WATERFALL®
Stronger Than Firewalls

Energetic People from India

UNIDIRECTIONAL SECURITY GATEWAYS

Protecting the Safety and Reliability of Industrial Control Systems

3
INTRODUCTION

5
UNIDIRECTIONAL SECURITY GATEWAYS

7
UNIQUE BENEFITS

9
HARDWARE

11
CONNECTOR SOFTWARE

13
BROAD APPLICATION SUPPORT

15
CONCLUSION

16
ABOUT WATERFALL

INTRODUCTION

Industrial digitization is steadily increasing cyber vulnerabilities in industrial control systems. The Industrial Internet of Things (IIoT), cloud connections, IT/OT integration, and Industry 4.0 all require the connection of critical operations networks to external, less trusted, and often Internet-exposed networks. This **increased connectivity greatly increases the "attack surface" for industrial networks** – the set of attack opportunities for cyber criminals.

Such attacks attempt to disrupt production, cause downtime, demand ransom, damage equipment, trigger environmental incidents, harm a company's brand and/or injure workers at the site or put public safety at risk. Unlike IT networks, where the priority for cybersecurity programs is to protect data, the **top priorities for ICS/SCADA security programs** are always:

1. Safety

Prevent physical harm to workers at the industrial site, environmental disasters, and public safety issues.

2. Reliability

Prevent unscheduled downtime, non-conformant product and unexpected damage to physical equipment.

When we start with different priorities for ICS cybersecurity programs, it is no surprise that the resulting programs differ as well. An important example of this difference is software security updates. IT networks are updated frequently with the latest security fixes. **On industrial networks though, every change to software and configurations is a potential threat to safe and reliable physical operations.** Significant testing and scrutiny are necessary to ensure that changed software introduces no unacceptable safety or reliability risks, and this scrutiny and testing takes time. For this reason, many control system software components are updated only very infrequently. That control software cannot be updated promptly does not make software vulnerabilities less important. **Compensating measures must be deployed** to address the vulnerabilities that industrial sites are unable to patch promptly.

IT security technologies such as firewalls, intrusion detection systems and encryption, though, are seen as insufficient security measures for many vulnerable industrial networks. These technologies are software after all, and **all software has defects and vulnerabilities**, both discovered and not yet discovered. Protecting vulnerable industrial software that cannot be frequently updated with yet more vulnerable software that must be frequently updated seems a poor choice to many industrial security practitioners.

All of these security issues are exacerbated by steadily increasing pressure on industrial sites to provide seamless monitoring of industrial systems by enterprise IT and cloud applications to facilitate::

- Predictive maintenance
- Production planning & visibility
- Inventory management
- Secure vendor and 3rd party monitoring
- "Big-data" analytics
- And many more.

The increased connectivity needed by these modern applications increases attack opportunities and safety and reliability risks for already-vulnerable industrial systems.

> "Increased connectivity increases attack opportunities and safety/reliability risks for already-vulnerable industrial systems."

UNIDIRECTIONAL SECURITY GATEWAYS

Waterfall Unidirectional Security Gateways enable **seamless and safe IT/OT integration**, enabling continuous monitoring of industrial operations by IT and even by Internet-based applications, without introducing the attack opportunities that always accompany firewalled connections.

Waterfall Unidirectional Security Gateways replace at least one layer of firewalls in industrial network environments, providing **absolute protection to control systems** and operations networks from attacks originating on external networks. The Gateways enable vendor monitoring, industrial cloud services, and visibility into operations for modern enterprises and their customers.

Unidirectional Gateways **replicate servers, emulate industrial devices and translate industrial data to cloud formats**. As a result, Unidirectional Gateway technology represents a **plug-and-play replacement for firewalls**, without the vulnerabilities and maintenance issues that always accompany firewall deployments.

Unidirectional Gateways contain **both hardware and software** components. Gateway hardware is physically able to transmit information in only one direction, most commonly from the industrial network to an external IT or Internet-based network. Unidirectional Gateways most commonly replace one layer of firewalls in a defense-in-depth architecture at the IT/OT boundary.

All cyber attacks are information – since the gateways physically prevent any information from reaching protected networks, they absolutely block all attacks as well. What's more, the unidirectional protection the gateways provide is hardware-enforced, not software-based. No software vulnerability is able to impair the protection provided by the gateways.

There is a software component to the gateways as well. Unidirectional Gateway software replicates servers from industrial networks to external IT or Internet networks. External users and applications interact with the replica servers as if those servers were the original, industrial systems. External users and applications are generally unaware that they are interacting with replica systems, making the gateways seamless replacements for vulnerable, software firewalls.

> “When considering security control networks, keep in mind innovative security such as unidirectional gateways.”
>
> Tim Roxey,
> Chief Cyber Security Officer NERC

UNIQUE BENEFITS

Absolute protection from

- **Remote-control attacks**: when an attacker on an external network attempts to send any message or command to an industrial asset through a Waterfall Unidirectional Gateway, that attempt fails.
- **Denial of service attacks**: when an attacker on an external network tries to transmit malicious traffic or high volumes of traffic through a Unidirectional Gateway, none of those packets arrive in the control system network.
- **Sophisticated worms and other malware**: no set of badly-configured, un-patched, or zero-day-vulnerable software can cause the gateway hardware to transmit any malware or other information into a protected network, no matter how sophisticated the attack.
- **Targeted ransomware**: no attempt to scan industrial networks or seed ransomware or other malware in those networks through a Unidirectional Gateway can succeed. No command, message or signal of any sort can pass through the gateway back into a protected network.

PROTECTION

VISIBILITY

Full operational visibility

- **Secure, plug-and-play IT/OT integration**: Unidirectional Gateways are a plug-and-play replacement for firewalls, with IT users and applications interacting seamlessly with accurate, real-time replicas of industrial equipment, all without introducing the network vulnerabilities and attack opportunities that always accompany firewall deployments.
- **Secure, seamless Internet connectivity**: Unidirectional Gateways enable direct connections between control system networks and the Internet, enabling data flows to cloud applications, vendor sites, customers and consumers, all without risk to industrial networks.
- **Secure remote support**: Waterfall's Remote Screen View solution enables remote vendors and other support personnel to view the displays of industrial equipment and advise site personnel, while preventing all unauthorized remote control and remote attacks.

UNIDIRECTIONAL
SECURITY GATEWAY

REDUCED COSTS

Compliance benefits

- Comply with: **global industrial cybersecurity standards**, including NIST, ANSSI, IEC, ENISA, NERC, US DHS, NITES and NISA standards and best practices.
- **Dramatically reduce compliance costs**: by simplifying and strengthening industrial network perimeter protections and exempting unidirectionally-secured sites from costly compensating measures such as access logging, denied access attempt logging, firewall rules reviews and testing and many other measures essential to firewalls networks that do not apply to unidirectionally-protected networks.
- **Common-Criteria EAL4+ certified**: providing assurance to industrial sites and their auditors that the Unidirectional Gateways meet the highest standards of security excellence.

COMPLIANCE

Cost reductions

- **Insurance premiums**: Waterfall has partnered with Lloyd's of London to provide comprehensive ICS cyber insurance and dramatically reduced rates for industrial sites protected by Waterfall equipment.
- **Security program operations**: operating costs for Unidirectional Gateways are dramatically lower than comparable costs for firewall-protected sites. Unidirectional Gateways reduce firewall configuration, documentation, revision and testing costs, firewall log management and review costs, and audit costs.
- **Security program training**: Unidirectionally-protected sites are simpler than firewalled sites, resulting in significant savings from simplified personnel and vendor training and awareness programs.

UNIDIRECTIONAL SECURITY GATEWAY HARDWARE

Unidirectional Gateway hardware is physically able to transmit information in only one direction. The hardware components include a TX Module containing a fiber-optic transmitter/laser but no receiver, an RX Module containing an optical receiver/photo-cell but no laser, and a short fiber-optic cable connecting the two Modules. The gateway hardware is thus able to transmit information encoded in an optical signal from a control system network to an external network, but is **physically incapable of propagating any remote control attack, malware, DOS attack, human error or any cyber attack at all back into the protected network**..

As illustrated below, the complete set of hardware that is part of a Unidirectional Security Gateway is a minimum of two conventional computers, one TX Module, one RX Module, and a minimum of five cables. The TX and RX Hosts are conventional computers running Unidirectional Gateway connector software. Each computer is connected to a local-area network (LAN) with a conventional, bi-directional network connection, and to one of the TX or RX hardware Modules.

Combination of hardware & software

- The TX Host uses the normal, bidirectional network interface to gather data from one or more manually pre-configured industrial source systems. The TX Host is configured as to which network addresses from which to gather data. The “gathering” of information is done using a specific Unidirectional Gateway Connector application developed to integrate and gather information from a specific type of industrial system.
- The TX Host takes the gathered industrial information and the meta-data describing the information and sends both to the dedicated cable connecting the TX Host to the TX Module. This information is sent using a Waterfall-proprietary, internal, point-to-point, non-routable ISO layer 2 protocol.
- The TX Module converts the content from copper to optical signaling, inserts error correction information, and transmits the content to the RX Module over the fiber optic cable.
- The RX Module receives content and error-correcting codes from the fiber optic cable, and corrects and transmits the contents to the RX Host using a Waterfall-proprietary, internal, point-to-point, non-routable OSI layer 2 protocol.
- Finally, the RX Host passes the received data to Waterfall application-specific software connector, which makes the data available to the IT network, usually sending the data to manually pre-configured servers or destinations on that network.

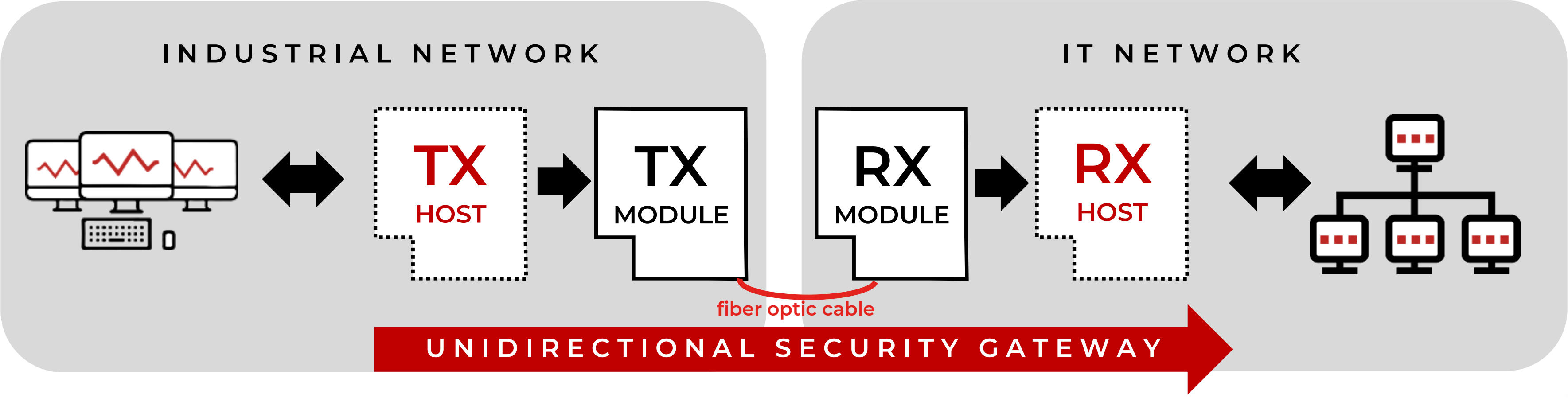

Figure 1: Waterfall Unidirectional Gateway Hardware

UNIDIRECTIONAL SECURITY GATEWAY CONNECTOR SOFTWARE

All gateway deployments involve one or more of Waterfall's software connectors. The connectors replicate industrial servers & emulate industrial devices.

REPLICATING A HISTORIAN SERVER

The most common Unidirectional Gateway deployment is illustrated in Figure 2. In this deployment, the gateway replicates a plant historian to an enterprise historian. In practice, the TX and RX Hosts can run multiple connectors and replicate multiple servers or devices. Only one connector is illustrated in Figure 2 for the sake of simplicity.

In this deployment, the gateway's Historian Connector logs into the plant historian as a conventional historian client, and requests a copy of all new data arriving in the historian. The communication protocol employed to receive the data is the historian's normal, supported client access protocol. The connection between the historian server and the TX Host terminates in the historian server and the TX Host/connector – no part of the connection extends through the Unidirectional Gateway TX and RX hardware modules. The Historian Connector software on the TX Host extracts historical data and meta-data from the information received from the plant historian and sends that information through the unidirectional hardware subsystem to the RX Host.

The Historian Connector software on the RX Host takes the historian data and meta-data received from the unidirectional hardware and inserts the data into the replica historian. The RX Connector application is configured according to which IP address it uses to communicate with the enterprise/replica historian. Only information regarding historian point names, data types, data values and other historian "content" is communicated through the unidirectional hardware. No addressing information is sent through the unidirectional hardware. None of the TCP/IP packets used to communicate with the plant historian are forwarded to the replica historian. The connection between the RX Host/Connector and the replica historian is completely independent of the connection between the TX Host/Connector and the plant historian.

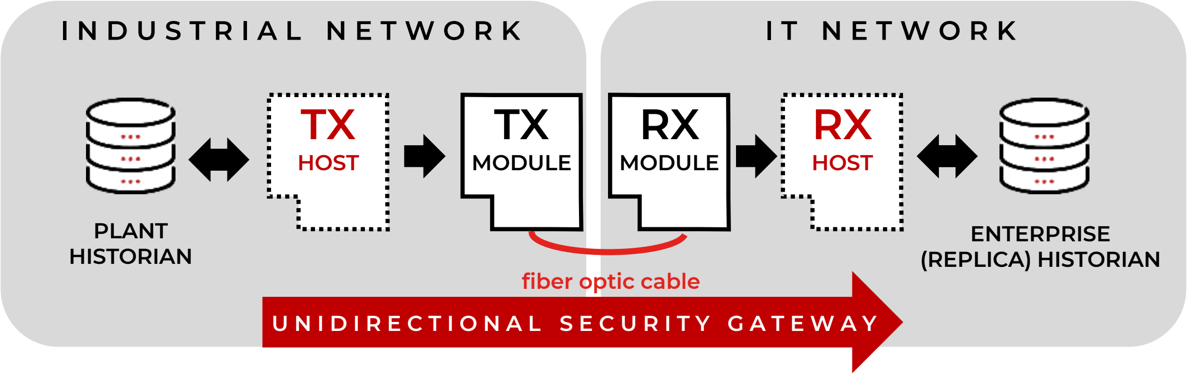

Figure 2: Historian Replication

The result of these efforts is that the enterprise historian becomes a faithful, real-time replica of the plant historian. In addition, when there are multiple plants the Historian Connector is generally able to optionally aggregate all of the data from all of the plants into a single enterprise/replica historian, with optional automatic renaming if necessary, to resolve point name conflicts that might arise between plants.

REPLICATING OPC SOURCES

Another popular deployment is the Waterfall for OPC-DA server emulation solution illustrated in Figure 3. The OPC-DA protocol is a complex, bi-directional, object-oriented protocol layered on the DCOM object model. The OPC-DA Connector makes no attempt to emulate this protocol across the unidirectional hardware subsystem. Instead, the connector regularly reads data from the plant OPC-DA server, and emulates that server on the IT network to IT users and applications.

In the figure, the source OPC server receives data from systems and devices on the protected network. The Waterfall OPC-DA Connector software running on the TX Host is a standard OPC client and pulls data from the plant OPC server using the normal OPC-DA protocol. The gathered data and associated meta-data are then transmitted through the unidirectional hardware subsystem.

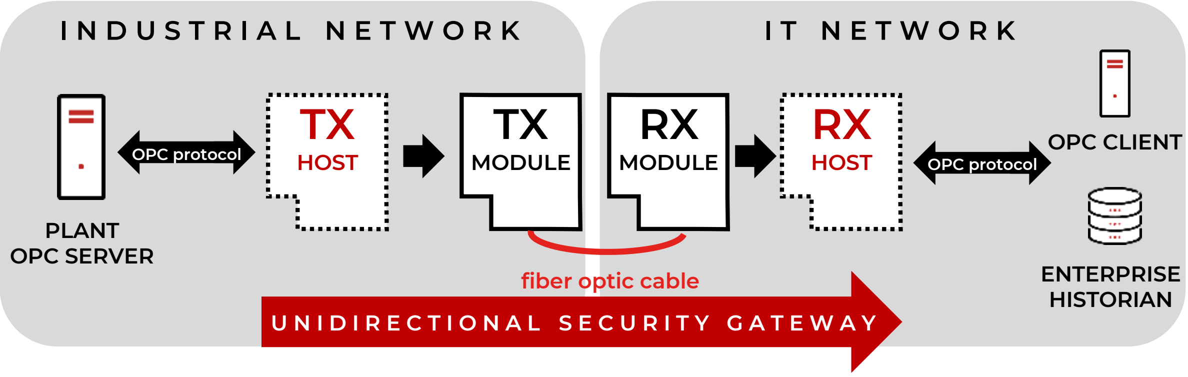

Figure 3: OPC Server Replication

The RX Host sends all the received data to the OPC Connector software running on that host. On the RX Host, the connector software is a standard OPC-DA server. With the plant server's OPC data in hand, the RX OPC server is a faithful emulator of the plant OPC server. All IT OPC clients, such as an enterprise historian for example, poll the Waterfall OPC-DA server/emulator and receive answers to those queries/polls from the latest snapshot of data sent from the plant OPC server.

Once again, rather than emulating or "supporting" the OPC-DA / DCOM protocol, the Unidirectional Gateway provides a standard OPC server on the IT network, a server that is updated in real-time with a copy of the data found in the plant OPC server on the industrial network.

BROAD APPLICATION SUPPORT

100+ COTS software connectors

Application support is essential to a successful deployment of Unidirectional Gateways. Waterfall Security Solutions supports commercial-off-the-shelf (COTS) connector software products for a wide array of industrial applications. Waterfall connectors include support for the following applications:

HISTORIANS & INDUSTRIAL APPLICATIONS

Osisoft: PI System, PI Asset Framework, PI Backfill

GE: iHistorian, iHistorian Backfill, OSM, Bently-Nevada System1, Proficy HMI

Schneider-Electric: Instep eDNA, Wonderware Historian, Wonderware Historian Backfill, ClearSCADA

Siemens: SIMATIC, WinCC, WinTS, SINAUT, Spectrum

Emerson: Ovation, EDS, EMS

Areva: PowerPlex, PowerTrax

AspenTech IP.21, Rockwell FactoryTalk Historian, Honeywell Alarm Manager, Scientech R*Time

FILE TRANSFER

Folder mirroring, Rsync, Local Folders

FTP, FTPS, SFTP, TFTP, RCP, SMB, HTTPFS

IT APPLICATIONS

FireEye: TAP, Helix and FaaS

Log Files, SMTP, SNMP, Syslog, CA Unicenter, CA SIM

HP Openview, IBM Tivoli, HP ArcSight, McAfee ESM, Splunk, QRadar

MSMQ, IBM Websphere MQ, Active Message Queue, TIBCO

SAP

RELATIONAL DATABASES

Microsoft SQL Server, Oracle

MySQL, PostgreSQL

REMOTE ACCESS

Remote Screen View

Secure Bypass (SBP)

INDUSTRIAL PROTOCOLS

OPC DA, A&E, HDA, HDA Backfill and UA

Siemens S7, Modbus, Modbus Plus, DNP3, ICCP, IEC 60870-5-104, IEC 61850

OTHER CONNECTORS

UDP, TCP, NTP, Multicast Ethernet

Video & audio streaming

Anti-virus updater, WSUS updater, OPSWAT updater

Remote printing

CONCLUSION

The threat environment facing national critical infrastructures and industrial sites necessitates a solution which goes beyond the call of traditional software protections. Hardware-enforced Unidirectional Security Gateways answer this call by providing absolute protection to industrial networks while enabling operational monitoring in real-time. The value provided by the Gateways to industrial plants is considered essential to a modern ICS cyber defense architecture.

Waterfall Unidirectional Security Gateways replace at least one layer of firewalls in industrial network environments, and protect the industrial site from attacks originating on external networks. The Gateways enable vendor monitoring, industrial cloud services, and visibility into operations for modern enterprises and customers. Unidirectional Gateways replicate servers, emulate industrial devices and translate industrial data to cloud formats. As a result, Unidirectional Gateway technology represents a plug-and-play replacement for firewalls, without the vulnerabilities and maintenance issues that always accompany firewall deployments.

Malicious actors have already proven the extent of damage - actual and potential - a cyber attack can have on critical infrastructure. To prevent these attacks from reaching their targets, while at the same time optimizing enterprise efficiencies, control networks need to be protected using a solution that eliminates external network attacks. ICS networks need a higher level of protection than traditional IT networks, after all, plant assets, the environment and human lives cannot be restored from back-up.

100% PROTECTION, 100% VISIBILITY, 100% COMPLIANCE

ABOUT WATERFALL SECURITY

Waterfall Security Solutions is the global leader in industrial cybersecurity technology. Waterfall products, based on its innovative unidirectional security gateway technology, represent an evolutionary alternative to firewalls. The company's expanding portfolio of customers includes national infrastructures, power plants, nuclear plants, offshore oil and gas facilities, rail transport, refineries, manufacturing plants, utility companies, and many more. Deployed throughout North America, Europe, the Middle East and Asia, Waterfall products support the widest range of leading industrial remote monitoring platforms, applications, databases and protocols in the market.

For more information, please contact: https://waterfall-security.com/contact

Waterfall's products are covered by U.S. Patents 7,649,452, 8,223,205, and by other pending patent applications in the US and other countries. "Waterfall", the Waterfall Logo, "Stronger than Firewalls", "In Logs We Trust", "Unidirectional CloudConnect", and "CloudConnect, and "One Way to Connect" are trademarks of Waterfall Security Solutions Ltd. All other trademarks mentioned above are the property of their respective owners. Waterfall Security reserves the right to change the content at any time without notice. Waterfall Security makes no commitment to update content and assumes no responsibility for any mistakes in this document.