INDUSTRIAL CYBERSECURITY

ASK DIFFERENT QUESTIONS

2024
Industrial Cybersecurity / Operational Technology Priorities

Safe physical operations

Reliable operations

- Continuous
- No equipment damage

Efficient production

Cybersecurity is essential to safety and to reliability
ICS – Human Machine Interface (HMI)
Purdue Model / IEC 62443

Level 5
Internet

Level 4
Enterprise: ERP, CRM

Level 3
Plant DMZ: AD, Historians

Level 2
Control: DCS & SCADA

WAN

Level 1
PLCs
RTUs

Level 0
Physical Process

Level 1 (Pumping Station)

Relays
Safety

Physical Process
Rapid Rise of OT Cyber Attacks with Physical Impacts

**Exponential Growth** – increasing 10x every 2.5 years – on track to hit 4500 attacks impacting 15,000 sites in 2027

**Threat Environment** – changed forever – does anyone believe we will ever go back to a year like 2018 with one (1) attack with physical consequences?

**Nation State Ransomware** – some ransomware group are nation-state backed, others are rich enough to buy nation-state-grade attack tools

*What we see nation states do to each other today, we should expect ransomware to do to all of us with money, within a year or three*

Essential IT / OT Difference

**Consequences** – we cannot restore human lives and damaged equipment “from backups”

**Engineering Change Control** – every change is a risk – control change to control risk

**Difficulty Patching** – and using passwords, and AV, and upgrading to new hardware and software versions – usually symptoms of change control risk management

*Critical network* – one with unacceptable (usually physical) consequences
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 pwd? Where is the valve in the NIST CSF? In IEC 62443?

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
Network Engineering – Criticality Boundaries

Worst-case consequences define criticality – if every CPU issues exactly the wrong instruction to the physical process...

Criticality boundaries – Must prevent propagation of pervasive nation-state-grade remote-control / malware attacks

Network engineering – EPRI IIoT, analog signaling, 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
EPRI – Industrial Internet of Things Methodology

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 an attack through the IIoT into the critical control network
Unidirectional Security Gateways
Absolute protection with complete network visibility

Absolute protection – The gateway hardware sends information in only one direction.

Network visibility – The software makes real-time copies of servers & devices from the industrial network to the enterprise network, avoiding all bidirectional connectivity with original industrial data and eliminating threat.

No attack – no matter how sophisticated, can propagate back to the industrial 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*
Cyber Risk – Design-Basis Threat

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
Where: c(o) = capability needed to exploit opportunity

Cyber Design-Basis Threat – describe the most capable adversary / attack we are required to defeat reliably
Insurance Expectations Changing

**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*
About Waterfall Security

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

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

Key Sectors:
- Power
- Oil & Gas
- Rails
- Facilities
- Water
- Manufacturing
- Government
Engineering-Grade OT Security

Public Safety – and national security threats demand engineering-grade solutions

Anticipate Evolving Threat Load – with a large margin for safety, to avoid constant change

Criticality Boundaries – demand network engineering protections

Design-Basis Threat – critical networks must reliably defeat pervasive nation-state-grade threats, but not necessarily nation-state insider threats

Insurance provides little comfort when bridges collapse or trains collide

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