WATERFALL®
Stronger Than Firewalls

WATERFALL FOR DNP3

SECURE ENTERPRISE MONITORING OF DNP3 DEVICES

Industrial enterprises frequently need enterprise-wide access to data from devices supporting the DNP3 industrial communications protocol. Connecting enterprise networks to DNP3 devices through firewalls is high risk. All software can be hacked and all firewalls and DNP3 implementations are software.

The Waterfall for DNP3 connector software supports Waterfall Unidirectional Security Gateway. The connector gathers data from DNP3 devices on industrial networks in real time, sends that data through the unidirectional hardware, and emulates the DNP3 devices for SCADA users and applications. SCADA users and applications can access the emulated devices bi-directionally, as if they were still communicating to the original DNP3 devices. The Waterfall unidirectional hardware physically prevents any attack or malicious command from reaching the protected DNP3 devices.

BENEFITS OF USING WATERFALL FOR DNP3

Secure, real-time unidirectional emulation of DNP3 devices to SCADA users & applications

SCADA users and applications interact normally with accurate, timely emulation of DNP3 devices on their networks

Eliminates all remote attacks and malware propagation from external networks

Facilitates and simplifies compliance with NERC CIP, NIST, CFATS, ANSSI, UK DfT and more

Simple deployment, off-the-shelf solution

WATERFALL®
Stronger Than Firewalls

WATERFALL SOLUTION FOR DNP3

The Waterfall for DNP3 TX connector is a DNP3 master and uses DNP3 polls and report-by-exception events to gather a snapshot of the state of DNP3-enabled devices. The TX module sends this snapshot to the RX module through the unidirectional hardware modules. The RX module is a DNP3 slave, which waits for polls from the DNP3 master, such as an EMS or SCADA master, or reports by exception to that master station. The RX software serves as a faithful emulation of the DNP3-enabled devices in the protected network, responding to interactions with the DNP3 master in the same way as the emulated device would have responded, without ever permitting any message back into the protected network to put reliability-critical equipment at risk. Enterprises deploying the Waterfall for DNP3 connector enjoy increased visibility for industrial data, reduced compliance costs and dramatically reduced cyber risk and cyber incident costs.

The Waterfall Unidirectional Gateway hardware deployed between both networks includes a TX Module containing a fiber-optic transmitter/laser, and an RX Module containing an optical receiver but no laser. The gateway hardware makes it physically impossible for attacks to flow from the corporate network towards the industrial network, eliminating any threats of online attacks, malware or human errors.

FULLY-FEATURED & ROBUST SUPPORT:

- Real-time replication of DNP3 protective relays, RTUs, IEDs, and other DNP3 equipment
- Replicates many DNP3 devices on a single host
- Supports both DNP3 master and slave emulation
- Supports all DNP3 data types and point types
- 1 Gbps throughput standard & High Availability option
- Fully supported with Waterfall Unidirectional Security Gateway software

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

ABOUT WATERFALL SECURITY SOLUTIONS

Waterfall Security Solutions is the global leader in industrial cybersecurity technology. 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