

CYBERSECURITY FOR ELECTRIC SUBSTATIONS

PROTECTING THE CONNECTED SUBSTATION FROM EVOLVING CYBER THREATS

Customer	American transmission utility
Customer Requirement	To comply with NERC-CIP standards and protect critical assets from cyberattacks while protecting operational and business process efficiency.
Waterfall's Unidirectional Solution	Secure substation network perimeters from external threats with Unidirectional Security Gateways, while enabling compliance with NERC CIP regulations and safe monitoring by central Energy Management and SCADA systems.

MODERN THREATS TO HIGH VOLTAGE SUBSTATIONS

High voltage substations are vital to the reliable operation of the bulk electric system. High voltage substations have been targeted in recent attacks though – compromised substations have been used to interrupt power flows to consumers, industries and critical infrastructures such as drinking water purification systems and vital government and military installations. When transmission substations are targeted, there is the potential for cascading failures when the demand for power is high. When substation protective relays are targeted, there is the potential for physical damage to transformers and other vital physical infrastructure. It is for these reasons that regulators in many geographies require electric utilities to provide strong protection for substation control equipment and protective relays.

THE CHALLENGE

To secure the safe, reliable and continuous operation of high voltage substations from threats emanating from SCADA Wide Area Networks (WAN) and other external sources, yet still provide central EMS/SCADA systems, Information Technology (IT) users and substation vendors with real-time access to substation data. In particular, ensure that substation protective relays are protected from compromise, to prevent damage to high-voltage equipment.



WATERFALL SOLUTION

A Waterfall Unidirectional Gateway was installed in all substations with physical equipment operating at or above 100KV. Gateway software connectors replicate protective relay event files to a central site for analysis by power engineers. Gateway software also replicates relay and Remote Terminal Unit (RTU) DNP3 servers.

Central EMS/SCADA systems interact normally and bi-directionally with the replica servers, sending them poll requests and configuring reporting by exception.

Unidirectional Gateway hardware physically prevents any external threat from reaching into and impairing substation or protective relay operations.

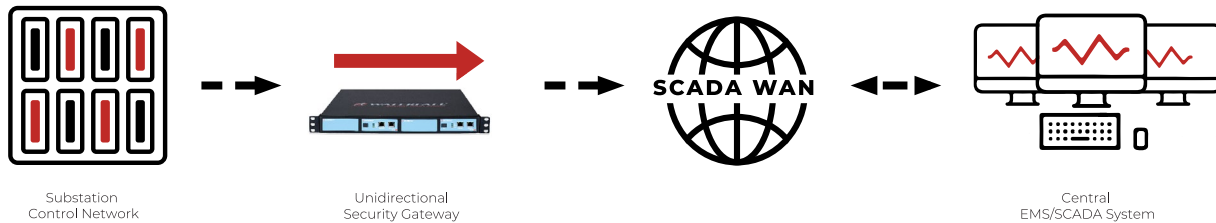
RESULTS & BENEFITS

100% Security: Critical substation relay networks and control networks are physically protected from threats emanating from external, less-trusted networks.

100% Visibility: The central EMS/SCADA system continues to operate normally. Instead of accessing substation servers directly, the system transparently accesses emulated devices for safe monitoring of substation equipment.

100% Compliance: Unidirectional Gateways are recognized by the NERC CIP, French ANSSI and other standards, and regulations as providing the strongest possible network perimeter protections.

THEORY OF OPERATION



Waterfall Unidirectional Security Gateways replace firewalls in high voltage substation environments, **providing absolute protection to protective relays and Remote Terminal Units from attacks emanating from external, less-trusted networks.** 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 an industrial 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 industrial network.

The Gateways **enable relay event reporting, vendor monitoring and safe monitoring of substation equipment by distant EMS/SCADA systems.** 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 accompany firewall deployments.

UNIDIRECTIONAL SECURITY GATEWAYS BENEFITS:

- » Safe, continuous monitoring of protective relays and RTU equipment by central EMS/SCADA systems
- » Prompt reporting of protective relay trip events to central power engineering teams for analysis and response
- » Absolute protection from online attacks from external networks
- » Support for current and future substation environments and requirements, including DIN-rail form factor and support for DNP3, IEC 60870-5, IEC 61850 Edition 2, IEC 61850 GOOSE and IEC 61850 MMS

GLOBAL CYBERSECURITY STANDARDS RECOMMEND UNIDIRECTIONAL SECURITY GATEWAYS

Waterfall Security is the market leader in Unidirectional Gateway technology with installations at critical infrastructure sites across the globe. The enhanced level of protection provided by Waterfall's Unidirectional Security Gateway technology is recognized as best practice by many leading industry standards bodies, including NIST, ANSSI, NERC CIP, the ISA, the US DHS, ENISA and many more.

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

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. Please contact: info@waterfall-security.com

Waterfall's products are covered by U.S. Patents 8,223,205, 7,649,452, 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.

Copyright © 2018 Waterfall Security Solutions Ltd. All Rights Reserved. www.waterfall-security.com