ENGINEERING-GRADE OT SECURITY

WHEN CONSEQUENCES ARE UNACCEPTABLE

Andrew Ginter
VP Industrial Security
Waterfall Security Solutions

ABOUT **WATERFALL SECURITY**

2007 Founded	**>1000** Sites	**>20** Verticals	**6** Global Sales & Ops Hubs	**14** Published Patents

Leading the world's OT unidirectional gateway market with superior solutions, worldwide presence, and proven track record of success

Key Sectors:

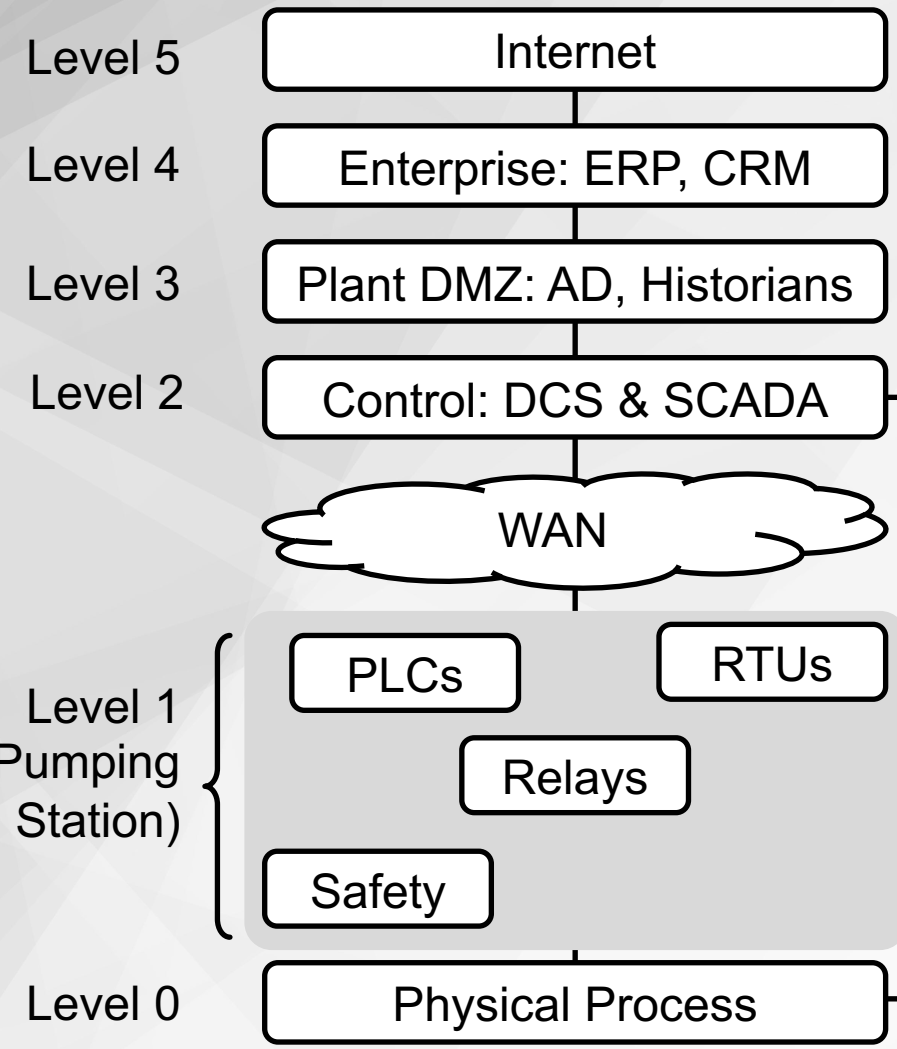
Power | **Oil & Gas** | **Water** | **Rails** | **Manufacturing** | **Facilities**

INDUSTRIAL CYBERSECURITY PRIORITIES

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

Cybersecurity is essential to safety and to reliability

PURDUE MODEL / ISA – IEC 62443 ZONES



CYBER INCIDENTS WITH PHYSICAL CONSEQUENCES

REAL CONSEQUENCES

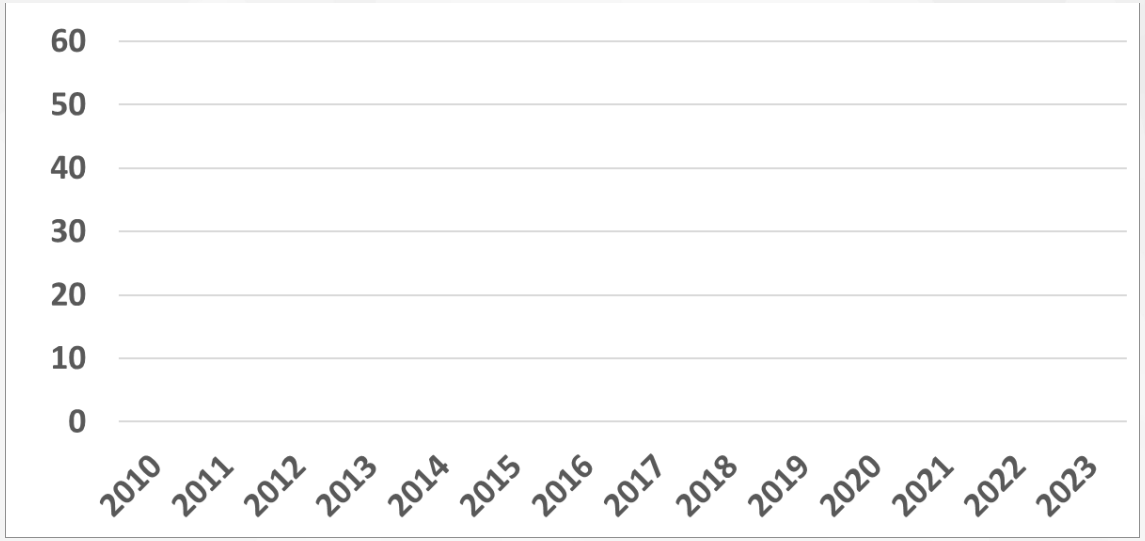
Shutdowns, equipment damage & worse

PROCESS INDUSTRIES

Power, oil & gas, rails, water treatment, food & beverage, agriculture, mining

MANUFACTURING

Automobiles, aircraft, consumer goods



IN THE PUBLIC RECORD

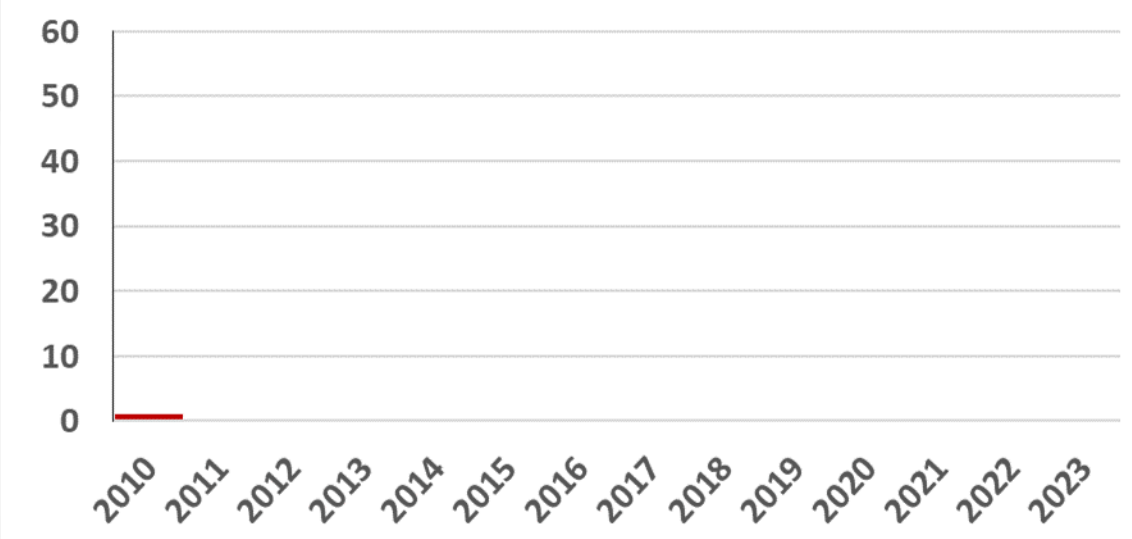
Independently verifiable by anyone with Internet access

waterfall-security.com/
2023-threat-report

CYBER INCIDENTS WITH PHYSICAL CONSEQUENCES

2010 - one

Stuxnet – destroyed 1000 centrifuges



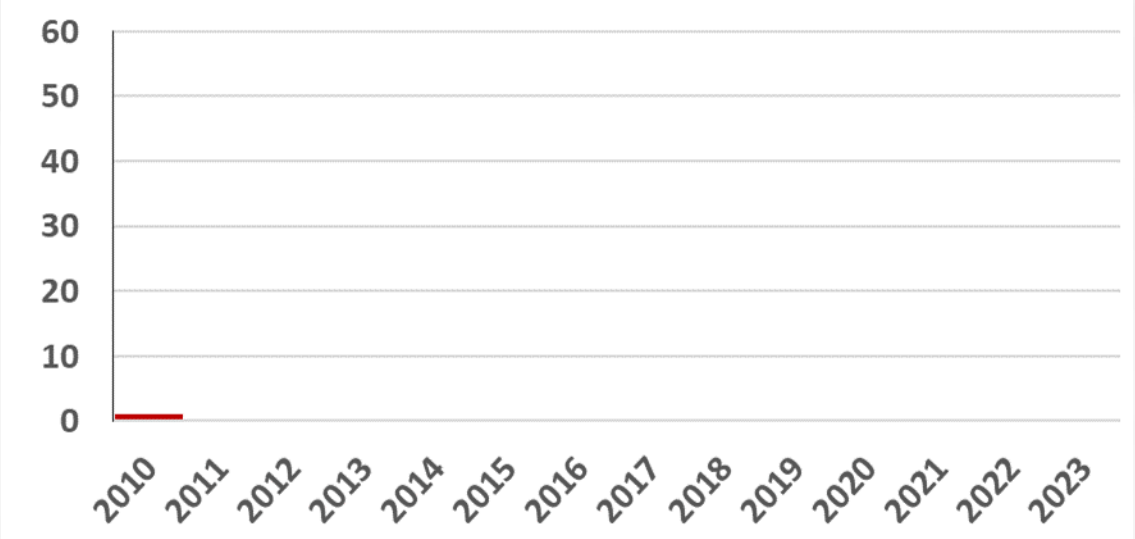
waterfall-security.com/
2023-threat-report

CYBER INCIDENTS WITH PHYSICAL CONSEQUENCES

2010 - one

Stuxnet – destroyed 1000 centrifuges

2011 - nothing



waterfall-security.com/
2023-threat-report

CYBER INCIDENTS WITH PHYSICAL CONSEQUENCES

2010 - one

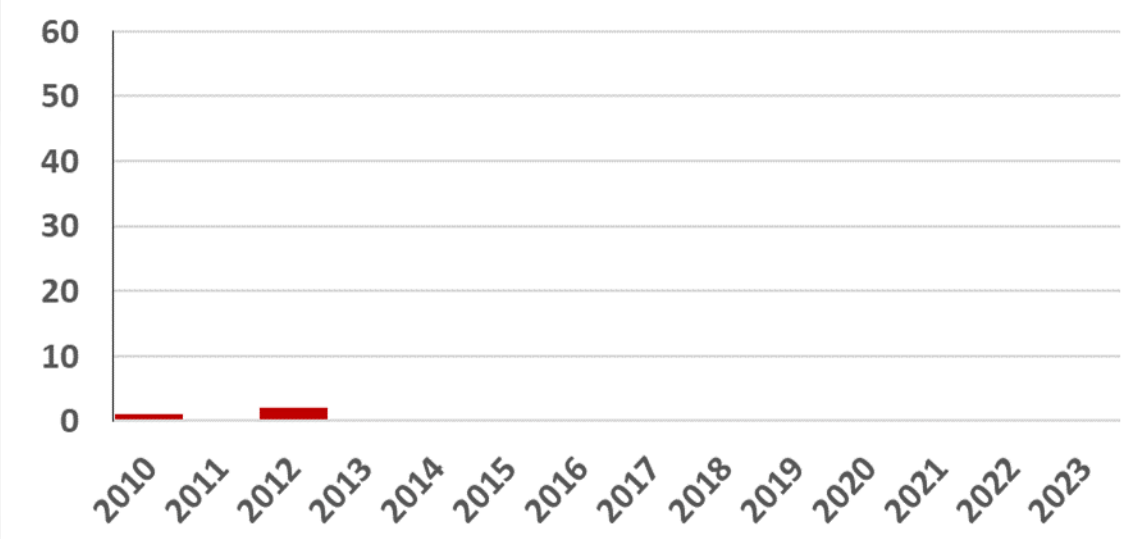
Stuxnet – destroyed 1000 centrifuges

2011 - nothing

2012 - two

Iranian gas stations – shut down

Unknown US power plant – 3 wk delay



waterfall-security.com/
2023-threat-report

waterfall

CYBER INCIDENTS WITH PHYSICAL CONSEQUENCES

2010 - one

Stuxnet – destroyed 1000 centrifuges

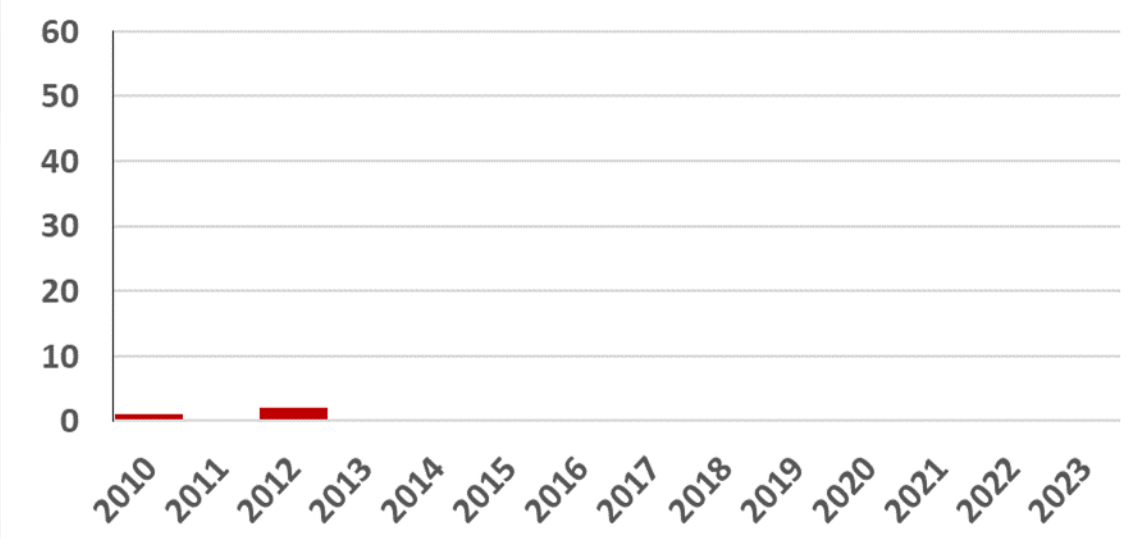
2011 - nothing

2012 - two

Iranian gas stations – shut down

Unknown US power plant – 3 wk delay

2013 - nothing



waterfall-security.com/
2023-threat-report

CYBER INCIDENTS WITH PHYSICAL CONSEQUENCES

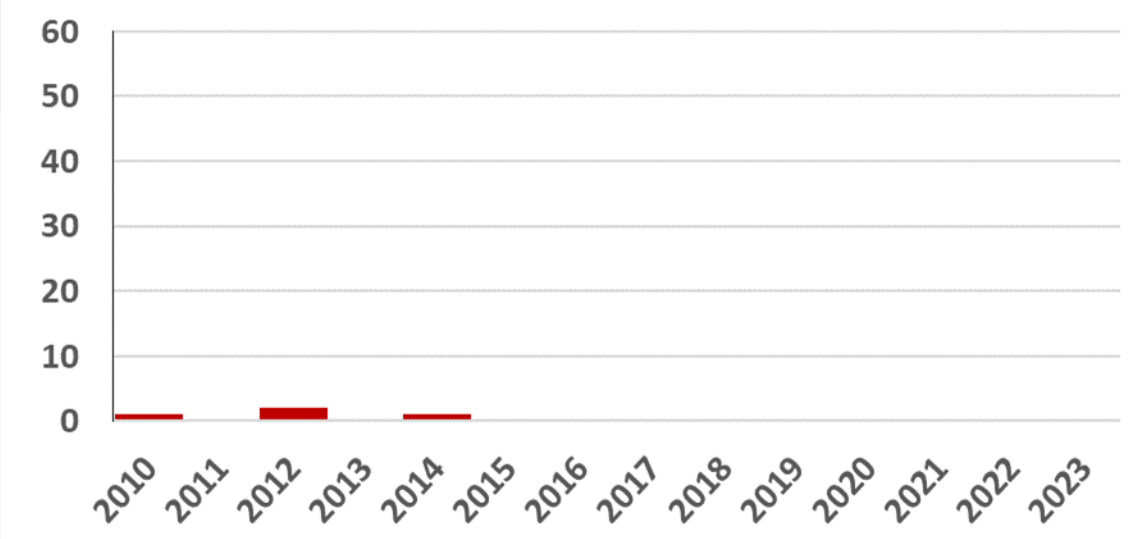
2010 - one
Stuxnet – destroyed 1000 centrifuges

2011 - nothing

2012 - two
Iranian gas stations – shut down
Unknown US power plant – 3 wk delay

2013 - nothing

2014 - one
German steel mill – “massive damages”



waterfall-security.com/
2023-threat-report

CYBER INCIDENTS WITH PHYSICAL CONSEQUENCES

2011 - nothing

2012 - two

Iranian gas stations – shut down

Unknown US power plant – 3 wk delay

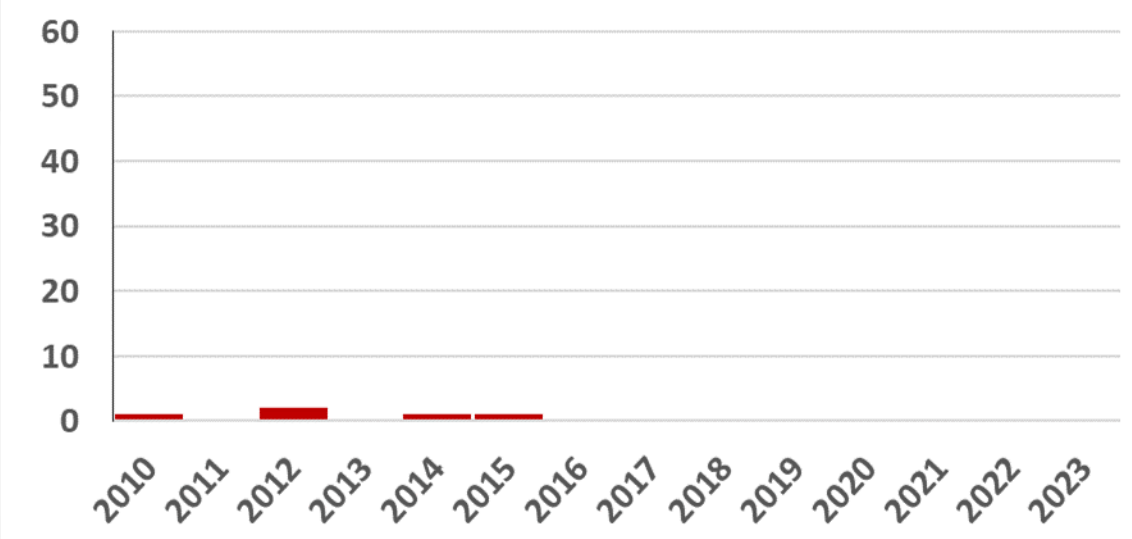
2013 - nothing

2014 - one

German steel mill – “massive damages”

2015 - one

Ukraine power outage – 225,000 x up to 6 hours



waterfall-security.com/
2023-threat-report

CYBER INCIDENTS WITH PHYSICAL CONSEQUENCES

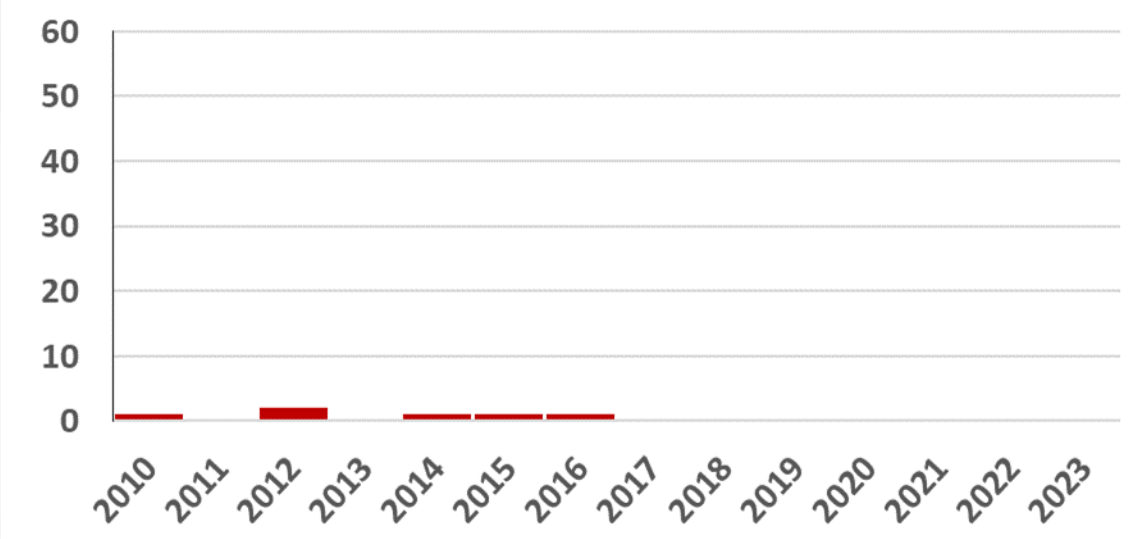
2012 - two
Iranian gas stations – shut down
Unknown US power plant – 3 wk delay

2013 - nothing

2014 - one
German steel mill – “massive damages”

2015 - one
Ukraine power outage – 225,000 x up to 8 hours

2016 - one
Ukraine power outage – Kiev x 1 hour



waterfall-security.com/
2023-threat-report

CYBER INCIDENTS WITH PHYSICAL CONSEQUENCES

2015 - one

Ukraine power outage – 225,000 x 8 hrs

2016 - one

Ukraine power outage – Kyev x 1 hour

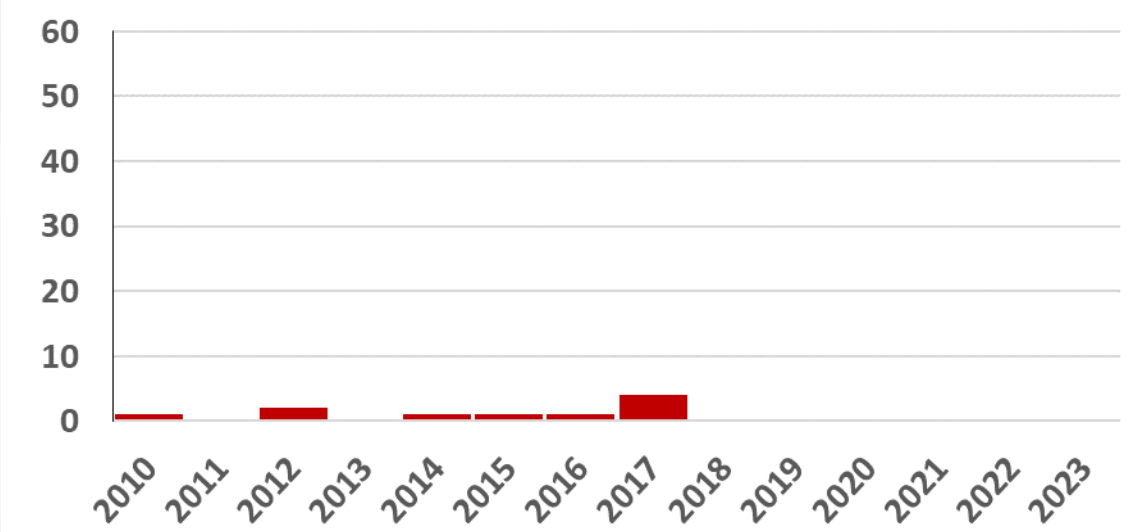
2017 - four

TRITON – one site, 2 shutdowns

NotPetya – one incident, countless victims

AW North Carolina (auto parts) – 4 hr. production outage

Renault-Nissan – WannaCry hit 5 plants – 1 day



waterfall-security.com/
2023-threat-report

CYBER INCIDENTS WITH PHYSICAL CONSEQUENCES

2015 - one

Ukraine power outage – 225,000 x 8 hrs

2016 - one

Ukraine power outage – Kyev x 1 hour

2017 - four

TRITON – one site x 2 shutdowns

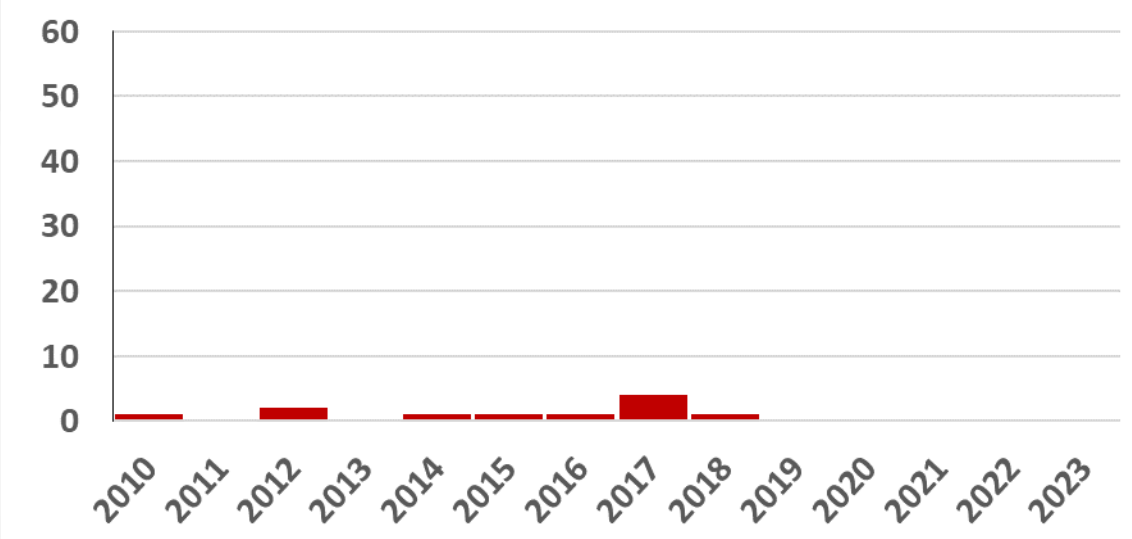
NotPetya – countless victims x 1 incident

AW North Carolina – auto parts – 4 hr. production outage

Renault-Nissan – WannaCry hit 5 plants – 1 day

2018 – one

TSMC – 3% annual revenue loss



waterfall-security.com/
2023-threat-report

waterfall

CYBER INCIDENTS WITH PHYSICAL CONSEQUENCES

2018 – one

TSMC – 3% annual revenue loss

2019 - five

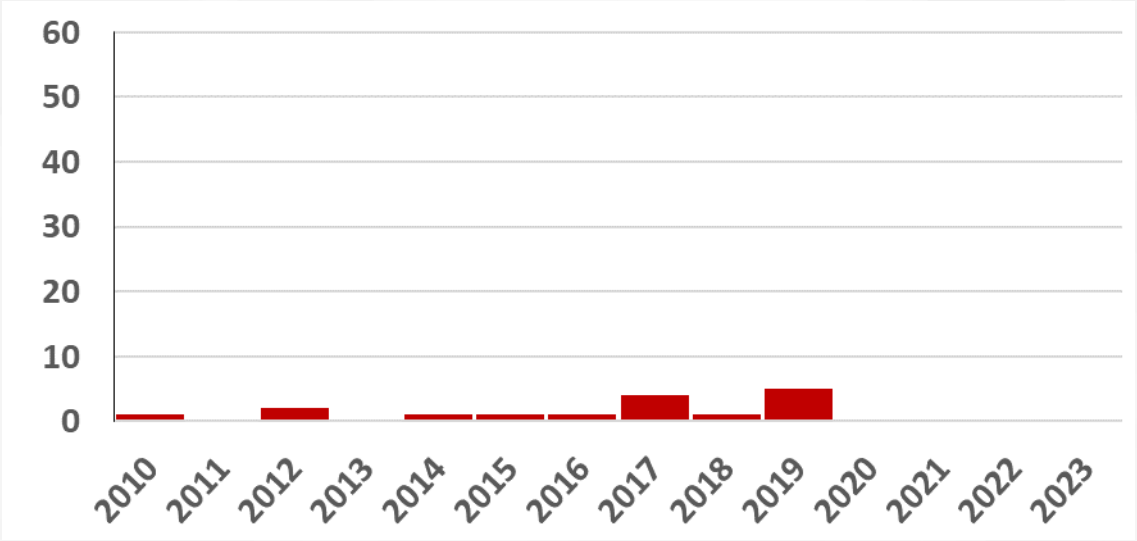
USA gas pipeline – down 30 hours

Norsk Hydro – 4 sheet aluminum plants

City Power Johannesburg – 250K no pwr

RavnAir – cancelled flights, maint sys out

Pilz – slowed production 1 week

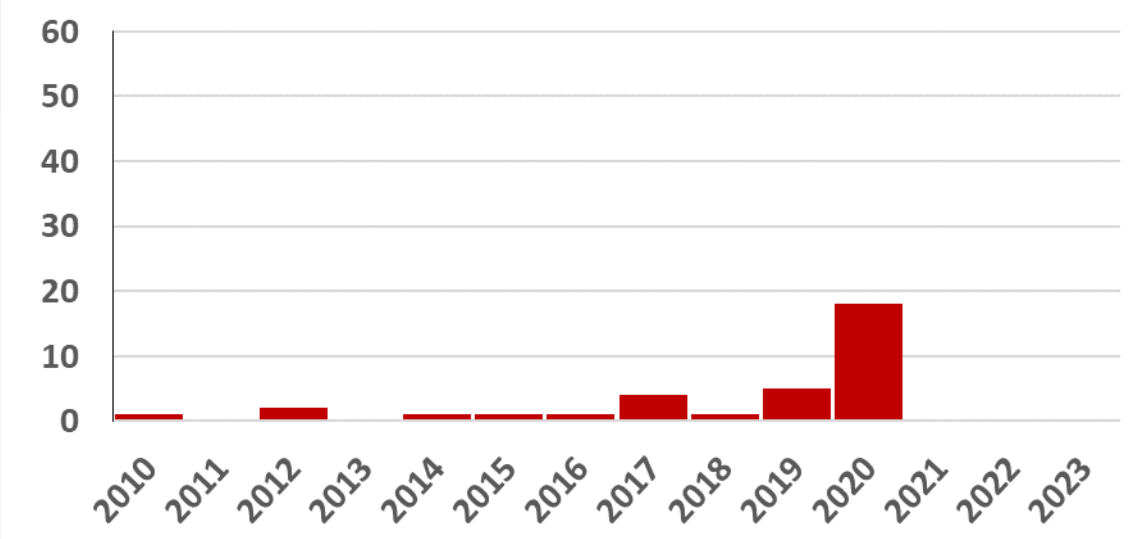


waterfall-security.com/
2023-threat-report

CYBER INCIDENTS WITH PHYSICAL CONSEQUENCES

2020 – 18

Picanol – weaving machine plants
Toll Group – deliveries delayed or disrupted
KHS Bicycles – delayed shipments 2 days
EVRAZ Steel – plants down, layoffs
Shahid Rajaee port – halted port terminal
Fisher & Paykel – consumer goods plants down
Honda – plants down up to 4 days
Lion – brewery operations down
X-FAB – plants down over 1 week
Tower Semiconductor – multiple plants down
Bluescope Steel – Australian plants down
IPG Photonics – laser mfg. production losses
STM Montreal – paratransit service down 1 wk.

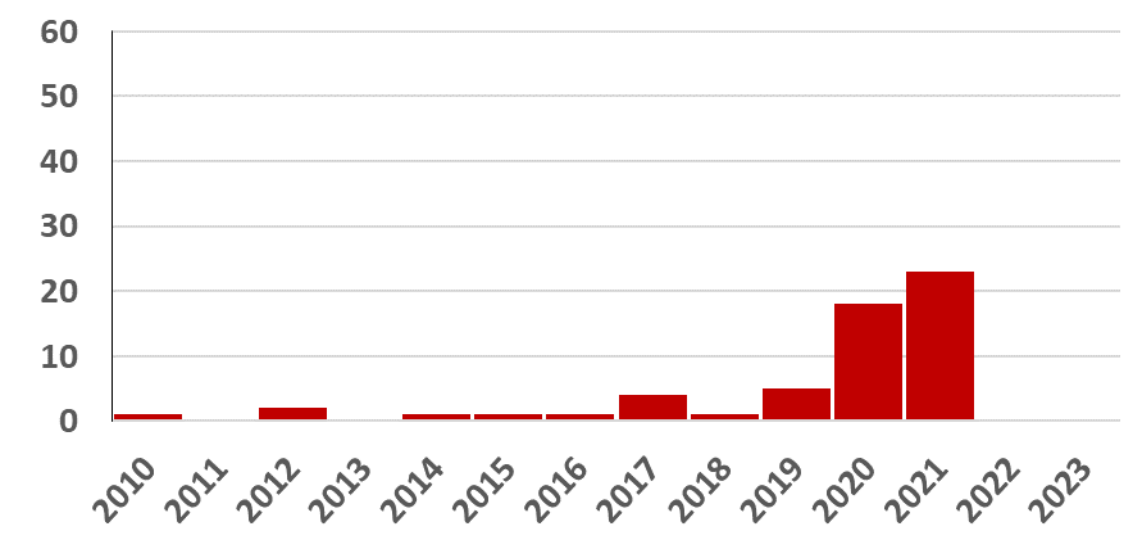


Steelcase – furniture plants down 2 wks.
Dr. Reddy's Labs – shut down 5 pharma plants
Stelco – shut down steel production
Symrise – production shutdown
Forward Air – shut down, shipments delayed 1 wk.

CYBER INCIDENTS WITH PHYSICAL CONSEQUENCES

2021 – 23

Palfinger – 2 weeks crane production
Westrock – lost 85,000 tons production
Beneteau SA – boatmaker, 3-4 weeks
Amsteel Flash – Multiple PC board plants
Bakkier Logistics – delayed shipments
Molson Coors – disrupted brewery ops
Sierra Wireless – halted all plants
Ardagh Group – glass prod shipping delays
Colonial Pipelines – down 6 days
JBS SA – 4 large plants shut down
Iran rails – signage hack disrupted ops
Transnet – port ops halted – force majeure
Weir Group – disrupted mfg & shipping
New Cooperative – interrupted grain receipts
JBI Bike – interrupted shipments



Crystal Valley Coop – some ops down 4 days
Schreiber Foods – cheese mfg down for days
Ferrara – candymaking shut down
Damm Brewery – halted production
Madix – store fixture manufacturing halted
Diamond Comic Dist – could not deliver product
Amedia – publisher missed 1-2 days printing
Nortura – food production halted at several sites

CYBER INCIDENTS WITH PHYSICAL CONSEQUENCES

2022

Bay & Bay Trans – shipments delayed 1.5 weeks
CPH Chemie & Papier – plants down 6 days
Kenyon Produce Snacks – halted production
Marquard & Bahls – shut down for 2 weeks
SEA-Tank – halted ops at EU and African ports
Evos Group – delayed unloading fuel at 3 ports
Swissport – delayed 22 flights
Jawaharlal Terminal – suspended unloading
Expeditors – could not ship for 3 weeks
Caledonian Modular – shut down manufacturing
Bridgestone – 23 plants down for 10 days
Belarus Railway – trains halted in 3 cities
Kojima – down 1 day, impacted Toyota & others
Rosetti Energy – deactivated EV charging stns
H.P. Hood Dairy – shut down 1 week
Hellenic Post – disrupted shipments 17 days
TAVR – shut down production – significant loss
Bulgarian Post Office – 14 days outage
Costa Rican Customs – slowed shipments 1 mo
Sunwing – delayed or cancelled 188 flights
AGCO – shut down production 15 days
SpiceJet – delayed flights 5 hours
Foxconn Baja – disrupted production for 2 weeks
CMC Electronics – disrupted and delayed ops
Yodel – delayed millions of parcels
Apetito – 5 day halt to food deliveries
Macmillan Publishers – halted orders & shipping
Khuzestan Steel – broke equipment & halted ops

CYBER INCIDENTS WITH PHYSICAL CONSEQUENCES

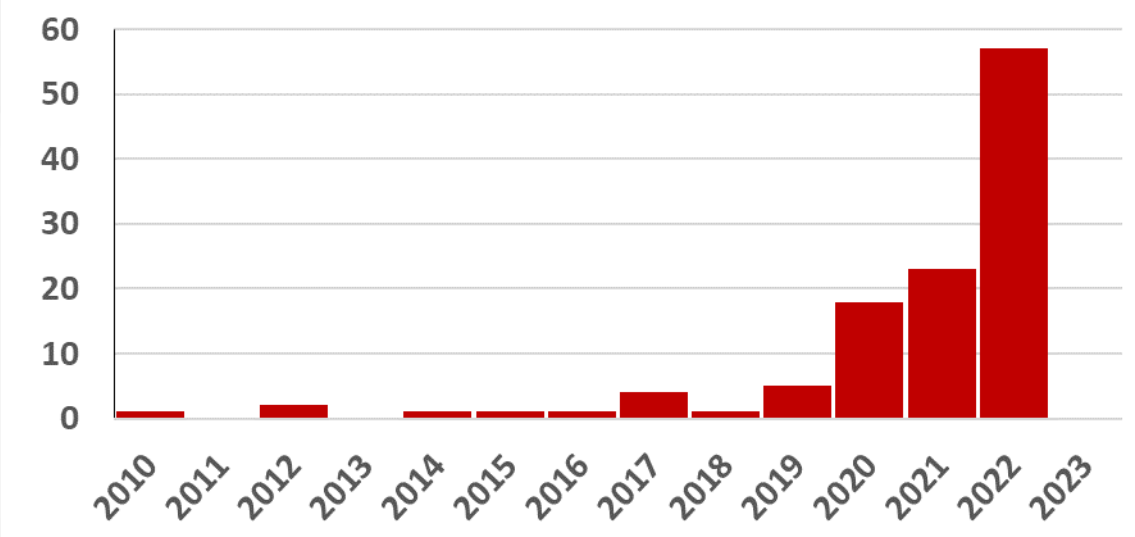
2022 (continued)

Knauf – shut down production 3+ weeks
Eglo – shut down production & shipping 12 days
Semikron – shut down production for months
Ontario Cannabis Retail – halted deliveries 5 days
Bombardier Recreational – halted production 1 wk
TCS Fuel – shut down operations 1 week
Novosibirsk Transit – stopped public transit 2 days
Yandex Taxi – routed all city's taxis to one place
Läderach – halted production 67 days
Ghana Electricity Co – prepaid customers lost pwr
HIPP – days-long production outage
Heilbronner Stimme – shut down production
Aurubis AG – metals production halted
Danish Rails (DSB) – train svc halted several hrs
Cartonnerie Gondardennes – 3 days downtime
Jeppesen – delayed flights at multiple airlines
Uponor Oyj – down 1 wk, reduced capacity 2 wks
PGT Innovations – 2 plants impacted, $12M cost
Maple Leaf Foods – disrupted production 2+ sites
Taxis Coop Québec – could not dispatch 2.5 hrs
Europea Microfusioni Aerospaziali – 6 days down
Communauto – shut down ride sharing 1 day
Prophete – shut down production, bankrupted
Cobolux – 1 day production loss, €400K costs
UNOX – no production for 2 days
Fruttagel – 4+ day shutdown
EPM (Colombia) – trucked water to 28K homes
Technolit – shutdown & sent employees home

CYBER INCIDENTS WITH PHYSICAL CONSEQUENCES

2022 (continued) – 57

Copper Mountain Mining – down 5 days



waterfall-security.com/
2023-threat-report

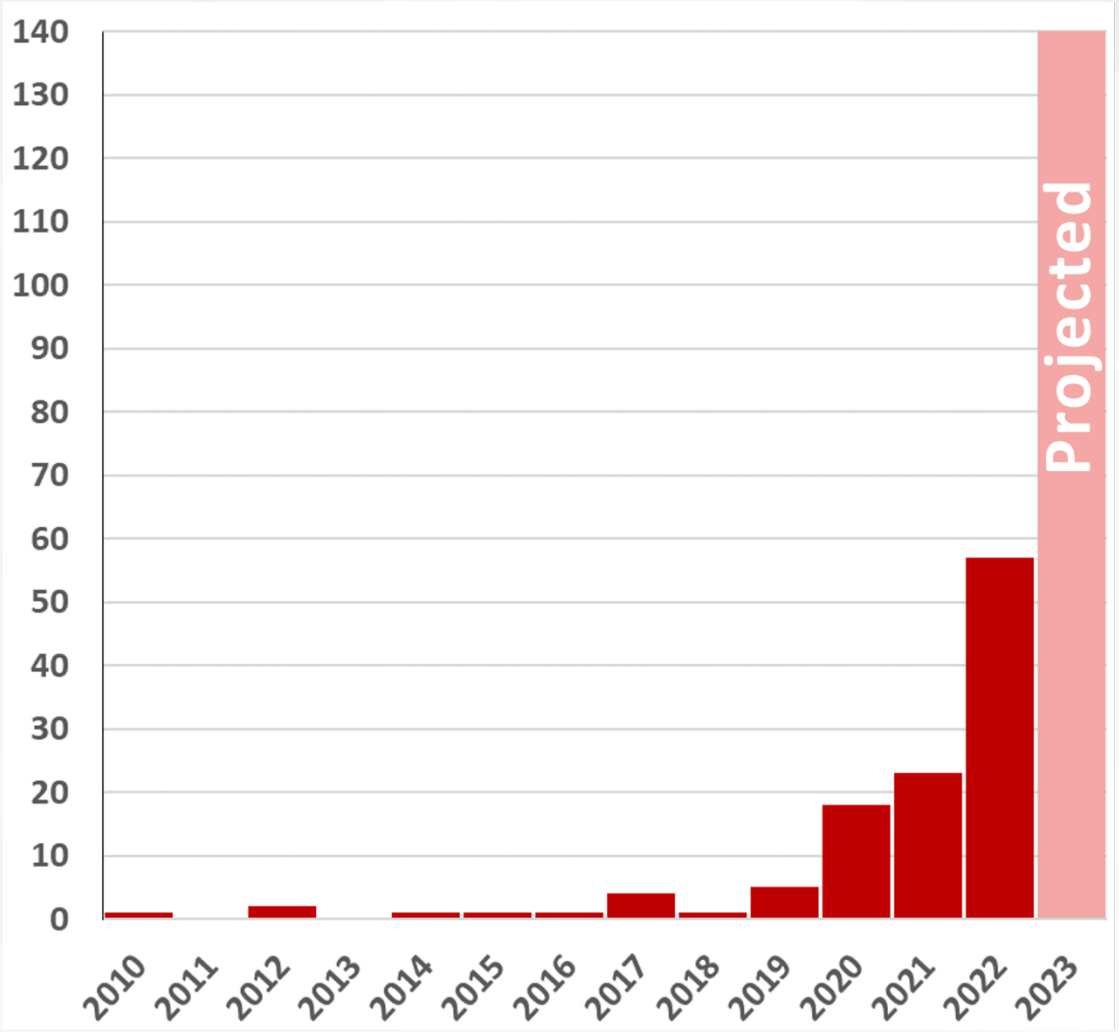
CYBER INCIDENTS WITH PHYSICAL CONSEQUENCES

2022 (continued) – 57

Copper Mountain Mining – down 5 days

2023 (projected) – 140

‘22 vs ‘21: > 2.5x incidents



OT CYBER RISK – CHANGED FOREVER

DOUBLING ANNUALLY

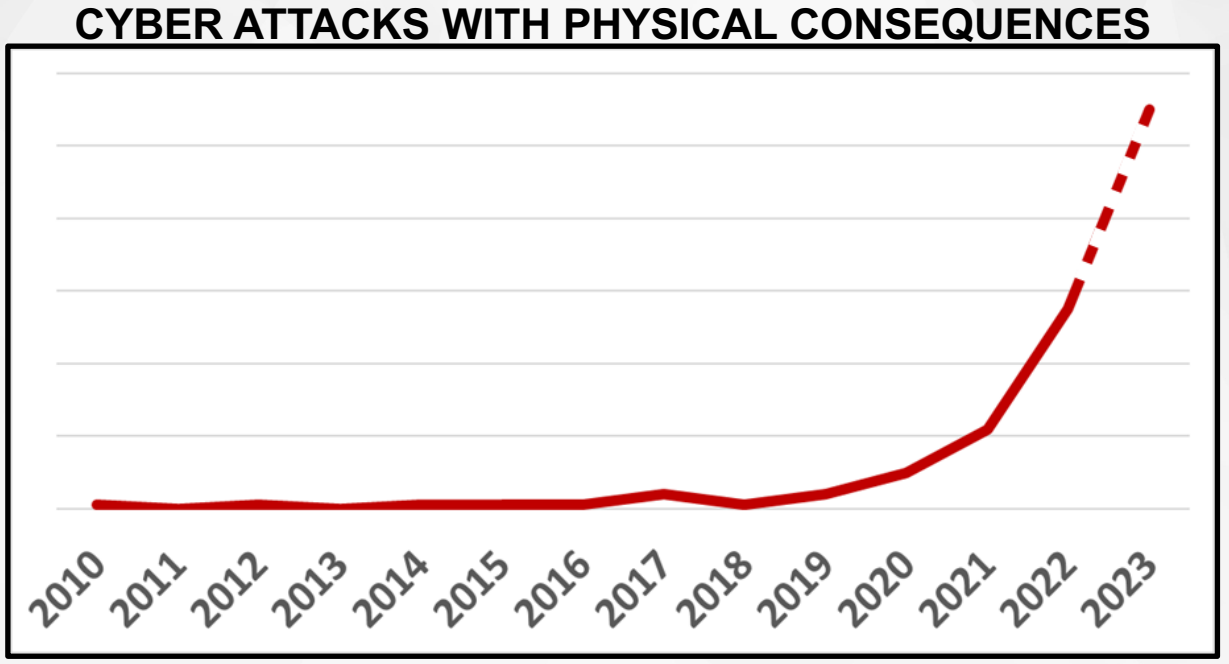
Exponential growth

RANSOMWARE IMPACTS

- Target OT systems directly
- “Abundance of caution” shutdowns
- OT depends on IT

HACKTIVISTS

15% of impacts and increasing



What nations do to each other today, ransomware criminals will do to everyone with money within a couple of years

waterfall-security.com/
2023-threat-report

LATEST RESPONSE: CYBER-INFORMED ENGINEERING

IF YOUR LIFE DEPENDS ON A BOILER NOT EXPLODING

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

ENGINEERING GRADE

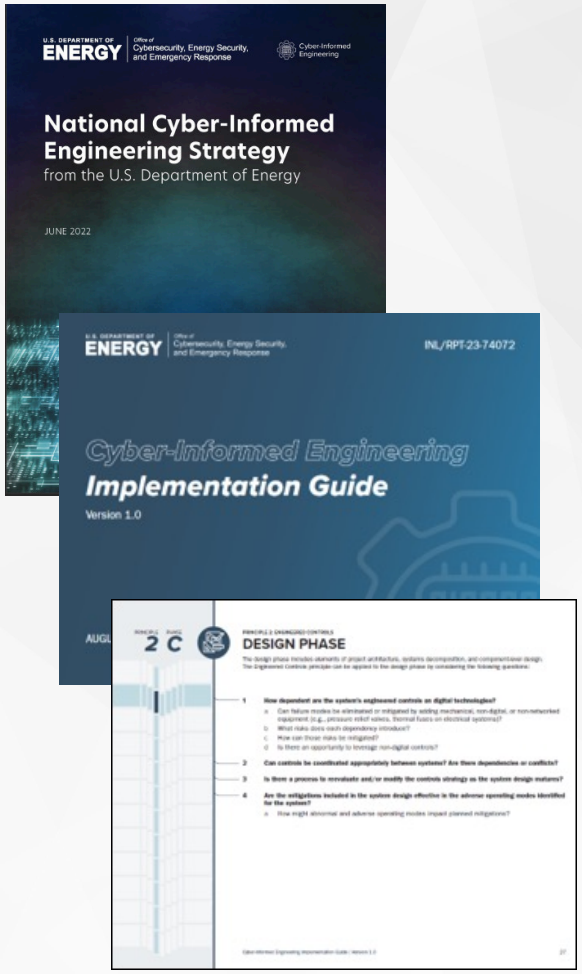
Would you trust a bridge whose designer hopes it will carry a specified load, for a specified number of decades?

MANUAL OPERATIONS – UNHACKABLE

Fall-back position while incident response cleans up the cyber mess

NETWORK ENGINEERING

Safe, reliable and efficient operations depend on cyber attacks not getting into our systems in the first place



CIE is a "coin with two sides" – IT-grade cybersecurity + engineering-grade designs – we always need both

OT CYBER RISK REVISITED

RISK != CONSEQUENCE X LIKELIHOOD

Does 1x3 really equal 3x1?

Cyber attacks are deterministic, not random

Errors & omissions confuse risk calculations

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

RISK = *f(conseq, intent, c(opportunity), capability)*

If intent & (capability > c(opportunity)) then consequence

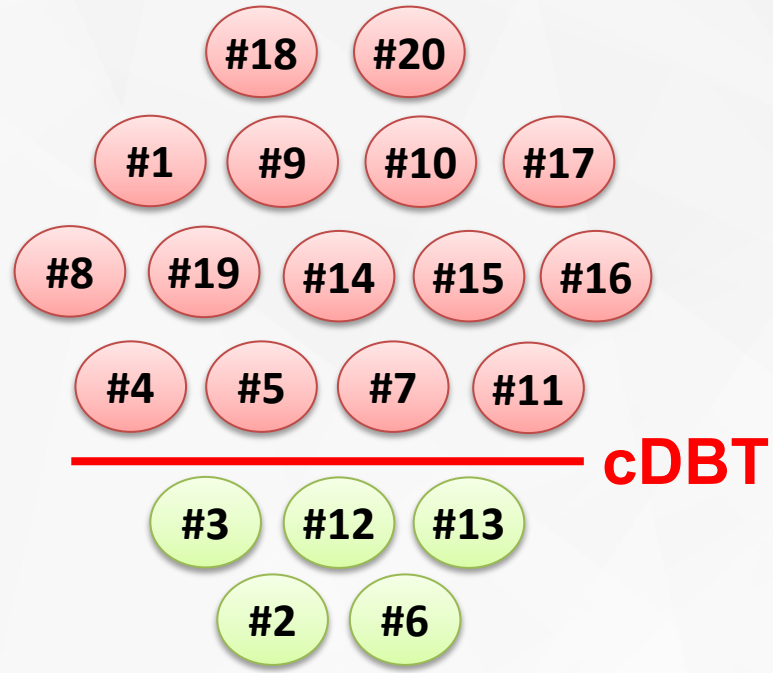
Consequence – result of compromise

Intent – does threat actor want to attack us?

C(Opportunity) – capability needed to exploit opportunity

Capability – ability of the threat actor to attack

Cyber Design Basis Threat – description of kinds of attacks we are required to defeat reliably



waterfall

CYBER DESIGN-BASIS THREAT

PROTECT AGAINST WIDELY-AVAILABLE CAPABILITIES

Intent can change in a heartbeat – literally

NATION-STATE RANSOMWARE = PERVASIVE THREAT

Demands network engineering for unacceptable consequences
Acceptable consequences – optional network engineering

INSIDER THREAT CDBT

No cyber attack produce unacceptable OT consequences without the deliberate cooperation of a compromised OT insider

Strong NIST / IEC 62443 – style posture is still needed to manage insider threat

EVOLVING INSURANCE EXPECTATIONS

LLOYDS REGULATOR

Last 5 years: $200M cap on cyber damages, nation-state exclusion, dropped silent coverage

DUE CARE EXPECTATIONS – INSURANCE QUESTIONNAIRES

Increased from less than one page to more than 5 pages of questions, including questions about unidirectional protections

LARGE BUSINESSES SELF-INSURE

For risks Lloyds won't touch? Is that wise?

Due care: doing what any reasonable person would do in similar circumstances

LLOYD'S

SECURITY ENGINEERING – SPR

SECURITY PHA REVIEW

Physical protection from safety incidents – security applications of OSHA Process Hazard Analysis

OBVIOUS IN HINDSIGHT

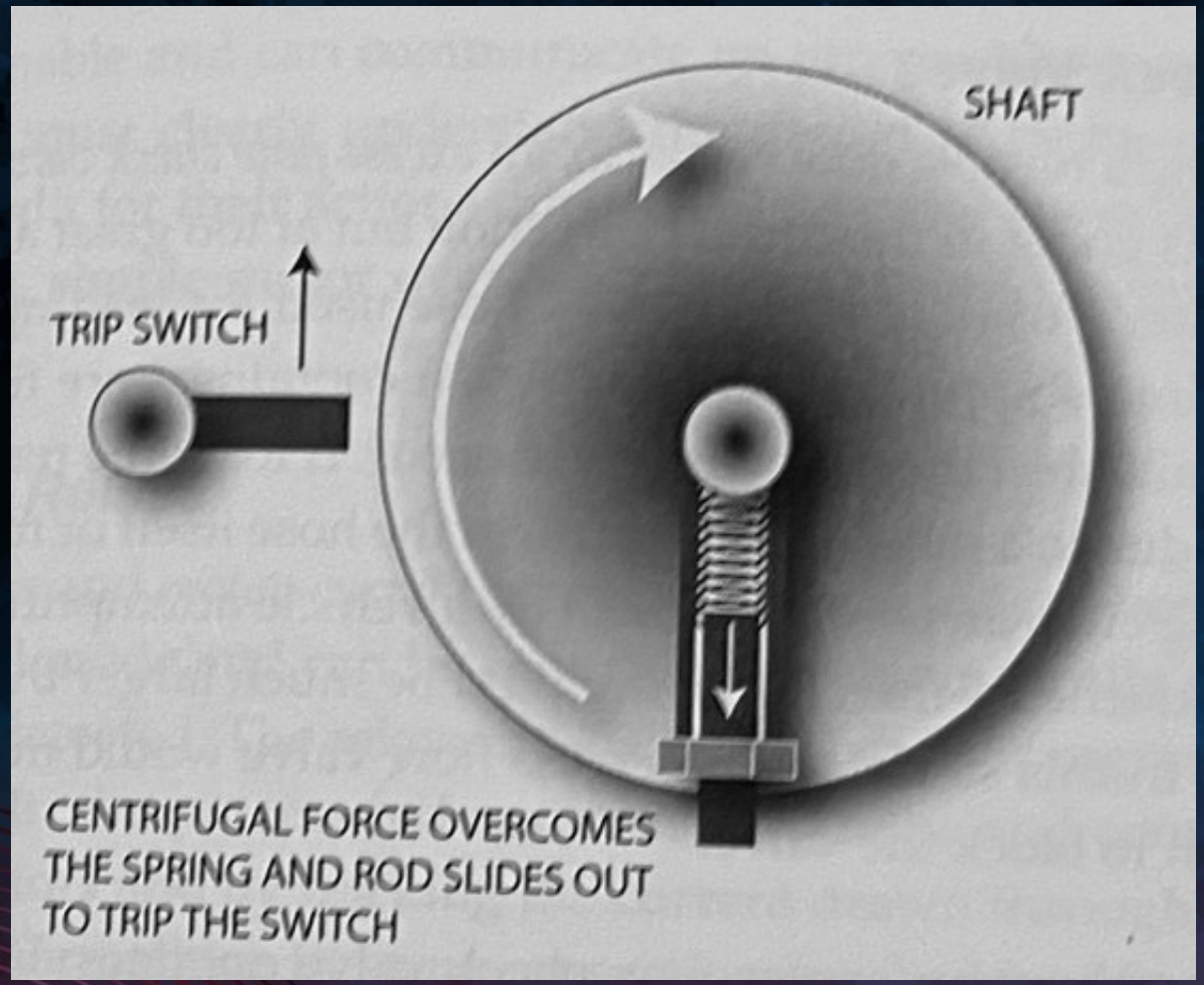
Brilliant book – finish the last page and the entire process is obvious in hindsight – of course this is the right way

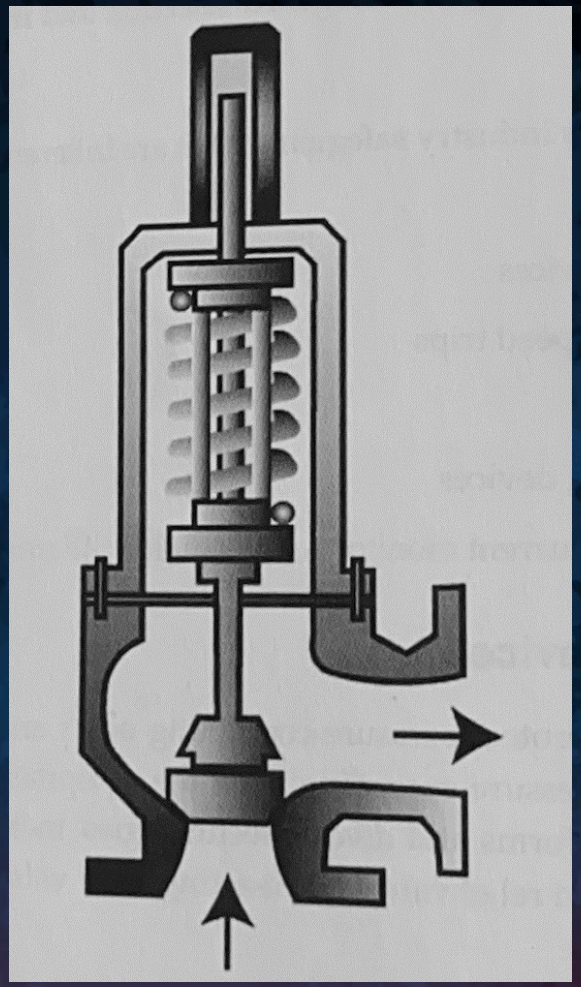
USE HAZOP / PHA SPREADSHEET

Extra columns – is any cause hackable? Are all mitigations hackable?

Engineering-grade solutions work predictably and deterministically

PHYSICAL MITIGATIONS





waterfall

SECURITY ENGINEERING – SEC-OT

SECURE OPERATIONS TECHNOLOGY

All cyber-sabotage attacks are information – complete inventory of incoming flows = inventory of attack vectors

ONLINE VS. OFFLINE

There are only two ways information can move

PHYSICAL MITIGATIONS

To greatest extent practical, physically control the movement of information / attacks

Do not "protect the information" – CIA vs. AIC
Protect physical operations FROM information

NETWORK ENGINEERING: EPRI IIOT

EPRI: SAFE CLOUD CONNECTIONS

How to safely connect vibration monitoring “edge devices” straight out to cloud / vendor turbine monitoring

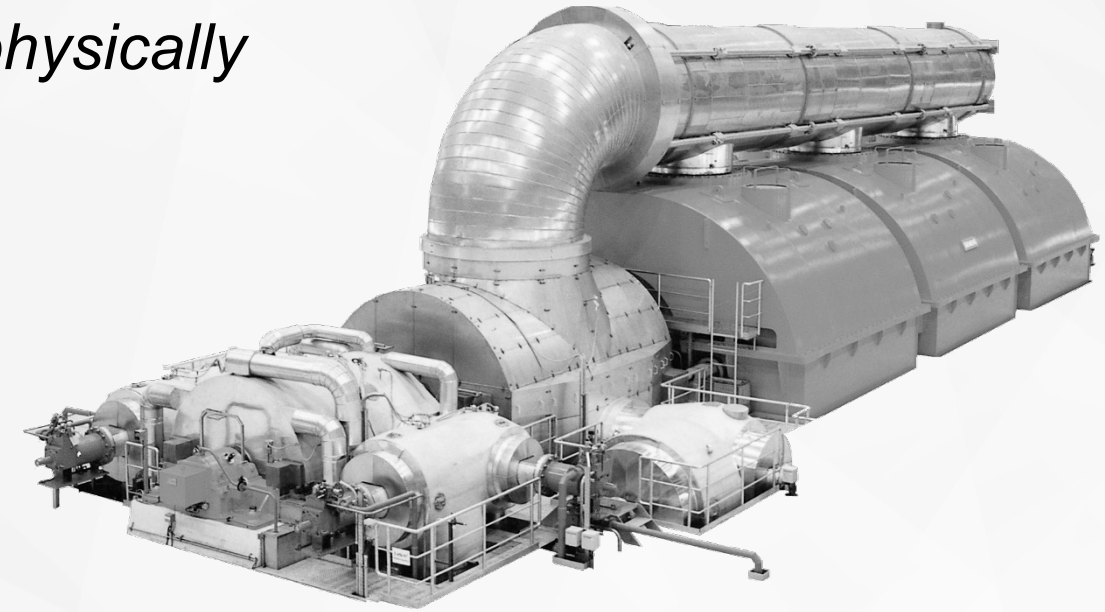
ENGINEERING STUDY – NO CONTROL

Convince yourself that the edge devices are *physically* incapable of control – truly monitor only

DEPLOY ON OWN NETWORK

Physically separate from control network, straight out to cellular Internet if you like

No longer any way to pivot attack from Internet / cloud into control network



NETWORK ENGINEERING

PERVASIVE THREAT – NATION-STATE RANSOMWARE

Launched across the Internet, propagates through firewalls into OT networks

WORST-CASE CONSEQUENCES DEFINE SECURITY PROGRAM

If every CPU issues exactly the wrong instruction to the physical process…

CONSEQUENCE BOUNDARIES

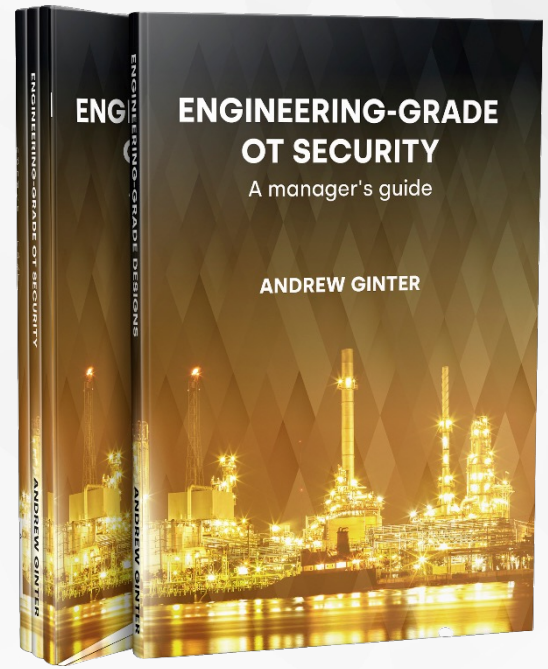
Must prevent propagation of these remote-control / malware attacks

NETWORK ENGINEERING

EPRI IIoT, analog signalling, dependency analysis, data abstraction

MOST WIDELY-DEPLOYED SOLUTION

Engineering-grade Unidirectional Gateways – enable visibility into OT networks without risk of compromise



https://waterfall-security.com/engineering-grade-ot-security

UNIDIRECTIONAL SECURITY GATEWAYS

UNBREACHABLE PROTECTION, UNLIMITED CONNECTIVITY

NIST 800-82: Unidirectional Security Gateways are a combination of hardware and software

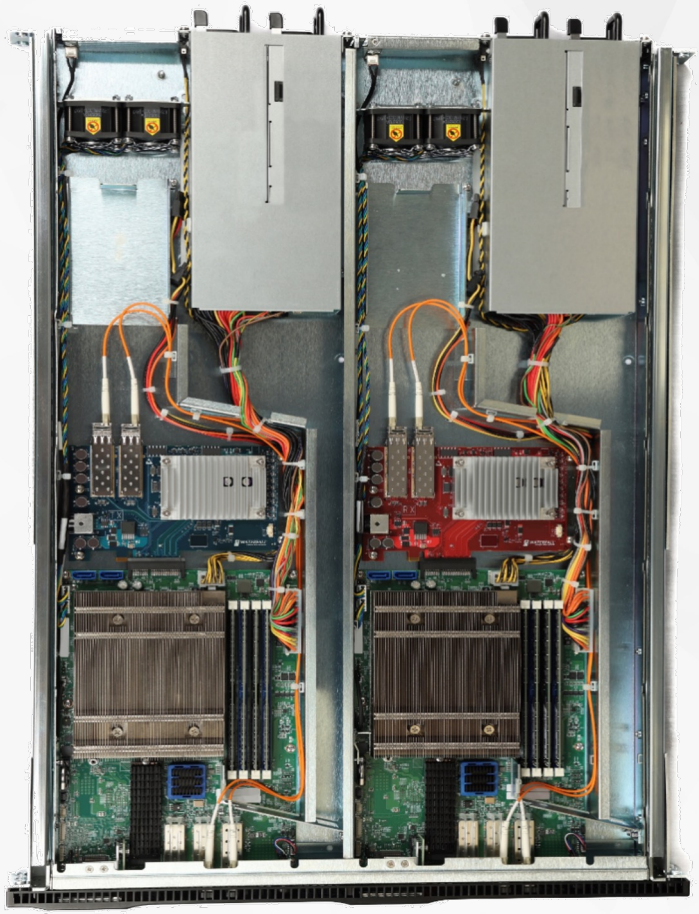
- The hardware sends information in only one direction
- The software makes copies of servers & devices from the OT network to the enterprise network
- No attack, no matter how sophisticated, can propagate back into the OT network through the gateway

CLEAR UNIDIRECTIONAL DESIGN

ENGINEERING-GRADE UNIDIRECTIONALITY

- Zero internal cross-connects – robust and certified unidirectional engineering
- Physically divided industrial and enterprise components
- Dual power supplies on each of sending & receiving sides
- DIN RAIL, split (2u) and 1u form factors

Not physically able to send attacks from the cloud, internet or enterprise back into the critical water plant network



WF-600

WATERFALL SOFTWARE CONNECTORS

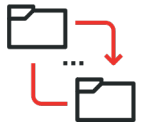
HISTORIANS & DATABASES

- Aveva (OSIsoft): PI, PI Asset Framework, PI Backfill
- GE: iHistorian, iHistorian Backfill, OSM, Bently-Nevada System1
- Schneider-Electric: Wonderware eDNA, Wonderware Historian, Wonderware Historian Backfill, SCADA Expert ClearSCADA, Siemens CFE & WinTS
- Rockwell FactoryTalk Historian , Honeywell Alarm Manager
- AspenTech IP.21, Scientech R*Time, Microsoft SQL Server, Oracle, MySQL

INDUSTRIAL APPLICATIONS AND PROTOCOLS

- Siemens S7
- Yokogawa ExaQuantum OPC, GE iFix, Leidos HBS
- OPC DA, A&E, HDA, HDA Backfill, OPC UA, UA Historians, UA Alarms & Events
- Modbus, DNP3, ICCP, IEC 60870-5-104, IEC-61850, BACNet IP

FILE TRANSFER



- Folder mirroring, Local Folders
- FTP(S), SFTP, TFTP, CIFS, SMB
- Remote Folder Transfer

ENTERPRISE CONNECTORS

- HP ArcSight SIEM, McAfee ESM, Splunk, Qradar
- MS Defender, Helix & Managed Defense, Dragos, Tenable.OT, Radiflow iSID, ForeScout Silent Defence,
- FireEye CloudConnect, Email/SMTP, SNMP, Syslog UDP/TCP, TCP/IP & Multi, UDP
- MSMQ, IBM MQ, Active Message Queue, AMQP, TIBCO EMS, MQTT
- SolarWinds Orion, Thales Aramis, Panorama, Emerson EDS

REMOTE ACCESS

- Remote Screen View
- Secure Bypass

OTHER CONNECTORS

- AV Updates
- WSUS updaters
- Netflow
- Remote printing, Rsync
- Video & audio streaming, Broadcast, Multicast

MATURE – WEB-BASED USER INTERFACE

THIN CLIENT: Easy, powerful web-based user interface

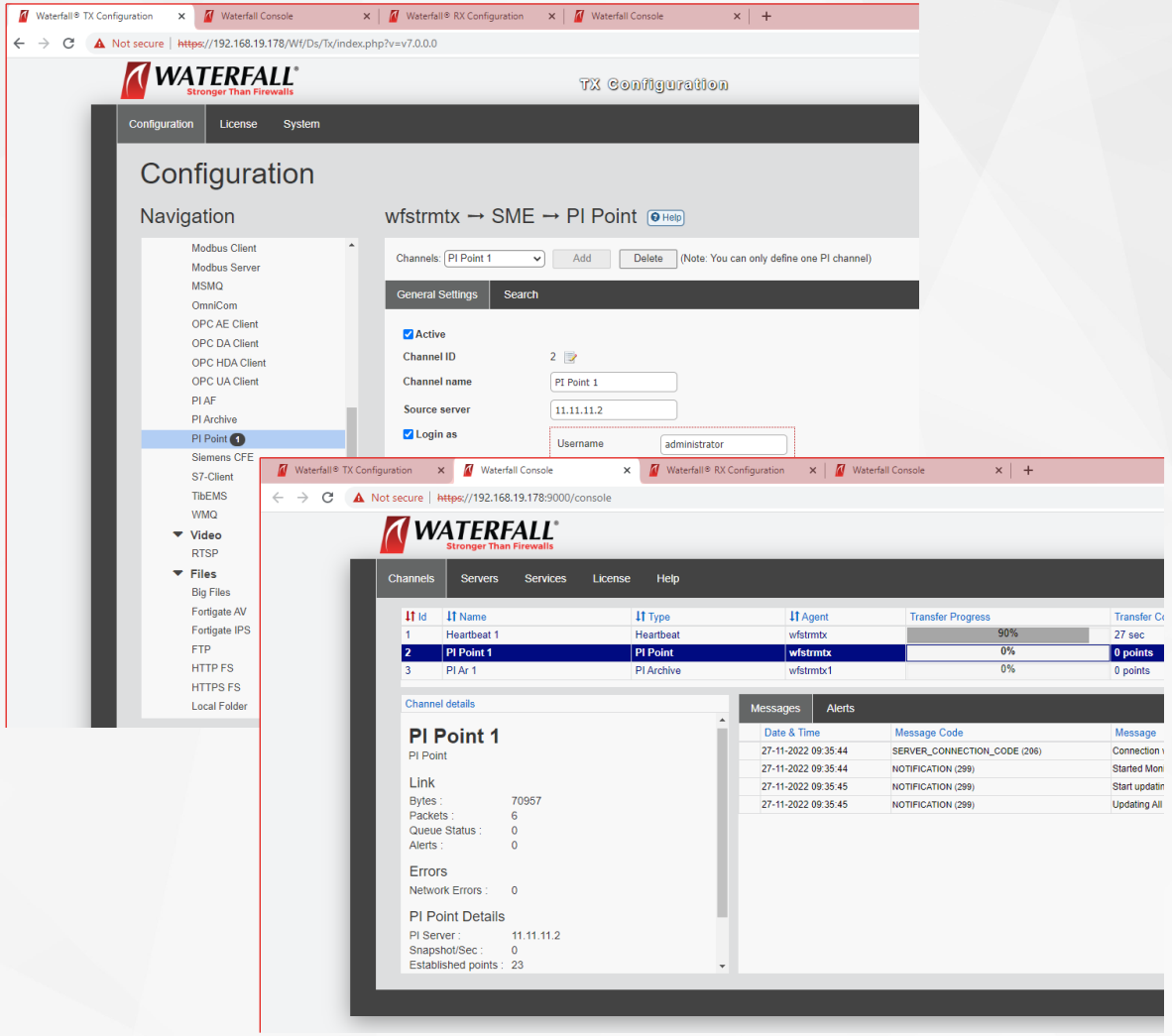
CONFIGURE: Licenses, connectors, filters, alerts, logs and many others

MONITOR: Status, throughput and connector-specific details

MANAGE: Start and stop connectors, services & manage licenses

TROUBLESHOOT: Connectors, connections, logs, hardware & software

True network appliance with no need to install hosts or software on industrial or IT networks



DEPLOYED AT IT/OT CONSEQUENCE BOUNDARY

MOST COMMONLY AT IT/OT INTERFACE

Physical vs business consequences

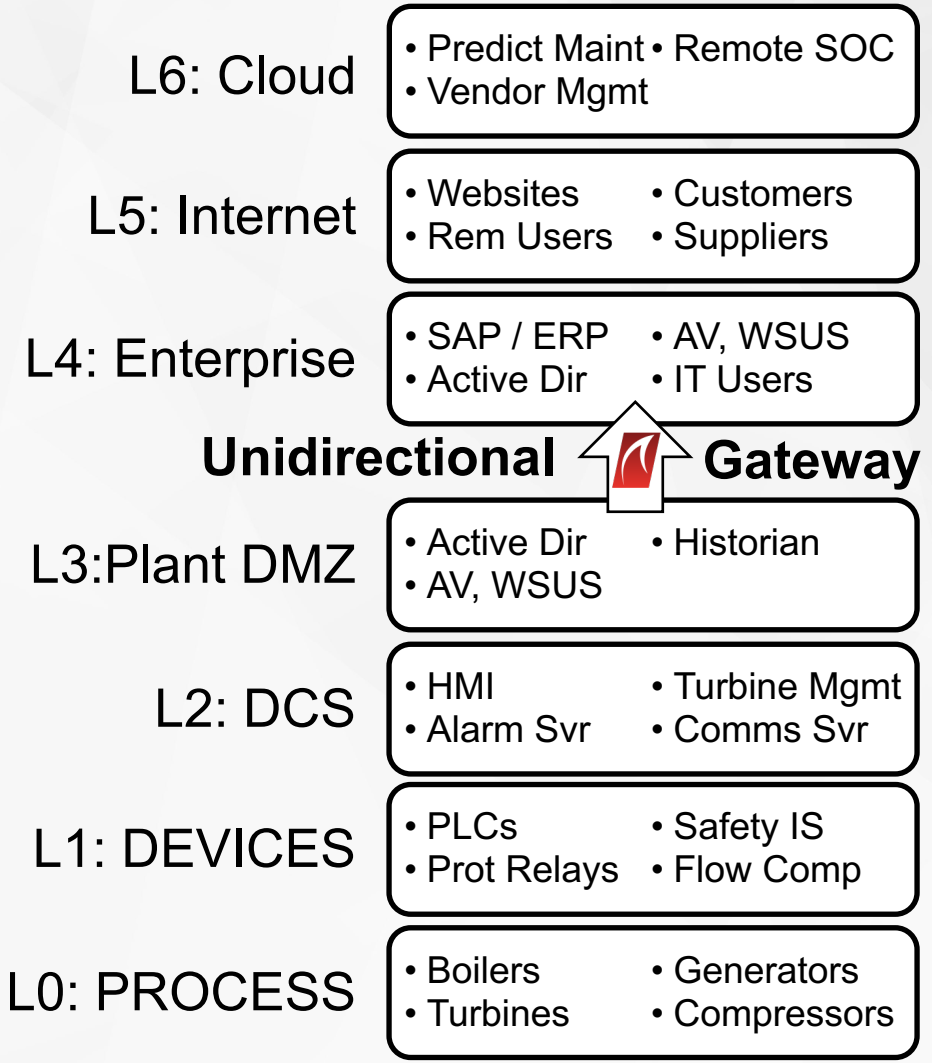
LESS COMMONLY – DIRECT TO CLOUD

No punching TCP connections thru 7 firewall layers

STRONGEST PROTECTION

When there is no other connection from industrial network to any external network

Because human lives, environmental disasters, and even lost production cannot be "restored from backups"



AND AT ICS / INTERNET CONSEQUENCE BOUNDARY

MOST COMMONLY AT IT/OT INTERFACE

Physical vs business consequences

LESS COMMONLY – DIRECT TO CLOUD

No punching TCP connections thru 7 firewall layers

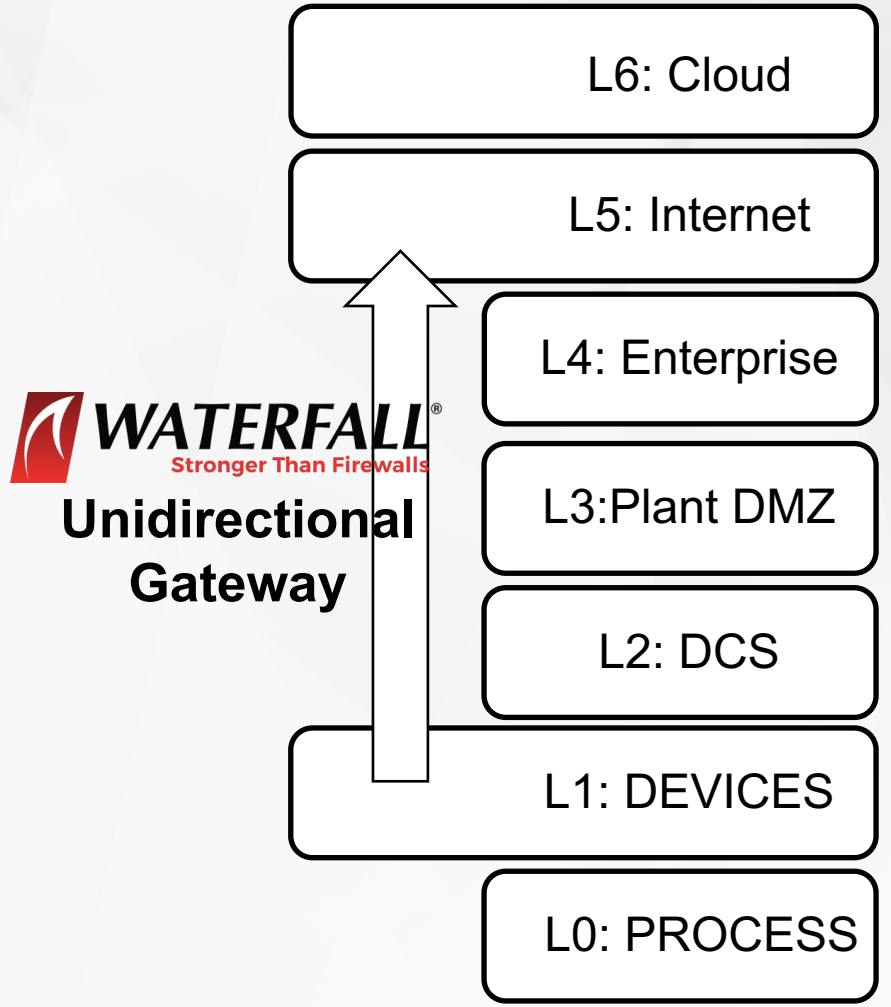
STRONGEST PROTECTION

For high risk connections

NATIVE REPLICATION OR TRANSLATION

Can gather industrial data, convert to RDB, then convert to cloud-friendly MQTT or other

Because all of our plants going down at once is unacceptable



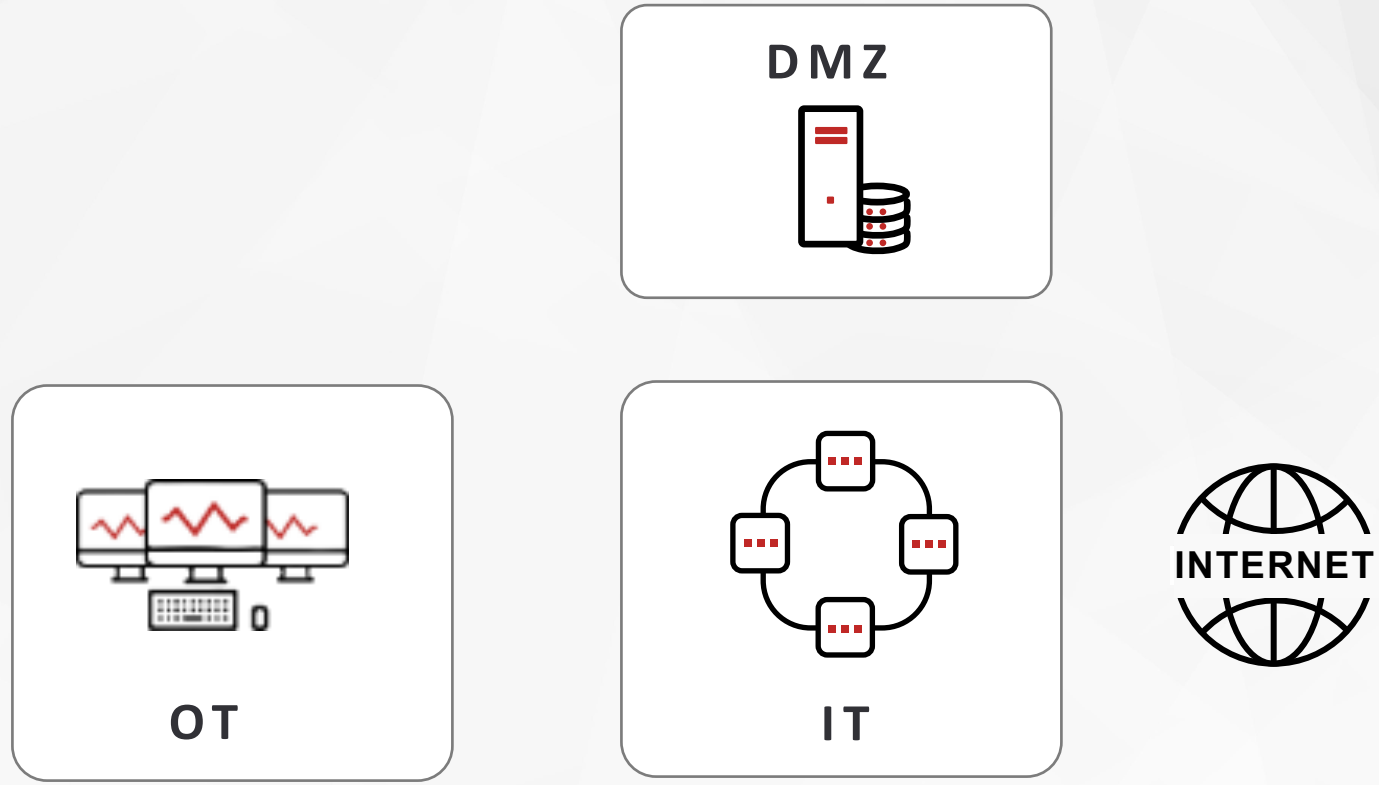
UNIDIRECTIONAL DESIGN PATTERNS

#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	

DEPENDENCY EXAMPLE – CONTAINER TRACKING

COMMON DESIGN

- Can be hard to draw the line – so ***secure*** all ops / OT networks as safety-critical



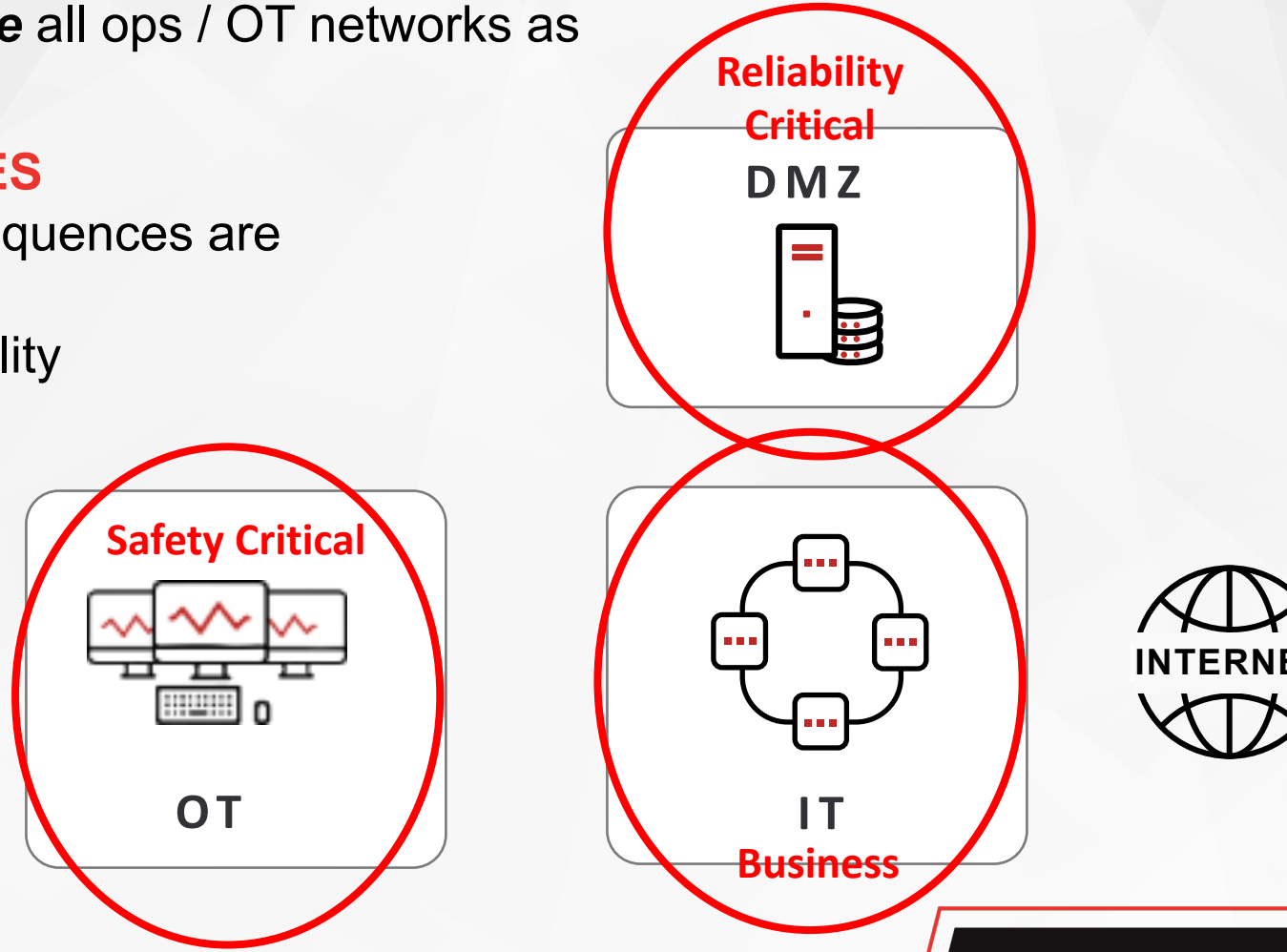
NETWORK ENGINEERING – INTERDEPENDENCIES

COMMON DESIGN

- Can be hard to draw the line – so ***secure*** all ops / OT networks as safety-critical

OFTEN THREE NETWORK CRITICALITIES

- **Safety-critical:** worst case safety consequences are unacceptable
- **Reliability-critical:** unacceptable reliability consequences – eg: container tracking
- **Business:** worst case consequences are acceptable



NETWORK ENGINEERING – INTERDEPENDENCIES

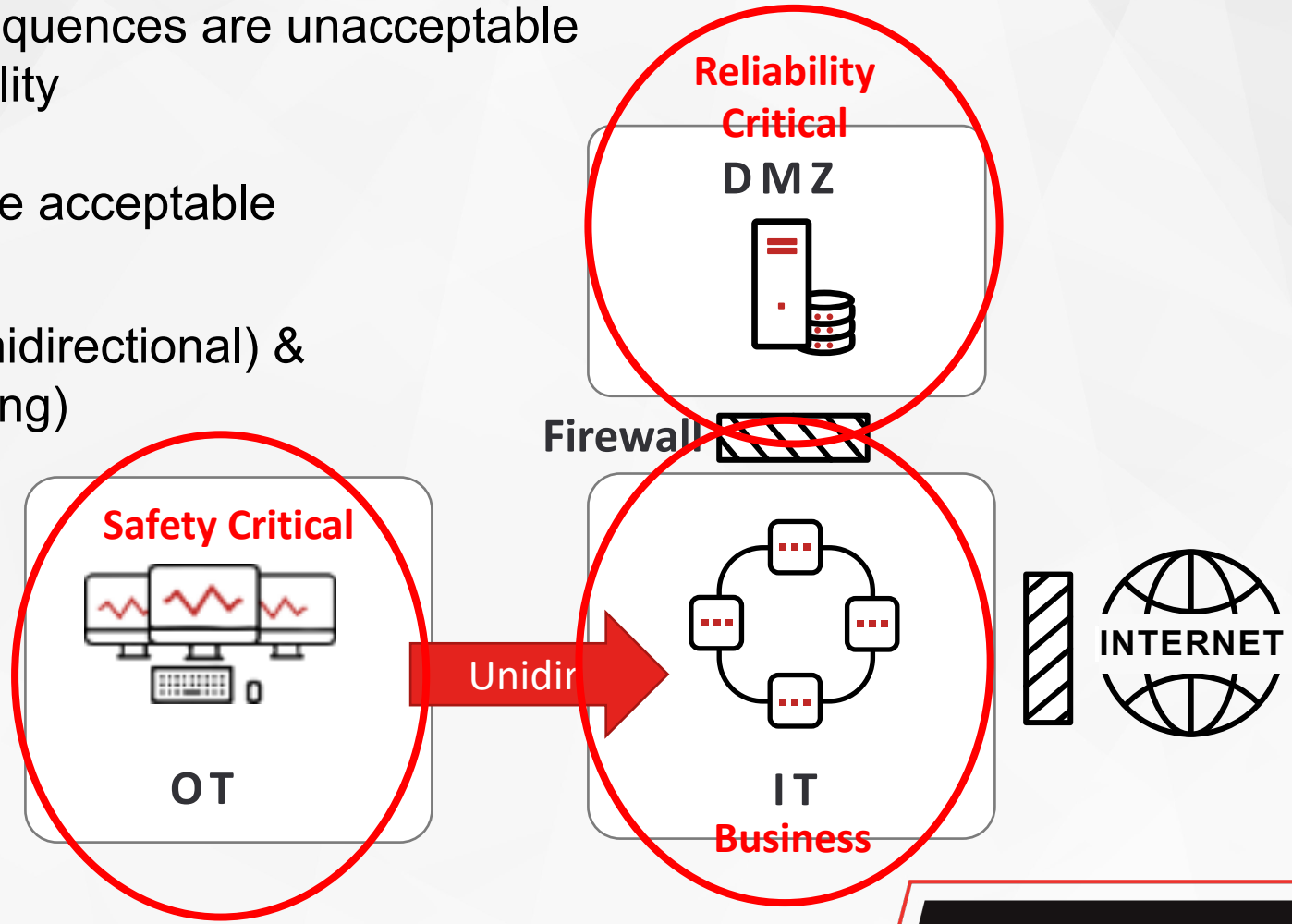
OFTEN THREE NETWORK CRITICALITIES

- **Safety-critical:** worst case safety consequences are unacceptable
- **Reliability-critical:** unacceptable reliability consequences – eg: container tracking
- **Business:** worst case consequences are acceptable

MANAGE DIFERENTLY

- **Safety-critical:** prevent compromise (unidirectional) & prevent consequences (safety engineering)
- **Reliability & business-critical:** prevent compromise (refining) & prioritize recovery – resilience
- **Business:** buy insurance

Eliminate or strictly manage dependencies at consequence boundaries



OT CYBER RISK REVISITED

RISK != CONSEQUENCE X LIKELIHOOD

Does 1x3 really equal 3x1?

Cyber attacks are deterministic, not random

Errors & omissions confuse risk calculations

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

RISK = *f(conseq, intent, c(opportunity), capability)*

If intent & (capability > c(opportunity)) then consequence

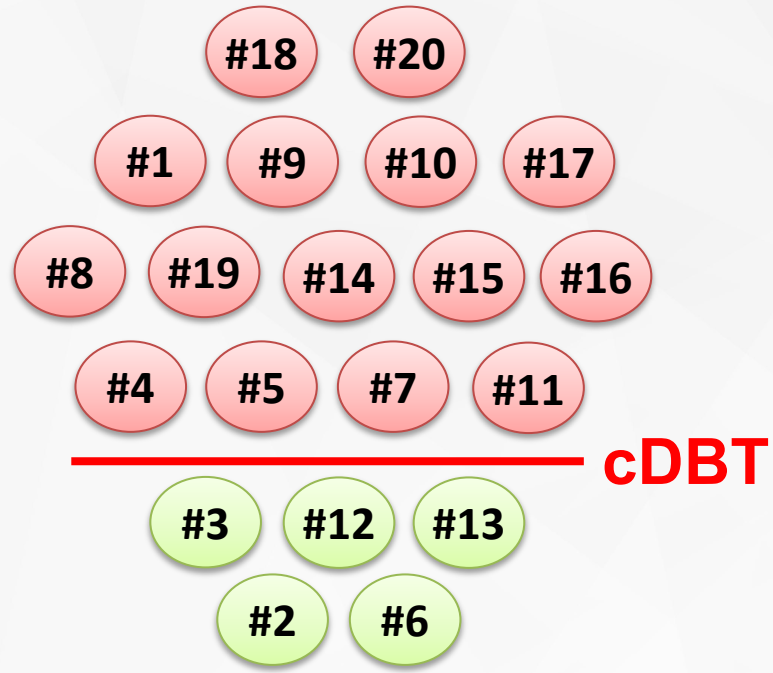
Consequence – result of compromise

Intent – does threat actor want to attack us?

C(Opportunity) – capability needed to exploit opportunity

Capability – ability of the threat actor to attack

Cyber Design Basis Threat – description of kinds of attacks we are required to defeat reliably



WHAT IS “CYBERSECURITY ROI?”

WRONG QUESTION

What is safety system ROI?

SAFETY IS BUILT INTO EVERY PROJECT

Same has to be true for security

SECURITY “AGES” QUICKLY

Long-lived designs engineer out cyber risk

Business decision-makers don’t care about security

Talk to them about risk, pervasive threats & due care

waterfall

ENGINEERING-GRADE OT SECURITY (COMING NOV 1)

PUBLIC SAFETY

Predictable & mathematically model-able designs and safety margins are preferred solutions

ENGINEERS ANTICIPATE EVOLVING THREAT "LOAD"

To avoid constant change in ECC systems

CRITICAL NETWORKS

Have unacceptable worst-case consequences and should be protected with engineering-grade designs

Insurance provides little comfort when trains collide and bridges collapse