OWL Cyber Defense

WHITE PAPER

Cybersecurity Solutions For The Digital Oil Field

Table of Contents

Cybersecurity Solutions for the Digital Oil Field

OVERVIEW

Upstream oil and gas companies rely on highly connected data and control systems to facilitate exploration, drilling, system monitoring and to optimize production from onshore and offshore resources. As their dependence on IT technology has grown, so too has their vulnerability to cyber-attack. The implementation of IT technologies that enables increased operational efficiencies also creates channels by which hackers can penetrate control networks and disrupt operations, steal data or attempt to cause physical damage to plant infrastructure and the surrounding environment.

Oil and gas production is a vital component of the world's economy and is increasingly becoming a prized target of cyber-attack. The often cited Stuxnet virus was the first of a new class of attacking viruses designed to take over control systems, cause significant disruption to operations and cause physical damage. Critical infrastructure operators are currently faced with the dilemma of either isolating their control systems and losing access to vital operational data or remaining connected and risking cyber-attack. A third option, long used by the U.S. intelligence community, Department of Defense and nuclear power plants as an integral part of their defense in depth strategy, is deploying data diode technology.

This paper focuses on the implementation of data diode technology to:

- Secure upstream oil and gas digital assets
- Defend digital systems from external penetration and malware insertion
- Enable the transfer of valuable OT data for remote monitoring, management and system support

Digital Oil Field

The deployment of IT technology has created a highly connected upstream oil and gas production ecosystem known as the Digital Oilfield. This cross vendor IT ecosystem creates an efficient and highly integrated infrastructure supporting exploration, drilling operations and production monitoring and control.

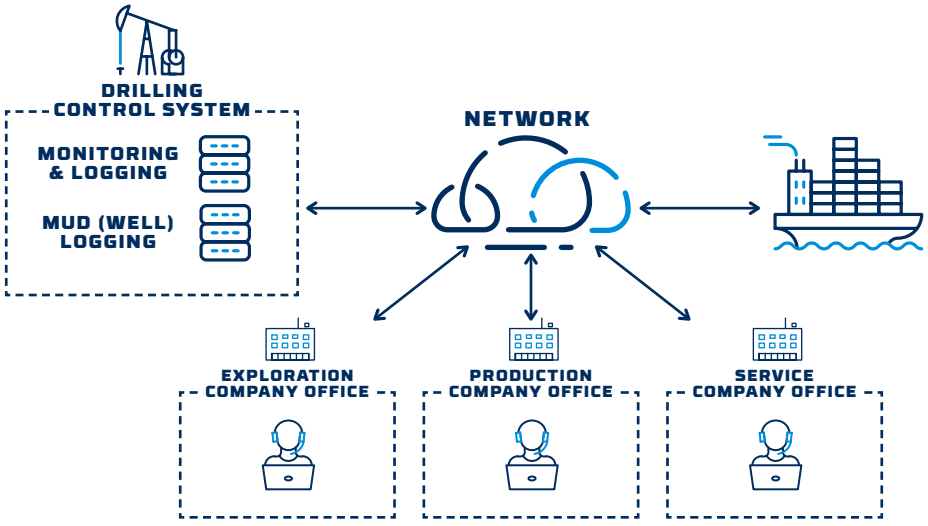


FIGURE 1: DIGITAL OIL FIELD CONCEPT ARCHITECTURE

Figure 1 *above depicts a high level representation of the Digital Oilfield architecture connecting exploration, drilling and recovery assets to back office resources and support systems. The economic advantage of investing in IT technology spans all stages of the upstream oil and gas lifecycle.*

+ New Operating Model and Workflow

Advanced IT technology is being applied to optimize production and extend the life of existing field assets, reduce operating costs and to enhance oil recovery. It supports continued improvement in decision making and operational effectiveness, operator safety, and the management of regulatory and environmental requirements through effective system monitoring and reporting. In addition, the technology addresses knowledge sharing and collaboration by integrating the various functional partners and operating companies involved throughout the process.

The implementation of Digital Oilfield technologies supports readily available information exchange between remote field assets and centralized management and support resources. Resulting improvements in upstream oil and gas workflow enabled by Digital Oilfield technology includes:

- **Real-Time Recovery Operation Control** – *Control of remote oil and gas recovery operations through monitoring and control of SCADA systems and facility environmental control systems*
- **Production Volume Management** – *Production data shared in real time between centralized and onsite resources creating more efficient control of production output*
- **Intelligent Wireless Wellheads** – *Wellheads equipped with wireless sensor networks allow remote monitoring of critical operation data and supports remote command and control, significantly reducing installation and operational cost*
- **Monitoring of Real-Time Drilling Data** – *Drill RPM, well pressure and other vital drilling data is collected and shared in real time enabling effective collaboration of onsite and remote resources*
- **Remote Visualization of Seismic Data** – *Centralized 4-D visualization of field captured seismic data drives efficiencies in field exploration*
- **System Status, Alarms and Event Monitoring** – *Centrally located support resources monitor unmanned or lightly manned field installations*

In each case, making real-time remote data available to centrally-located, skilled resources is essential to realizing productivity gains. Operational decisions, command and control, cross vendor information sharing and system maintenance and updates are cost effectively managed by centrally-deployed skilled resources, either independently or in close collaboration with onsite resources. While the economic advantages enabled by the Digital Oilfield are indisputable, so too is the increased risk of cyber-attack.

+ Vulnerability to Cyber Threats

According to Ernst & Young, *"Most oil and gas companies don't have high enough network security standards. This is demonstrated by the rising incidents of external cyber-attacks. Some companies in the industry don't even have a formal security framework in place."* This is also true for oil exploration companies as hackers are being hired for corporate espionage that targets confidential data. All upstream oil and gas assets are at risk of cyber-attack.

New viruses are designed to target and affect control systems, not just business IT. They are designed to penetrate traditional firewall enforced security networks and take over programmable logic controllers that control pumps, motors, valves, and other critical assets. Stuxnet and other similarly designed viruses penetrate process control systems and alter system operations while spoofing monitoring systems by presenting data that indicates normal operating conditions.

Other viruses meant for intelligence gathering propagate themselves into systems without any immediately noticeable affects. They remain undetected while collecting data, eventually connecting with its source to transmit the collected data. These viruses can also corrupt targeted files making them unrecoverable, and can act as a time bomb, creating a denial of service attack at a predetermined time.

Further complicating cyber security is the growing dependence on oil and gas employees to use their own mobile devices to connect to their company's network. Infected thumb drives and other PMDs are carried across security boundaries. Viruses can be inadvertently uploaded to critical infrastructure the moment the device is connected.

Upstream oil and gas companies require cyber security solutions that don't hinder the productivity gains achieved by the Digital Oilfield architecture while enforcing a security perimeter around critical exploration, drilling and recovery assets. They also need to secure trade secrets while making information available to trade partners and subcontractors.

+ Defense in Depth Strategy

Managers assigned to protect critical infrastructure are developing and deploying defense in depth security strategies to protect their systems and facilities from cyber threats. The term “defense in depth” refers to a comprehensive security strategy that utilizes a layered security architecture designed to block or, at a minimum, impede the propagation of threats. The basic idea behind defense in depth strategy is applying multiple layers of defense to protect information and control systems from both outside originated and insider threats, assuring a high degree of system availability and data integrity.

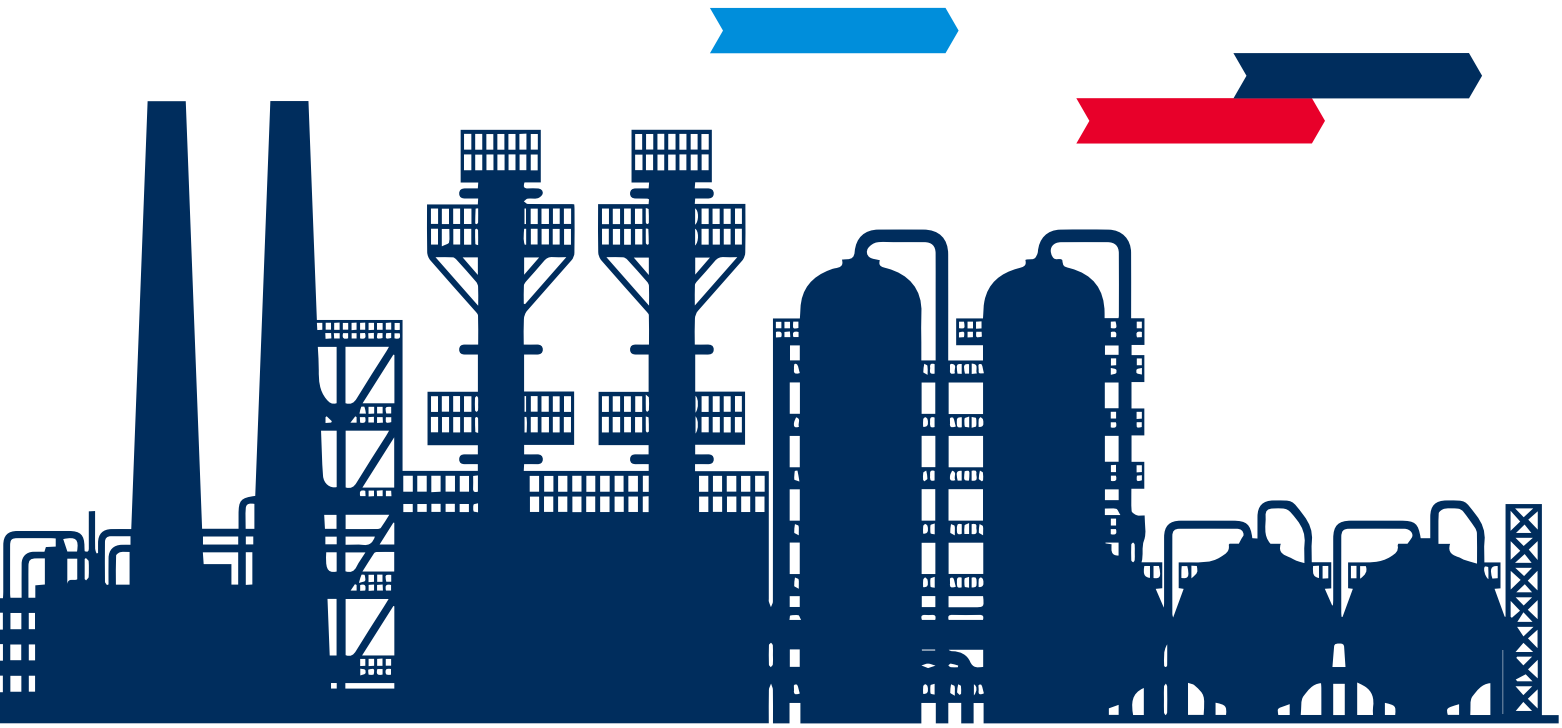
In critical infrastructure such as nuclear power plants, the industrial control network (ICN) is isolated from the business network, creating distinct security enclaves. At the boundary, an appropriate security device is positioned to protect the ICN while enabling managers to monitor the network at every level. Such network protection devices are required to create a security perimeter, provide additional enforcement points and segment the network for fault containment.

Increasingly, data diodes are seen as the preferred network protection device. In the nuclear power industry, deploying data diodes to secure the critical control systems is mandated by the NRC. Data Diodes provide the most effective enforcement of the electronic security perimeter, protecting critical assets while allowing real time control system data, system alarms, operations information and surveillance data to be securely transferred to centralized management and support resources.

Data Diode Cybersecurity

Data diode technology is a hardware-enforced, highly reliable communication link that enforces security at the physical and protocol layer. Among other advantages, data diodes deny the possibility of network probing for vulnerabilities, a prelude to cyber-attacks. When a one-way data transfer security policy is rendered in hardware, it is physically impossible to send messages of any kind in the reverse direction. Physical one-way links cannot be hacked with software and are used by the U.S. Department of Defense (DoD) and intelligence community (IC) for isolating their high-security networks.

The US National Institute of Standards and Technology (NIST) provide a specific security control (AC-4.7) that describes hardware-enforced, one-way information flow control as a threat-mitigation method.



+ Owl Cyber Defense's Data Diode Hardware

Owl's DualDiode hardware comprises a pair of one-way communication cards that are specifically engineered to transfer data in one direction only. The Send-Only card is installed in the Send Host Server platform and the Receive-Only card is installed in the Receive Host Server platform as shown below in Figure 2. The two cards (and the two platforms) communicate through a single optical fiber that connects the communication cards.

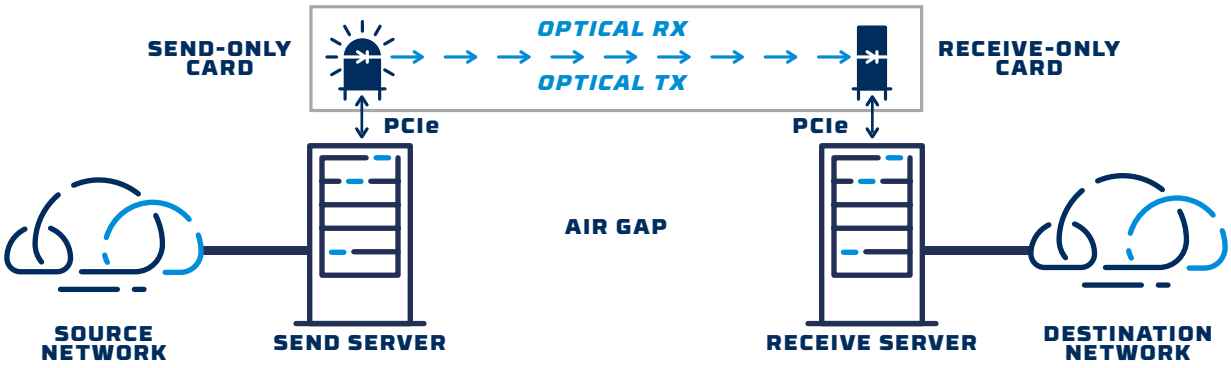


FIGURE 2: DATA DIODE CARD CONFIGURATION

Once cards are installed in their respective host servers, the servers operate as Send and Receive communication gateways for their respective networks. Send and Receive gateway platforms may be packaged in a single 1U rack-mount enclosure as shown below in Figure 3.

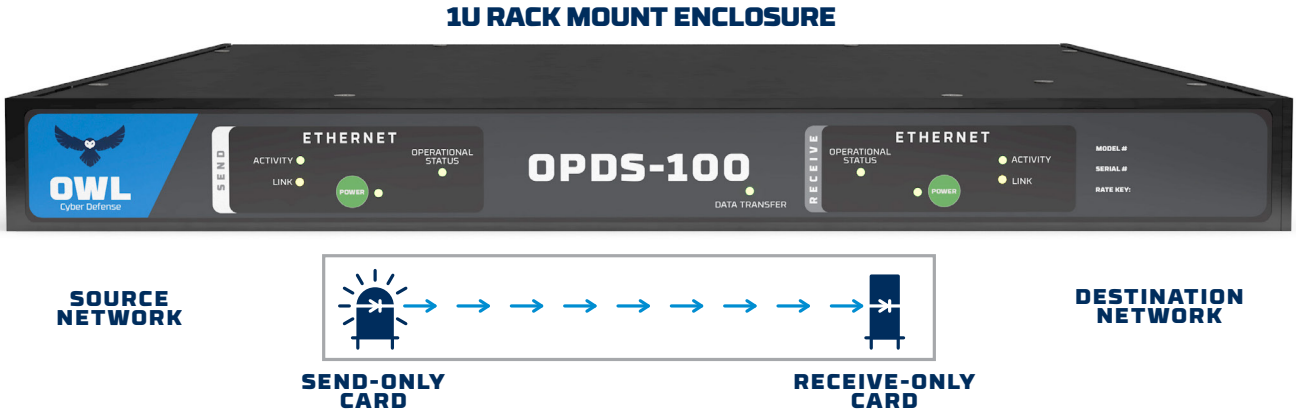


FIGURE 3: SMALL FORM FACTOR DATA DIODE AND SERVER PACKAGE

Note that the Data Diode solution comprises a hardware architecture that contains two diodes and a clear network boundary located between the diodes. Should one diode fail, the other will be unable to pass any kind of data, including malicious data; the networks remain isolated.

+ Hardware Enforced Dual Path ReCon Solution

In most implementations, data diodes are deployed to protect a high security environment while simultaneously transferring critical operational data to a remote facility. However, uses cases arise where receiving monitoring and other data from within the protected environment isn't enough to satisfy operational requirements; sometimes support staff need remote access. For these cases, Owl provides a dual, one-way path solution called ReCon that allows highly restricted round-trip communication. The send path and receive path maintain complete autonomy and are configured to only support a single application using white listing. Per Department of Homeland Security recommendations, all other ports are locked down only allowing a single data path.

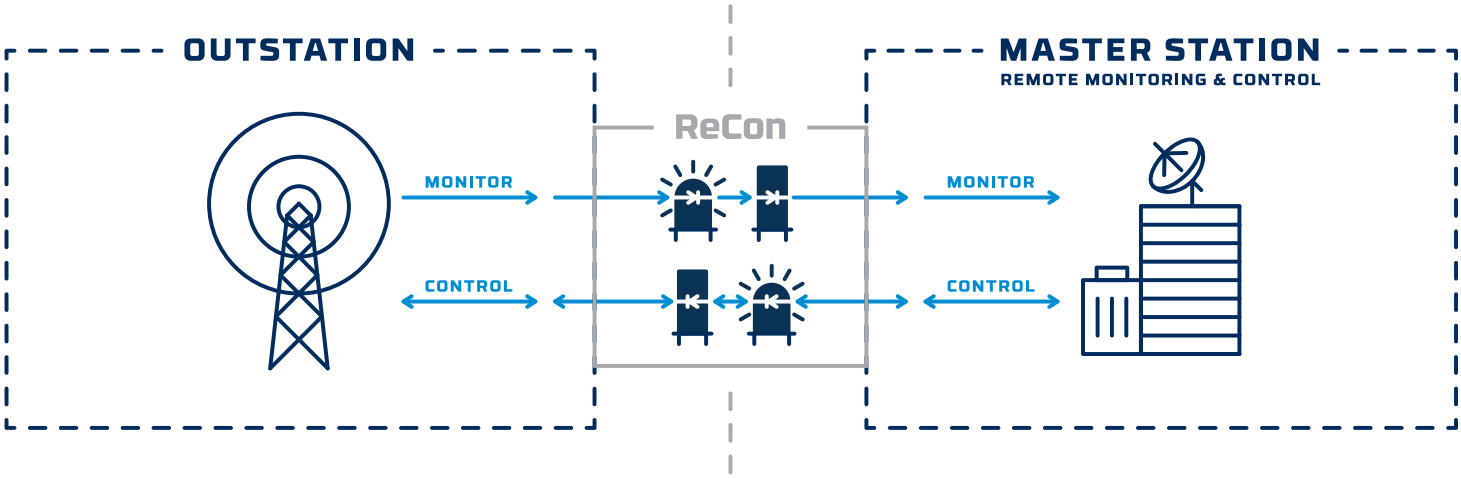
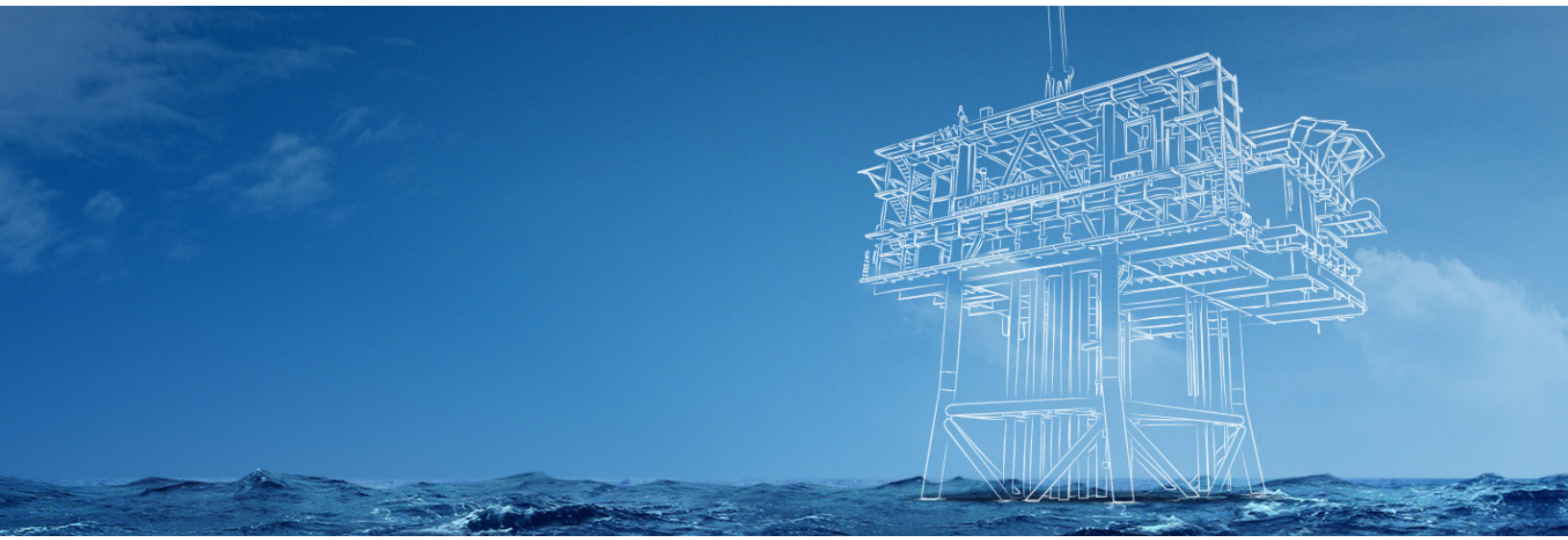


FIGURE 4: DUAL PATH DATA DIODE

The data diode solution shown in Figure 4 utilizes two independent one-way paths, enforced in hardware, with defense-indepth security at the protocol layer. The "non-routable" protocol break, effectively disables any protocol which attempts to communicate over the data diode, protecting the network from being probed by hackers.

Reference Architectures

The upstream oil sector, also commonly known as the exploration and production (E&P) sector includes the searching for potential underground or underwater crude oil and natural gas fields, drilling of exploratory wells, and the subsequent drilling and recovery operation needed to bring the crude oil and/or raw natural gas to the surface. In addition, the transportation of recovered oil and gas to storage facilities and refineries is considered part of the upstream ecosystem.



+ Exploration

Oil exploration companies use a method called reflection seismology to explore and estimate the properties of the earth's subsurface to find oil and gas reserves and to determine their potential. In digitally-connected exploration, seismic exploration datasets that can reach several terabytes in size need to be securely transferred to the exploration company's corporate office. 3D or 4D (time elapsed) images of the subsurface are created and analyzed by corporate resources who instruct field resources of their analysis.

In order to reduce analysis turnaround time, maximize productivity and lower operating costs, high bandwidth networks are deployed to eliminate the need to ship physical media between field sites and corporate office. However, the data is now more exposed to corporate or state-sponsored cyber Ttheft which will undermine the exploration firm's investment and future revenues.

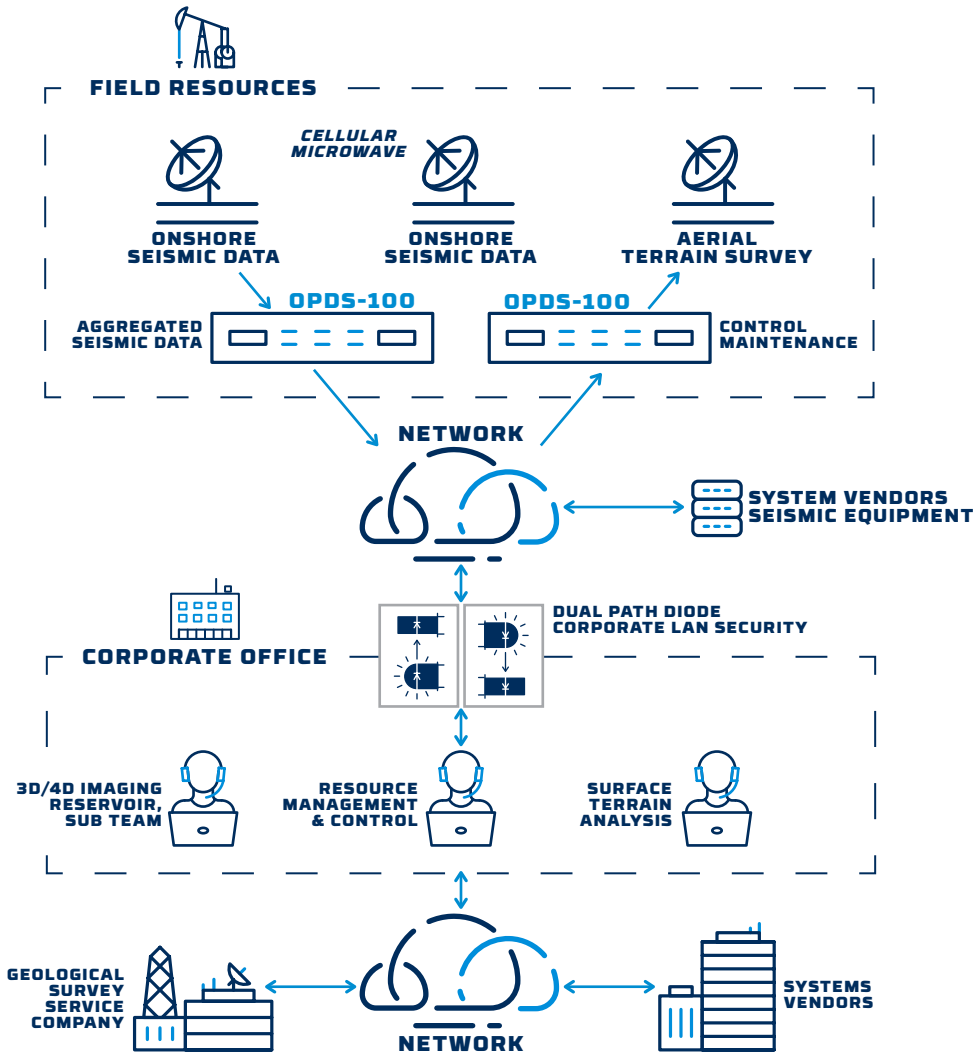


FIGURE 5: EXPLORATION

Owl's highly scalable, dual path diode technology shown above completely isolates exploration and corporate resources from cyber-attack while maintaining the real time flow of data between field seismic data collection points and centralized analysis resources. With transfer rates exceeding 20 Gbps, Owl's DualDiode platform can be installed at seismic data aggregation points and securely transfer high volumes of data between the field and corporate 3D/4D imaging and analysis centers. Owl's DualDiode Technology™ can also securely transfer command and control information back to field resources.

+ Drilling and Oil/Gas Production Operations

Both onshore and offshore oil drilling have become highly specialized, integrating the latest technology from multiple vendors to control and monitor all vital aspects of the drilling operation and supporting systems. Real time well data, drilling equipment data, and geological data are monitored onsite and/or from remote offices located anywhere in the world.

During the production operation phase, SCADA systems control the oil and gas recovery from onshore or offshore wells. Raw output is separated into oil and gas while extracted water is treated before being expelled back into the environment.

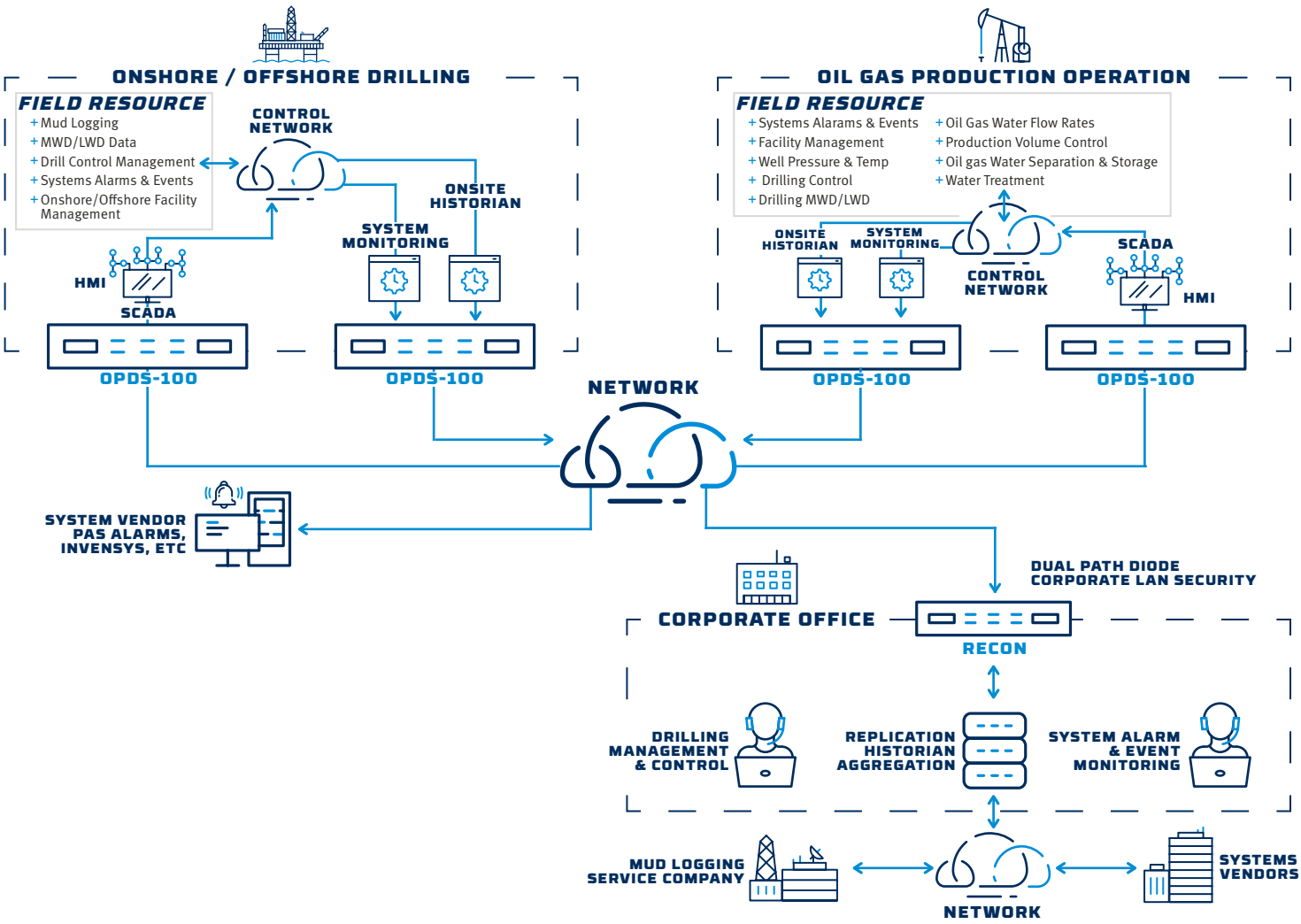


FIGURE 6: DRILLING AND PRODUCTION OPERATIONS

The architecture depicted in Figure 6 is optimal for managing drilling and production operations. The diagram shows the application of Data Diodes to protect field assets and the corporate network.

Owl's patented DualDiode Technology™ deployed as shown in Figure 6 addresses attacks originating from both outside and inside the secure network. Owl's Perimeter Defense platforms can be optioned to support OPC data transfer, OSIsoft PI and other historian connectors, thus enabling the real-time replication of process control points across an electronic security perimeter. The historian databases deployed in the field are secured and the flow of real-time drilling data to the control centers is preserved.

Owl's DualDiode platform also securely aggregates and transfers system logs, alarms and event data so remote monitoring centers can monitor and respond to issues in real time. Data can also be segmented allowing equipment vendors to securely monitor the equipment they supplied.

As with all critical infrastructure environments, data files such as software patches need to be securely moved from lower security business domains into the higher security drilling or recovery operations domain. Owl's Secure Software Update Solution (SSUS) was designed specifically to address this need. SSUS supports establishing security policies for moving information and system software updates into higher security domains, and controls the movement of data based on established policies. Data files and software patches are scanned, ensuring they are virus free before they are released for system upgrades. SSUS can eliminate or greatly reduce the need to use portable mobile devices (PMD) to manually carry files into the higher security domain, thereby reducing recurring costs associated with securing mobile devices.

Owl's technology also addresses the growing threat from insider attacks. Owl's DIN rail based DualDiode platforms which are used to isolate subnets and prevent the propagation of viruses introduced by on site resources through their personal or corporate issued PMDs.

Many production sites are unmanned. Monitoring and control of those sites are performed by centralized resources at corporate locations. As shown in Figure 6, Owl's Dual Diode technology can be deployed at both the production site and corporate network boundary to effectively secure the real time flow of vital information from production sites and also secure command and control data originating from centralized corporate resources.

+ Oil & Gas Distribution

Upstream oil and gas distribution spans thousands of miles of pipelines, connecting drilling rigs to crude oil and gas storage facilities and refineries. In order to efficiently monitor and control pipelines, the pipeline is segmented into manageable zones and each zone is controlled by a SCADA system. Each zone SCADA system monitors and controls several hundred remote terminal units (RTUs) that measure pressure, temperature, and pipeline flow rates as well as control the valves and pumps located along the entire length of the pipeline. RTUs communicate with the zone SCADA systems over wired or wireless wide area networks.

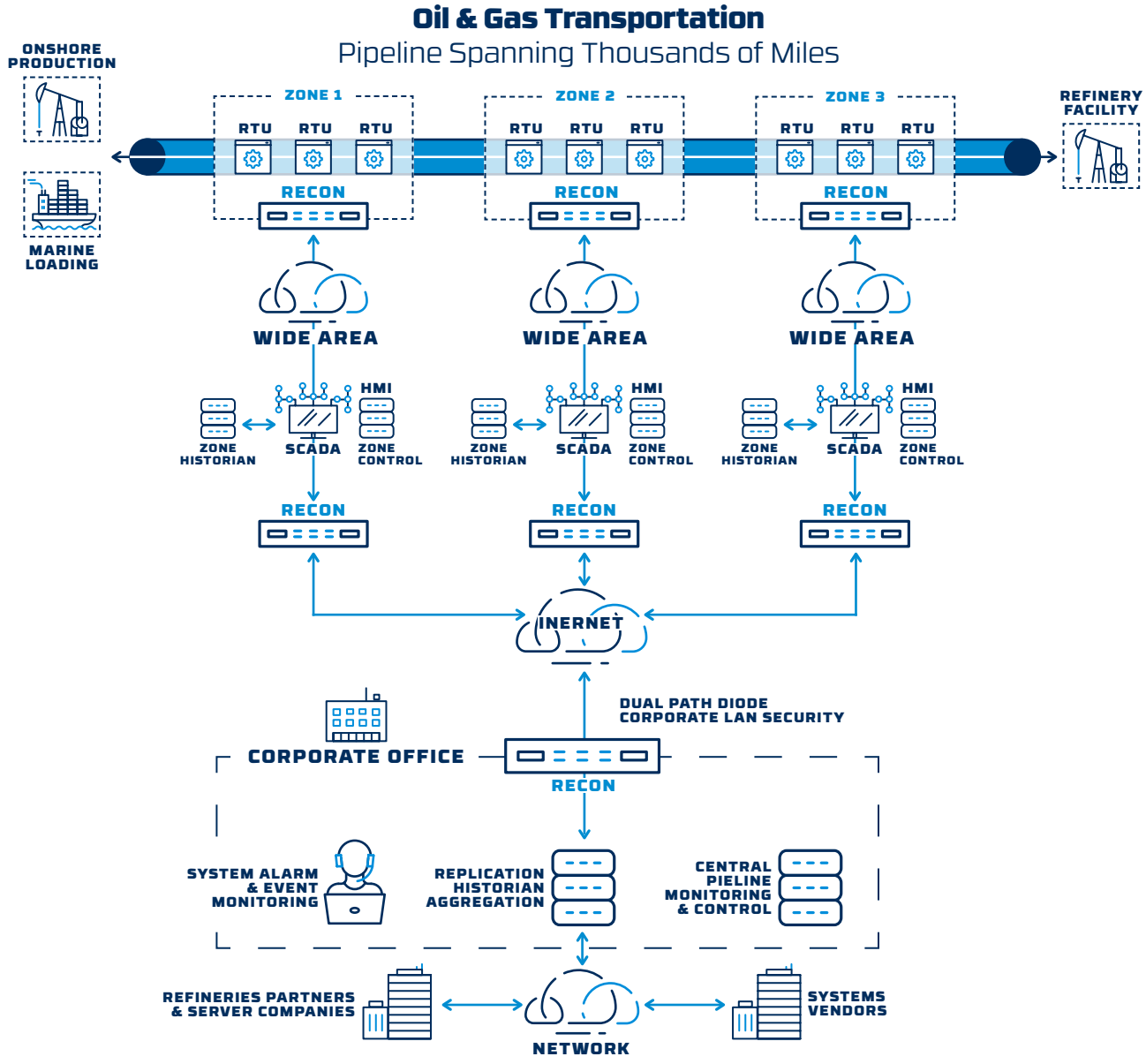


FIGURE 7: TRANSPORTATION

The entire pipeline is monitored from a central office, allowing remote and centrally located resources to collaborate on pipeline control and maintenance.

Owl's ReCon data diode solution prevents hackers from attacking RTUs, SCADA systems or historian databases while supporting remote command and control within each zone. Easy to deploy and interoperable with a number of OEM SCADA and historian solutions, ReCon supports real time replication of historian data between pipeline zones and the centralized historian. Whether originating within a zone-based SCADA system or from corporate based resources, every system along the pipeline is completely protected from cyber threats.

Implementing Perimeter Defense

+ System Monitoring, Alarms & Events

Both onshore and offshore exploration, drilling and production assets require real time monitoring of system status in order to ensure systems are operating efficiently and within operational guidelines. Remote monitoring of control systems deployed at upstream oil and gas assets yield significant economic advantage as it allows support staff to be centrally located and shared across many assets. It has the added advantage of reducing or completely eliminating support staff from being located near potentially hazardous operating environments.

The advantages remote system monitoring provides can and most likely will be negated if the network design does not consider cyber threats. Real-time access to remote system log files, syslog messages and application alarms and events require a secure link that cannot be penetrated by hackers.

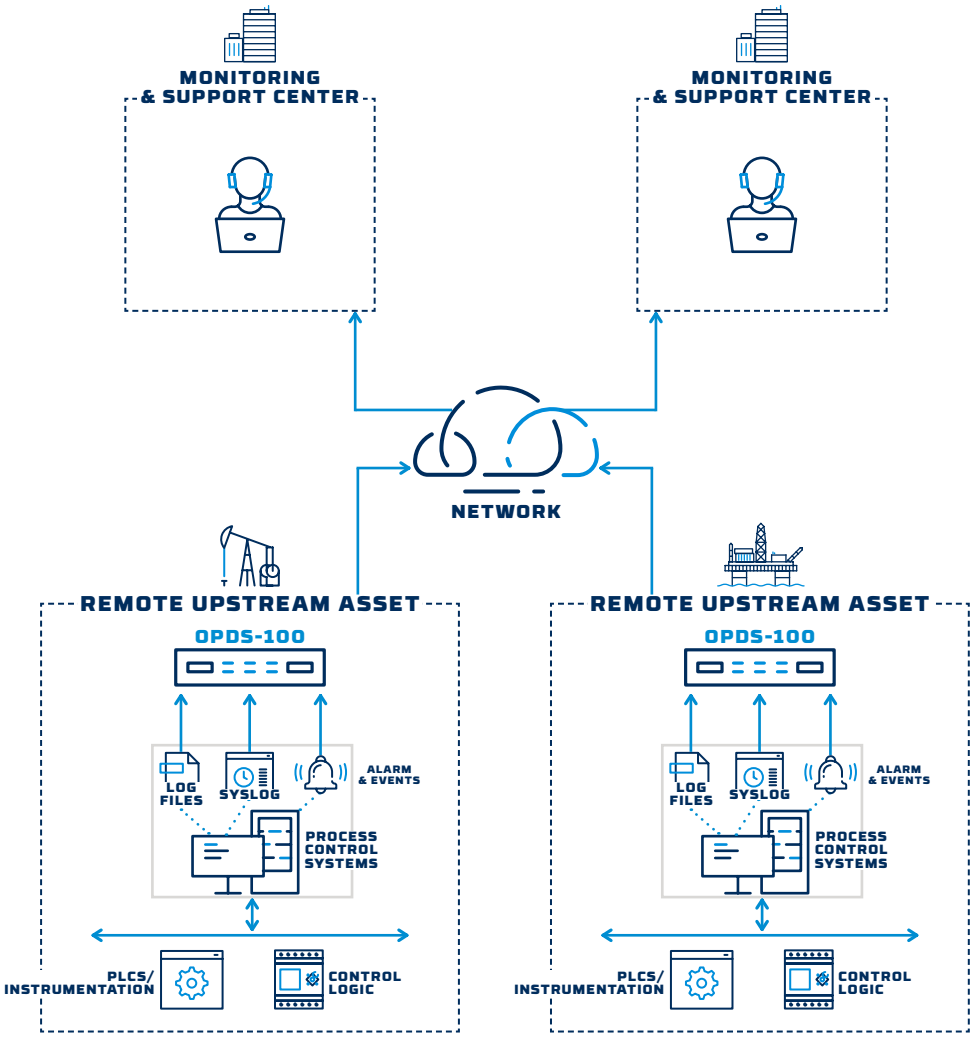


FIGURE 8: SECURE MONITORING OF REMOTE ASSETS

Referring to Figure 8, secure remote monitoring is accomplished using Owl's data diode platform. Each platform can aggregate multiple streams of system and application level alarms and event data, and securely route the alarm and event data to multiple monitoring centers. A single Owl data diode platform can be configured to simultaneously transfer system log files, syslog messages, industry standard alarm and event messages, such as OPC A&E and PAS Alarms, as well as vendor-specific proprietary messages.

In addition, Owl Virtual Screen View Service is a software application that can collect real-time screen images from monitored computer platforms within a remote asset and deliver the images to client platforms at the monitoring and support centers. Secure one-way transfer of screen content enables remote support staff to either independently, or in close collaboration with onsite resources, monitor system activity, troubleshoot issues, and recommend process changes.

In addition to system alarm and event monitoring, video data can be securely transferred across the DualDiode to remote monitoring and support centers. Secure remote monitoring can be applied to physical plant video surveillance systems, preventing hackers from compromising surveillance systems.

+ Minimal Maintenance Requirements

Data diodes provide a cybersecurity solution that requires virtually no maintenance in the field. With IT and OT support resources being extremely scarce or non-existent in the field, data diodes are pre-configured for specific data flows and then once deployed need no further updates or configuration changes. Unlike firewalls and other software-based solutions, hardware-based data diodes do not require any recurring updates or changes to keep them operating securely at full capacity.

+ "Defense in Depth" - Protecting Subnets

Network perimeter defense based on Owl's data diode Technology effectively eliminates cyber threats origination from outside the critical infrastructure. However, insider threats launched by a disgruntled employee or inadvertently carried in to the secure network by an employee's portable device can be just as detrimental. Effective protection against cyberattack requires a "Defense in Depth" strategy. System protection must be composed of multiple security layers. If one layer is compromised, the next layer will protect critical assets from the virus.

Upstream oil and gas assets require a security solution based on "Defense in Depth" principles. It is important that critical assets are secured at the network perimeter from outside attacks and additional security measure are implemented within the critical infrastructure to prevent the propagation of threats originating from within.

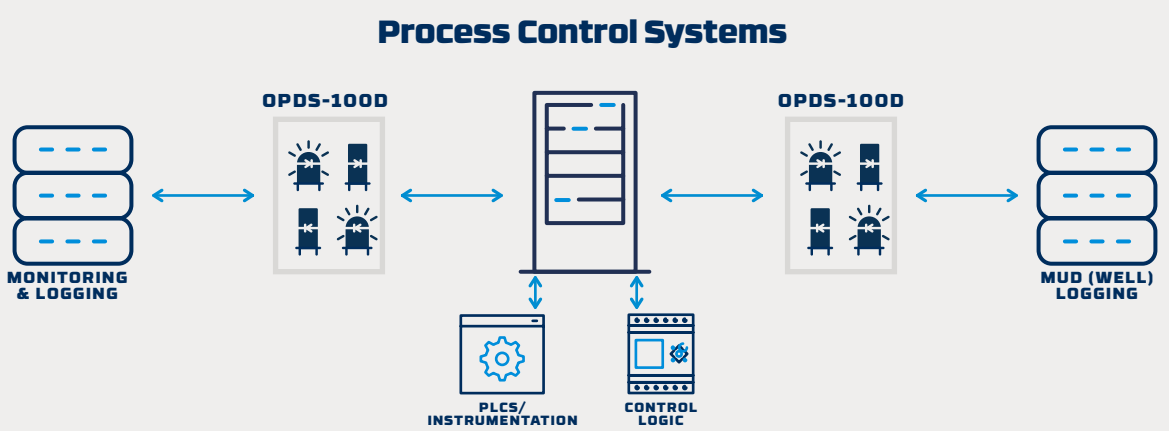


FIGURE 9: Dual Path Data Diode Protects Critical Asset Subnets

Referring to Figure 9, the components of a critical asset network can be logically grouped based on function and physical proximity to subnets. Subnets are created as a way to partition networks into logical segments for greater ease of administration. Installing Owl's dual path DIN rail solution between subnets provides the needed isolation, completely eliminating any possibility of a virus propagating throughout the critical asset. As with the Perimeter Defense platform, Owl's DIN rail solutions are scalable and support a wide range of applications. The ruggedized, DIN rail enclosures make them simple to install and reliable even in the most demanding operating environments.

Secure Software Patch and Maintenance Updates

Equipment used in all phases of upstream oil and gas operations need to be maintained and keep current with the latest software releases. In addition, electronic documents are transferred from the corporate network to the field exploration and operation sites. This necessary flow of data back to field exploration and operation sites creates vulnerability to cyber-attack, even if the network is disconnected and updates are physically moved using portable media.

Owl has developed the Secure Software Update Solution (SSUS) specifically to address this threat vector. Files originating from the corporate network (or from any location outside the secure ICN) are thoroughly examined before they are transferred across an Owl DualDiode enforced electronic security perimeter. With Owl's SSUS, executable and data files are individually validated against administrator definable scan sets which can include any or all of the following:

- A manifest (or white list) consisting of pre-configured hash numbers, or signatures, held within the platform
- Anti-malware scanning with the option of running multiple anti-malware scan on a file
- File type check where only a preapproved file types can be transferred
- File size check

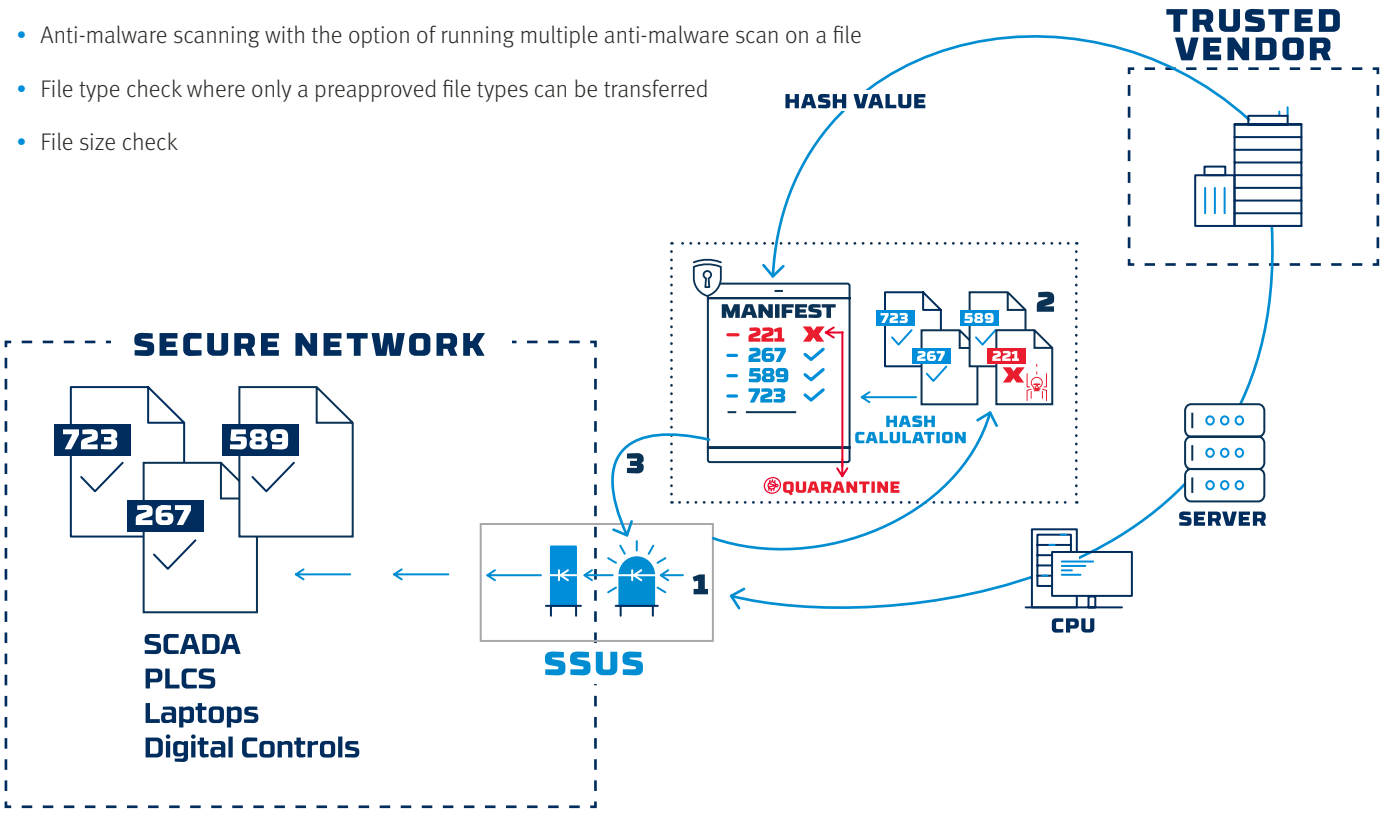


FIGURE 10: SSUS CONCEPT

The SSUS is flexible, supporting multiple options for transferring a file across the security perimeter into a secure ICS network. ***The SSUS concept is shown above in Figure 10.***

+ Secure Software Update Solution Functions and Feature Summary

SSUS is a robust, highly-scalable solution that cost-effectively addresses the need to thoroughly screen files for malware prior to transferring them across an electronic security perimeter. Owl's architectural approach is designed to reduce operational cost and maintenance time by deploying a centralized scan engine resource that can support hundreds of geographically-dispersed users. Antivirus scan or manifest signature updates are applied instantly and uniformly to all users regardless of their location.

The following is a summary of key features of Owl's SSUS solution:

- SSUS is a highly-scalable solution that can be configured to support up to three unique scan paths: an AV scan path, a manifest path, and a combined AV scan and manifest scan path.
- The system can support multiple AV scan engines and allows the Security Administrator to add, delete, and update AV scan engines.
- SSUS supports a manifest file which can be updated by the Security Administrator. The manifest file stores the hash keys for files that are allowed to be transferred to the high-security domain.
- SSUS can be integrated into an existing active directory. The System Administrator has the ability to define system access privilege on a per-user basis.
- SSUS can be optioned with the Owl Performance Management Service (OPMS) to enhance Administrator notification of malware detection or other alert conditions.
- The Security Administrator role can restrict file scans and transfers to specific file classes by creating a white list of file classes. All other files types will be quarantined. In addition, the Security Administrator is able to view system
- status and system logs, view user activity, and access all files transferred across the security boundary by any user.

Replicating Process Control and Historian Data

Digital Oilfield technology spans the entire spectrum of upstream activities, enabling centralized resources to have access to vast quantity of real time data. In the past, a large number of chart recorders were deployed to record temperature, flow rate, pressure, levels and other analog data originating from discrete control devices used in oil and gas production. Today, Historians are used to digitally store the trend data from the various monitoring and control devices distributed thought the upstream control network. Data from each device or point is captured in real time and available for analysis by local and remote resources.

Connectivity to historian data opens vulnerability to cyber-attack. A solution required in many ICN and perfected by Owl is to replicate the ICN historian to a historian in the business network across an electronic perimeter secured by a data diode. Owl's Perimeter Defense solutions support historian replication for all of the industry's leading historian vendors. By performing replication across Owl's DualDiode platform, the electronic security perimeter protecting field assets is maintained while resources in the business domain have access to real time data from the industrial control plant.

Owl's Perimeter Defense solutions natively support a number of historians including General Electric Historian; InStep eDNA Data Historian; Rolls-Royce DS&S and Scientech R*Time.

In addition Owl has developed and maintains software connectors supporting:

+ **OSIsoft® PI System®** -- Owl-PI System connector moves PI database records, snapshot data, and historical archive data to the lower level PI server. A single UDP connection is used to move all three types of information. Date and time stamps from the originating server are preserved; time synchronization between the two servers is maintained. Point record data and archive data are repainted to the receiving PI server.

+ **Secure ArchestrA Gateway Transfer (SAGT)** -- The SAGT connector provides operators and their IT associates with the means to transfer ArchestrA live process values and InSQL historical data from the secure process control environment to the corporate plant environment. The SAGT applications run on Microsoft Windows platforms, with the Windows machines recognized as members of a named ArchestrA Galaxy. Owl SAGT applications may reside on standalone servers, or integrated in the Owl 1U Windows Extended Services rackmount chassis.

+ **OwlOPC** -- an OPC interface designed to replicate an OPC client in a secure environment using Owl DualDiode Technology™. OPC functions by actively exchanging information between the client and the server. In the unidirectional environment of OPDS, the Owl OPC software connector intercepts and transmits OPC related data across the process control security boundary.

+ **Modbus** -- OMBI transfers real-time PLC sensor data one-way from PLCs within a segregated control network to databases on business and open engineering networks. OMBI can either communicate directly with a Modbus enabled device, or monitor existing Modbus Master/Slave communications. In either case, the Modbus data is collected in a secure environment, and made available to customer client applications requiring Modbus data.

Conclusion

Upstream oil and gas companies will invest billions over the coming years on Digital Oilfield technology needed to streamline operations while expanding exploration and production operations needed to meet the growing global demand for energy. Securing assets from cyberattack is critical and is a major area of focus for exploration, drilling and pipeline operators.

Owl's line of highly scalable cyber security solutions, backed by Owl's team of industry and technical experts have become the solution of choice for government and military applications, power generation, water management, and other industrial control verticals. As the market leader with over 1500 solutions deployed, Owl's solutions enable secure, reliable and robust information sharing and real-time collection for all data types.

At its core, Owl uses data diode Technology for hardware enforced secure data transfer. All data application types are supported, including historian replication, streaming full motion video, scanned file, and SMTP email systems, which allow Owl's solution to secure a wide range of critical applications. All Owl products are engineered to meet demanding environmental requirements and to achieve industry leading system reliability metrics.

OWL Cyber Defense

Owl Cyber Defense Solutions, LLC leads the world in data diode and cross domain network cybersecurity. With a constant focus on customers in the military, government, critical infrastructure, and commercial communities, Owl develops market-first, one-way data transfer products to meet a variety of operational needs, from entry level to enterprise.

For more information on Owl, or to schedule a demo, visit www.owlcyberdefense.com

@OwlCyberDefense

203-894-9342 | Info@owlcyberdefense.com