Offshore Oil and Gas Platform: Cyber Security Implementation

Case Study #301
CS-301
Version 1.0

Customer Application

An oil and gas production company operates a **fixed natural gas and oil gathering and processing platform** located in deep water on the US continental shelf. The platform serves multiple natural gas and oil wells connected by pipes running along the seabed back to the platform. The facility was designed to handle a high volume, thus there is a strong emphasis on reliability. Any downtime, whether caused by accidental or malicious forces, would interrupt oil and gas production and be very costly.

Figure 1: Natural Gas and Oil Processing Platform

Project: Improve Reliability, Security and Availability

The production company presented Cimation, a Tofino Certified System Integrator, with the challenge of maximizing the reliability and uptime of the platform. They also opened the door for Cimation to recommend industry best practices.

Challenges

To kick off the project, the customer tasked Cimation with a broad range of objectives:

- A higher-than-average emphasis on Security, Safety and Reliability, including cyber security.
- To address the lack of internal automation / SCADA best practices at the facility.
- A requirement for extensive documentation of the installation, down to the level of training manuals.
- The need to test as much of the system as possible in the office, before installation offshore.
- A microwave communications hub which needed to be relocated twice (with minimal interruption) during the facility upgrade.

The job of the integrator was to design and install SCADA, business, security and third party equipment and networks, while addressing all the challenges noted above.

Security Requirements

Many offshore facilities do not produce enough oil or gas, or do not have a large crew living on board, and thus avoid MTSA (Maritime Transportation Security Act) regulation.

However, this particular platform was large enough to fall under the MTSA regulation. This meant that the level of security was significantly more stringent on this platform than on many others. As well, due to the large production volumes, TWIC® (Transportation Worker Identity Credential) compliance was also a requirement.

Physical security included card readers, closed circuit TV and local/remote monitoring. The customer wanted to extend these measures to include cyber security.

The Control Systems

The facility interconnects a large quantity of Programmable Logic Controllers (PLCs), instrumentation, 'smart' automated equipment, and packaged process control equipment. It also has a very high I/O count. The combined size and complexity of the system could have been a significant burden if not properly planned and executed.

In addition, the platform communicates with subsea systems and virtual flow meters using the OPC Classic protocol. Consequently, there was the potential for large amounts of network traffic and crosstalk.

Some of the automation controllers deployed on the platform used a UDP broadcast/multicast protocol, which further increases the volume of network traffic. Since many automation and control devices cannot filter out extraneous network messages, it was necessary to protect those devices from excessive traffic.

The Customer's Security Philosophy

The client looked to Cimation to define an aggressive security philosophy which would minimize the possibility of unintended network or automation system shutdowns.

Cimation developed a "Defense in Depth" network architecture, in accordance with ANSI / ISA 99 Standards and the Department of Homeland Security guidelines. This architecture isolated layers of the business and process control network, using routers and firewall

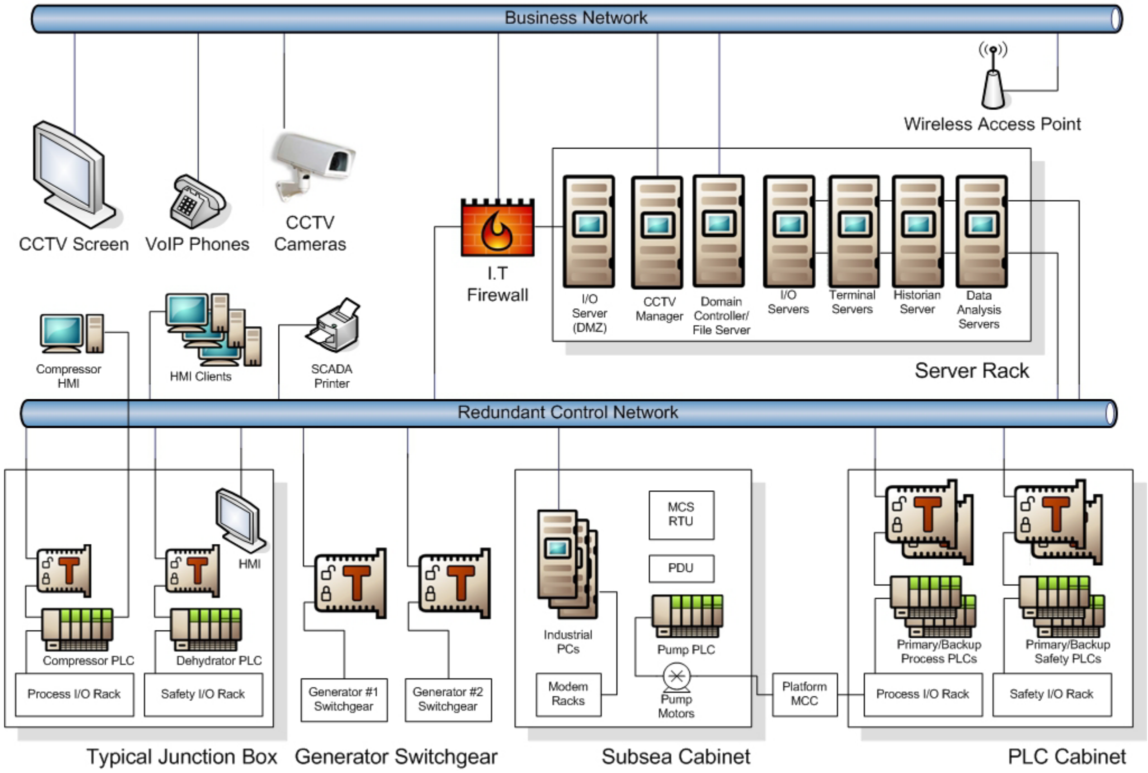


Figure 2: Simplified Network Diagram of the Installation

represents a Tofino Security Appliance

appliances to permit only the minimum traffic that was necessary between these layers.

The Cyber Security Solution

The network on the platform spans across business, operations and safety systems. As is common on offshore facilities, a wireless backbone connects back to the office and control facilities "on the beach".

To protect the facility, a perimeter firewall was used along with a Defense in Depth approach for operational systems. The automation and business networks were isolated using managed switches and logical network segregation. Demilitarized Zones (DMZ) were used to protect the process control system from the Internet and from the business network.

The PLCs shown in the Figure 2 network diagram, as well as switchgear and various packaged process units, were protected with Tofino SAs loaded with the SCADA specific Tofino Firewall module. Only the necessary operating protocols were allowed through the firewalls based on a data exchange strategy.

Eric Byres, CTO of Tofino Security:

"To effectively secure a facility today Defense in Depth principles must be applied. In this case Cimation did a very good job of isolating the business layers and the process control layers.

Then the control devices and systems were individually and collectively hardened using Tofino products. The result was that only necessary traffic moved between layers, resulting in high security, reliability and availability."

The Tofino Industrial Security Solution

The Tofino Security product line was selected because:

- The Tofino Security Appliances can be DIN rail mounted, the standard for offshore industrial cabinets.
- It is rated for Class 1, Division 2 hazardous areas (important on offshore facilities) – Not available for all Tofino models.
- It has a Central Management software platform with automation-specific, configurable loadable security modules.
- The solution is simple to install and operate by operations and maintenance staff.

Redundant Communications and Security

Redundant Tofino Security Appliances (Tofino SAs) were installed in front of redundant Allen-Bradley Controllogix PLCs. The Tofino SAs were configured and tested to assure that the failover of the primary PLC processor to the backup processer would not impact control communications. In turn the Tofino SAs needed to maintain their security functionality regardless of the switchover state of the PLCs.

In total, twelve Tofino SAs were used at various locations on the platform. All were loaded with the Tofino Firewall Loadable Security Module. The Tofino Central Management Platform, which manages all of the Tofino SAs from a central location, was installed on a server in the facility.

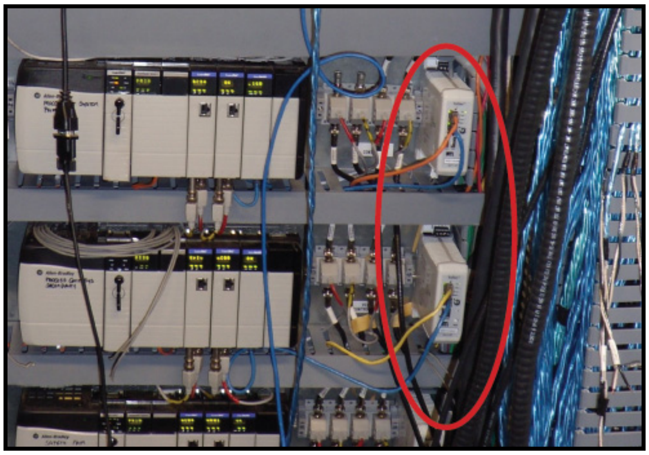


Figure 3: Installed Tofino Security Appliances

Offshore Oil and Gas Platform: Cyber Security Implementation

Case Study #301
CS-301
Version 1.0

Implementation Challenges

As with many IT devices deployed into an automation environment, a challenge on the project was the perception that firewalls make the job of operations and maintenance more difficult. Some staff had a 'knee jerk' reaction to blame the firewalls any time there were network or communications problems. With a thorough testing regime, Cimation proved that the proper protocols were enabled to accommodate all operations.

"Hidden" devices, that is, hardware which were necessary for facility operation, but which contractors neglected to include in the network planning process, also posed a challenge.

Offshore platform builds typically involve a myriad of contractors working on inter-related systems. At one point the network was exposed to a computer virus from an unwitting contractor, likely using an infected USB drive. The Tofino firewalls limited the spread of this malware traffic and protected the core PLCs and safety systems.

Subsequently, Cimation led the remediation effort which included cleaning systems of the virus and then locking down USB ports. They also implemented a strict policy preventing vendors from using their own laptops on the facility network.

Outcomes

Cimation provided the client with a complete "turnkey" industrial IT solution including network design, physical and cyber security design, installation, configuration and hardening of security appliances.

The cyber security solution, utilizing the Tofino Industrial Security Solution, has been in operation for 4 years and the result has been increased reliability and availability on this major oil and gas platform.

TOFINO SECURITY

TELEPHONE: +1 250 390 1333
TOLL FREE: 1 877 297 3799 (N. America)
EMAIL: sales@tofinosecurity.com

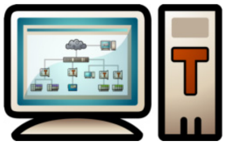
Product Details

Tofino Security Appliance

- Hardware platform for creating Plug-n-Protect™ zones of security within control and SCADA networks
- Installed without pre-configuration, network changes or plant downtime

Tofino Firewall LSM

- Firewall software for operational systems
- Traffic rules are easy-to-define for > 60 protocols
- Unique "Test Mode" allows firewall testing with no risk to operations



Tofino Central Management Platform

- Management software for configuring and monitoring all Tofino Security Appliances from one workstation or server

About Tofino Security

Tofino® Security provides practical and effective industrial network security and SCADA security products that are simple to implement and that do not require plant shutdowns.

Tofino Security is part of Belden® Hirschmann™

www.tofinosecurity.com, www.belden.com

About Cimation

Cimation delivers total automation, Enterprise Data, and industrial IT solutions for the energy sector. By taking a client-first approach, Cimation ensures the entire project lifecycle will improve safety, operational reliability, and efficiency.

Cimation is a Tofino Certified System Integrator.
www.cimation.com

Cimation Innovation Beyond Automation

TOFINO®