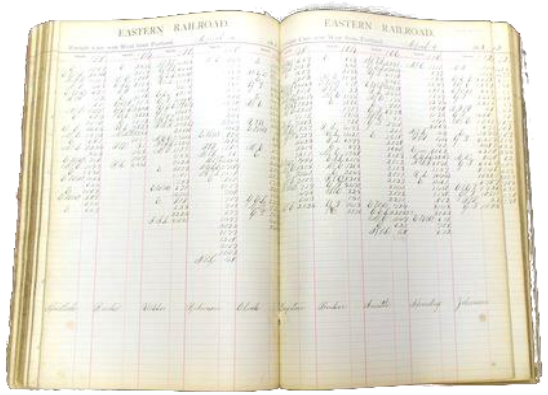
WATERFALL®
Stronger Than Firewalls

Defending ICS Perimeters with Unidirectional Gateways

Stuart Bailey CISSP, GICSP
Director of Industrial Security
Waterfall Security Solutions

IT vs OT – Different Approaches

- IT history: leger books / accounting data / transactions
- Industrial network history
  - Gauges = monitoring = IT data
  - Switches & dials = control signals
- IT experts say "it's all data," but this blinds us to crucial difference between monitoring and control
- Correct control is vital to physical safety and physical reliability

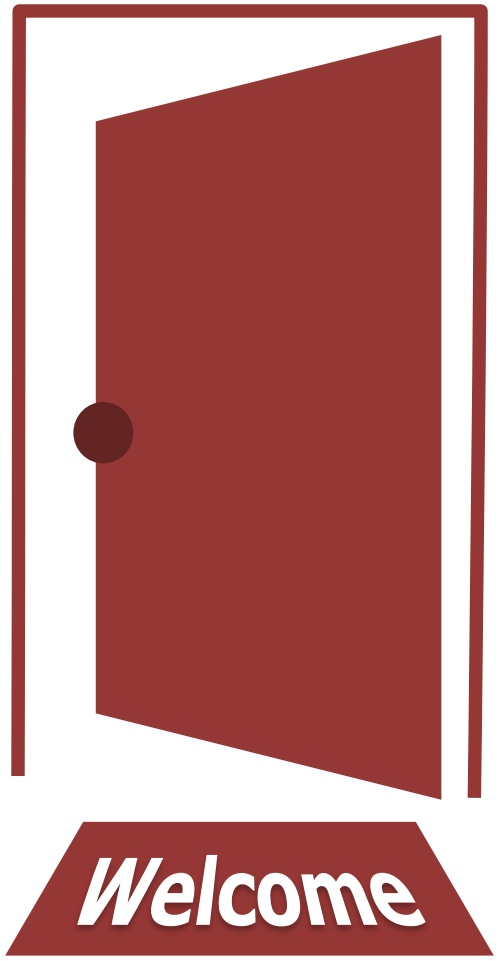


Control is not AIC, CIA or "IT data" – control is really important

Classic IT Defense In Depth

- Firewalls, encryption & security updates are poor fits for reliability-critical, change-controlled networks
- Intrusion detection – how long does it take?
- IT mantra: assume we have been compromised, and find, isolate, erase and restore equipment. Can we restore human lives? A massive spill?

Any security program dependent on the latest indicators of compromise, security updates and attack signatures is fundamentally inadequate to OT needs



IT Approaches Wrong for OT

"An organization cannot expect that an architecture and design originally meant to protect information can address requirements specific to physical systems."

-- Earl Perkins in Gartner's "Demystify Seven Cybersecurity Myths of Operational Technology and the Industrial Internet of Things"

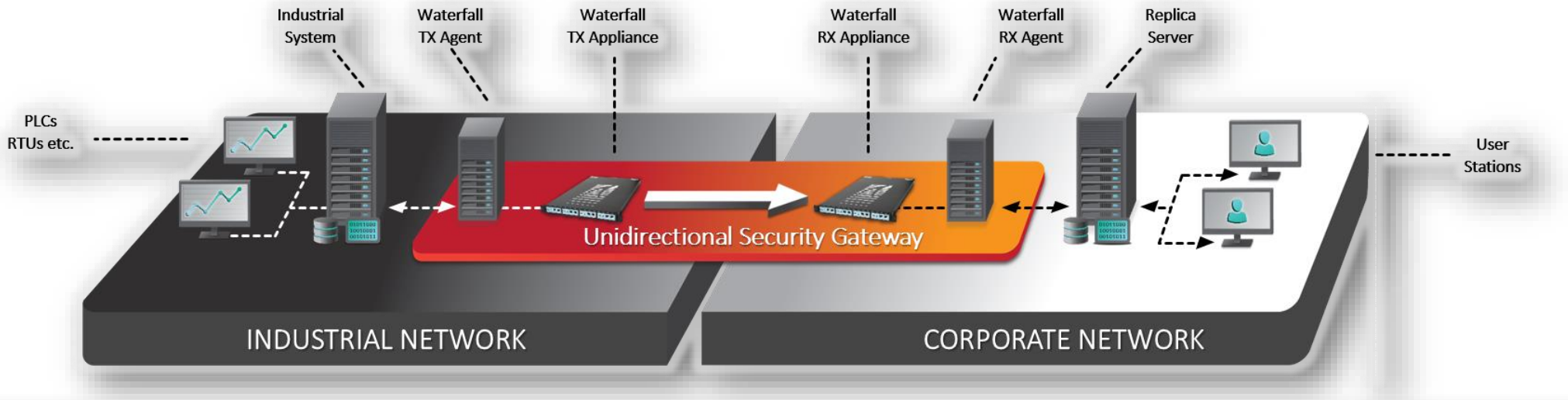
Focus On The Perimeter

- There are only 3 ways to compromise an ICS:
  - Sneakernet – media, devices, supply chain
  - Online – bits
  - Wetware – malicious intent
- To compromise a control system, every attack must cross a perimeter – cyber or physical

Philosophy – be deeply suspicious of control signals from Internet-exposed networks, and of any device that has ever been exposed to the Internet

Unidirectional Security Gateways

- One-way hardware + software that replicates servers & emulates devices
- Unlike firewalls, gateways never forward network traffic
- Cannot be breached with software-based attacks
- Enables secure IT/OT Integration, remote support and cloud Ssrvices



WATERFALL®
Stronger Than Firewalls

Available Connectors

Leading Industrial Applications / Historians

- Instep eDNA, Scientech R*Time, Areva: PowerPlex, PowerTrax
- *GE*: iHistorian, iFIX, OSM, Bently-Nevada System 1 v17+, Proficy HMI
- *OSIsoft*: PI System, PI Asset Framework, PI Historian Backfill
- *Siemens*: SIMATIC, WinCC, WinTS, SINAUT, Spectrum
- *Schneider*: Wonderware & Backfill, ClearSCADA
- *SAP*, *AspenTech* IP21, *Matrikon* Alarm Manager
- *Emerson*: Ovation, EDS, EMS, Rockwell FactoryTalk

Leading IT Monitoring Applications

- Log transfer, SMTP, SNMP, Syslog, CA Unicenter, CA SIM
- *HP* Openview, *IBM* Tivoli, *HP* ArcSight SIEM, *Intel* ESM, *Splunk*
- IBM Websphere MQ, MSMQ, TIBCO, active message queue

File/Folder Mirroring

- Folder mirroring, local folders, remote folders (CIFS)
- FTP, FTPS, SFTP, TFTP, RCP, SMB, MIR, HttpFS, RSync
- Mail server, mailbox replication

Leading Industrial Protocols

- OPC DA, OPC A&E, OPC HDA, OPC UA, IEC 61850
- DNP3, ICCP, Modbus, Modbus plus, GENA, IEC 60870-5-104

Databases

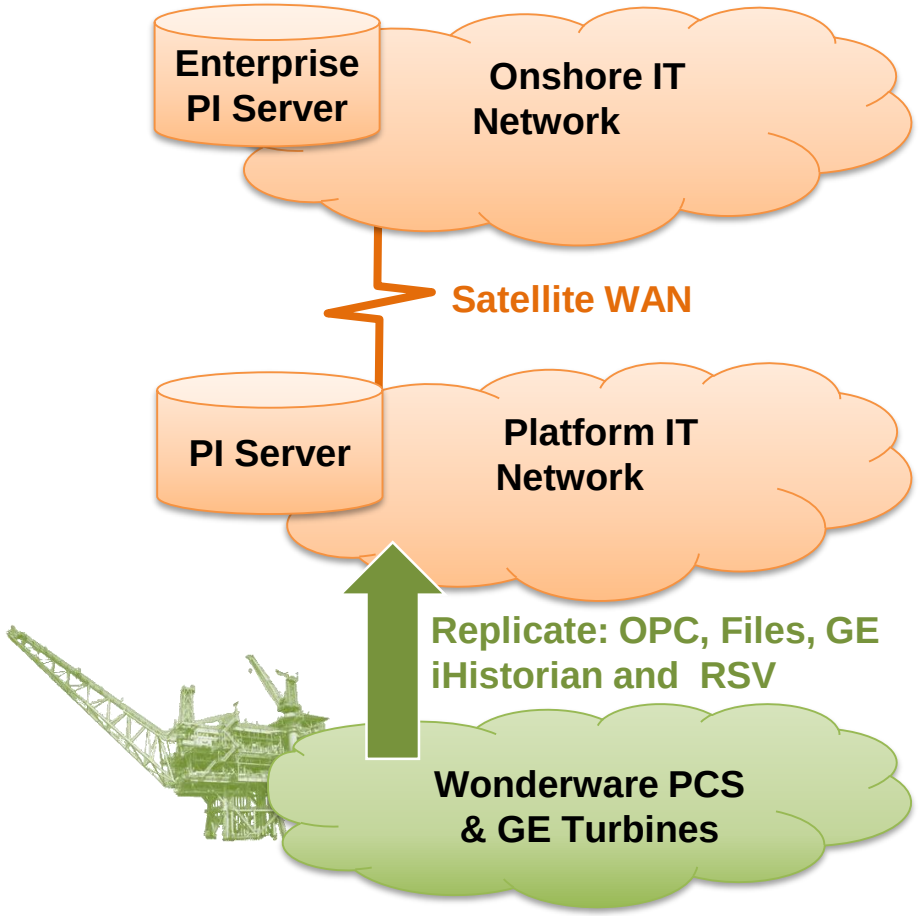
- *Microsoft* SQL Server, *Oracle*
- MySQL, Postgres

Other Connectors

- UDP, TCP/IP, NTP, Multicast Ethernet
- Video & audio stream transfer
- Anti-virus updater, patch (WSUS) updater, OPSWAT
- Remote screen view
- Remote printing
- Web Services

Gateways Offshore

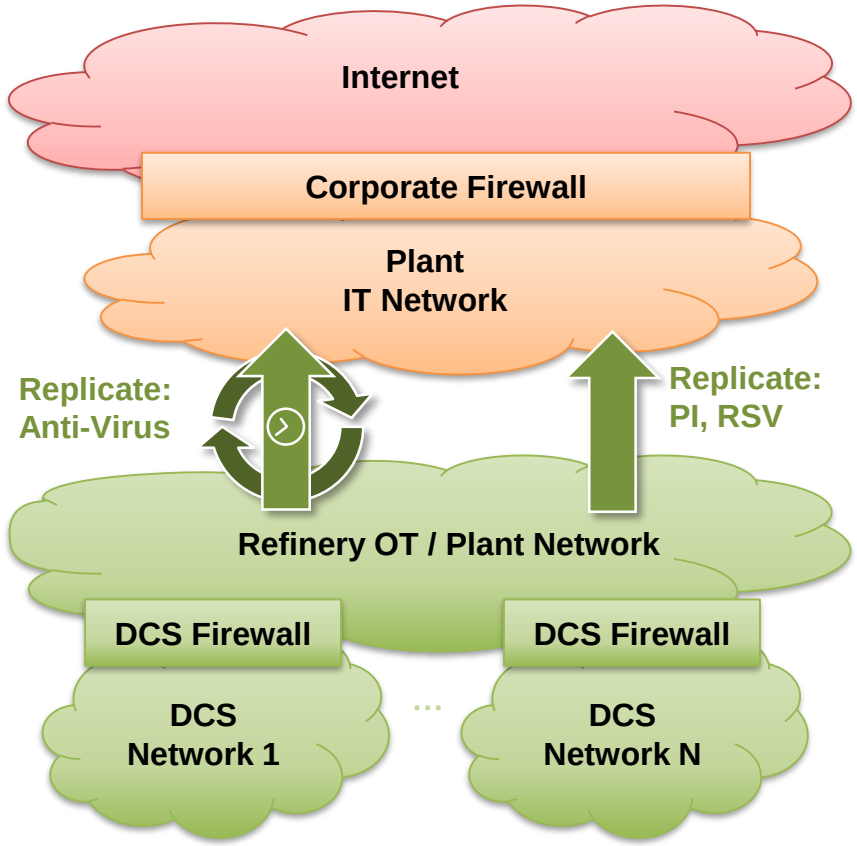
- Unidirectional Security Gateways defeat all remote control attacks
- Replicate OPC to platform PI, files for ad-hoc needs, GE iHistorian for gas turbines, RSV for secure remote access
- Strict controls over removable media & transient devices



Gateways At Refineries

- Operations Technology (OT) plant systems protected unidirectionally
- Replicate & integrate many systems to corporate network
- FLIP for periodic AV updates, batch orders
- Replicate untrusted vendor systems & RSV
- Traditional internal segmentation with firewalls

A layer of unidirectional protections eliminates the threat of remote attacks



NERC CIP V5+

- CIP V5 encourages the use of Unidirectional Security Gateways
- External Routable Connectivity: The ability to access a BES Cyber System that is accessible from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.
- 37 of 103 medium-impact requirements apply only if the affected cyber asset has external routable connectivity

"When you are considering security for your control networks, you need to keep in mind innovative security technologies such as unidirectional gateways" Tim Roxey, E-ISAC

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

WATERFALL®
Stronger Than Firewalls

Secondary Defenses

- Endpoint Security-AV/Whitelisting
- Security updates / patching - control rate of software change, control risk to reliability – match reliability risk to residual attack risk
- Intrusion detection - tune to minimize false positives, alert on new devices & new communications patterns
- Firewalls for internal segmentation
- Encryption wherever practical

Scale investment in secondary defenses to value of residual risk reduction

About Waterfall

- Founded in 2007
- Headquarters in Israel; sales and operations in the US, EU & APAC
- Hundreds of sites deployed in all critical infrastructure sectors in NA, Asia, Europe and Israel
- Holds multiple registered US patents
- Global partners worldwide for both technology and sales collaboration

Market leader for Unidirectional Security Gateways

FROST & SULLIVAN

2012, 2013, 2014, 2015 - **Best Practices Award** for Industrial Network Security

kuppingercole ANALYSTS

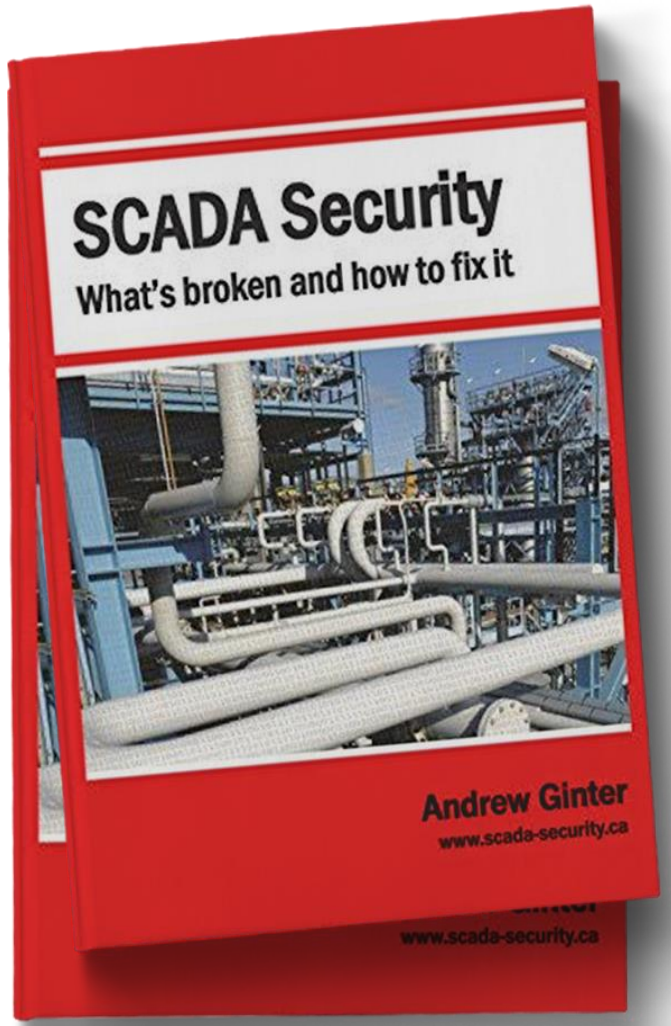
"Waterfall solutions deliver an innovative, well though-out, fast-track solution for quickly securing OT infrastructures against ever-changing cyber-threats."

ARC Advisory Group

"Waterfall is a thought leader in remote access technology for high-security applications."

SCADA Security – What's Broken

- Nothing is secure
- All software can be hacked
- All attacks are information,
  and every bit of information can be an attack



In a connected world, our enemies can attack our control systems while sipping coffee on another continent

Raising the Security Bar

- Today's cyberattacks disrupt production, damage equipment and demand ransom
- IT-class security and firewalls are not sufficient to secure industrial perimeters.
- Unidirectional Gateways prevent remote control attacks, and eliminate entire classes of online threats.

We can and should defend our SCADA systems so thoroughly that even our most resourceful enemies tear their hair out and curse the names of our SCADA security designers