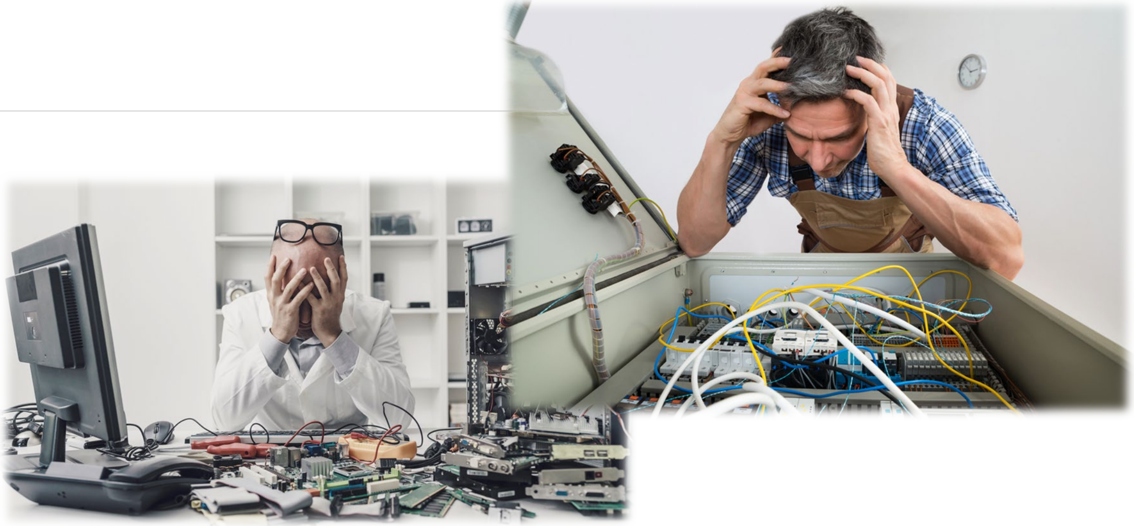
Encrypted Protocols
Zero Trust
Micro-segmentation



Logic protections
Secure provisioning
Directory integration

Design

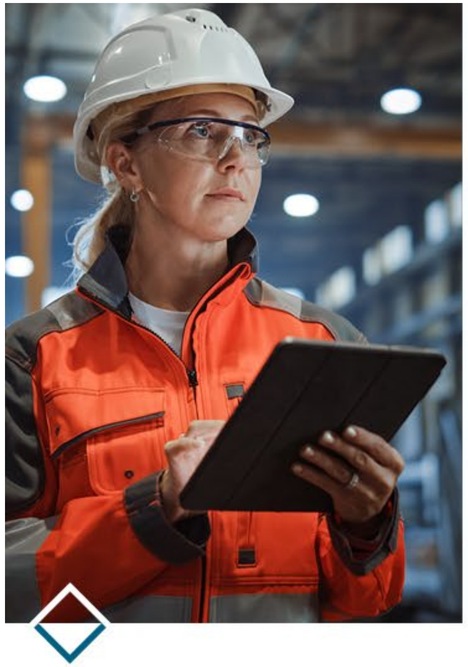
- ❑ Insecure By Design



- ❑ Secure By Design

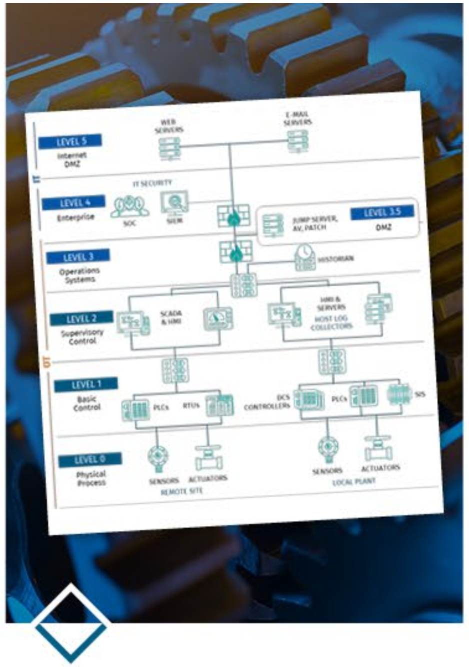
- ❑ Secure By Deployment

Five Critical Controls for ICS/OT Cybersecurity



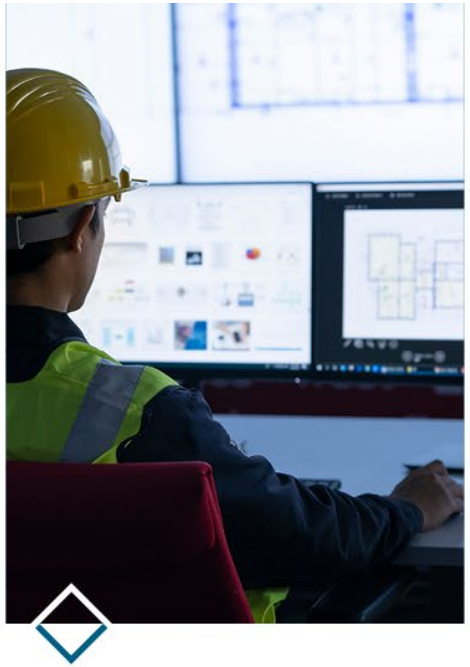
ICS INCIDENT RESPONSE

Operations informed IR plan with focused system integrity and recovery capabilities during an attack. Exercises designed to reinforce risk scenarios and use cases tailored to the ICS environment.



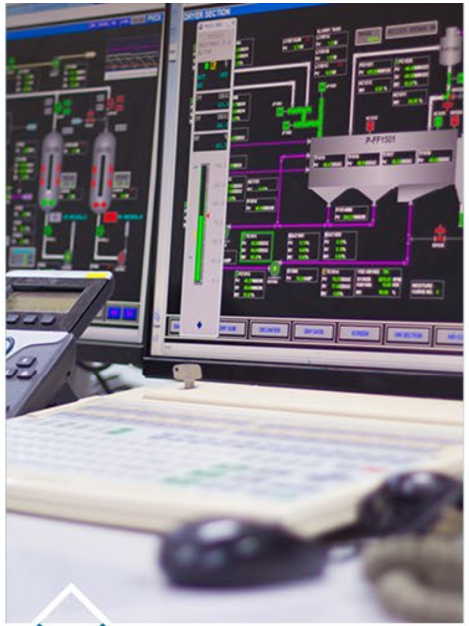
DEFENSIBLE ARCHITECTURE

Architectures that support visibility, log collection, asset identification, segmentation, Industrial DMZ's, process communication enforcement.



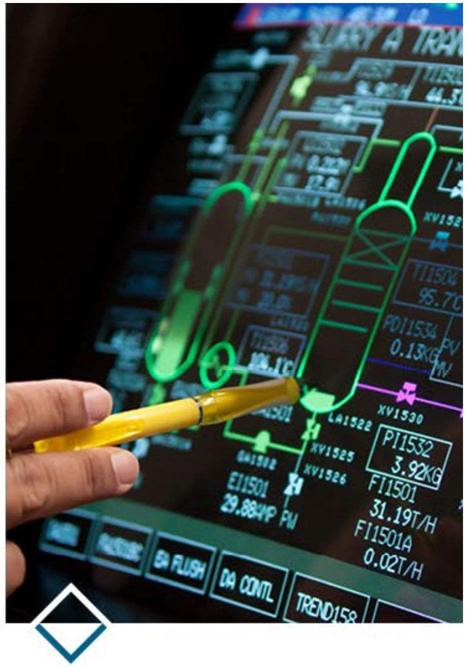
ICS NETWORK VISIBILITY AND MONITORING

Continuous network security monitoring of the ICS environment with protocol aware toolsets and system of systems interaction analysis capabilities used to inform operations of potential risks to control.



SECURE REMOTE ACCESS

Identification and inventory of all remote access points and allowed destination environments, on demand access and MFA where possible, jump host environments to provide control and monitor points within secure segment.



RISK BASED VULNERABILITY MANAGEMENT

Understanding of cyber digital controls in place and device operating conditions that aid in risk-based vulnerability management decisions to patch for the vulnerability, mitigate the impact, or monitor for possible exploitation.

Q&A

SANS | ICS SECURITY

Tim Conway

tconway@sans.org

ICS RESOURCES

@sansics

https://ics.sans.org

https://ics-community.sans.org/