AVEVA PI WORLD EU - 2022

Safe Access to PI Data: Anytime, Anywhere - Waterfall

Andrew Ginter, VP Industrial Security, Waterfall Security Solutions

AVEVA

Critical Infrastructure Connectivity

- Increased automation = more software = more targets
- Increased connectivity = more opportunities to attack
- EU-wide power market: communications only increase: TSO-TSO, TSO-DSO & TSO-Generation
- Water systems comms: predictive maintenance, supply chain / parts / scheduling crews
- Smart cities: "everything" is connected

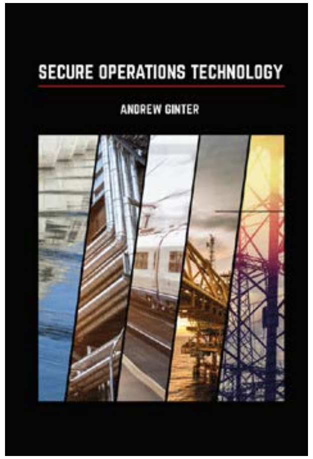
Cheapest connectivity
is cellular Internet
= least secure / most exposed

FIRST 3 LAWS OF INDUSTRIAL SECURITY

#1 Nothing is secure

#2 All software can be hacked

#3 Every connection can propagate attacks



Source: Secure Operations Technology
https://waterfall-security.com/sec-ot

Attacks With Physical Consequences Are Increasing

- 150% increase year over year
- Almost all targeted ransomware, none USB
- Typical outage affects many sites, for days or longer
- Cloud connections guarantee a pivoting path from the Internet – using already-compromised machines to attack other machines
- Consequences – can't restore public confidence "from backups"

Ransomware tools & tactics
trail nation-states
by less than a handful of years

ICS STRIVE

WATERFALL
Stronger Than Firewalls

OT Security Incidents

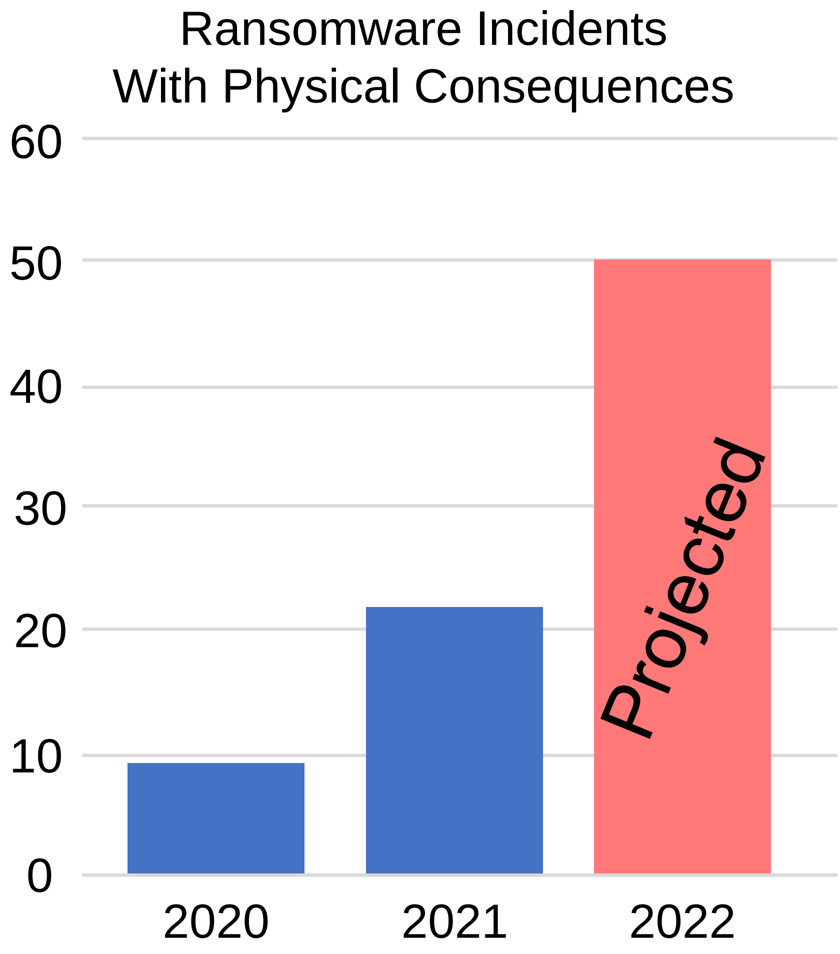
2021 Trends and Analyses

Andrew Ginter
VP Industrial Security
Waterfall Security Solutions

Greg Hale
Editor & Founder
Industrial Safety & Security Source

Copyright © 2022 Waterfall Security Solutions Ltd

Source:ICSStrive.com

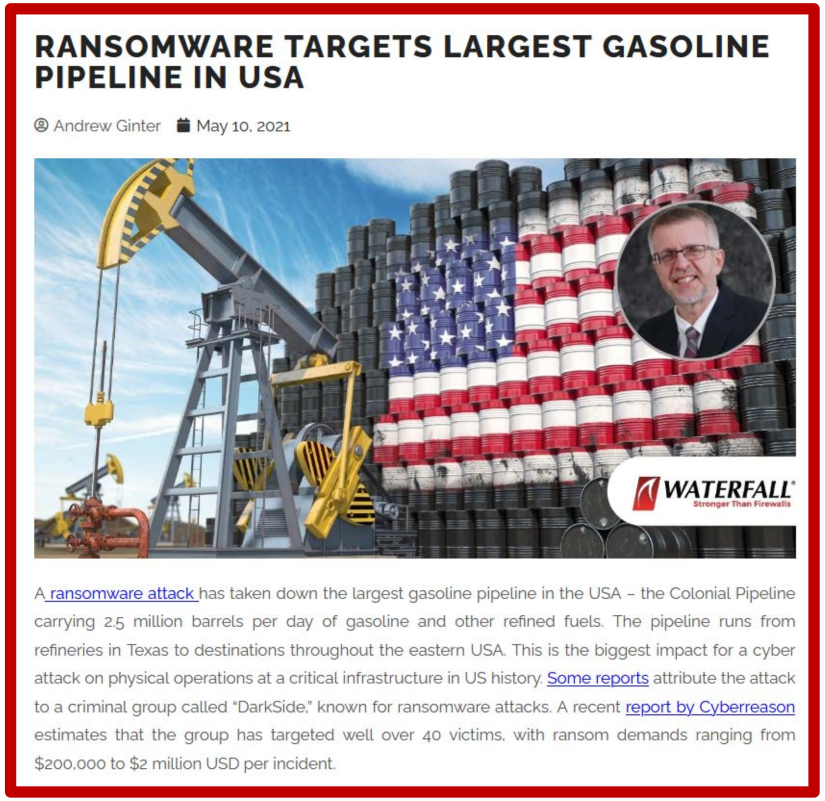


Ransomware Incidents
With Physical Consequences

How Ransomware Affects Industrial Targets

- Some ransomware targets OT systems directly – eg: EKANS / SNAKE
- Shut down operations when IT is infected in “an abundance of caution” – does not trust the strength of own OT security program
- Sometimes IT network hosts systems that are essential to minute-by-minute operations
- Ransomware shuts down supplier – Kojima / Toyota

TSA Directive 30 days after Colonial:
Keep OT systems running at full capacity,
even if IT systems are compromised



RANSOMWARE TARGETS LARGEST GASOLINE PIPELINE IN USA

Andrew Ginter May 10, 2021

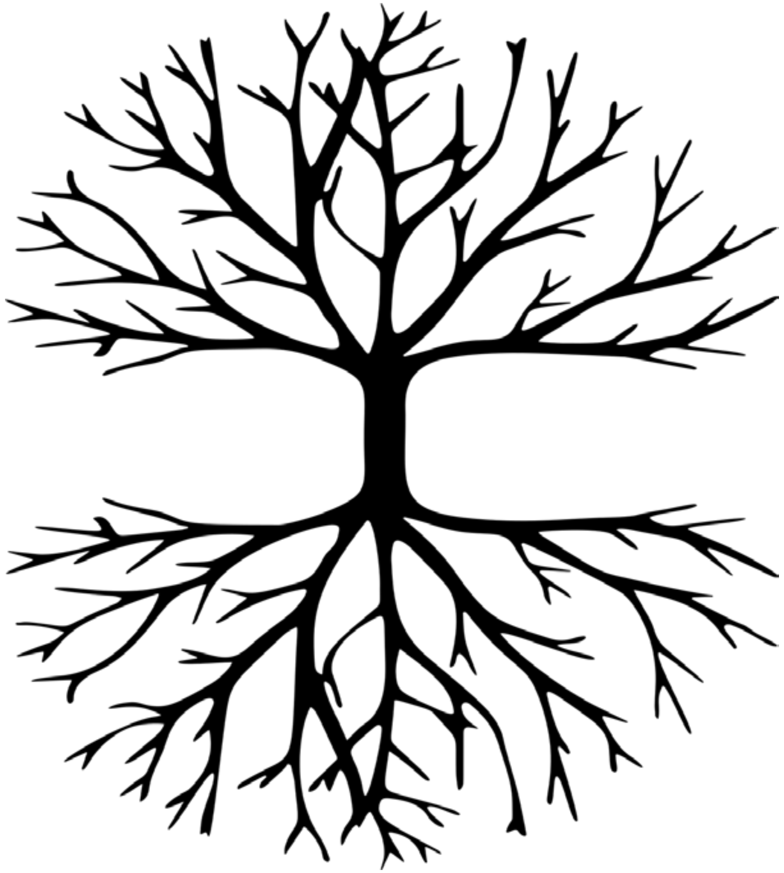
A ransomware attack has taken down the largest gasoline pipeline in the USA – the Colonial Pipeline carrying 2.5 million barrels per day of gasoline and other refined fuels. The pipeline runs from refineries in Texas to destinations throughout the eastern USA. This is the biggest impact for a cyber attack on physical operations at a critical infrastructure in US history. Some reports attribute the attack to a criminal group called “DarkSide,” known for ransomware attacks. A recent report by Cyberreason estimates that the group has targeted well over 40 victims, with ransom demands ranging from $200,000 to $2 million USD per incident.

Emerging: Supply Chain Threats

1. Is supplier under the influence of hostile governments or other entities?
2. Does supplier have a cybersecurity program?
3. What software & hardware components are embedded in a supplier's products?

- *Should* be asking – I trust supplier, but:
  - Should I trust their website? (Kaseya scenario)
  - Should I trust their security updates? (SolarWinds scenario)

Security updates are getting harder & instrumenting test beds for security is important



Source: Image by Gordon Johnson from Pixabay

AVEVA

Strategic Implications

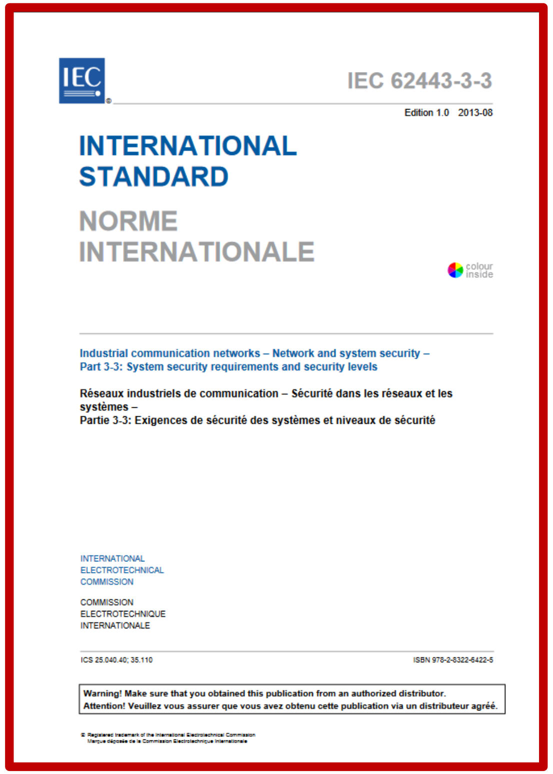
- Dispatchable generation more attractive target – solar & wind are intrinsically intermittent
- EU-wide market increases TSO-TSO, TSO-DSO and TSO-generation communications
- Water systems are strategic targets, especially small ones
- “Connected cities” – entirely new risks not considered in conventional assessments

CI risk landscape changing rapidly
Eg: insurance does not address
biggest risks

IEC 62443 – Aging As Adoption Increases

- IEC 62443 is the most widely-used and widely-cited industrial security standard in the world
- 62443-3-3 (2013) is security levels & controls
- Security is hard – do what you can – defense in depth
- Four security levels being revised because today ransomware uses tools and techniques of 2013's nation states
- Reasonable to expect all IEC 62443 SL4 recommendations to migrate to SL3

Anyone using any standard needs to be aware that adversary capabilities continue to increase, while the standard is static



IEC 62443-3-3

Edition 1.0 2013-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Industrial communication networks – Network and system security –
Part 3-3: System security requirements and security levels

Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes –
Partie 3-3: Exigences de sécurité des systèmes et niveaux de sécurité

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 25.040.40; 35.110

ISBN 978-2-8322-6422-5

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

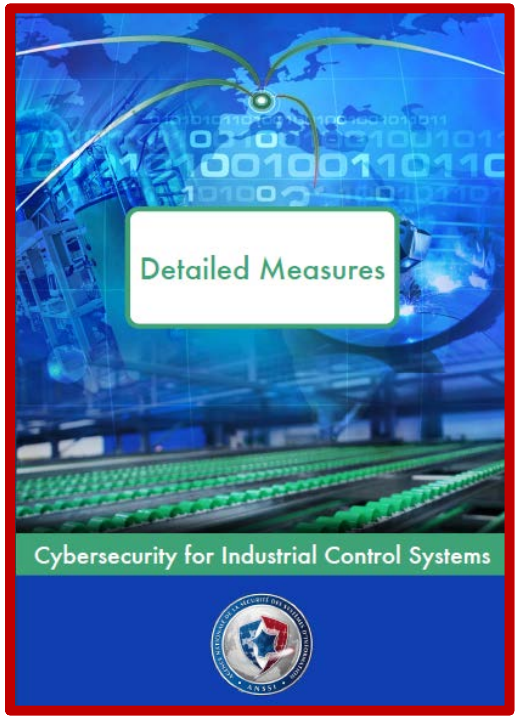
International Electrotechnical Commission

AVEVA

French ANSSI (2016) – More Modern

- Three security levels defined largely in terms of worst case consequences - safety vs. reliability vs. business critical
- All incoming information is a threat
- Class 3 – strict removable media controls, only outbound unidirectional communications permitted
- Class 2 – strong media controls, only outbound unidirectional comms recommended, remote access strongly discouraged
- Class 1 – business-critical – use conventional IT-SEC

Information-flow-based controls will stand the test of time – all cyber-sabotage attacks are information, and will always be information



Detailed Measures

Cybersecurity for Industrial Control Systems

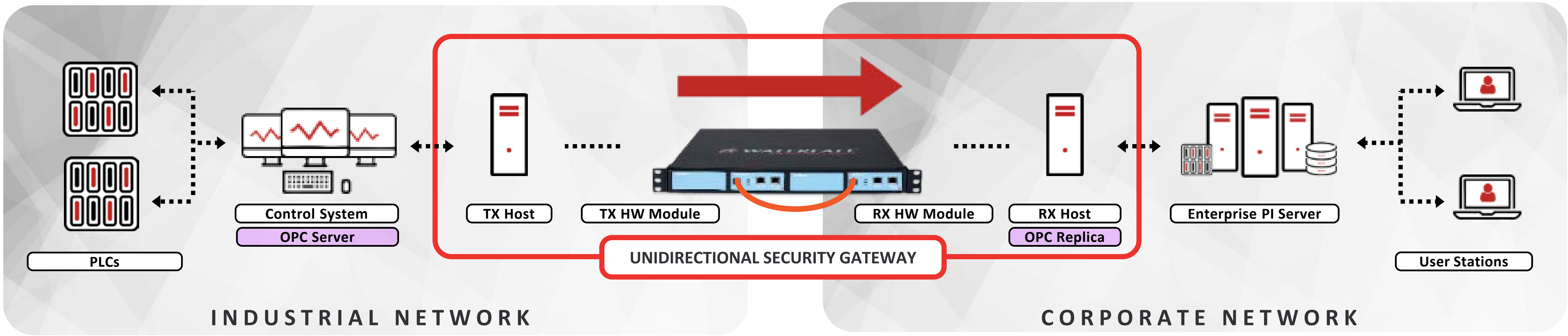
Most Recent Advice – Physical Protection

- SPR – Security PHA Review – use physical safety systems in addition ot cyber systems – unhackable
- CCE – Consequence-Driven, Cyber-Informed Engineering from Idaho National Labs – mostly industrial risk assessment, but strong recommendation for physical, unhackable protections
- SEC-OT – Secure Operations Technology – physical protection against incoming information flows, esp: unidirectional gateways

COUNTERING CYBER SABOTAGE
Introducing Consequence-Driven, Cyber-Informed Engineering (CCE)
Bochman and Sarah Freeman
CRC Press
Security PHA Review for Consequence-Based Cybersecurity
SECURE OPERATIONS TECHNOLOGY
ANDREW GINTER

With ransomware trailing nation-states
by less than 5 years
we need security designs
to stand the test of time

Unidirectional Security Gateways – What Are They?

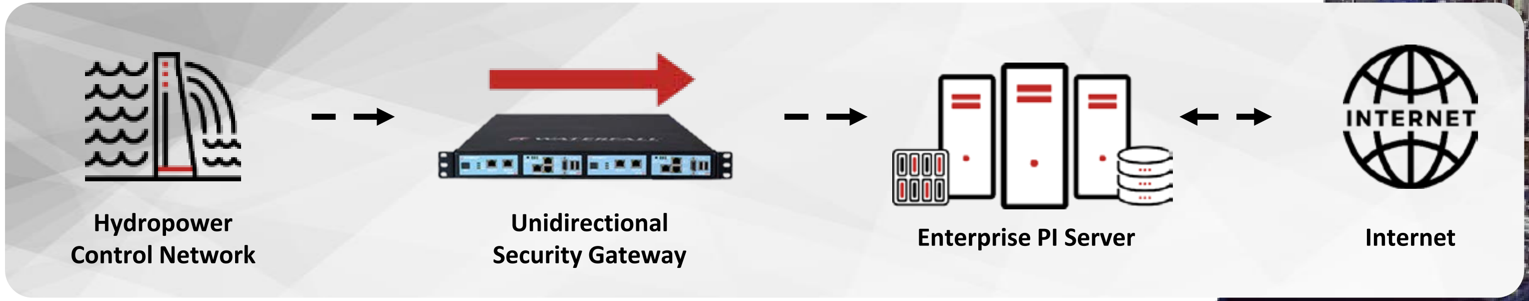


Per NIST 800-82 r2 – unidirectional gateways are a combination of hardware and software

- The hardware sends information in only one direction
- The software makes copies of servers & devices from the industrial network to the enterprise network
- No attack, no matter how sophisticated, can propagate back into the industrial network through the gateway

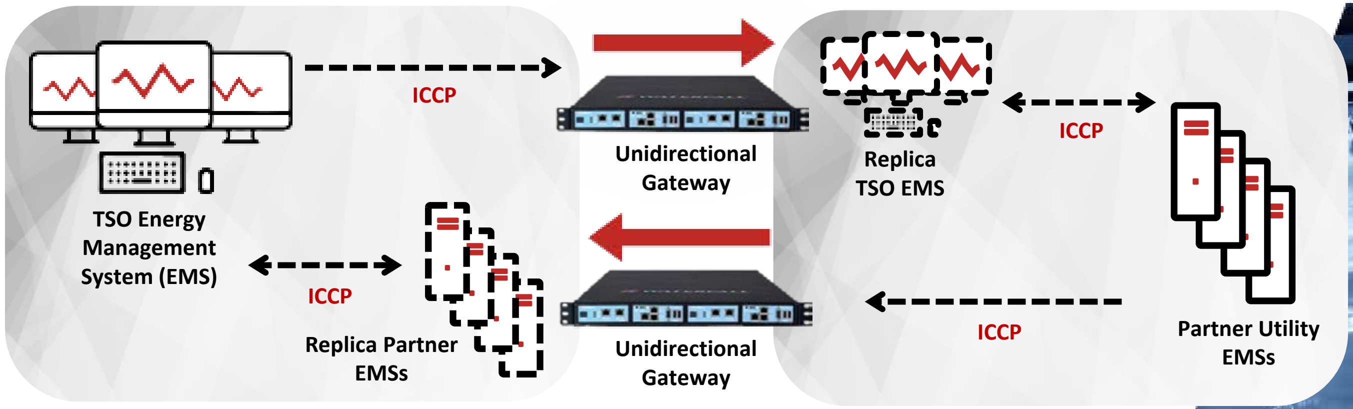
Power Generation

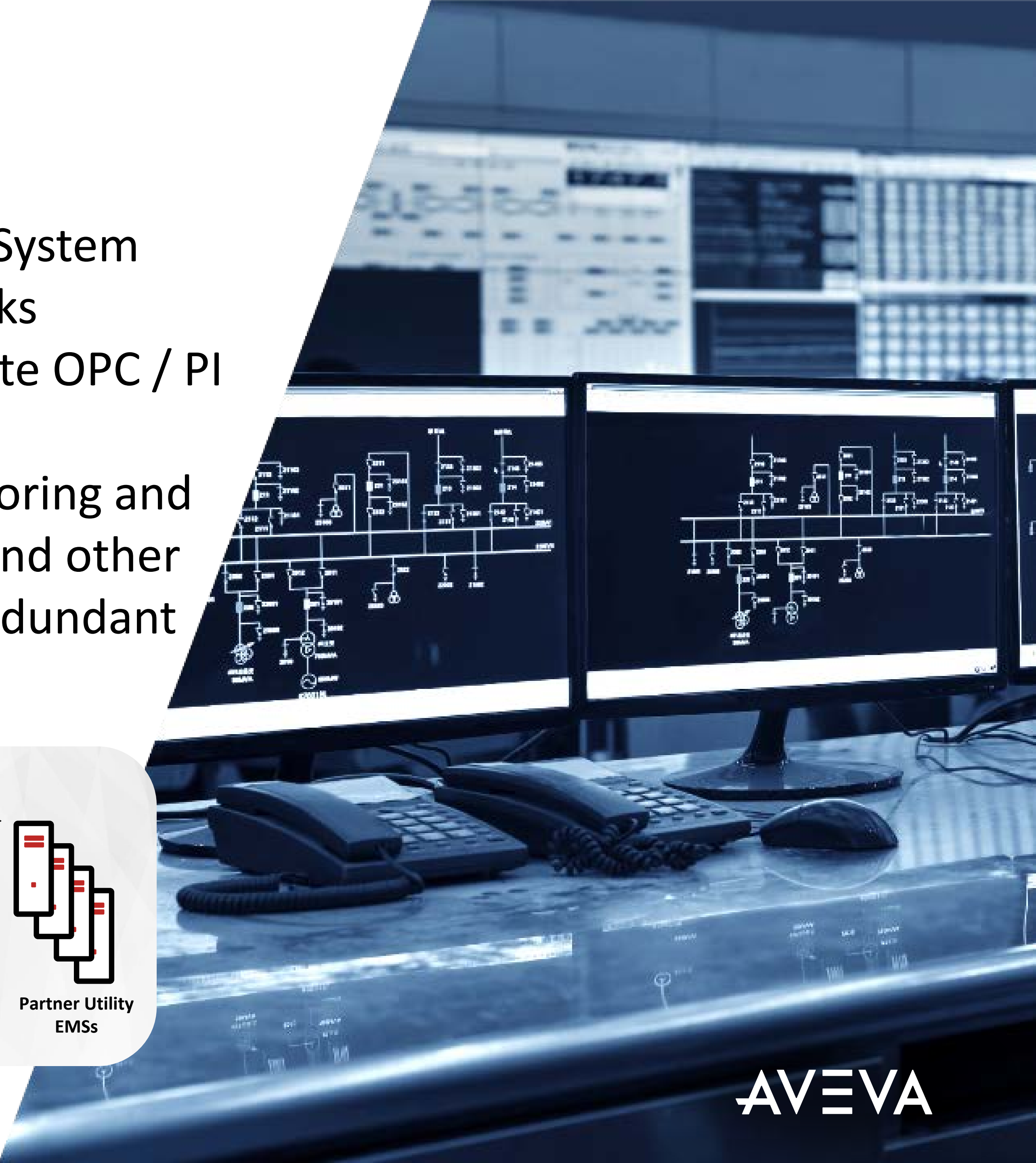
- CHALLENGE: Secure the control system network perimeter from external threats while enabling enterprise visibility & third-party management
- SOLUTION: Unidirectional gateways replicate PI Systems, OPC servers and turbine management systems to enterprise networks
- RESULT: Corporate users go to enterprise PI system for all allowed to be shared with IT



Transmission System Operator

- CHALLENGE: Protect Energy Management System (EMS) control systems from potential attacks
- SOLUTION: Unidirectional gateways replicate OPC / PI Systems & EMS / ICCP servers
- RESULT: Safe, continuous, compliant monitoring and control of partner utility generation, load and other status information, deployed in multiply-redundant **High Availability** configuration.





AVEVA

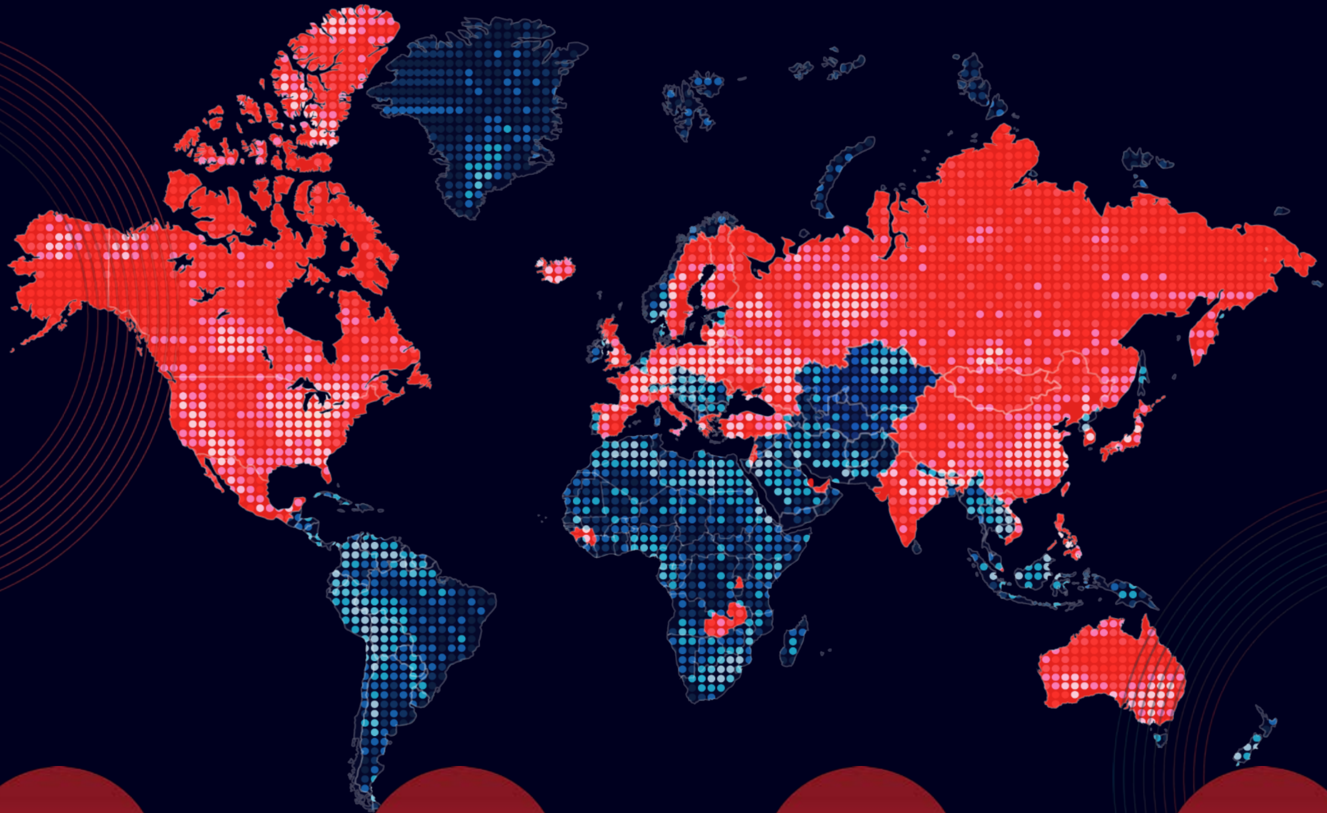
Waterfall – The OT Security Company

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

WATERFALL®
Stronger Than Firewalls

OIL & GAS

Safe Access to PI Data: Anytime, Anywhere

WATERFALL®
Stronger Than Firewalls

Challenge

- Enable business automation that requires access to industrial data, without risk that cyber attacks, no matter how sophisticated, today or in the future, can impair physical operations

Solution

- Deploy – unhackable physical safeties and unhackable digital equipment protection
- Deploy unidirectional gateway technology - unhackable physical protection against incoming information / attack flows

Benefits

- Enjoy the benefits of connected automation - predictive maintenance, hydraulic optimization, operational equipment effectiveness and many others, safely
- No cyber attack, present or future, mundane or sophisticated, can threaten physical, analog, non-cyber digital or unidirectional protections

AVEVA

Andrew Ginter

VP Industrial Security

- Waterfall Security Solutions
- andrew.ginter@waterfall-security.com

Questions?

Please wait for the microphone

- State your name and company

Please remember to…

Complete the survey!

- Navigate to this session in the mobile agenda for the survey

This presentation may include predictions, estimates, intentions, beliefs and other statements that are or may be construed as being forward-looking. While these forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could result in actual outcomes differing materially from those projected in these statements. No statement contained herein constitutes a commitment by AVEVA to perform any particular action or to deliver any particular product or product features. Readers are cautioned not to place undue reliance on these forward-looking statements, which reflect our opinions only as of the date of this presentation.

The Company shall not be obliged to disclose any revision to these forward-looking statements to reflect events or circumstances occurring after the date on which they are made or to reflect the occurrence of future events.

linkedin.com/company/aveva

@avevagroup

ABOUT AVEVA

AVEVA is a global leader in industrial software, driving digital transformation and sustainability. By connecting the power of information and artificial intelligence with human insight, AVEVA enables teams to use their data to unlock new value. We call this Performance Intelligence. AVEVA's comprehensive portfolio enables more than 20,000 industrial enterprises to engineer smarter, operate better and drive sustainable efficiency. AVEVA supports customers through a trusted ecosystem that includes 5,500 partners and 5,700 certified developers around the world. The company is headquartered in Cambridge, UK, with over 6,500 employees and 90 offices in over 40 countries.

Learn more at www.aveva.com

AVEVA