WATERFALL®
Stronger Than Firewalls

CYBERSECURITY FOR RAIL SIGNALING SYSTEMS AND ROLLING STOCK

PROTECTING DIGITIZED RAIL NETWORKS FROM IMMINENT CYBER THREATS

CYBER ATTACKS ON RAILWAY SWITCHING SYSTEMS ARE NO LONGER A HYPOTHETICAL THREAT

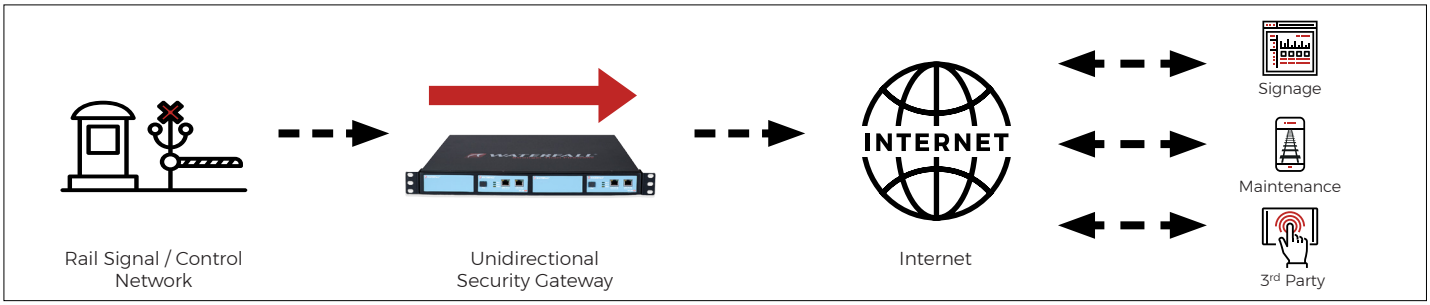
Cyber attacks have already impacted rail systems in the USA, UK, Poland, Korea, Japan and many countries. The more digitized rail networks become, the more vulnerable critical signaling systems are to cyber sabotage. Increased signaling network connectivity and digitalization enable the adoption of modern positive train control (PTC) systems, cloud analytics, enterprise visibility into signaling operations, and vendor-monitored predictive maintenance systems, but at the same time introduce threats to safe, reliable and cost-effective operations. To maintain the highest level of safety and reliability, signaling network perimeters must be protected by Unidirectional Security Gateways.

RAIL SYSTEM CHALLENGES	WATERFALL SOLUTION	RESULTS & BENEFITS
Signage updates & maintenance alerts Provide safe, real-time access to locomotive location information for station signage and web applications, as well as cell-phone-based access to track outage information for track maintenance personnel, so that technicians can be confident tracks closed for maintenance will not be used by any locomotives. Provide all of these capabilities to IT and Internet applications while preventing any online attack from reaching signaling networks.	**Signaling network replication** Waterfall Unidirectional Gateways replicated Microsoft SQLServer databases to external networks, to communicate locomotive location and track lockout information. SQL clients and Internet web servers on these external networks interacted normally and bi-directionally with the replica servers. The gateways also replicated file servers to enterprise networks to enable routine file transfers to IT networks and so eliminated routine use of USB drives and other removable media.	**Hardened signal network perimeter** ✔ Enables safe integration of control networks with external networks by eliminating remote cyber threats ✔ Provides public visibility into real-time locomotive status ✔ Provides visibility into real-time track closure status ✔ No attack from an Internet-exposed network can reach switching/signaling systems ✔ Drag-and-drop file transfers minimize the use of removable media
Rail operators on shared infrastructure Communicate locomotive location, track outage status and other information to transport enterprises using the shared rail infrastructure in real-time. Communicating this status information must not put signaling systems at risk.	**Signaling network protection** Waterfall Unidirectional Gateways replicated Microsoft SQLServer databases managing locomotive location, track lockout information and other status information to business partners. SQL clients and web servers on external networks interacted normally and bi-directionally with the replica servers.	**Hardened signal network perimeter** ✔ Real-time status information is available on-demand to shared infrastructure operators and other rail operators ✔ Signaling networks are protected absolutely from any threat propagating via connections to business partners
Onboard public network Provide passengers with access to locomotive status, schedule information and Internet connectivity, without putting locomotive controls or the signaling system as a whole at risk of attack.	**Train control network protection** Vibration and environmentally-hardened Waterfall Unidirectional Gateways mounted in locomotives replicated a variety of locomotive control systems to passenger and comfort networks, to share information with those networks.	**Securing onboard control networks** ✔ No attack from Internet-exposed passenger networks can reach locomotive control system ✔ Passengers enjoy real-time status information and Internet connectivity with no risk to locomotive control or signaling networks

100% SECURITY, 100% VISIBILITY, 100% COMPLIANCE

WATERFALL®
Stronger Than Firewalls

THEORY OF OPERATION



Waterfall Unidirectional Security Gateways replace firewalls in control network environments, **providing absolute protection to signaling systems and locomotive controls from attacks emanating from external less-trusted 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.

Unidirectional Gateways contain both hardware and software components. The hardware components include a TX Module, containing a fiber-optic transmitter/ laser, and an RX Module, containing an optical receiver, but no laser. The gateway hardware can transmit information from a signaling system network to an external network, but is physically incapable of propagating any virus, DOS attack, human error or any cyber attack at all back into the protected network.

UNIDIRECTIONAL SECURITY GATEWAYS BENEFITS:

- Enable safe, real-time reporting of locomotive location, track and other operational status to business management, track technicians, the general public, infrastructure partners, and other rail operators
- Eliminate risks to reliability, worker safety and public safety due to external cyber attacks
- Reduce compliance costs and efforts
- Protect rail operator brands from damage due to service outages

RAIL CYBERSECURITY STANDARDS POINT TO UNIDIRECTIONAL GATEWAYS

- In France the Agence nationale de la sécurité des systèmes d'information **(ANSSI)** Cyber Security for Industrial Control Systems standard forbids firewalls and interactive remote access between signaling systems and less-critical networks, and permits only Unidirectional Gateways at such connections.
- In the UK, the **Department for Transport** recommends Unidirectional Security Gateways for the protection of signaling networks.
- **NIST** Special Publication 800-82 Revision 2 recommends unidirectional gateways for network access restriction and network boundary protection – two major security objectives for rail control networks.
- The European Union Agency for Network and Information Security **(ENISA)** recommends unidirectional technology to harden rail transport control networks to reinforce security from unauthorized access, insecure protocols, malicious code, and cascading network outages.

INFO@WATERFALL-SECURITY.COM | WWW.WATERFALL-SECURITY.COM

ABOUT WATERFALL SECURITY SOLUTIONS

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. Please contact: **info@waterfall-security.com**