



Waterfall for NERC-CIP Compliance

Using Waterfall's Unidirectional Security Solution to Achieve True Security & NERC-CIP Compliance

Date: Jul. 2009

The material in this document is proprietary to Waterfall Security Solutions Ltd. No part of this document may be passed to any third party, copied, reproduced or stored on any type of media or otherwise used in any way without the express, prior, written consent of authorized officers and/or executives of Waterfall Security Solutions Ltd.

Abstract

Critical National Infrastructure is under a constant, yet invisible, threat from cyber hacking and cyber terror attempts that are being launched from external networks. These attacks (mainly - from the Internet) are targeting industrial Process Control Networks (PCN), Supervisory Control and Data Acquisition (SCADA) Networks and lower level Distributed Control Systems (DCS) and Process Control Systems (PCS) networks. In the Electricity Utilities' domain, these critical networks control and operate the very machinery which powers modern day civilization. Throughout North America, electricity utilities are challenged with the task of complying with the reliability standards mandated by NERC (North American Electric Reliability Corporation). The NERC-CIP (Critical Infrastructure Protection) standards, recently revised in May 2009, provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System. The following whitepaper introduces the reader to the Waterfall One-Way™ unidirectional cyber security solution, and explains its ideal fit for achieving both powerful cyber-security as well as NERC-CIP compliance.

About Waterfall Security Solutions (www.waterfall-security.com):

Waterfall Security Solutions Ltd. is the leading provider of secure unidirectional connectivity for Process Control systems, Industrial Networks, SCADA systems, Remote Monitoring and Segregated Networks. Waterfall's products have been deployed in many critical national infrastructures, homeland security agencies and mission critical organizations in North America, Europe and Israel, and include security solutions for leading industrial applications such as Historian systems and Remote Monitoring platforms as well as leading industrial protocols such as OPC, Modbus, DNP3 and ICP.

Waterfall One-Way™ for NERC-CIP Reliability Standards

NERC-CIP Standards CIP-002 through CIP-009, currently in their 2nd revision, provide a cyber security framework for the identification and protection of Critical Cyber Assets (CCAs) to support reliable operation of the Bulk Electric System. In addressing CIP compliance, the primary focus has been on CIP-005, which mandates the definition and operation of an electronic security perimeter (ESP), encompassing all Critical Cyber Assets. This ESP requirement defines the scope and breadth of assets to be protected and defended according to the overall NERC-CIP framework. All access points and communication connections' end-points to this perimeter must be defended and protected. The NERC-CIP standards do not mandate the specific types of defenses or the specific method of defining the ESP, and this task is left to the discretion of the regulated utility. While traditional (i.e. software based) IT Security products or systems (firewalls, intrusion detection systems, anti-malware etc.) can be used, they are vulnerable to the same risks and dangers targeting the CCAs themselves: Firewalls can be hacked, IPSs and IDSs must be patched and updated, zero-day exploits are a permanent risk, configuration is tiresome and prone to mistakes, etc. When seeking a NERC-CIP solution, one that indeed achieves compliance while realizing the true spirit of high assurance and defense in depth, it is evident that traditional, software-based protection solutions are not enough. This is especially true when considering the immense implications of a successful cyber-attack on a major electricity utility.

Waterfall One-Way™ is a consolidated hardware and software security solution that provides the most powerful defense of the electronic security perimeter available. Affording an unparalleled level of protection to all Critical Cyber Assets residing within critical infrastructure network perimeter(s), Waterfall One-Way™ provides a solid foundation for the NERC compliance framework. It addresses the NERC compliance framework requirements by supplying a true level of security at all layers of the networks' communications protocols, enforcing the electronic security perimeter in accordance with NERC-CIP-005 requirements and by providing robust and truly unidirectional communication to devices outside the perimeter. In addition successful implementation of NERC-CIP-007, detailing the required Systems Security Management within the electronic security perimeter and at its access points, is much easier to achieve with Waterfall One-Way™ integrated into the critical infrastructures' cyber security framework. In fact, Waterfall One-Way™ potentially eliminates access points and supporting critical cyber assets.

The importance of the reliability of the bulk electric system to our modern way of life is central and undisputed. The imminent dangers of cyber terror and cyber hacking activities are clear and publicly known. Waterfall Security Solutions supplies a win-win

solution which not only provides a unique and robust foundation for NERC-CIP compliance, but true and unparalleled security against all external cyber threats.

Introducing Waterfall One-Way™

Waterfall's hardware based unidirectional core is shared by all of its products and solutions. The core is coupled with software agents that mediate its integration into the surrounding environments, while providing added functionalities and flexibility. The basic Waterfall architecture is as follows:

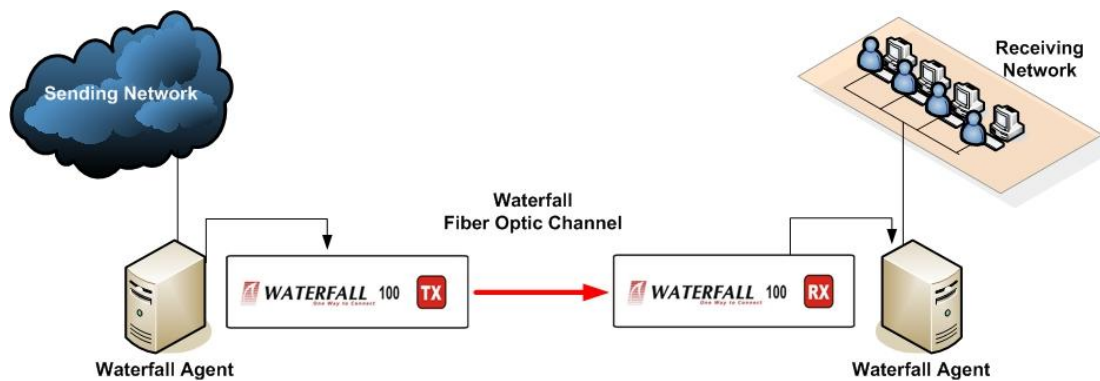


Figure 1 – Basic Waterfall One-Way™ Architecture

The basic components are:

- A Waterfall Tx Software Agent, residing on a host which is part of the sending network. The agent interacts with applications (e.g. OSIsoft PI™, GE Proficy™) and protocols (e.g. OPC, Modbus) on the network, receives the relevant information and mediates the connection of the Waterfall One-Way™ with the sending network. Designated data is passed, in real-time, from the Tx software agent to the Waterfall Tx appliance.
- An appliance pair comprised of:
 - A Waterfall Tx Appliance, transmitting information from the Tx software agent via a single fiber optic cable to the Waterfall Rx Appliance.
 - A Waterfall Rx Appliance, receiving information from the Waterfall Tx appliance and transmitting it to the Waterfall Rx software agent, residing on a host which is part of the receiving network.
- A Waterfall Rx Software Agent, residing on a host which is part of the receiving network. The agent receives data from the Waterfall Rx appliance, mediates the connection of the Waterfall One-Way™ with the receiving network and interacts

as required with applications and nodes on the receiving network, passing the designated data into the receiving network.

Waterfall One-Way™ Customer Benefits

The unique Waterfall architecture and its attributes provide two basic benefits for all Waterfall One-Way™ installations and deployments:

- Complete protection against external cyber attacks – hacking sessions are an interactive process in which a hacker initiates a working session with his target node, elicits a response, and accordingly makes his next move. When trying to hack across a Waterfall One-Way™, the hacker will be unable to initiate a successful session.
- No data backflow – The hardware based appliance core of the Waterfall One-Way™ enforces unidirectional data flow at the physical layer (Layer 1 of the OSI model), which in turn *ensures* unidirectional communication will be totally preserved at all higher layers of the protocol stack, regardless of the communication protocol chosen and the applications being used. Thus, regardless of networks and applications used, there will be no data backflow across a Waterfall One-Way™.

Waterfall One-Way™ provides customers with the most powerful electronic security perimeter available, enforced by hardware, software and the very basic laws of physics. This unique technology and architecture helps ensure that compliance with NERC-CIP-005 requirements is fully reached, while providing true cyber-security to all critical assets and cyber assets residing within the Waterfall defined electronic security perimeter.

As an added benefit, Waterfall installations provide a hassle-free and zero-maintenance implementation of an electronic security perimeter, requiring a one-time configuration with no need for follow-up configurations, patches or updates. Thus overhead and related investments are minimized.

Only Waterfall can provide *full visibility* into the critical infrastructure networks running the bulk electric system, while still *fully segregating* them from any externally generated activities, in essence effectively air-gapping them to achieve unprecedented protection and security.

Annex Waterfall One-Way™ for NERC Compliance – Network Architecture samples

Below are several examples of network architectures implementing Waterfall One-Way™ to define electronic security perimeters compliant with NERC-CIP-005. All are meant to provide a more in-depth technical view into the logic and structure of Waterfall One-Way™ deployment in critical industrial environments.

The basic layout of a NERC-CIP compliant Waterfall deployment is presented, followed by several examples of how this basic architecture is leveraged to provide different solutions and flexible applications' & protocols' support.

Waterfall One-Way™ Defining an Electronic Security Perimeter

The most common NERC-CIP compliant basic architecture is as follows:

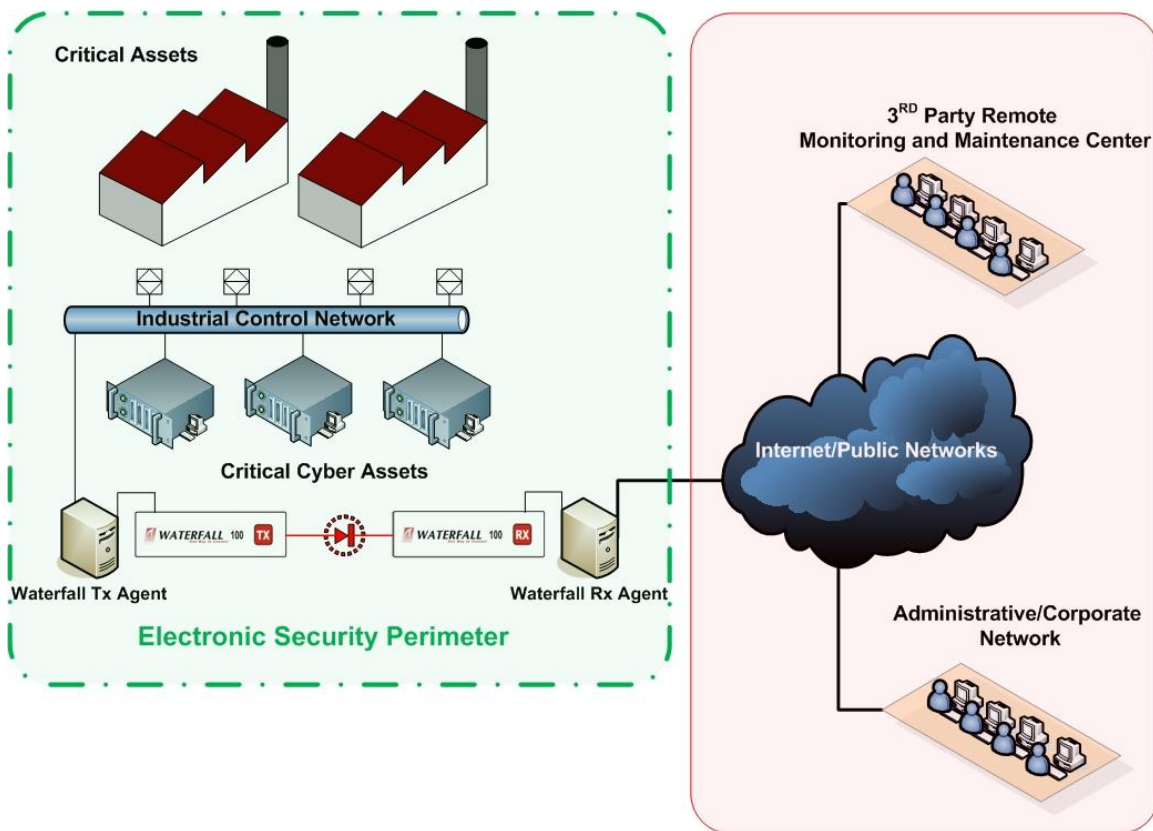


Figure 2 – Basic Waterfall One-Way™ NERC-CIP Compliant Architecture

This architecture allows data and information to be exported and transmitted from the security enclave created by the ESP towards all external data consumers, without

exposing critical assets and cyber assets to any external dangers. Full visibility to the industrial information is afforded to all external users.

This basic architecture can be leveraged in several different possible sub-architectures, employing different Waterfall-based solutions which transport different types of data across the waterfall link, from the industrial control network towards the external networks.

Transporting Files using the Waterfall File Transfer Enabler (WF-FTE)

This is a common Waterfall security solution for transferring files from a security enclave, across the electronic security perimeter to external networks. The following diagram shows the general layout involving dedicated file servers (which are not a part of the Waterfall One-Way™):

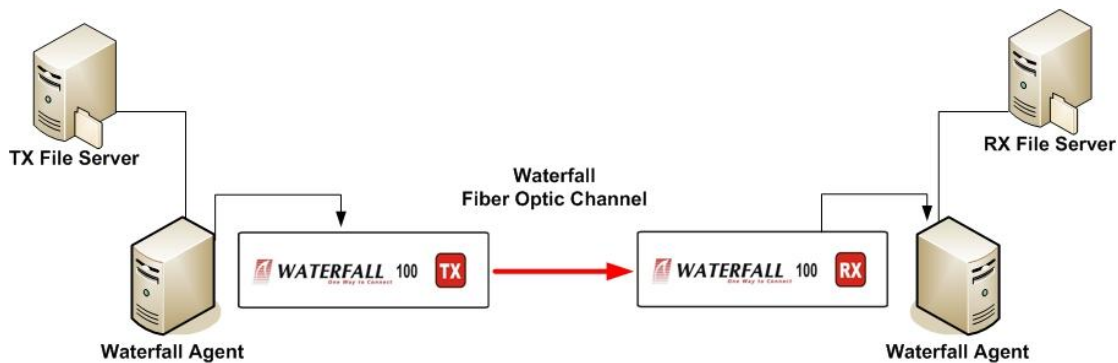


Figure 3 – Waterfall File Transfer Enabler (WF-FTE)

In this configuration, files are simply being transported from the origin server to the destination server. The Tx file server is completely secured from external attacks, while the files themselves can be further protected by encryption (for example Waterfall's FTE supports FTP as well as SFTP and TFTP).

Historian Replication using the Waterfall SCADA Monitoring Enabler (WF-SME)

In this scenario, an operational Historian is replicated from the secured operational network to a replica Historian residing on the corporate or external network. Waterfall performs this replication by leveraging the Historian's low level API in order to achieve maximum performance and real-time high throughput. Supported Historians today include the OSIsoft PI™ Historian, GE's Proficy Historian and others. The basic architecture for a Historian replication would look as follows:

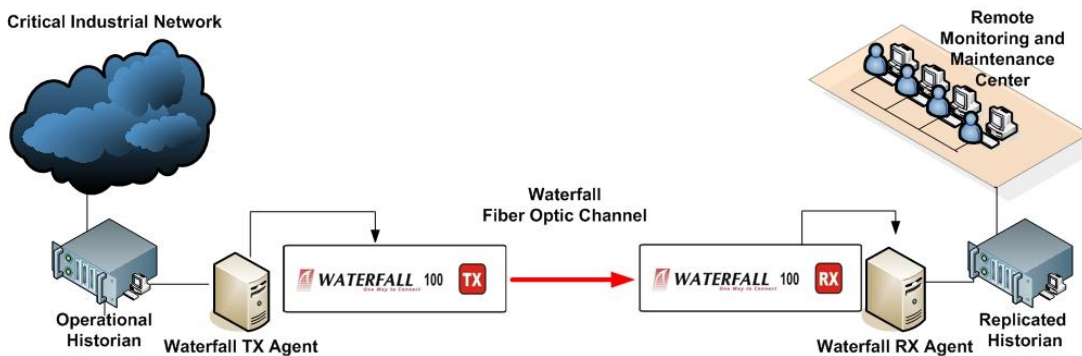


Figure 4 – Basic Historian replication via Waterfall One-Way™

Although all Historian data would be readily available to corporate users, external hackers cannot reach the operational Historian residing within the secure industrial network. Hackers may be able to impact the replica Historian, but the operational processes related to the critical operational Historian will continue unharmed.

Industrial Protocol Gateway using the Waterfall WF-SME

In this architecture, a Waterfall One-Way™ is used as a unidirectional gateway which enables extraction and export of messages, data and information from within industrial networks, *carried upon industrial protocols*, to external networks. This allows reuse of HMI displays and reporting services, within external or public networks, without the risk of command and control.

The following diagram shows a DNP3 unidirectional gateway utilizing the WF-SME for DNP3:

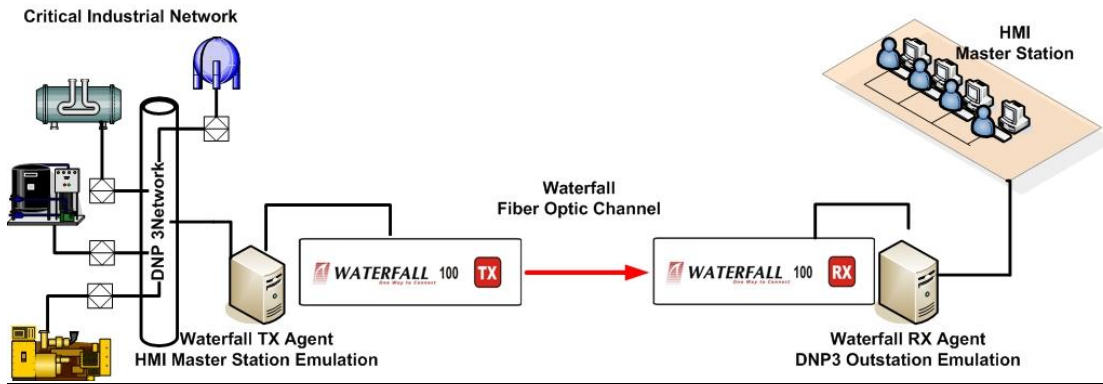


Figure 5 – Waterfall WF-SME as a DNP3 unidirectional protocol Gateway

Waterfall supports additional industrial protocols, such as Modbus, OPC, ICP and others, and performs custom development of protocol support according to specific customer requirements and requests.