waterfall

Operational Technology (OT) Cybersecurity

State of the Art

Andrew Ginter, VP Industrial Security

Waterfall Security



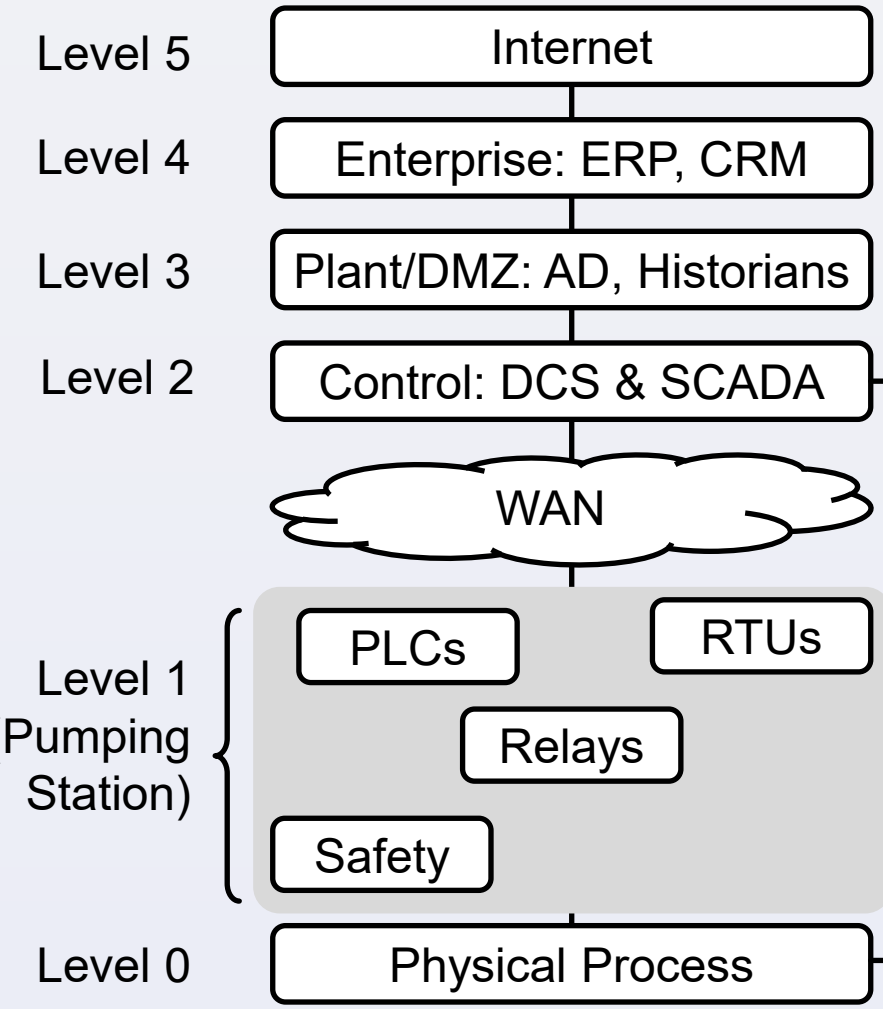
Copyright © 2026 Waterfall Security Solutions Ltd.

What is OT? Human-Machine Interface - HMI



Copyright © 2026 Waterfall Security Solutions Ltd.

Purdue Model / IEC 62443









Copyright © 2026 Waterfall Security Solutions Ltd.

Industrial Control System (ICS) & Operational Technology (OT)

Consequences – define the difference between IT & OT

Safe –assure worker safety, public safety & the environment

Reliable – physical ops: continuous & no equipment damage

Efficient - production

Engineering Change Control (ECC) – every change risks mistakes - study change before implementing – more consequential = more engineering

Most Engineers – have budget for projects to improve efficiency, worry about reliability, and largely assume safety is "covered" by safety engineering / cyber is "covered" by IT

The essential difference between IT sec and OT sec –
we cannot restore human lives
nor damaged physical equipment
from backups



Copyright © 2026 Waterfall Security Solutions Ltd.

waterfall

Ransomware Step Change

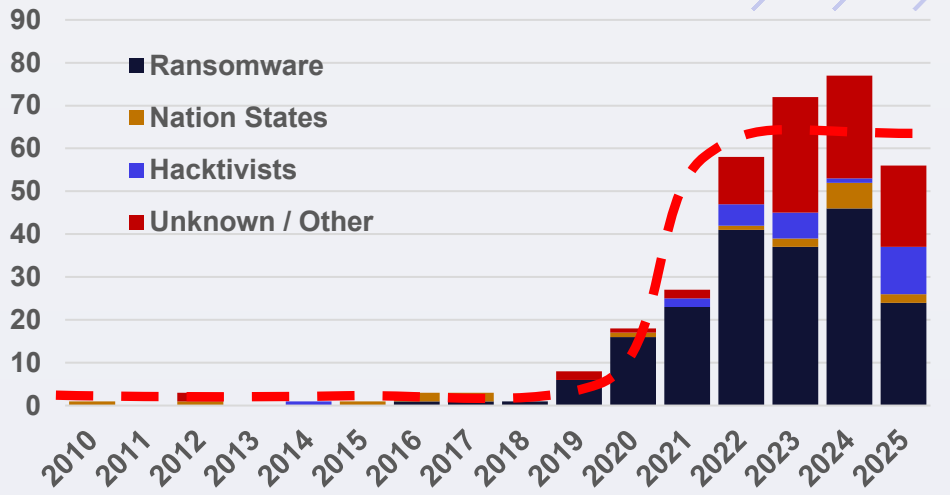
57 breaches in 2025 – mostly ransomware

"Abundance of caution" – not confident of strength of OT security program

Dependencies – shut down because physical ops need crippled IT systems

Direct OT attack – shut down ops because automation is compromised

Supply chain – supplier or customer is compromised, and so victim shuts down



Step change at the beginning of the decade was due to ransomware

Copyright © 2026 Waterfall Security Solutions Ltd.

waterfall

Pervasive Threat – Pivoting Attacks

Compromised machines – "phone home" and are operated manually by remote control – "Remote Access Trojan" (RAT)

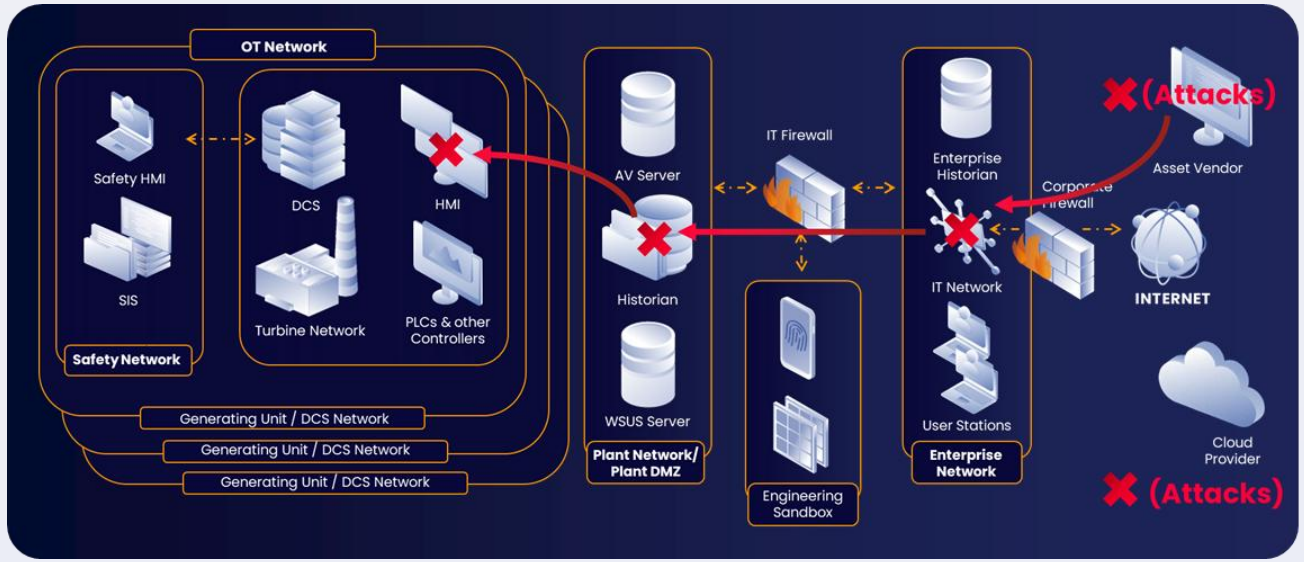
Use compromised machines – to attack other machines – "pivoting"

Break firewalls – shoulder-surf the admin password, exploit a new vulnerability, phish a password to any service exposed through the firewall

Break encryption – steal a key, hijack a session (eg: web cookie), attack from a trusted endpoint

Living off the land – no RAT, use native operating system facilities to maintain remote control

After all – ransomware criminals pivot routinely through IT-Internet firewalls to compromise IT, don't they?



Copyright © 2026 Waterfall Security Solutions Ltd.

waterfall

Hacktivists and Nation States

Breaches – doubled over the previous year

Nation-state-sponsored hacktivists – the boundary is blurring – especially in kinetic conflicts

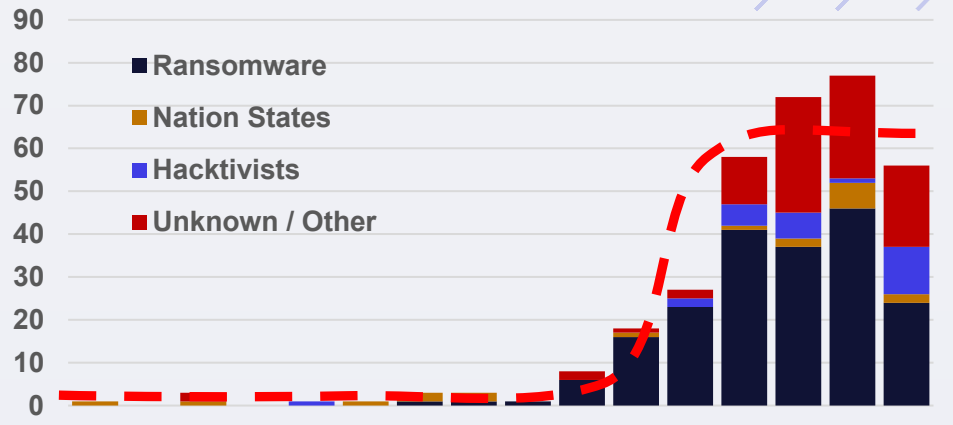
Stryker – erased 85-200,000 devices via breached cloud – factories down for days

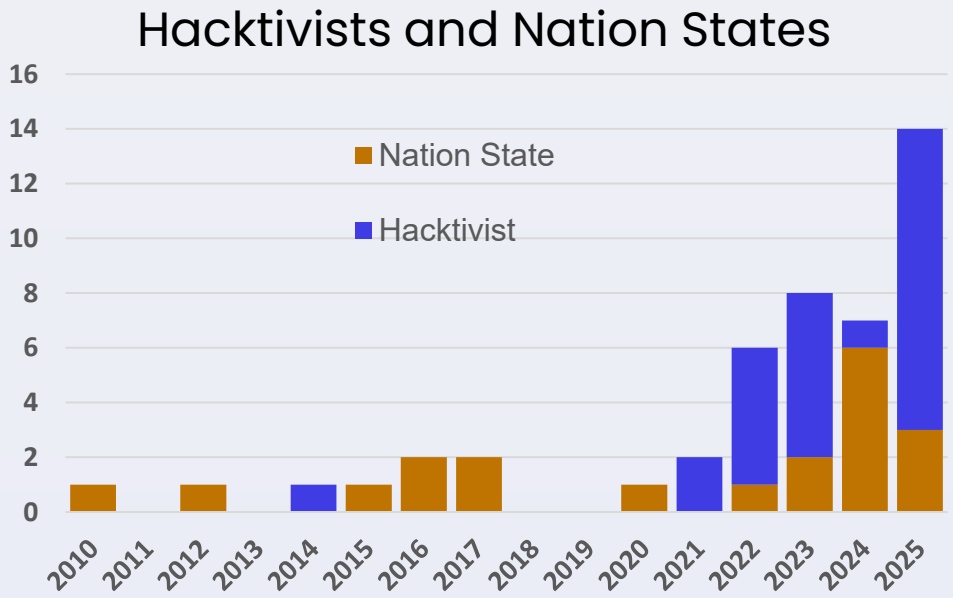
Destroyed chillers – Iranian attack destroyed multiple CO_2 chillers

100 water sites – Internet-exposed PLCs

Polish power plant – Internet-exposed HMI

Nation states are cheap – have more powerful tools in their pockets – include a large margin for error when we are credible nation-state targets





Copyright © 2026 Waterfall Security Solutions Ltd.

waterfall

The Era of Zero Days Is Upon Us

AIs find zero days fast - Anthropic's Claude Mythos & other AIs have proven very effective at finding zero days in executable files

AIs chain zero days – taking many apparently low-severity vulnerabilities and combining them into powerful exploits

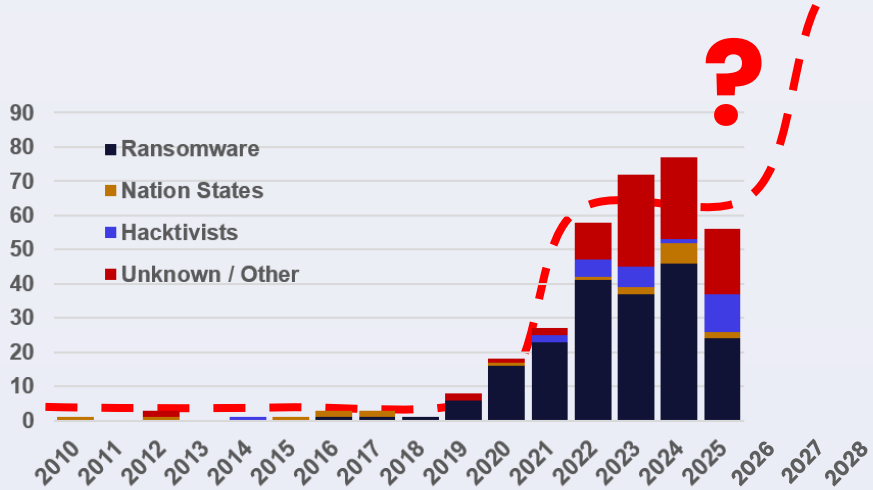
AIs speed up attacks – automating entire attack sequences and increasing attacker productivity 5-10x – soon more

Not new kinds of attacks – but simpler, faster, more sophisticated attacks

We are entering the era of AI-augmented attacks

Ransomware was the 2020 step function

AI will be the next step



Copyright © 2026 Waterfall Security Solutions Ltd.

Today's Frontier AI Limitations

Need expert supervision – user must be able to reverse engineer firmware, find zero days, build exploits and carry out attacks, but high-end ransomware groups and nation states have those experts

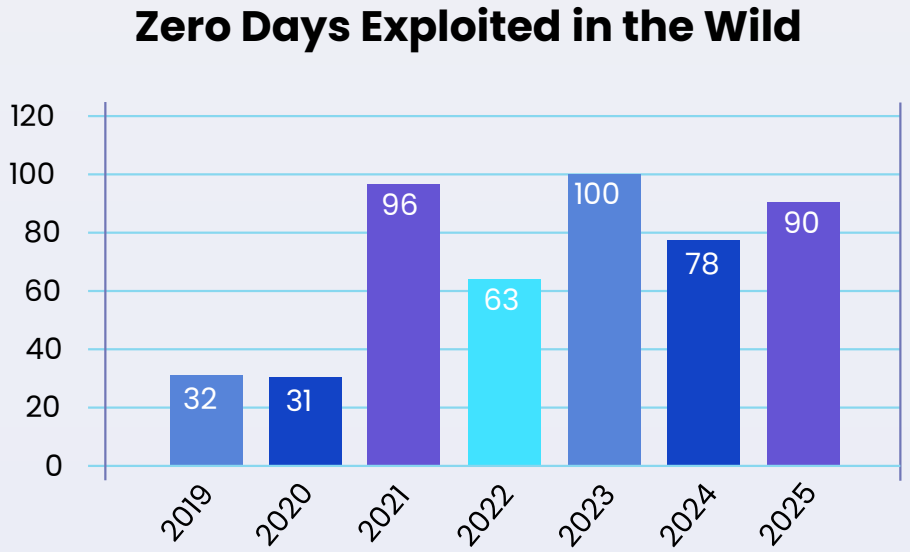
AI vendors – are building guardrails into their products, but will vendors enforce guardrails for their own intelligence agencies?

Knowledge distillation attacks – steal advanced models – without guardrails

In the wild – AIs are not creating new types of attacks – experts are using AIs to reduce cost and increase speed of existing attack types

Different experts – find different zero days

Expect all this to change over time



Copyright © 2026 Waterfall Security Solutions Ltd.

Defender's Advantage Is Disappearing

Common wisdom – defenders have the advantage because every target is different and learning how to bring about physical consequences takes time

Bricking takes no on-site learning – prepare exploits for common PLCs

Completely autonomous attacks – are credible threats in the future, and faster than detect / respond can react

Completely autonomous defenses – may never be possible for safety-critical or critical infrastructure systems

Engineering-grade defenses – are becoming increasingly urgent – hardware-enforced, deterministic, analog and digital non-cyber

Society expects – infrastructure that works acceptably safely and reliably

All software has zero days



Copyright © 2026 Waterfall Security Solutions Ltd.

Near-Term AI Threat – Imagine…

Ransomware criminals use AI – to find vulnerabilities our site's standard firewall types, break in and take over all our firewalls

They take over an XP machine – and demand a ransom – we pay, but they spook because they see authorities coming for them

The deadline expires – without them sending us their deactivation tool.

Our compromised *firewalls* launch the attack – not our XP machines.

The attack "bricks" 80% of our PLCs – erases the firmware so thoroughly the devices cannot be restored

How long will we be down?



Copyright © 2026 Waterfall Security Solutions Ltd.

waterfall

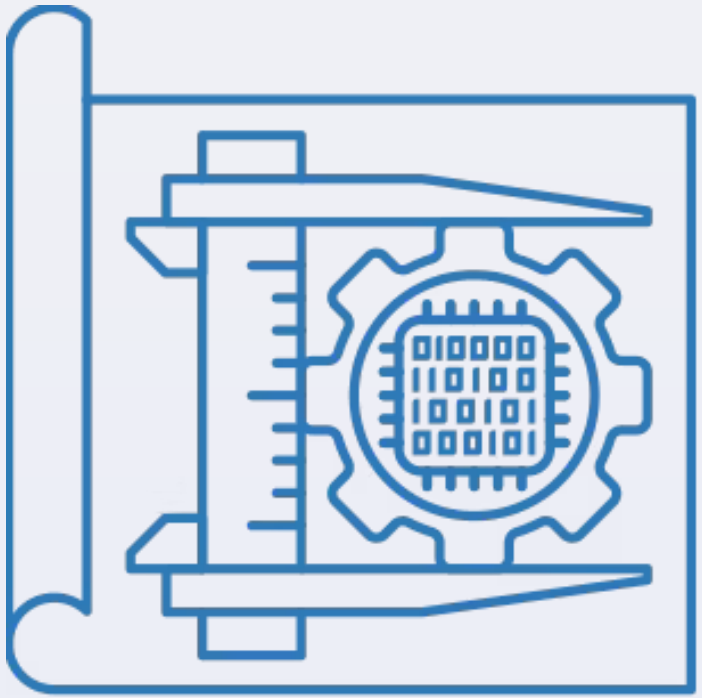
Cyber-Informed Engineering

Resilience focus – until CIE “resilience” was more of a headline than a methodology

If your life depends on a boiler not exploding – in a cyber attack – would you prefer protection by a spring-loaded relief valve? Or longer PLC password? Where is the valve in ISO 27001? NIST CSF? IEC 62443?

Manual operations – operate through compromise manually – can we still? Have we practiced? (Ukraine)

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



https://inl.gov/national-security/cie/

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

Copyright © 2026 Waterfall Security Solutions Ltd.

waterfall

IT-Grade vs. Engineering Grade

Some OT networks are more stable than IT – and we can apply anomaly detection more aggressively

But … imagine a bridge – with harmonic frequencies and active hydraulic dampers

Design engineer "hopes" – we can detect attacks on damper controls before the bridge collapses

"Hopes" that if we detect the attack – we can scramble an incident response team fast enough to prevent disaster

"Hope" is not what we expect of design engineers – we expect engineering-grade protection, not IT-grade "hope"



Copyright © 2026 Waterfall Security Solutions Ltd.

waterfall

#1 – Consequence Drives Security

Consequence – most OT networks have truly unacceptable worst credible consequences of compromise

Consequences define required security – the more consequential the system, the more thoroughly we must protect it



Despite most IT / OT differences reducing the strength of OT security programs, we really need our most consequential OT installations to be materially more secure than we secure our IT systems

Copyright © 2026 Waterfall Security Solutions Ltd.

waterfall

#2 Engineered Controls – CIE Controls Database

Design features – that remove avenues of attack, or limit the consequences of such attacks

62,000 records – across 1800 industries

Seven classes:

- **Physical logic –** relief valves, relays, governors
- **Redundant designs –** both magnetic & thermal elements in breakers
- **Physical properties –** fusible plugs, bimetallic switches
- **Digital engineering –** adaptive / anomaly-tolerant controllers
- **Passive dynamics –** flywheels, water hammer arresters
- **Irreversible actions –** ratchets, clutches, data diodes
- **Fail-safe defaults –** fail open / fail closed / spring-return valves

Deterministic control over movement of attack information are the most universally-applicable mitigation – useful in practically all industries

Copyright © 2026 Waterfall Security Solutions Ltd.

#3 Secure Information Arch – Network Engineering

CIE is more than analog – digital protections assure critical infrastructure reliability, even with software SIS

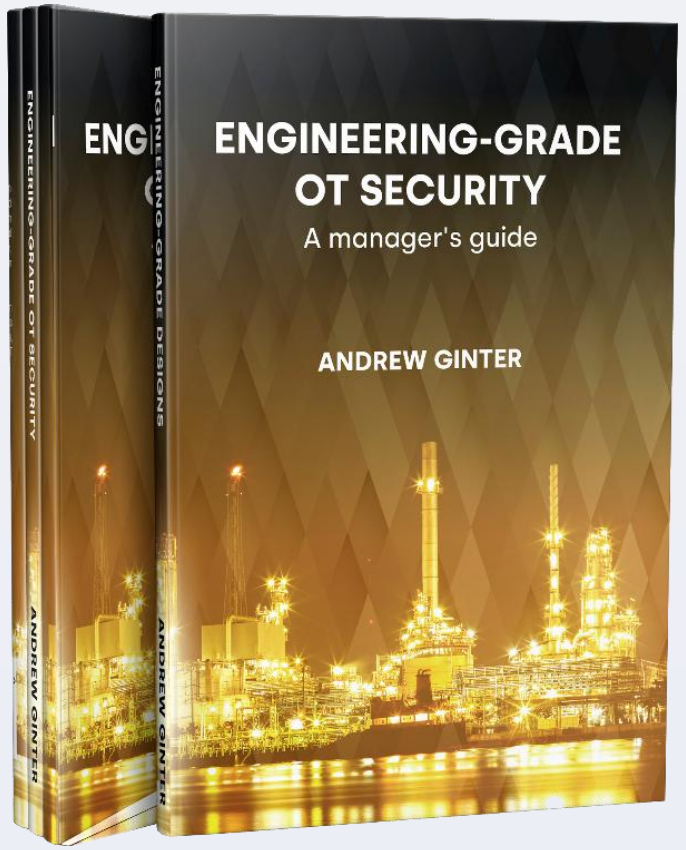
Consequence boundaries – connections between networks - very different worst-case consequences

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

Network engineering – deterministic prevention of attacks pivoting through consequence boundaries

Information is the threat, not the asset – only way a system can change from normal to compromised state is if attack information enters the system

We cannot restore human lives nor damaged equipment from backups



Free copies at

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

Copyright © 2026 Waterfall Security Solutions Ltd.

waterfall

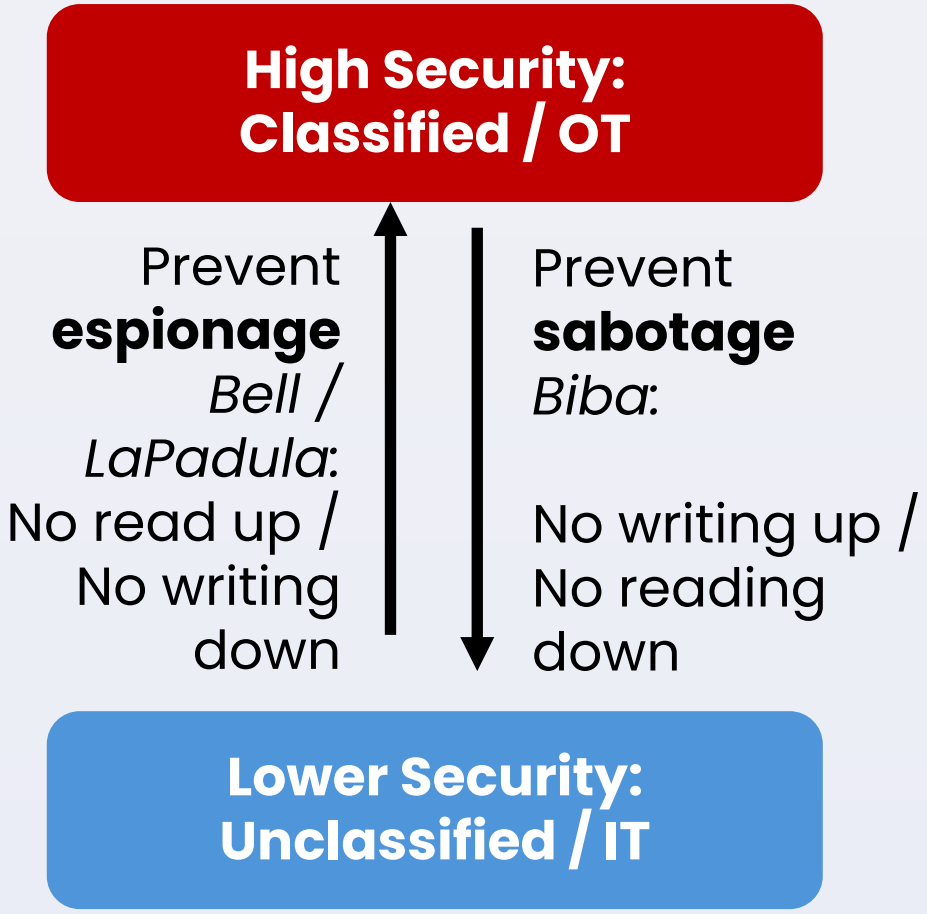
Espionage vs. Sabotage

IT – information is the asset – (Bell / LaPadula) prevent information theft / leakage – stop lower-security enclaves from pulling information & high-security from pushing / leaking information to lower security

OT – operations is the asset – (Biba) information is the threat – prevent low-security enclaves pushing information to high-security, and prevent high-security pulling from lower

The only way OT changes from normal to compromised is if attack info enters OT

Controlling movement of attack information is fundamental, not a compensating measure



Copyright © 2026 Waterfall Security Solutions Ltd.

2026 – Secure Connectivity Principles

Eight Authorities – controlling the movement of attack information is fundamental, not a compensating measure

Eight Principles – balance risk / limit exposure / centralize & standardize / standard & secure protocols / harden OT boundary / limit impact / log connectivity / isolation plan

Hardware-enforced unidirectionality – to prevent OT compromise

Hardware filtering – for inbound data / attack flows

Isolation – in emergency, isolate OT & keep running

When preventing sabotage, controlling connectivity is FUNDAMENTAL, not a "compensating measure"



Copyright © 2026 Waterfall Security Solutions Ltd.

waterfall

Unidirectional Gateways



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

- **Gateway hardware –** is physically able to send information in only one direction.
- **Software –** copies OT servers to IT networks. IT users use the replicas normally
- **No attack –** no matter how sophisticated can propagate back to OT network through the gateway.

Copyright © 2026 Waterfall Security Solutions Ltd.

Engineering-Grade / Deterministic 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

Multiple industrial form factors –
DIN rail, split (2u) and 1u form factors



Not physically possible to send information from the receiving network back to the sending network through the device

Copyright © 2026 Waterfall Security Solutions Ltd.

waterfall

2026 – CI Fortify – Connected vs. Isolated

Assume extended disruption – survivable OT operations for up to 3 months

Isolate – separate OT networks or segments from external networks (eg: IT) and the Internet (consequence boundary)

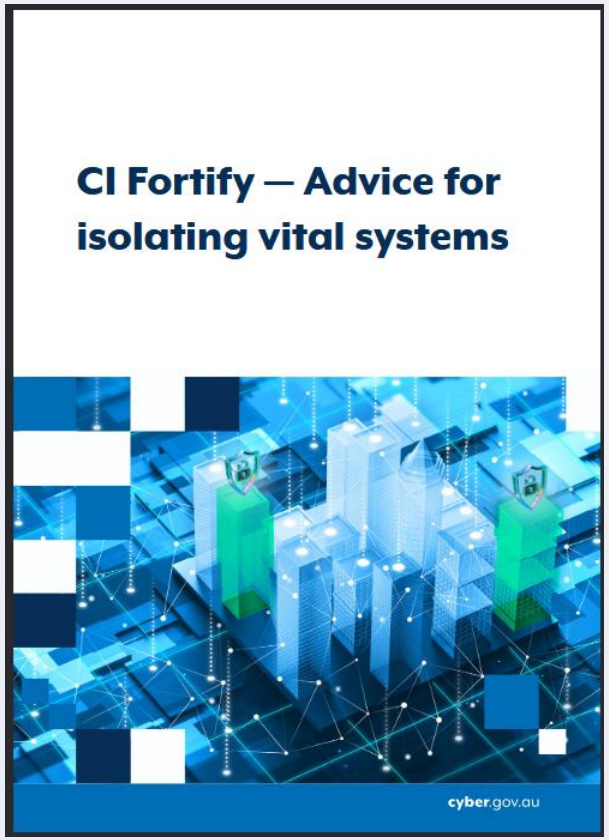
Benefits – preserve essential ops, reduce exposure to new attacks, impede C2, reduce ability to exploit zero-days

Implement physical separation & isolation – is the most effective form of protection – use firewalls if forced to

Dependencies – analyze and address dependencies on IT

Isolation is expensive – unidirectional gateway tech provides benefits of isolation, and of connectivity

Endorsed – by CISA, FBI, ASD, CCCS, NZ NCSC, UK NCSC



Cloud & AI inputs can enhance efficiency, but should not be essential to CI reliability

Copyright © 2026 Waterfall Security Solutions Ltd.

waterfall

Islanding Is Expensive

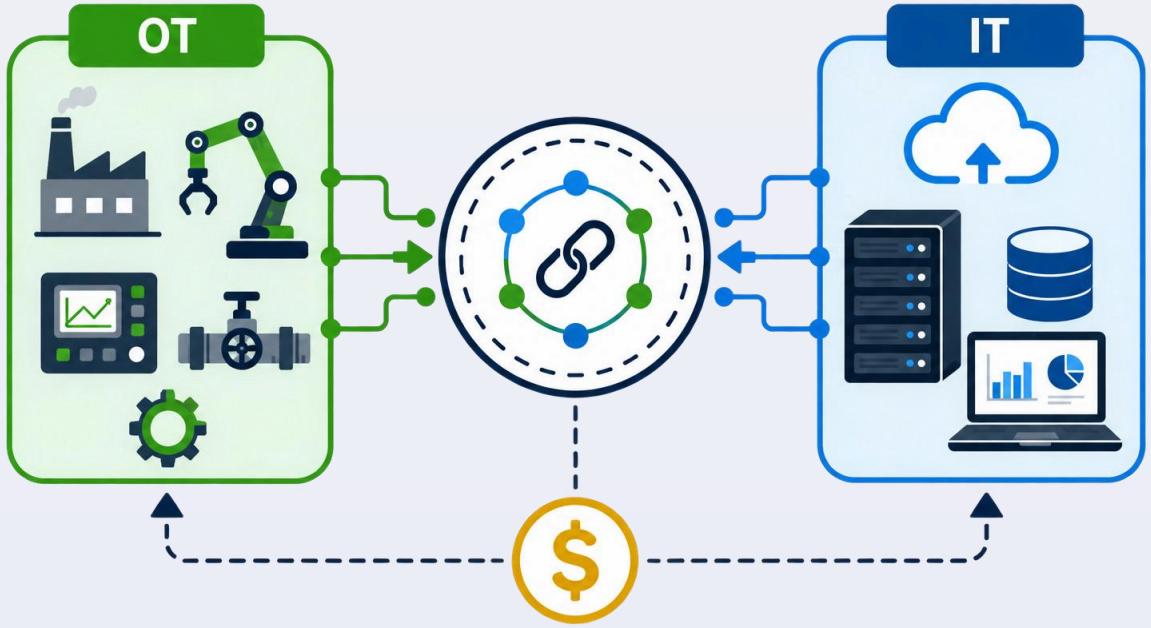
IT/OT integration – relies on IT "business automation" systems having reliable access to recent, or real-time OT data

Real business benefits – arise from IT/OT integration – we don't move the data for our health:

- Predictive maintenance
- Work crew scheduling
- Spare parts ordering
- Raw materials re-ordering
- Finished goods inventory & routing
- Power usage optimization
- Equipment effectiveness

And many more

Isolation impairs or erases those business benefits



Copyright © 2026 Waterfall Security Solutions Ltd.

waterfall

Tools of the Trade

Air gaps – power off firewall, or unplug network cable. *NB: clear labelling is critical + practice*

A/B switch – on power, or network cables – reduces "unplugging / re-plugging" errors & omissions

Unidirectional gateway / data diode – recognized by CI Fortify, TSA & others as legitimate islanding – prevents attack pivoting

Manual ops – power off all OT equipment and operate physical process manually

Continuous unidirectional islanding provides all the benefits of islanding while preserving the benefits of IT/OT integration & IT access to OT data



Copyright © 2026 Waterfall Security Solutions Ltd.

waterfall

Dependencies Are Tricky

Dependencies – impair islanded operation

Direct dependencies – eg: cloud SCADA - continuous remote operations

Indirect dependencies – eg: shipping / container tracking system or pipeline custody transfer system, battery backups

Shared trust – eg: IT Active Directory becomes single point of compromise for all of IT and OT

External dependencies – eg: GPS timing? Satellite comms? Cloud services?

For each dependency, either figure out how to do without it in an emergency, or figure out how to isolate / rapid-recover that dependency in an emergency



Copyright © 2026 Waterfall Security Solutions Ltd.

waterfall

Network Engineering - Interdependencies

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



Copyright © 2026 Waterfall Security Solutions Ltd.

Network Engineering - Interdependencies

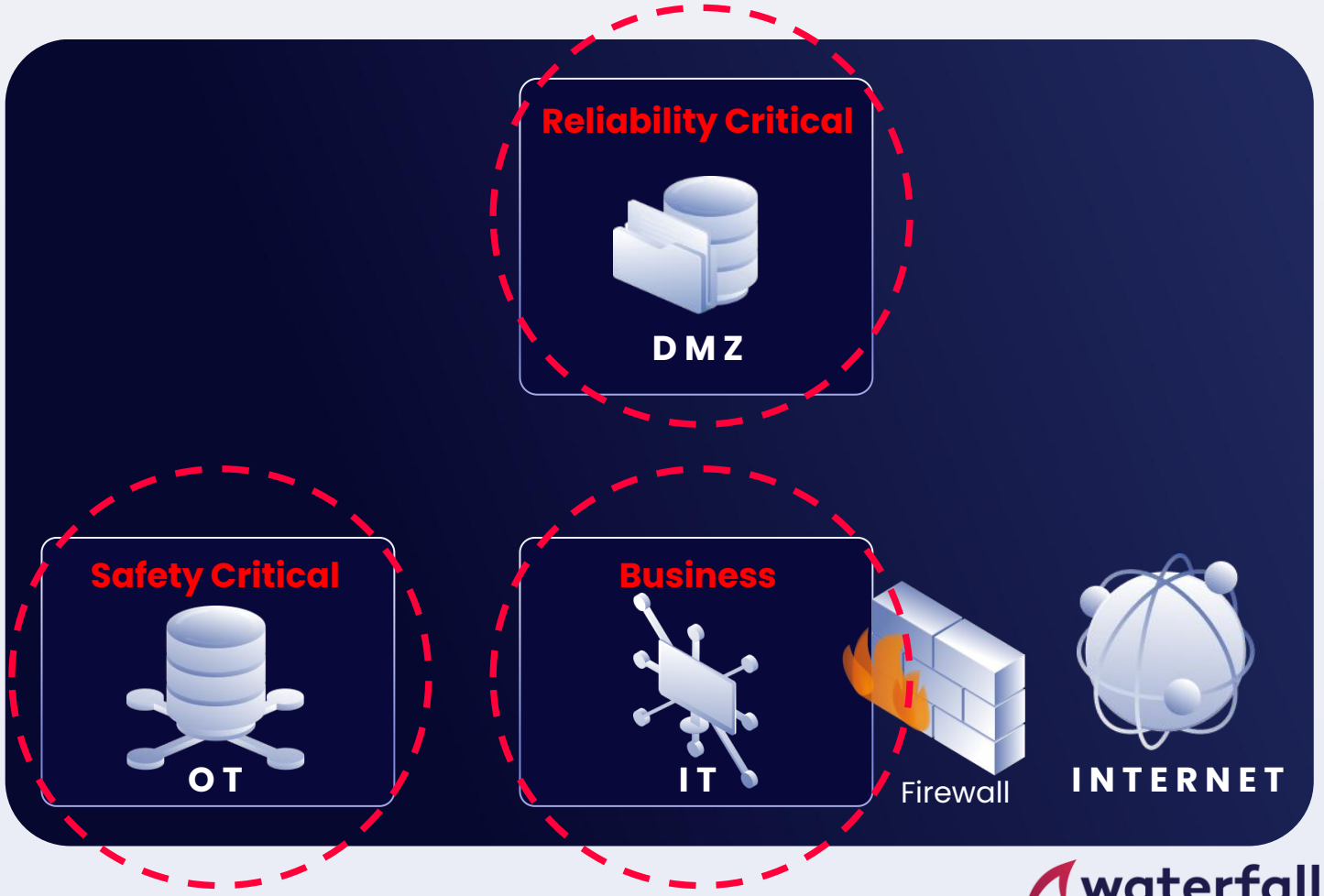
Common Design: Can be hard to draw the line – so secure all ops / OT networks as safety-critical

Often three network criticalities:

Safety-critical: worst case safety consequences are unacceptable

Reliability-critical: unacceptable reliability consequences – eg: smart meter payment systems

Business: worst case consequences are acceptable



Copyright © 2026 Waterfall Security Solutions Ltd.

Network Engineering - Interdependencies

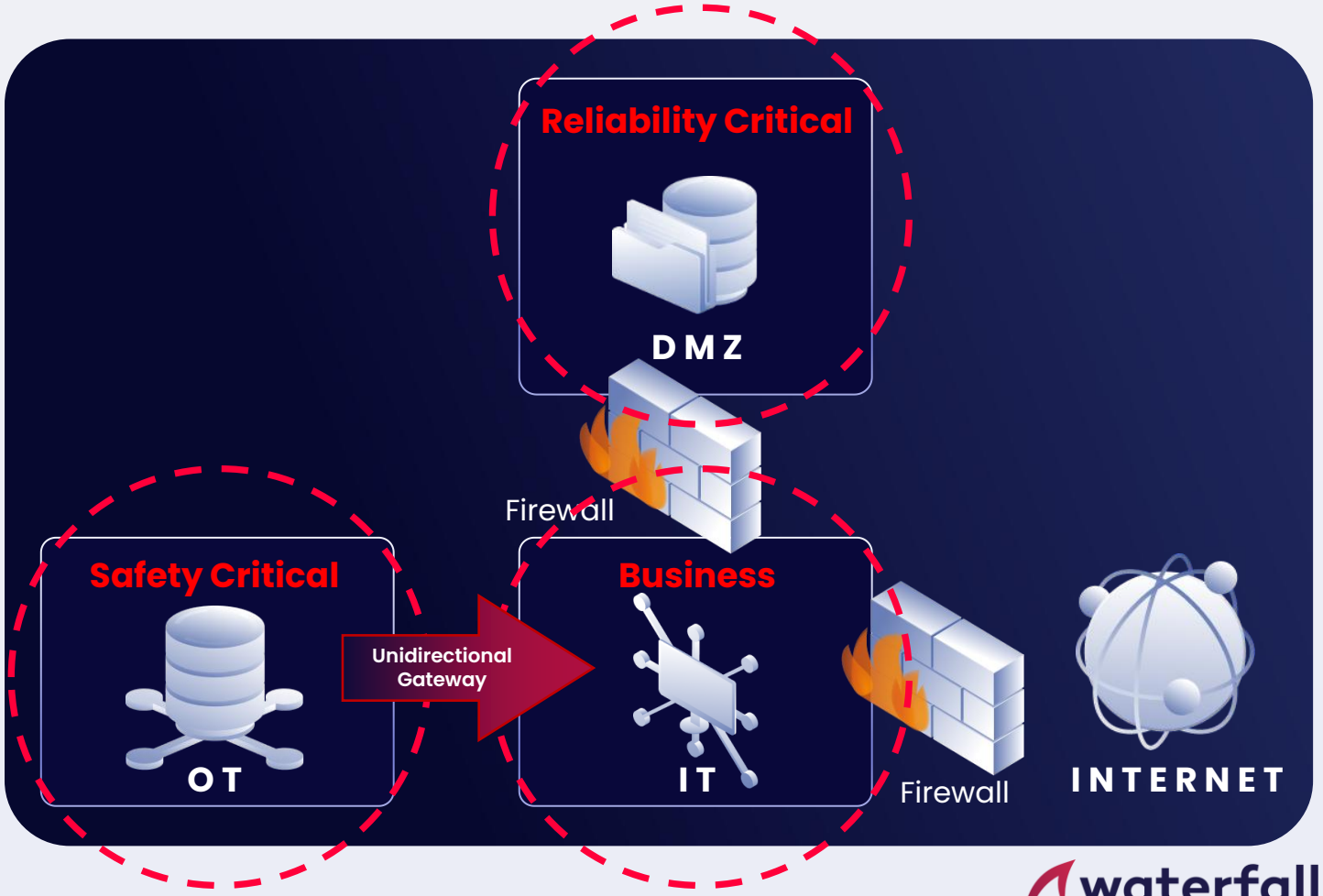
Manage differently:

Safety-critical: prevent compromise (unidirectional) & prevent consequences (safety engineering)

Reliability & business-critical: prevent compromise of OT networks & prioritize recovery – resilience

Business: buy insurance

Eliminate or strictly manage dependencies at consequence boundaries



Copyright © 2026 Waterfall Security Solutions Ltd.

Remote Access Considerations

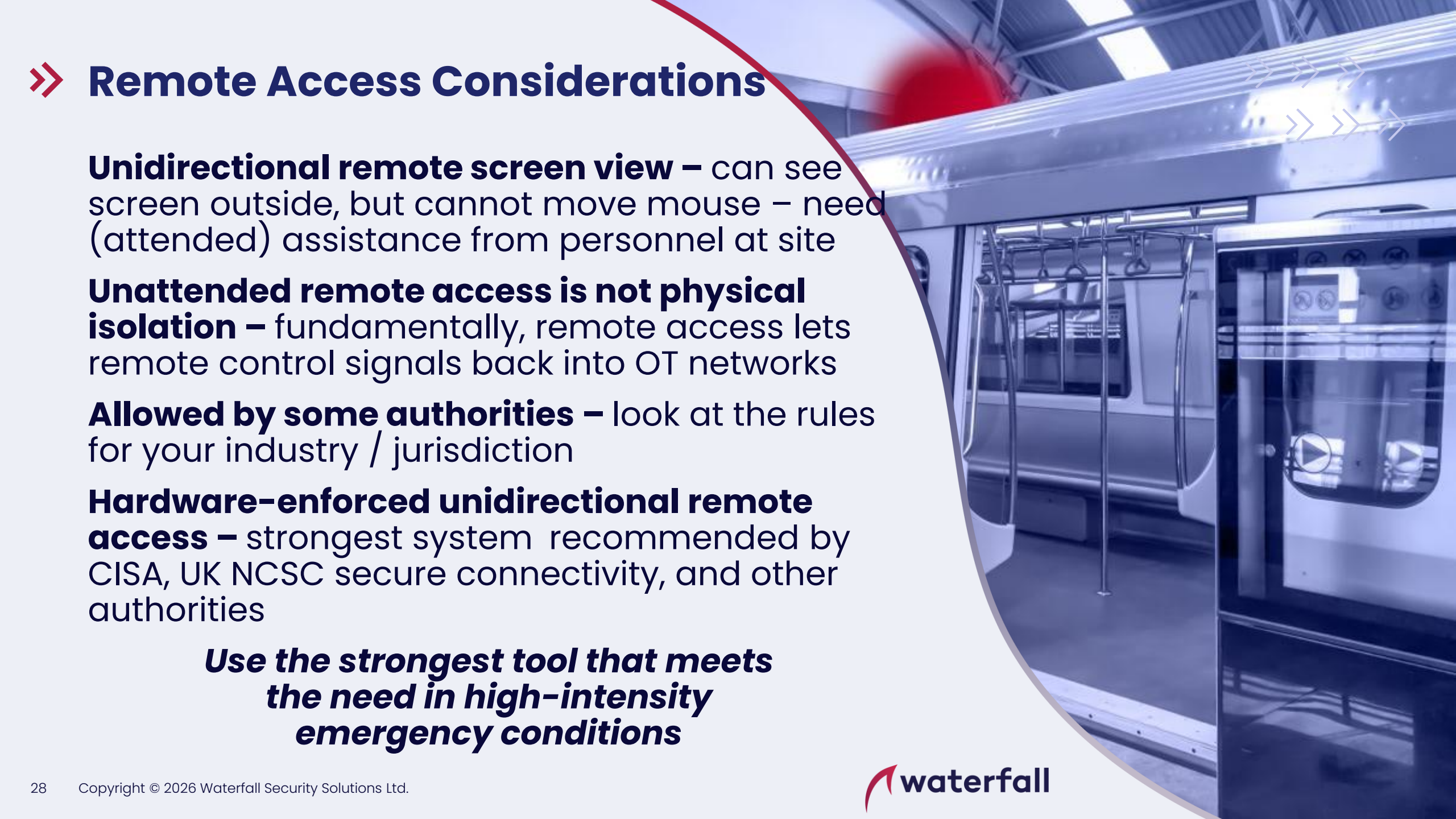
Unidirectional remote screen view – can see screen outside, but cannot move mouse – need (attended) assistance from personnel at site

Unattended remote access is not physical isolation – fundamentally, remote access lets remote control signals back into OT networks

Allowed by some authorities – look at the rules for your industry / jurisdiction

Hardware-enforced unidirectional remote access – strongest system recommended by CISA, UK NCSC secure connectivity, and other authorities

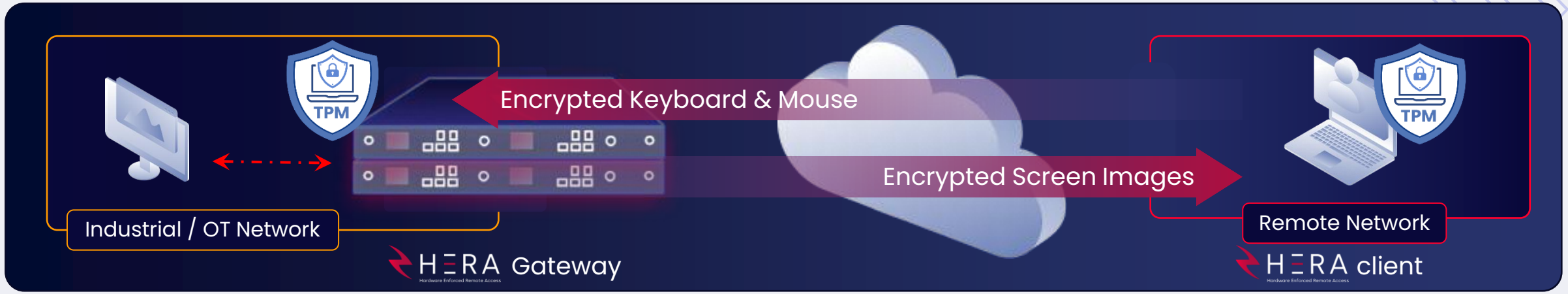
Use the strongest tool that meets the need in high-intensity emergency conditions



Copyright © 2026 Waterfall Security Solutions Ltd.

waterfall

Hardware-Enforced Unidirectional Remote Access



HERA Gateway

Hard protocol break

eliminates TCP pivoting path

Remote access without an exploit pivoting path into OT

Hardware-Filtered Security

Defeats IP-based pivoting

in hardware,
not only in software

No Man-in-the-Middle
No session hijacking

Hardware-Bound Identity

Leverages TPM hardware

to secure communications and prevent credential & session hijacking

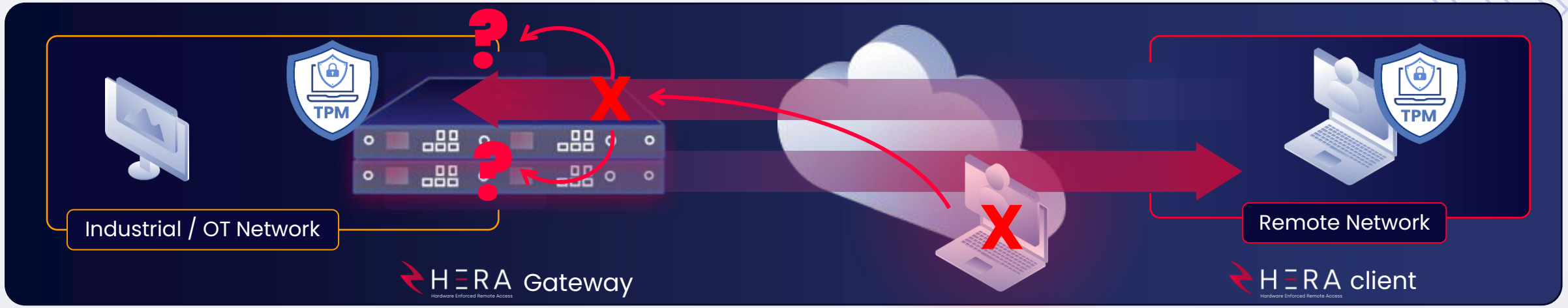
Dramatically reduced attack surface

Copyright © 2026 Waterfall Security Solutions Ltd.

HERA Hardware Enforced Remote Access

waterfall

Hardware Filtering



Exploit a Vulnerability

- **Find a zero-day**
  Or a recent patch / update with a public proof of concept exploit – that has not yet been installed
- **Exploit the vulnerability**
  Take over Gateway's IT-side CPUs
- **Try to pivot**
  Send SYN floods or buffer overflows attacks into OT network
- **Hardware saves us**
  Lower gateway is "pointed" outward – no attacks get in, and upper gateway throws out everything except encrypted keystrokes and mouse

Cannot fake keystrokes – key information is in laptop TPM & OT-side TPM

Enormously harder to pivot through HERA into OT network

Copyright © 2026 Waterfall Security Solutions Ltd.

OT Security – State of the Art

Zero Trust – and detect / respond / recover make OT at best as strong as IT – may be enough for less-consequential systems, not for big-iron

CIE is the right way to look at OT security – address high-consequence first

Control information flows – to prevent sabotage

CI Fortify – latest example of controlling information flows

CIE's digital mitigations are powerful tools for controlling the flow of attack information

In an era of AI-generated zero-days and sophisticated attacks at machine speed, the time has come to rethink our defenses

andrew.ginter@waterfall-security.com



Copyright © 2026 Waterfall Security Solutions Ltd.

waterfall