

India Smart Utility Week 2022

ORGANISED BY INDIA SMART GRID FORUM

Managing OT Cyber Risk – More than Cybersecurity

Speaker : *Andrew Ginter, VP Industrial Security*
Waterfall Security Solutions
The OT Security Company

2021 Attacks

- **150%** – Increase in attacks with physical consequences in utilities, process manufacturing & discrete manufacturing
- **95% Ransomware** – 5% Hacktivist
- **Modern ransomware** – Very sophisticated – using tools and techniques that 5 years ago were used only by nation-states
- **Kaseya** – Ransomware delivered from a compromised cloud to 1500 victims simultaneously

Ransomware groups use nation-state attack techniques.

They target everyone with money.



2022 Predictions

- **30% Victims** – By 2025, 30% of critical infrastructure organizations will experience a security breach that will result in the halting of operations (Gartner¹)
- **Cloud Ransomware** – by 2024 ransomware groups will cause production outages at hundreds of victims at a time via cloud-delivered ransomware (Waterfall)
- **Safety** – by 2025 cyber attackers will have weaponized operational technology environments to successfully harm or kill humans (Gartner²)

Unplanned outages are not the worst consequences of compromise
Public safety, casualties at the site, damaged transformers and turbines,
and environmental disasters

None of these can be “restored from backups”

- [1] <https://www.gartner.com/en/newsroom/press-releases/2021-12-2-gartner-predicts-30--of-critical-infrastructure-organi>
- [2] <https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we>

Managing Risk - Options

- **Mitigate** – Cybersecurity reduces cyber risk, especially for High-Frequency, Low-Impact (HFLI) events. Expanding to prevent LFHI events is very expensive
- **Transfer** – Usually by buying insurance. But insurance protects only the business, not society. And not all insurance claims are paid out – look for cyber exclusions
- **Eliminate** – Change business so that risk no longer exists – eg: change chemical plant to produce same output with non-toxic inputs
- **Accept** – Do nothing – if risk is realized, suffer the consequences

Too many businesses mitigate HFLI risks and transfer what they can

They accept the remainder – LFHI risks

The problem – today's nation-state tools will be used by ransomware in 5 years

Powerful OT Tools

- **Security PHA Review** – Spring loaded valves prevent explosions, centrifugal switches prevent over-speed. *Eliminates* safety risks
- **Secure Operations Technology** – All cyber-sabotage attacks are information. A complete inventory of incoming information flows is a complete inventory of attack vectors. Control each physically, not just with cybersecurity software
- **Manual Ops** – When automation is impaired, turn it off and keep going

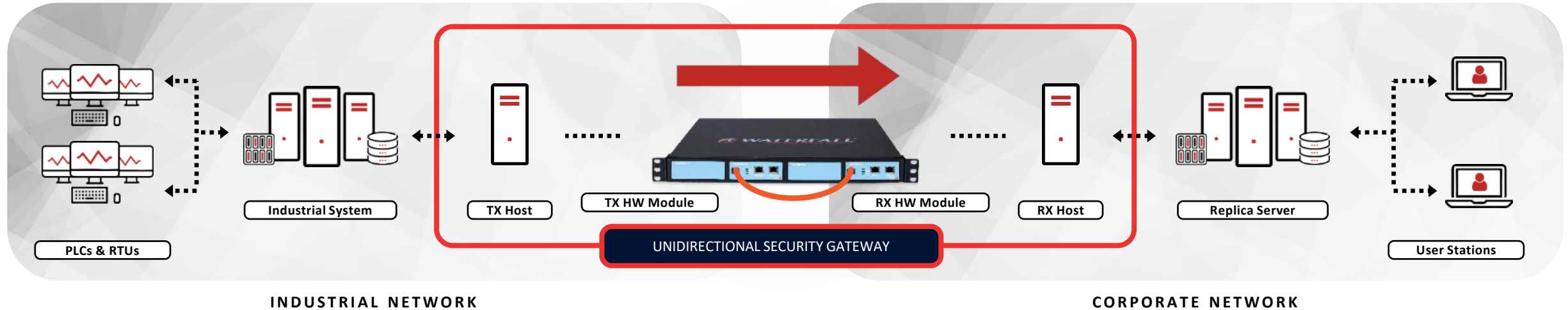
Cybersecurity protects the information

These powerful OT risk management tools get limited mention in cybersecurity guidance

<https://waterfall-security.com/sec-ot>



Unidirectional Gateways



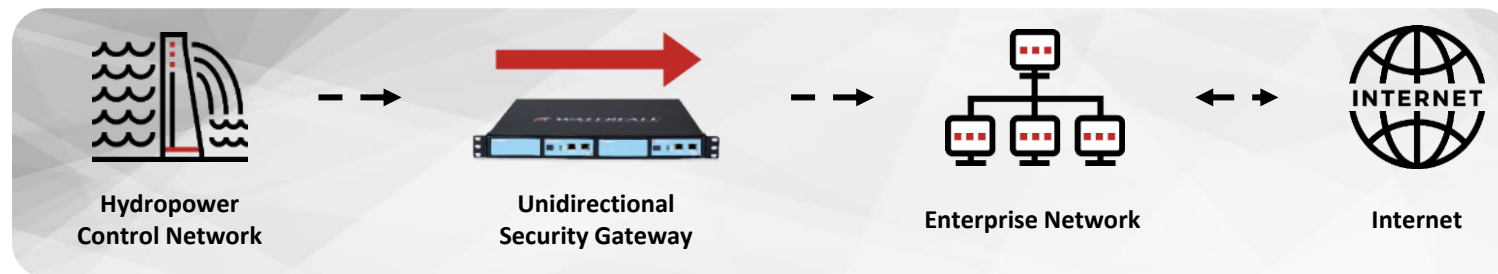
- **Unidirectional Security Gateway** – Combination of hardware and software
- **Hardware** – Sends information in only one direction – physical protection
- **Software** – Software synchronizes servers & emulates devices
- **External users** - Use copies of servers & devices normally

No attack information can propagate back into industrial operations


Use Case: Power Generation

- **Historian** – Replica is used by business users & automation for dashboards, visibility, optimization & analysis
- **Syslog, SNMP, OT mirror ports** – Replicas used by Enterprise SOC for security monitoring
- **iHistorian & Remote Screen View** – Replicas used by turbine vendor to diagnose problems & provide remote support

Corporate users & applications can use replicas without risk to physical operations



About Waterfall



Founded in 2007

**Sales & Ops in
NA, EU, APAC, ME**

**Global
Installed Base**

Israel HQ




**All types of critical
infrastructure**

**Global tech & sales
partners**

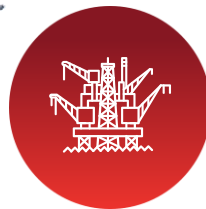
**Multiple registered
US patents**



FACILITIES



POWER



OIL & GAS



WATER



RAILS



MANUFACTURING

Risk Is More Than Security

- **OT Cyber Risks Increasing** – OT consequences are increasing rapidly and attack sophistication is tracking nation-state capabilities
- **Cybersecurity** – Does a good job of addressing HFLI threats – very expensive to get even limited coverage of LFHI risks
- **Safety** – Physical safeties (in addition to cyber) make safety unhackable
- **Manual Operations** – keep the lights on
- **Unidirectional Gateways** – prevent even nation-state grade remote-control attacks

***We can accept safety incidents and damaged equipment
or we can eliminate those risks***

<https://waterfall-security.com/sec-ot>

andrew.ginter@waterfall-security.com

