
13TH ANNUAL LEADERSHIP EVENT
CYBER SECURITY SUMMIT
cybersecuritysummit.org
RESILIENCE UNLOCKED
TITLE SPONSOR
Island
#cybersecuritysummit #css13

OT Security Engineering

Powerful New Tools to Address Cyber Risk to Industrial Operations and Critical Infrastructure

Rees Machtemes, P.Eng.

Director of Industrial Security
at Waterfall Security Solutions Ltd.

About **WATERFALL SECURITY**

waterfall

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

OT Cyber Risk: Changed Forever

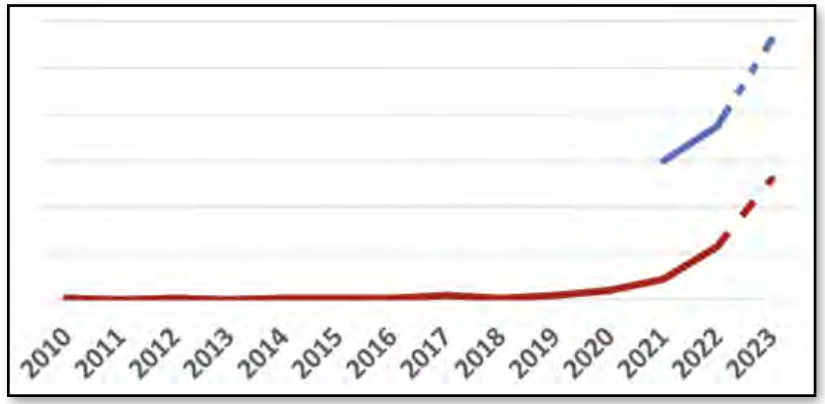
Exponential growth
More than doubling annually

This is a state change
From “theoretical possibility” to “real and growing exponentially”

Will we ever go back
To a year like 2018 with one attack?

Similar trend in FBI stats (2021-22)
www.ic3.gov/Home/AnnualReports

At 150% annual growth, we will see 4,500 attacks in 2027 affecting 15,000 sites



Legend:
- WF Threat Report
- FBI OT Incidents Reported

waterfall-security.com/2023-threat-report

Who Is Behind All This?

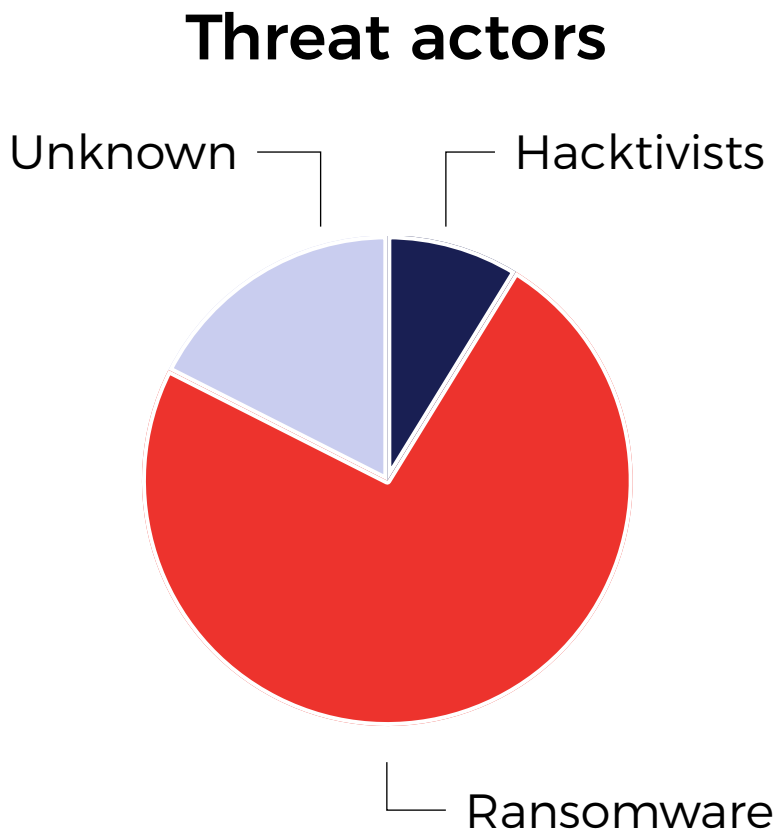
waterfall

Almost all ransomware – how?

1. Some ransomware targets OT specifically
2. Some victims stop OT in an “abundance of caution”
3. Some OT systems fail because of OT to IT dependencies

Ransomware uses nation-state tools

2023 US Cyber Strategy: ransomware criminals are using nation-state tools and techniques



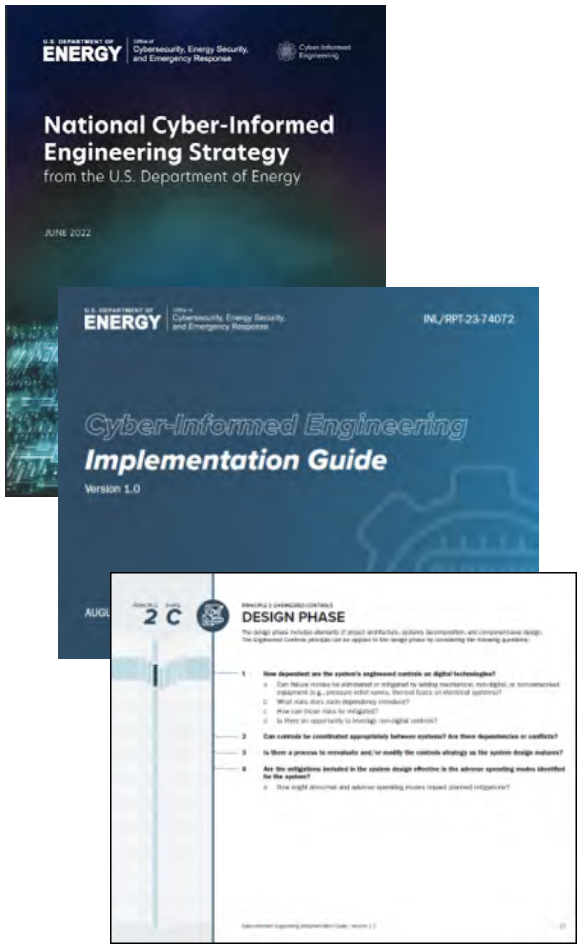
Cyber-informed Engineering

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 profession
Managed physical risk for a century or more
New threat, same risks to public, safety and environment

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

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



Security Engineering – SEC-OT

waterfall

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

Consequence-driven, Cyber Informed Engineering
Risk assessment + unhackable mitigations

Secure Operations Technology
All cyber attacks are information – control information flows physically, and you control the attack vectors

Engineering-grade solutions work predictably and deterministically

Cyber Design Basis Threat (cDBT) model

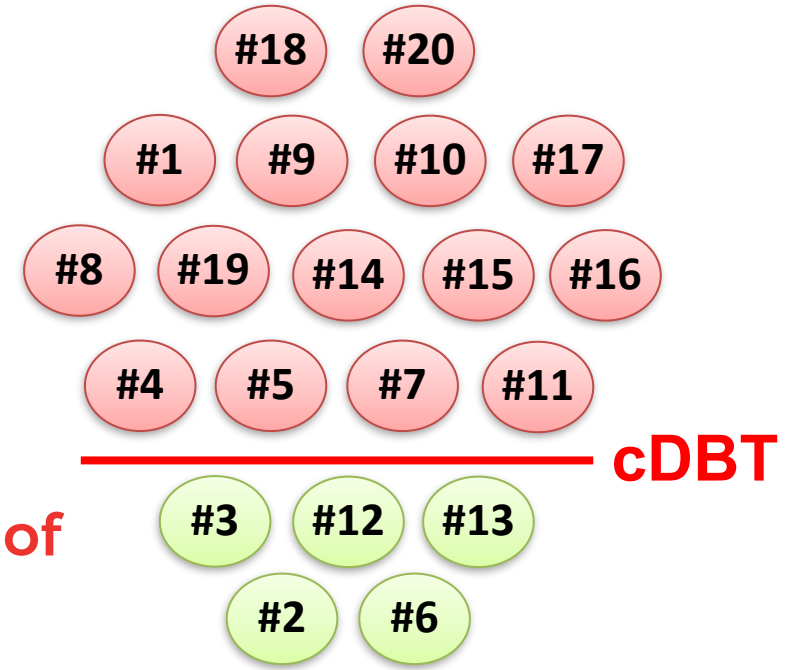
waterfall

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

RISK != CONSEQUENCE X LIKELIHOOD
Does 1x3 really equal 3x1?
Cyber attacks are deterministic, not random
Errors & omissions confuse risk calculations

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 the kinds of attacks we are required to defeat reliably

Network Engineering Concepts

waterfall

Consequence boundaries and network segmentation
Must prevent propagation of these remote-control / malware attacks
EPRI IIoT model

Most widely-deployed solution
Engineering-grade unidirectional gateways enable visibility into OT networks without risk of compromise

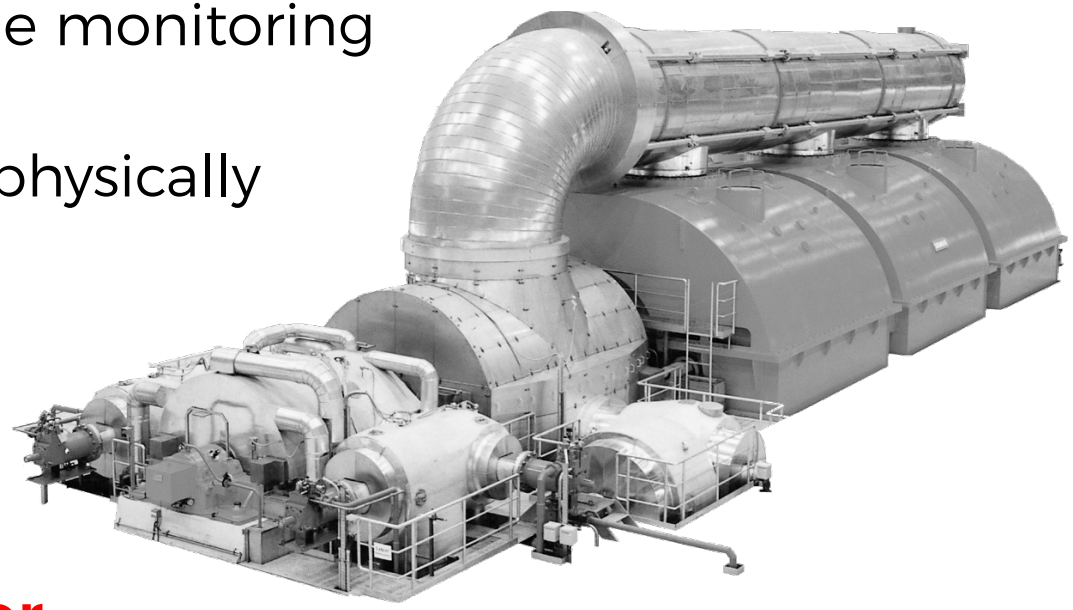
Dependencies and resilience
dependency analysis, trust relationships, manual operations fallback

Segmentation Example: 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 way to pivot attack from Internet or cloud into control network

Unidirectional Security Gateway Technology

Absolute protection with complete network visibility

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

- The hardware sends information in only one direction
- The software copies 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

Engineering-Grade Unidirectionality

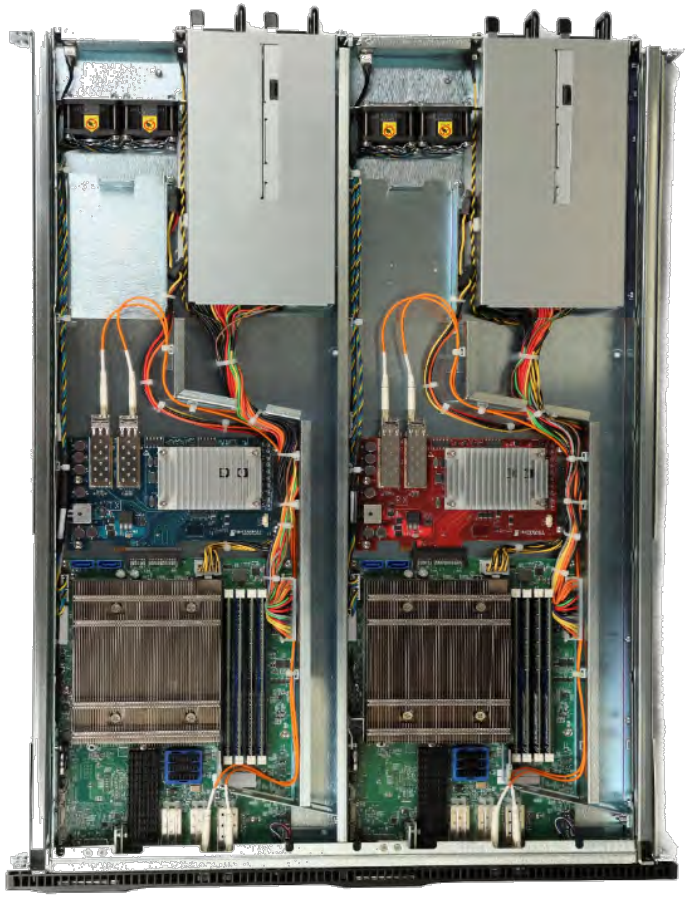
waterfall

Zero internal cross-connects provide 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

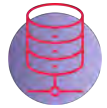


Physical divider down center of unit ensures that there are no cross-connects inside the unit

Mature Software Connectors

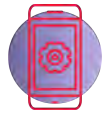
waterfall

Historians & databases



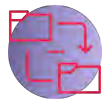
- Aveva (OSIsoft): PI, PI Asset Framework, PI Backfill
- GE: iHistorian, iHistorian Backfill, OSM, Bently-Nevada System1
- Schneider-Electric: Wonderware eDNA, Wonderware Historian, Wonderware Historian Backfill, SCADA Expert ClearSCADA, Siemens CFE & WinTS
- Rockwell FactoryTalk Historian , Honeywell 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, BACNet IP

File transfer



- Folder mirroring, Local Folders
- FTP/S, SFTP, TFTP, CIFS, SMB, NFS
- Remote Folder Transfer

Enterprise monitoring

- FireEye CloudConnect, Email/SMTP, SNMP, Syslog UDP/TCP, TCP/IP & Multi, UDP
- HP ArcSight SIEM, McAfee ESM, Splunk, Qradar
- CyberX (Microsoft), Helix & Managed Defense, Dragos, Indegy, Radiflow iSID, Ethernet Spoofing, ForeScout Silent Defense,
- MSMQ, IBM MQ, Active MQ, AMQP, TIBCO EMS, MQTT, RabbitMQ, HTTP-Request
- SolarWinds Orion, Emerson EDS

Remote access

- Remote Screen View
- Secure Bypass

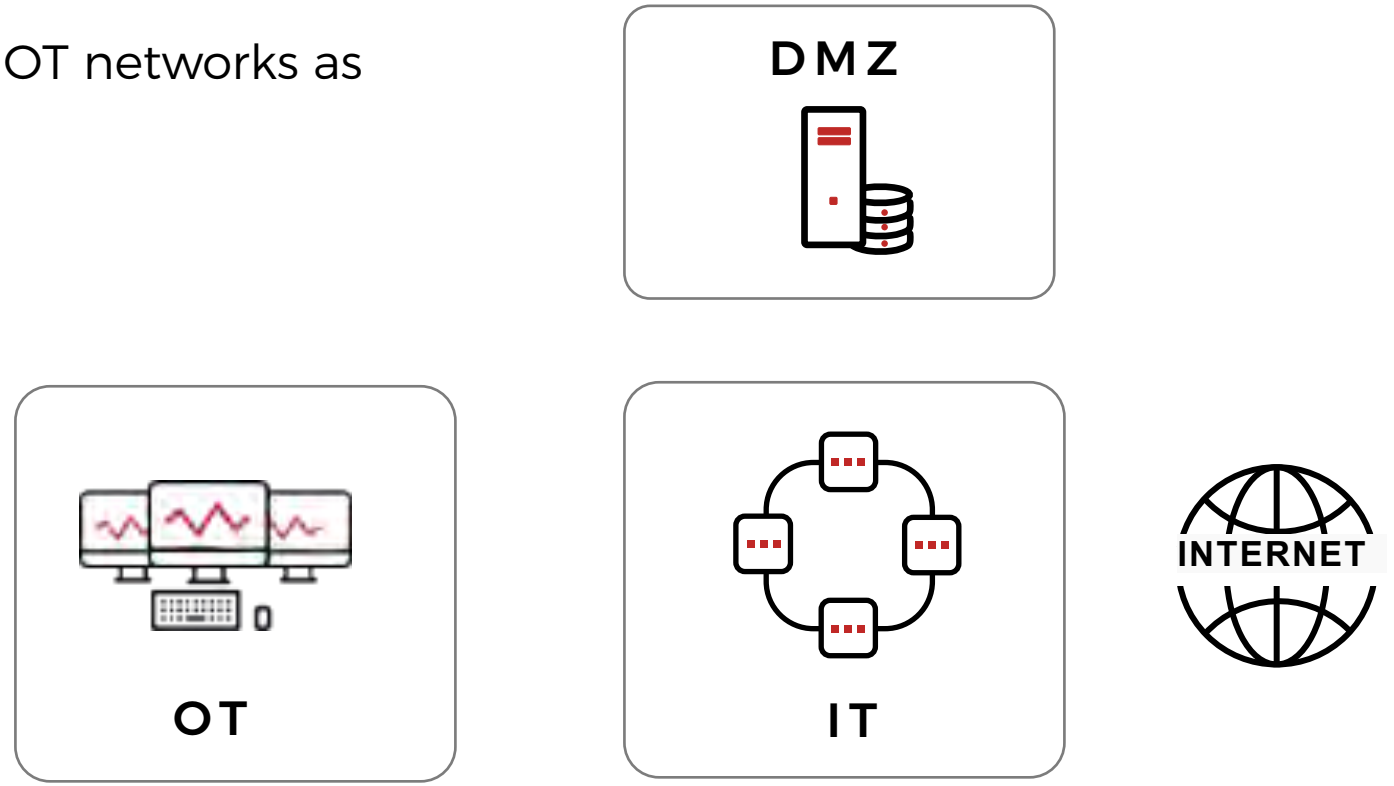
Other connectors

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

Dependency Example: Container Tracking

waterfall

Common design
Can be hard to draw the line, so secure OT networks as safety-critical

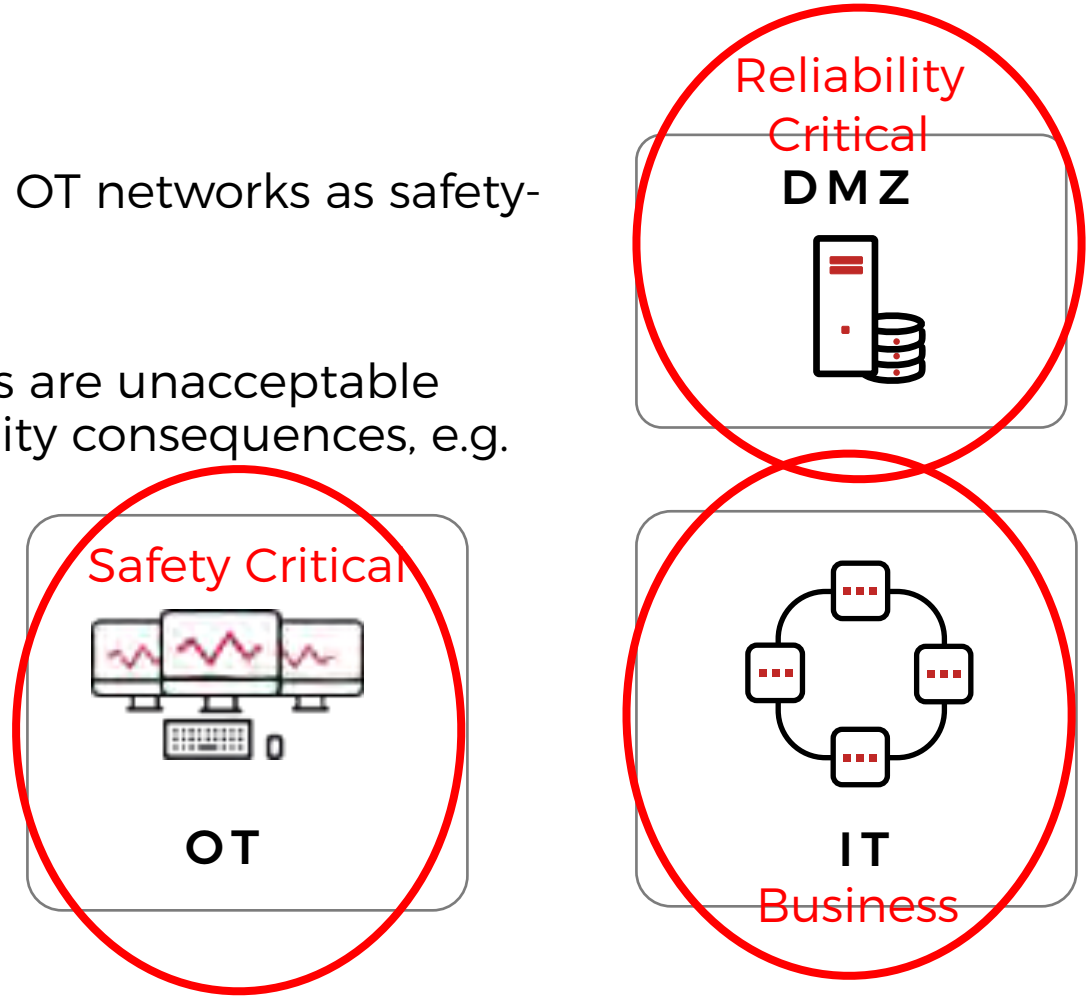


Network engineering: Interdependencies

waterfall

Common design
Can be hard to draw the line, so secure OT networks as safety-critical

Often three network criticalities
Safety-critical: worst case consequences are unacceptable
Reliability-critical: unacceptable reliability consequences, e.g. container tracking
Business: worst case is accepted



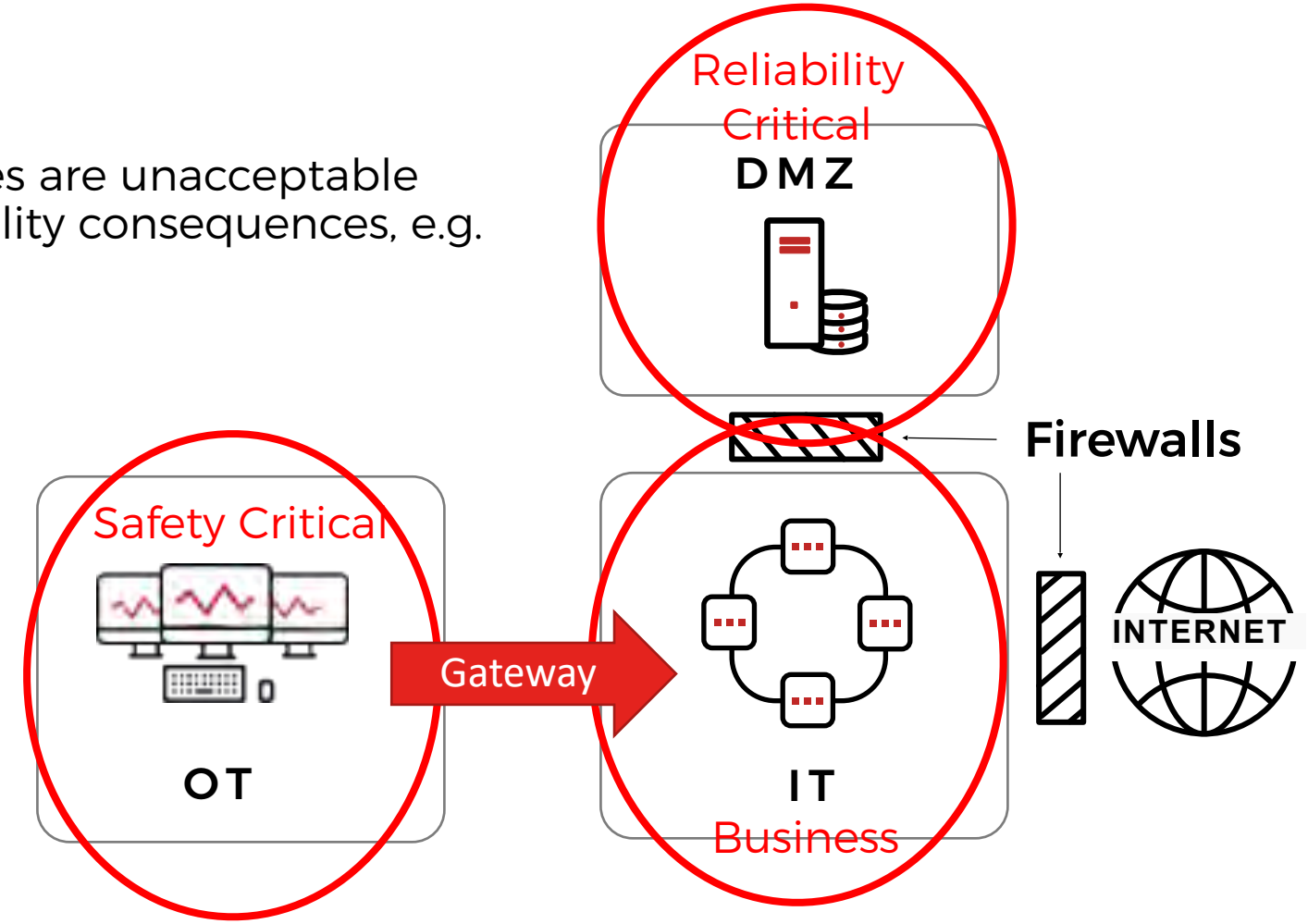
Network engineering: Interdependencies

waterfall

Often three network criticalities
Safety-critical: worst case consequences are unacceptable
Reliability-critical: unacceptable reliability consequences, e.g. container tracking
Business: worst case is accepted

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

Eliminate or strictly manage dependencies at consequence boundaries



New Book: Engineering-Grade OT Security

FREE copies at our booth and online for a limited time

waterfall

Public safety
Demands predictable & mathematically model-able designs and safety margins

Engineers must anticipate threat "load"
To avoid constant change in ECC systems

Critical networks
Have unacceptable worst-case consequences and must be protected with engineering-grade designs

Official Launch & Webinar Nov 1st

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