waterfall

Changing the Equation

2024 Threats, Credible Attacks & Hardware-Enforced Remote Access

Andrew Ginter, VP Industrial Security, Waterfall Security

Attack / Consequence Credibility

Threat environment changed – at the turn of the decade

Sophisticated attack tools – high-end ransomware buys / sells w/nation states

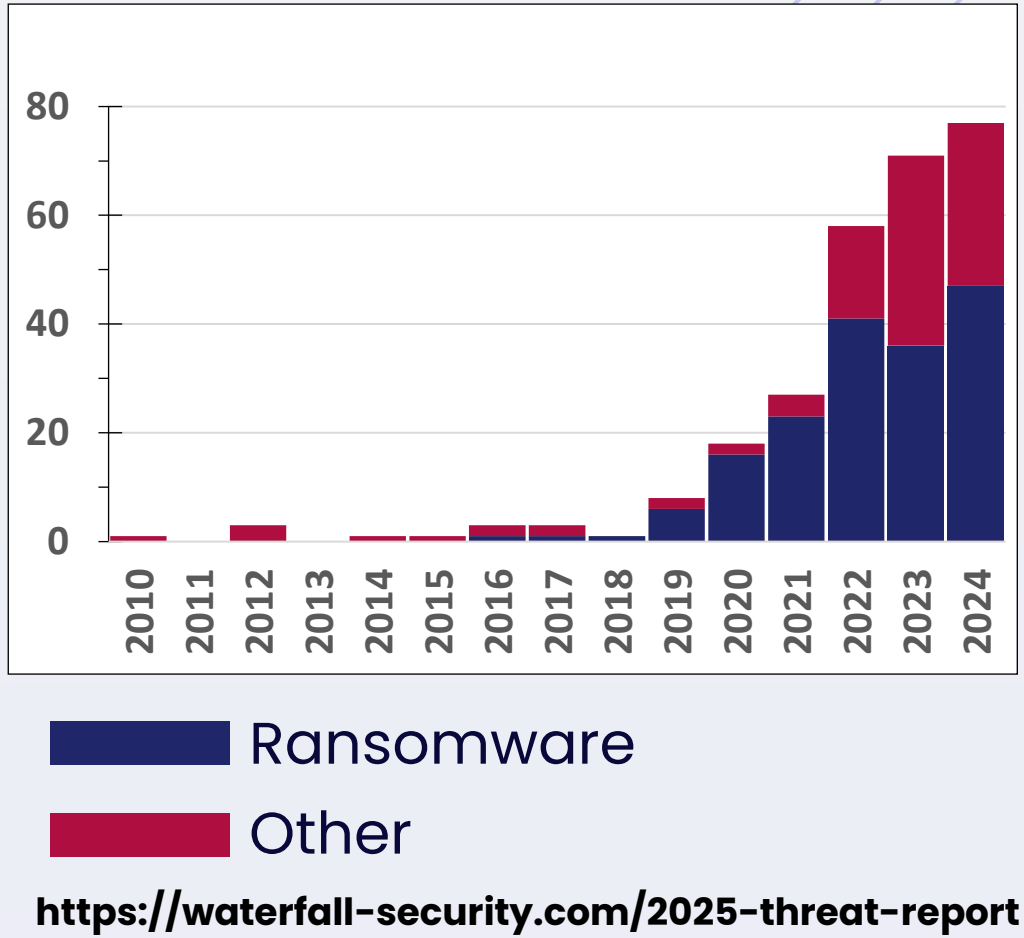
Safety systems – have been breached, protected relays have been targeted

Substation gear – has been bricked & transformer damage targeted

Nation state attacks – tripled last year, targeting physical operations

ICS-designed malware – as many last year than in last 6 years combined

Attacks not credible a decade ago are commonplace today



https://waterfall-security.com/2025-threat-report

Attack / Consequence Credibility

Threat environment changed – at the turn of the decade

Sophisticated attack tools – high-end ransomware buys / sells w/nation states

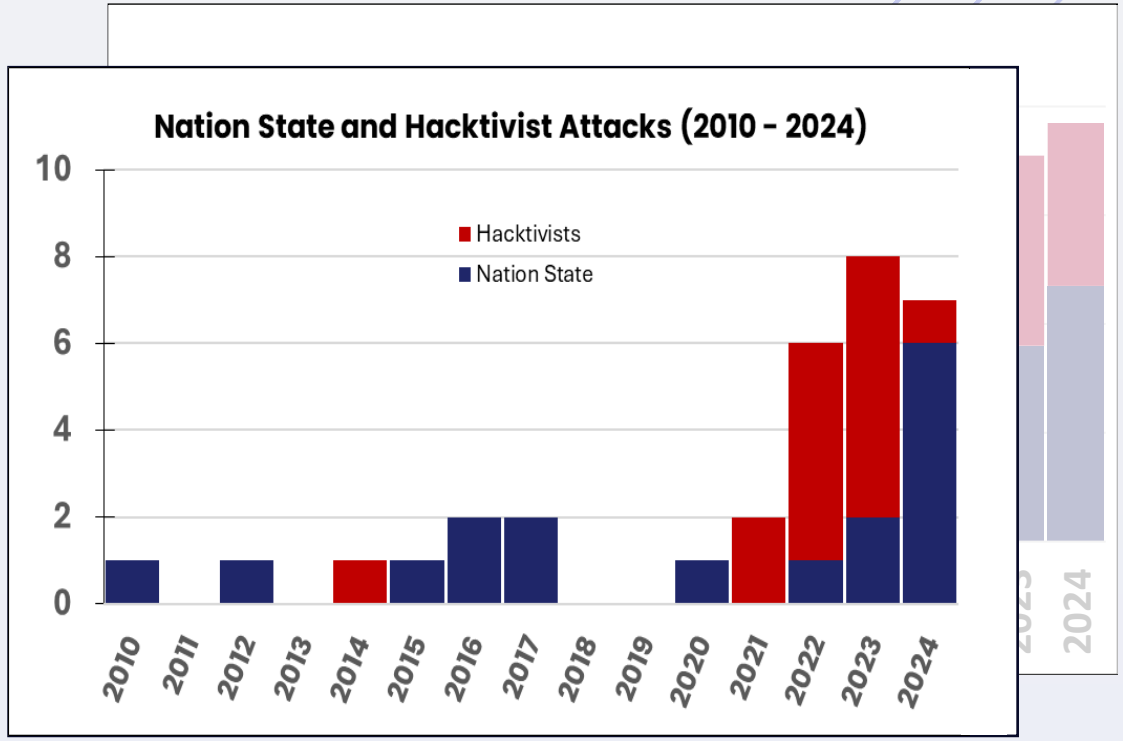
Safety systems – have been breached, protected relays have been targeted

Substation gear – has been bricked & transformer damage targeted

Nation state attacks – tripled last year, targeting physical operations

ICS-designed malware – as many last year than in last 6 years combined

Attacks not credible a decade ago are commonplace today



Nation States

Hacktivists

https://waterfall-security.com/2025-threat-report

waterfall

ICS-Capable Malware

Ten total since 2010 – comparatively rare

Three of these in 2024 – vs. 7 in the previous 14 years

Nation-state grade – investments in physical consequences

Significant because of the potential to cause physical consequences over and above simple shutdowns

Malware	Year	Details
Stuxnet	2010	Autonomous
Havex	2013	OPC espionage
Crash-Override	2016	Four ICS protocols
Triton	2017	SIS Sabotage
EKANS	2020	Kills ICS servers
Pipedream	2022	“Swiss army knife”
Cosmic-Energy	2023	IEC 60870-5-104
FrostyGoop	2024	Modbus TCP
IOControl	2024	ARM-based IoT
Fuxnet	2024	Mbus

Cyber-Informed Engineering

If Your Life Depends On A Boiler Not Exploding – in a cyber attack, would you prefer protection by a spring-loaded valve? Or longer PLC password? Where is the valve in the NIST CSF? In IEC 62443?

Manual Operations – operate through compromise manually – can we still? Have we practiced?

Engineering Profession – has managed risks to public & worker safety for a century

Would You Trust A Bridge – whose design engineer "hopes" it will carry the specified load, for the specified number of decades?

Engineering-grade solutions protect public safety and national security, deterministically.

Cyber-informed Engineering - Principles

1. **Consequence-focused design**
2. **Engineered Controls**
3. **Secure Information Architecture**
4. Design Simplification
5. Layered Defenses
6. Active Defense
7. Interdependency Evaluation
8. Digital Asset Awareness
9. Cyber-Secure Supply Chain Controls
10. Planned Resilience
11. Engineering Information Control
12. Organizational Culture

The first three are arguably the most important

waterfall

Consequence Blind Spots

Safety-instrumented systems – are software, often connected to control networks, or their engineering / programming workstations are so connected

Equipment damage – causing long-term outages – resilience demands we prevent such damage

Protective relays are software – and network-connected - equipment protection functions be defeated by sufficiently sophisticated / pivoting cyber attacks

"Bricked" equipment – over-write firmware so that machine cannot be booted up far enough to restore good firmware

- **Brick most of your PLCs –** how long will it take to upgrade to a model you can buy
- **Brick a million smart meters –** in the "turn off power to the consumer" state – how long does it take to turn the power back on?

Cloud-pivot – with outage or damage to hundreds of sites at once

Other conditions – for which there are no safeties: hydraulic hammers, autonomous vehicles mis-directed

Qualitative Impact / Likelihood Rankings

Risk = impact x likelihood

Likelihood						
Very high	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low
	Very Low	Low	Moderate	High	Very High

Level of Impact

Problem: risk level should determine the thoroughness and the nature of security programs designed to address the threat

Qualitative Impact / Likelihood Rankings

Risk = impact x likelihood – but does 1x5 = 5x1 ?

Likelihood						
Very high	**Very Low**	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	**Very Low**
	Very Low	Low	Moderate	High	Very High

Level of Impact

We defend small shoe factories very differently than we do passenger rail switching systems – formula does not distinguish

Eg: Spanish Rail Systems

By law…

Likelihood					
Very high	**SL2**	SL2	SL3	SL4	SL4
High	SL2	SL2	SL3	SL4	SL4
Moderate	SL1	SL2	SL3	SL4	SL4
Low	SL1	SL2	SL2	SL4	SL4
Very Low	SL1	SL1	SL2	SL4	**SL4**
	Very Low	Low	Moderate	High	Very High

Level of Impact

In practice, high-consequence assessments ignore likelihood / frequency for unacceptably high impacts

High-End Cyber Attacks Are Not Random

Likelihood
Implies that cyber attacks are random, like random safety equipment failures

But … high-end attack success/failure is deterministic
The same high-end ransomware attack on the same target succeeds or fails almost always exactly as did the first one

High-end attacks use repetition
To eliminate randomness - like human errors

High-end attacks are persistent
Not independent once one succeeds or when a target is strategic

Designing defenses assuming attacks are launched at random, or succeed at random, risks repeated compromise

Propose “Credibility” To IEC 62443-3-2 (Revised)

3.1.N credibility
How reasonable it is to believe something will happen

Note 1 to entry:
Credibility can be based on frequency data, when such exists

High frequency – risk = impact x frequency
Use the formula for high-frequency threats only

HILF risk – drop the formula
There is no formula for exercising judgement

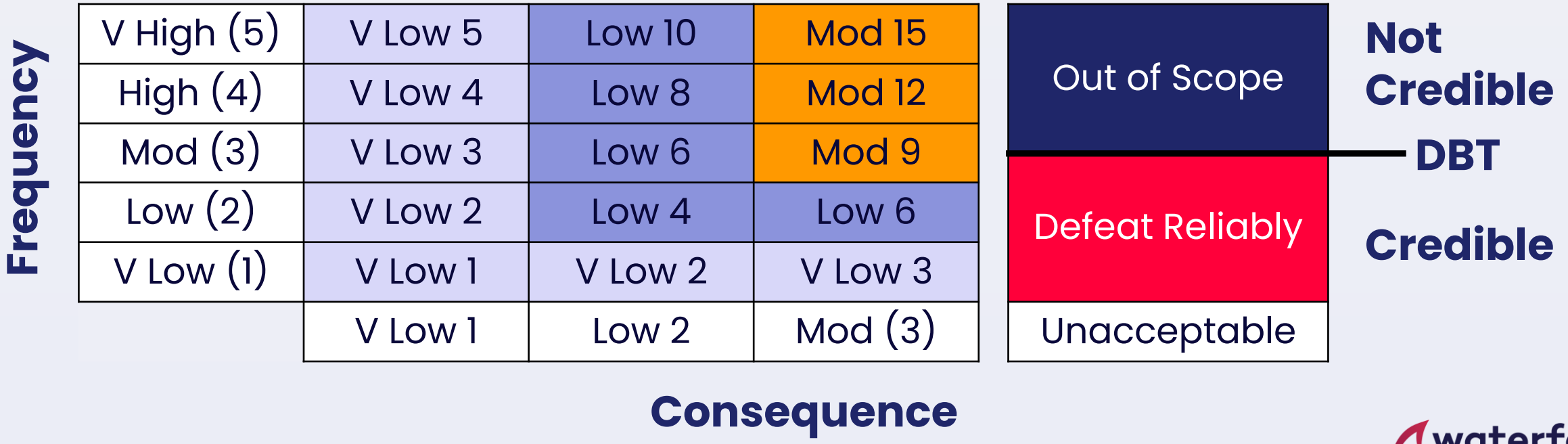
Attacks are becoming steadily more capable
CIE focuses on high-impact threats first

Selection Criteria – Risk-Based

Credible consequence severity – acceptable vs unacceptable

Defeat with a high degree of confidence – all credible attacks with unacceptable consequences

Experts disagree – are all credible attacks detectible? Are only detectable attacks credible?



Principles of Operational Technology Cyber Security

AU ASD, AU ACSC, US CISA, US NSA, US DoJ, MS ISAC, UK NCSC, CA CCCS, NZ GCSB, NZ NCSC, DE BSI, NL NCSC, JP NISC, JP NPA, KR NIS, KR NCSC

Safety is paramount – consequence drives IT/OT differences

Knowledge of the business is crucial – a CIE principle

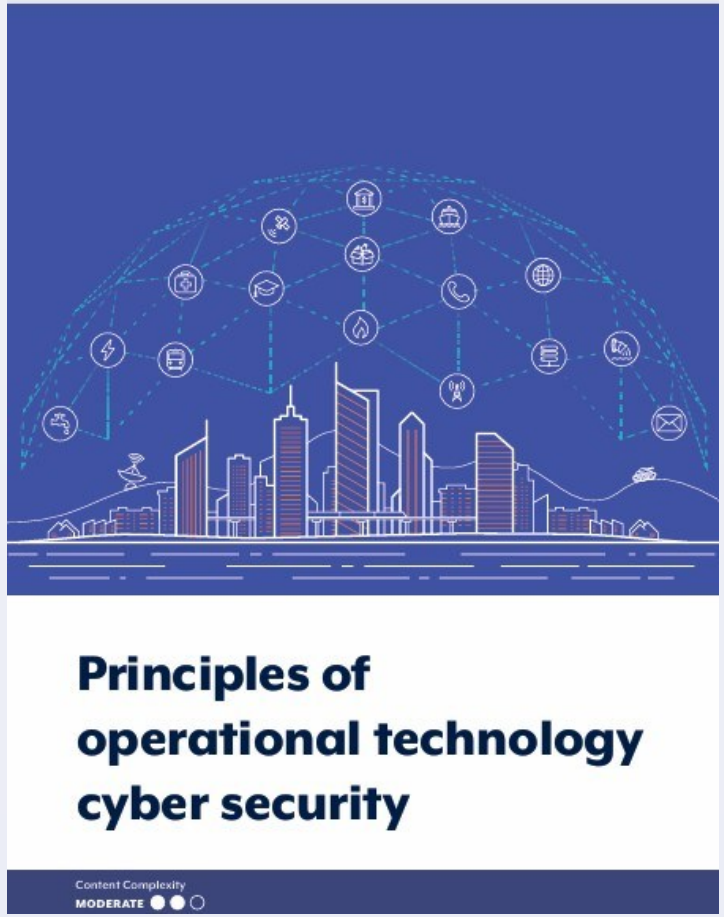
OT data is extremely valuable and needs to be protected – data about how OT system is designed & configured

Segment and segregate – firewalls can be bypassed – especially easily if administered from vulnerable side

Supply chain must be secure – every printer, router and controller can be a threat vector

People are essential for OT cybersecurity – for everything from assessing risk to responding to incidents

If there is a cyber incident in an area that requires software running correctly for the work environment to be considered safe […] is an organization prepared to send staff to that site knowing that a bad actor has been, or is currently, on the network?



Network Engineering - at Consequence Boundaries

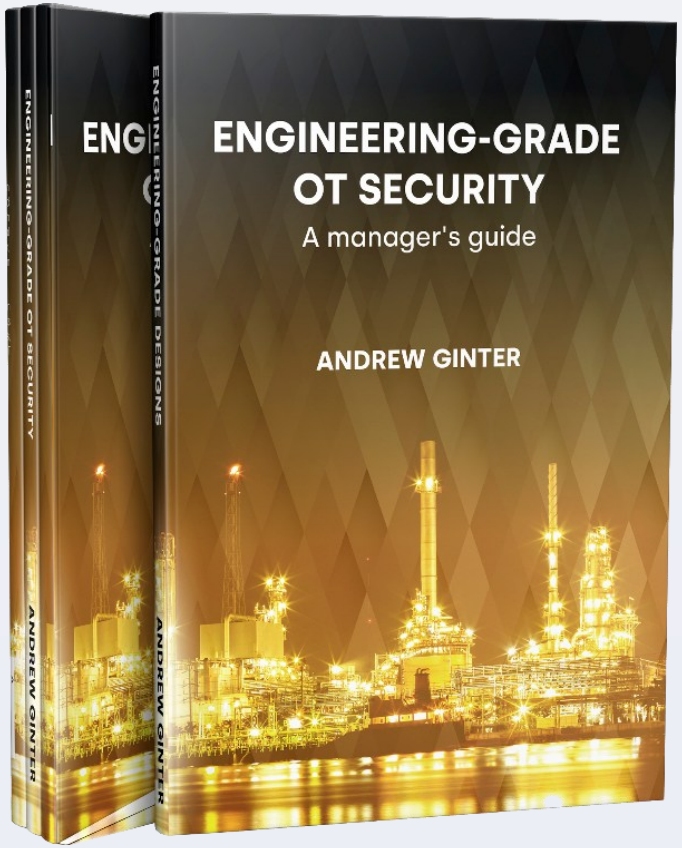
Worst-case consequences define criticality – when every CPU issues exactly the wrong instruction

Consequence boundaries – connections between networks - very different worst-case consequences

- Safety-critical
- Reliability-critical
- Business-critical

Network engineering – engineering-grade prevention of attacks pivoting through network connections at criticality boundaries

Safety engineering shuts down ops in an emergency. Network engineering prevents emergencies from shutting down CI



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

waterfall

Unidirectional Security Gateways

Engineering-grade unidirectionality

Engineering-grade protection – the gateway hardware is physically able to send information in only one direction

Network visibility – the software makes real-time copies of servers & devices – IT users access the replicas normally"

No attack - no matter how sophisticated, can propagate back to the industrial network through the gateway

French ANSSI – Consequence Boundaries

Class 3 – "safety critical"

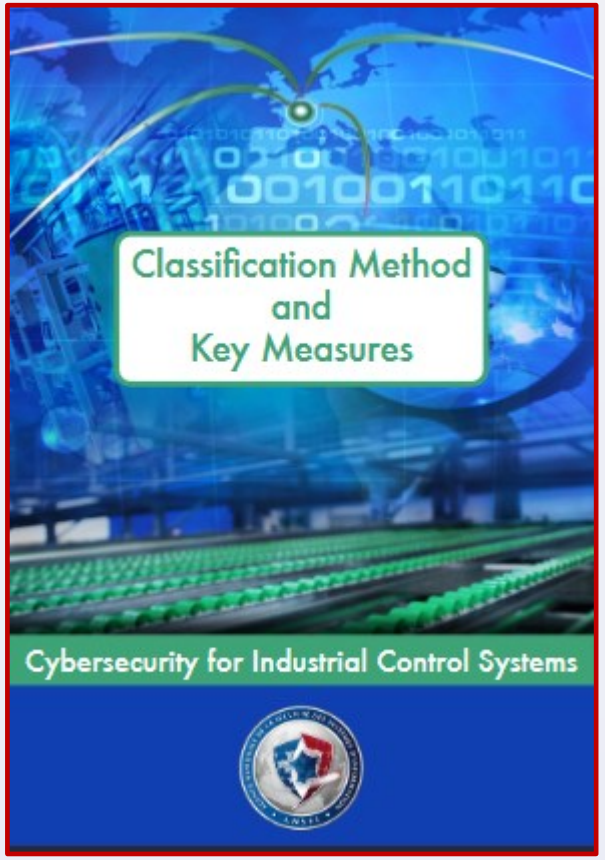
- Must use unidirectional protection for connections to less-critical networks
- Remote access from less-critical networks is forbidden

Class 2 – "reliability critical"

- Should be unidirectional towards Class 1 networks
- Strongly discourages remote access from Class 1 networks

Class 1 – business networks (IT)

Did not use the term but clearly stated what are becoming widespread requirements for consequence boundaries



TSA Pipelines Security Directive SD 2021-02E

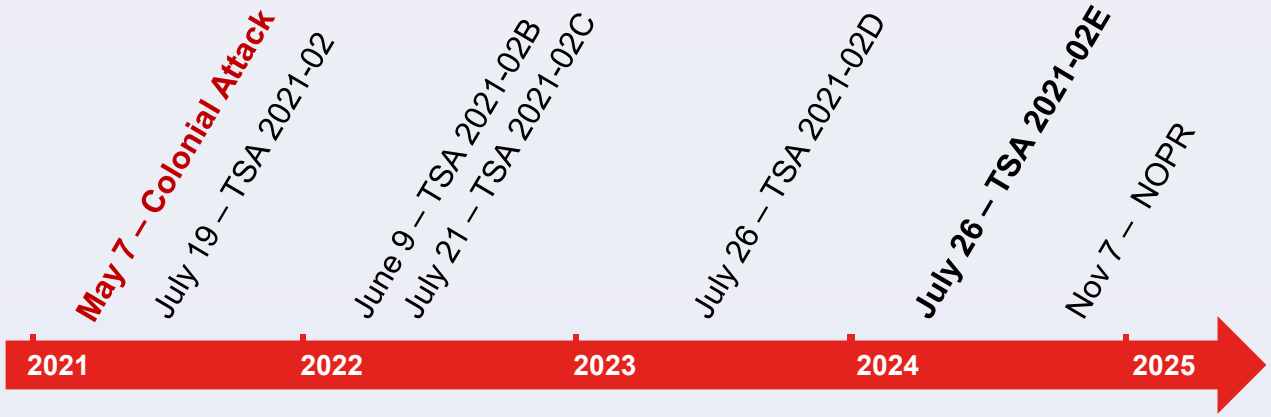
Keep OT at necessary capacity when IT fails – first time this goal was ever stated explicitly

Require OT to continue – even if IT is compromised

Require OT to be isolated – from IT networks when IT networks have been compromised

Require understanding of dependencies – so OT can continue when isolated from IT during an IT cyber emergency

Many policies specific to IT / OT interface & relationship



Modern Approaches to Network Access Security

US CISA, US FBI, NZ GCSB, CERTNZ, CA CCCS

Discourages VPNs and Jump Hosts – too much access to too many systems

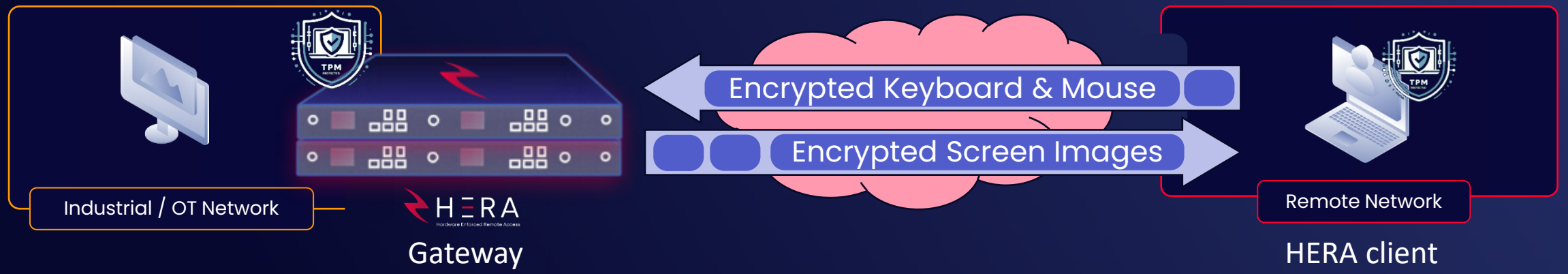
Zero trust – authenticate everyone, all the time, providing only the access needed

Secure (access) service edge– modern cloud-based IT-grade remote access, with secure web gateways, access security brokers and firewall as a service

Hardware-enforced network segmentation – for the most consequential OT networks, use hardware-enforced unidirectional protections

- **Remote screen view** – attended remote access
- **Timed A/B switch –** provides site with physical control over remote access
- **Hardware-Enforced Remote Access –** two unidirectional gateways, one in each direction

Hardware Enforced



HERA Gateway

Hard protocol break eliminates TCP pivoting path

Remote access without an exploit pivoting path into OT

Dual Encryption

Leverages TPM hardware in HERA gateway and HERA client, with protocol so simple hardware can filter it

No Man-in-the-Middle
No session hijacking

Remote Hardware

Leverages TPM hardware to secure communications and prevent session hijacking

Dramatically reduced attack surface

About Waterfall Security

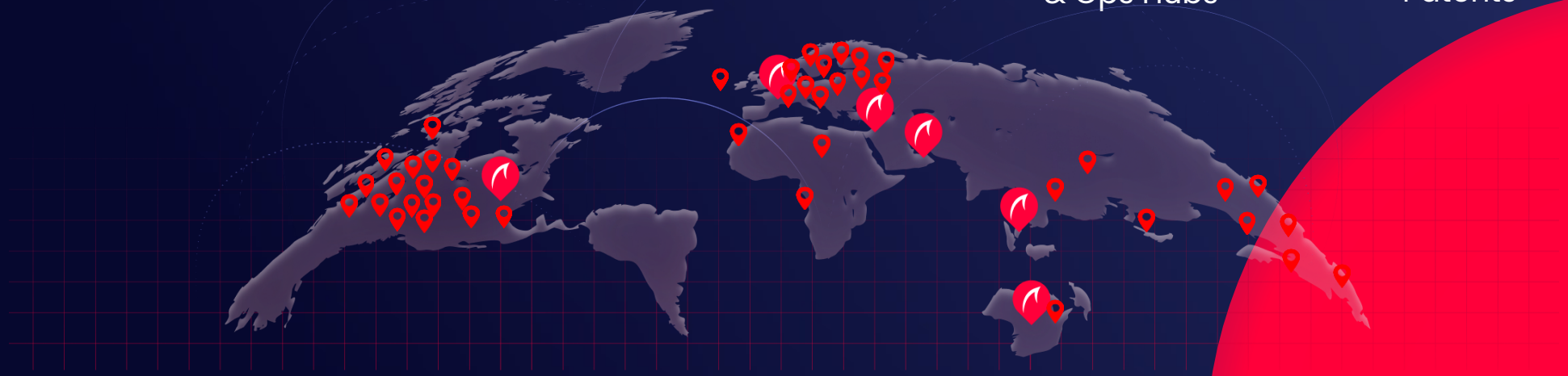
2007
Founded

>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:

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

waterfall

When Did You Last Overrule A Safety Engineer?

What happens

When there is not budget to meet project safety requirements?

High-impact security engineering
is becoming more like safety engineering

Credible threats with unacceptable consequences are show-stoppers

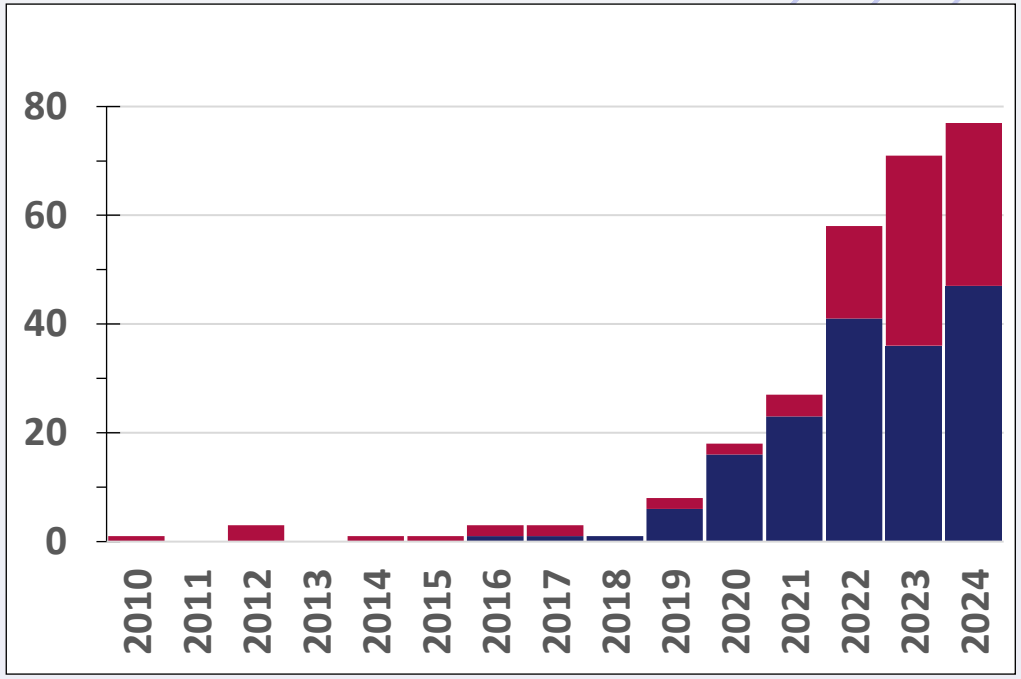
Due Care – What Is Reasonable To Believe? To Do?

6 people died in the explosion

In your planning, did you determine that this type of attack was a credible threat?

If not, why not?

If so, then why did you not address this type of attack more effectively?



Credible threats, attacks and consequences should drive decision-making, especially regarding engineering-grade protections in high-consequence designs