WATERFALL
one way to connect

Waterfall Help NB Power Comply with NERC-CIP Standards

Case Study

NB Power' Challenges

NB Power's management recognized that their critical assets, within their industrial networks, are under the threat of cyber-attack attempts that may result in power outages, loss of revenue and other sorts of damages. Additionally, with the growing concern of the North-American government's authorities regarding the vulnerability of the electricity utilities and power plants, NB Power was challenged with the task of complying with the NERC-CIP standards and cyber security requirements.

Due to these threats and in order to comply with the NERC-CIP standards, NB Power decided to separate the industrial networks and the NB Power corporate network. Notwithstanding that, all business and operational applications, specifically the ICCP and OSIsoft PI application operation, must continue without any degradation to maintain the smooth operation and maintenance of the power stations.

"As cyber-attack risks increase and become more pertinent, it is evident that we need a solution that offers maximum level of security," says Greg Wright, NB Power's IT Specialist. "In addition, NB Power needed a security solution that will assist in compliance with North America Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards,"

Introduction

NB Power Generation (NB Power) supplies wholesale energy products in a competitive environment. Electricity is generated at 14 hydro, coal, oil, and diesel-powered stations, with an installed net capacity of 3,142 MW comprised of 1,724 MW of thermal, 893 of MW hydro and 525 MW of combustion turbine capacity. NB Power's industrial and corporate networks support several power generation plants as well as business offices, all with different business needs. Over these networks the OSIsoft PI™ application and ICCP are used for monitoring of the power stations.

The Solution

After much consideration and following a deep technical investigation, NB Power decided to implement several Waterfall Unidirectional Security Gateways at each plant. Waterfall's solutions for OSIsoft PI™ server replication and the ICCP SCADA protocol were deployed.

The Waterfall Unidirectional Security Gateway consists of a pair of Waterfall appliances (Waterfall TX appliance and Waterfall RX appliance) connected with fiber optic cord and WF Software Agents that reside on standard servers.

The Waterfall appliances provide the unidirectional data flow from each plant's industrial network to the NB Power corporate network. Reverse data flow from the corporate network to the industrial network, through the Waterfall appliances, is not physically possible thus ensuring the highest level of security of the industrial network. The Waterfall software agents communicate with the PI Server and ICCP Servers (accordingly) at each local network. The Waterfall for OSIsoft PI™ provides secure unidirectional, real time and foolproof replication of PI Server - PI tags, out of order data; edited archive data and tag configuration changes are replicated from a master PI server located on the critical industrial network to a replica PI server located at the corporate network.

NB Power Challenges

To comply with NERC CIP standards and protect their critical assets from cyber-attacks while retaining operational and business processes efficiency.

The Solution

NB Power deployed Waterfall Unidirectional Security Gateways supporting OSIsoft PI and ICCP protocol.
The Waterfall Unidirectional Security Gateways use hardware based unidirectional technology, supporting real time ICCP transfer and OSIsoft PI™ server replication from NB Powers industrial to corporate network.

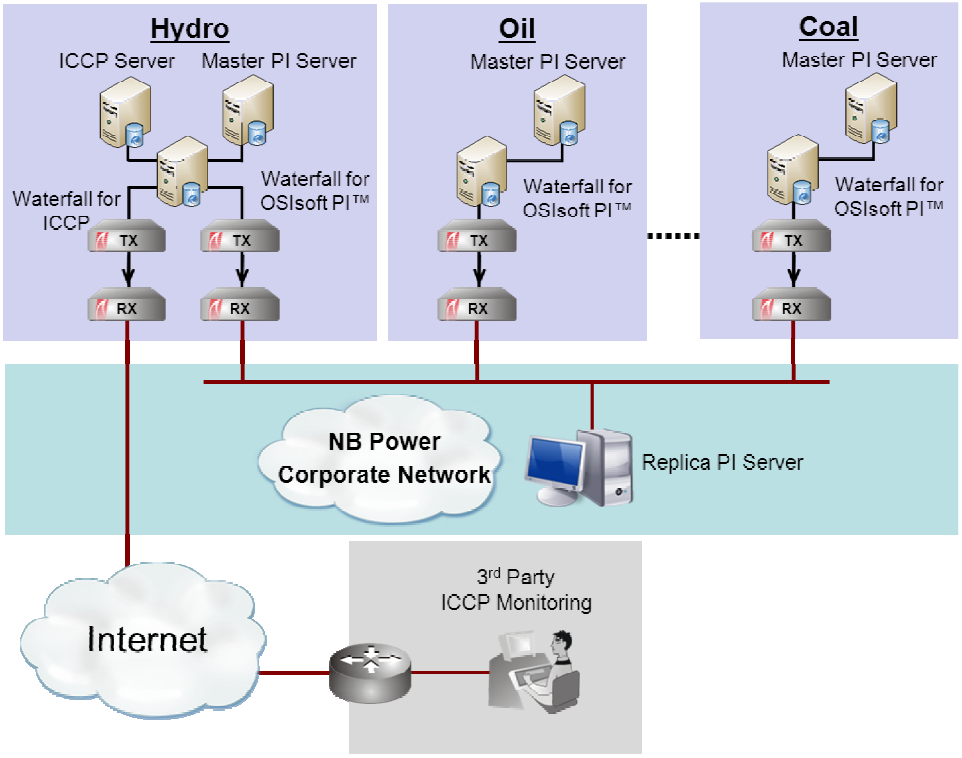
The Benefits

NERC Compliance
Assists NB Power to address the NERC-CIP compliance framework requirements.

Cyber Security
NB Power's critical assets are fully protected from any external cyber-attack or threat.

Operational
Unsurpassed performances of the OSIsoft PI application and ICCP protocol over the physically segregated networks.

The Waterfall for OSIsoft PI™ has been benchmarked for performance and manageability in collaboration with OSIsoft Inc. Waterfall and OSIsoft are official partners.
The Waterfall for ICCP securely transmits the ICCP protocol from the secured industrial network to the NB Power network. The Waterfall for ICCP supports ICCP blocks 1 to 7 (except block 5). It also supports ICCP auto discovery, thus enabling automatic configuration of tags (points) from existing systems.



NB Power Benefits

Implementing the Waterfall Unidirectional Security Gateway addressed NB Power network's security, regulatory and operational challenges.

- Integration of the Waterfall Unidirectional Security Gateways into NB Power's critical infrastructures played a significant part in the NERC-CIP compliance plan. It addresses the NERC compliance framework requirements by supplying high level of security at all layers of the networks' communications protocols, enforcing the Electronic Security Perimeter (ESP) in accordance with NERC-CIP requirements.
- The Waterfall Unidirectional Security Gateway provides physical separation between the industrial network and the corporate network. It ensures that any access to the industrial network is impossible thus providing the highest level of security eliminating any risks from external cyber-attacks or hacking and also human errors.
- NB Power's operation retains efficiency and a high operational level, as the Waterfall Unidirectional Security Gateway solution enables secure, high-throughput and real time access to the ICCP and PI information.
-

"Waterfall's technology fits perfectly into our overall regulatory compliance and cyber security planning,", Greg Wright, NB Power's IT Specialist, "Waterfall's Unidirectional Security Gateways have proven to be highly reliable and easily integrated into our existing networks. It is instrumental in helping us comply with the NERC-CIP standards and secure our critical assets against any type of external cyber-attack or hacking threats"