Owl Computing Technologies®

Cybersecurity Solutions Since 1998

White Paper

Meeting the Cybersecurity Standards of ANSI/ISA-62443-3-3

Owl Comprehensive Security Solution

38A Grove St, Ste 101, Ridgefield, CT 06877, USA
Toll Free: 866-695-3387
Phone: +1 203-894-9342
Fax: +1 203-894-1297

SECURED BY OWL

DualDiode TECHNOLOGY®

www.owlcti.com

The Security Landscape

As industrial control systems become more automated and increasingly digitized, the threat to the production systems moves from physical threats and attacks to cyber assaults. This means that your electronic perimeter is now as – if not more – important as the physical fence you have around your facility. But there's a critical problem.

When you have a physical gate, fence, or barrier, your facility is isolated from the outside world. There are actual gatekeepers controlling the flow into and out of your plant, which impedes movement speed but nevertheless moves everything where it needs to be. There are monitors, video and sensor, observing the traffic entering and leaving the plant and reporting anomalous behavior.

With a cyber system, this is much more difficult. What if, as happened in the Middle East in August 2012, you're struck by a cyberattack that compromises your perimeter security? Your digital "gatekeepers" have a weakness, and you're forced to go on lockdown to prevent hackers from accessing critical industrial automated control systems. The problem that results from this "lockdown" approach is the prevention of necessary information from leaving or entering the control network, creating significant operational inefficiencies. To regain the operating efficiencies and mitigate cyberattacks, data needs to flow in a secure manner between authorized networks and monitoring systems need to be in place to alert management to activity outside the acceptable norms – similar to the physical control system.

Background

The International Society of Automation (ISA) volunteers have worked long and hard to adapt the National Institute of Standards (NIST) for information technology (IT) systems to the security and operational requirements of operating technologies (OT). The ISA99 committee has produced policies and practices that, when implemented properly, go a long way towards achieving the security needed for industrial automated control systems. The convergence of IT and OT through information sharing to achieve enterprise efficiencies raises the stakes for the security policies governing both the production systems and the information sharing processes. The data flowing from the production systems to the business systems is critical to achieving the competitive edge companies are seeking. At the same time, important information must flow from the business network to the production network to support operating plans, application software updates, and security practices. The boundary between the business network and production network must be carefully monitored to ensure the security policies are providing effective protection of the industrial automated control systems.

Owl Computing Technologies® (OwlCTI) DualDiode Technology™, a fundamental component of the security solutions widely used in the U.S. National Intelligence Community and Department of Defense, is also integral to security solutions for the critical infrastructure market. OwlCTI has a variety of products to enforce security policies and mitigate threats for information flowing into, out of, and within a production plant. Additionally, OwlCTI provides monitoring applications to report information flow activity and to alert management of anomalous data transfer events. In summary, OwlCTI offers a comprehensive security solution for mitigating cyber threats to a production plant.

When protecting process control systems, the Owl Comprehensive Security Solution (CSS) provides the "defense wall" around the production network. A crucial element of "defense-in-depth" security, the Owl CSS' embedded data diodes deliver a non-routable protocol break across electronic security perimeters. When Owl CSS is implemented to complement physical security, it ensures network segregation, enables the convergence of OT and IT for critical systems, and prevents unauthorized access to networks, databases, and storage.

DualDiode Technology

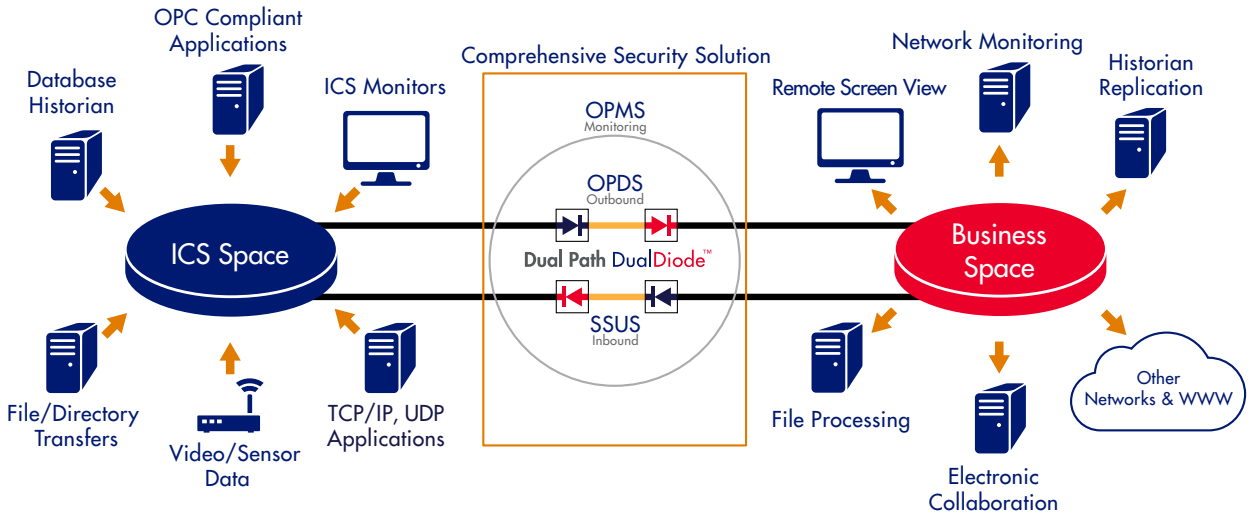
DualDiode Technology is at the core of Owl perimeter defense solutions and provides a one-way data transfer that secures communication across network boundaries. DualDiode Technology results in hardware-enforced, one-way data flow passing between two Owl-designed communication cards via optical fiber. DualDiode Technology

ensures no information of any kind, including handshaking protocols (TCP/IP, SCSI, USB, serial/parallel ports, etc.), will ever travel from the destination network back to the source network. The Owl proprietary process involves deconstructing network packets and then using an optical coupling system to transmit the data payload from one zone to another where the network packets are rebuilt and transmitted on the other network. This process includes a protocol break and makes anonymous the source and destination IP addresses which is fundamental.

The hardware optical coupling system used in DualDiode Technology restricts data flow to one-direction. As such, some of the applications that are part of the CSS have been specifically designed to compensate for breaking the bidirectional nature of some network protocols. In addition to the software, Owl has developed a bidirectional version of its DualDiode Technology called the Dual Path DualDiode that allows the secure information flow to support both the production and business networks, permitting IT and OT efficiency.

The Owl Perimeter Defense Solution (OPDS) outbound data flow product is combined with the Owl Secure Software Update Service (SSUS™) to bring validated and verified files across the perimeter boundary to achieve the data exchanges necessary for efficient and secure operations. The Owl Performance Management Service (OPMS™) product provides system monitoring and audit log management to grant cross-boundary traffic activity, and identifies and alerts to anomalous activity. To move specific information types, the OPDS can utilize additional software products such as the Owl PI Transfer Service (OPTS™), the OPC Server Transfer Service (OSTS™), and the Owl VirtualScreen View Service (OV2S™). OwlCTI OPDS supports all major industrial control vendors.

Owl Comprehensive Security Solution Architecture



Network Monitoring Using OPMS

The Owl Performance Management Service (OPMS) enables users to manage electronic perimeter defense solutions with timely system operating data. Performance, system health, and application status may be examined nearby or remotely via a web-based interface, monitoring, and displaying log file information. OPMS allows privileged administrators the ability to oversee the health and effective throughput of a single perimeter solution, multiple application instances on a single system, or multiple discrete systems.

[1] Source: ISA 62443 3 3 (99.03.03) Security for industrial automation and control systems Part 3-3: System security requirements and security levels

Meeting the Standards of ANSI/ISA-62443-3-3

In November 2013, Kenexis Consulting Corporation performed a third-party validation to assess the capabilities of the Owl CSS against the requirements in the ANSI/ISA-62443-3-3-2013 standard. An international standard, ISA-62443-3-3 provides detailed technical requirements regarding cybersecurity controls for industrial control systems (ICS).

To evaluate a complete system as per ISA-62443-3-3, the Owl CSS, containing the OPDS, including the OwlCTI proprietary Dual Path DualDiode Technology, an SSUS product, and an OPMS application, was assessed. Together, OPDS, SSUS, and OPMS represent a comprehensive security solution, hence Owl CSS, capable of securing the network perimeter between the ICS and corporate network.

Owl CSS is specially designed to protect isolated networks from cyberattack through network interfaces by acting as an autonomous information flow control system. Due to the specialized nature of its intended function, the Owl CSS does not fully satisfy every security control identified in ISA-62443-3-3. Instead, the Owl CSS is designed to complement other security systems at the deployment site that satisfy security requirements outside the scope of network connectivity, such as physical access security, reliable data storage, and authentication of personnel.

The associated four SLs are defined as:
SL 1 – Prevent the unauthorized disclosure of information via eavesdropping or casual exposure.
SL 2 – Prevent the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, generic skills, and low motivation.
SL 3 – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, IACS specific skills, and moderate motivation.
SL 4 – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extended resources, IACS specific skills, and high motivation.
Due to varying recommended operating and deployment conditions, the Owl CSS performed better in some requirements than others. The system's capability security levels (SL) are displayed for each requirement.

- System Integrity – SL 4
- Data Confidentiality – SL 4
- Restricted Data Flow – SL 4
- Timely Response to Events – SL 4
- Resource Availability – SL 4
- Identification and Authentication Control – SL 2
- Use Control – SL 2

The lower SL2 Identification and Authentication Control and SL2 Use Control values reflect the fact that the Owl CSS is usually implemented as a stand-alone configuration that operates autonomously without direct human interaction. Here, the requirements not met involve multi-factor authentication of human user interactions, centralized management of human user accounts, dual approval for certain actions, and determining the security status of portable and mobile devices.

Securing Industrial Control Systems

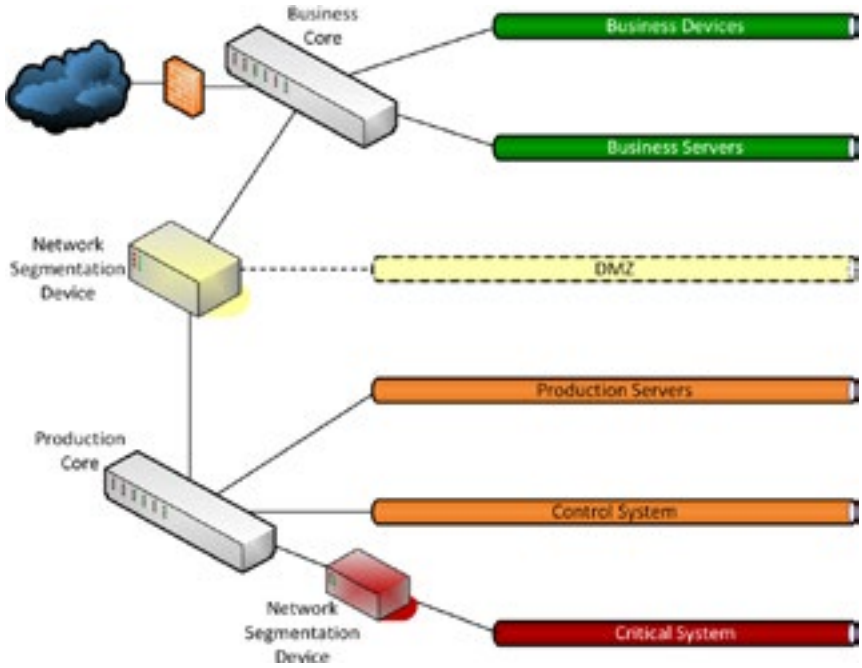
Owl's system combines hardware and software components to transmit data between the ICS and business environments securely. The next generation of network segmentation devices are using hardware-enforced, one-way transmission for a more secure ICS environment. The Owl CSS, and all Owl perimeter defense solutions, address this need with the proprietary DualDiode Technology.

Systems that control network segregation with a firewall can also enlist the use of a demilitarized zone (DMZ). The DMZ provides a means to talk to both the business and production networks in a controlled way, and is configured with the firewall to prevent direct communication between the networks. Production systems communicate with devices in the DMZ, with separate communications to the business and external networks.

The Owl CSS is a system that utilizes one-way transfer devices which allows services normally produced by the DMZ to be moved to the production network. The installation of the Owl CSS eliminates the need for a DMZ in the network architecture.

The production networks are segmented into a set of main production network servers; the control system, and critical system networks, with smaller groups available for fast or deterministic control loops. The production networks may also contain critical systems requiring a managed network connection to prevent external interference and exposure. These include safety instrumented systems (SIS), legacy equipment not easily upgraded, highly deterministic control equipment sensitive to extraneous network traffic, and control equipment that can run nearly independently and has high uptime requirements. These critical systems need a network segmentation device between them and production networks, which need not be as feature-rich as the one between the business and production networks.

Generic ICS Network Architecture



Use Cases

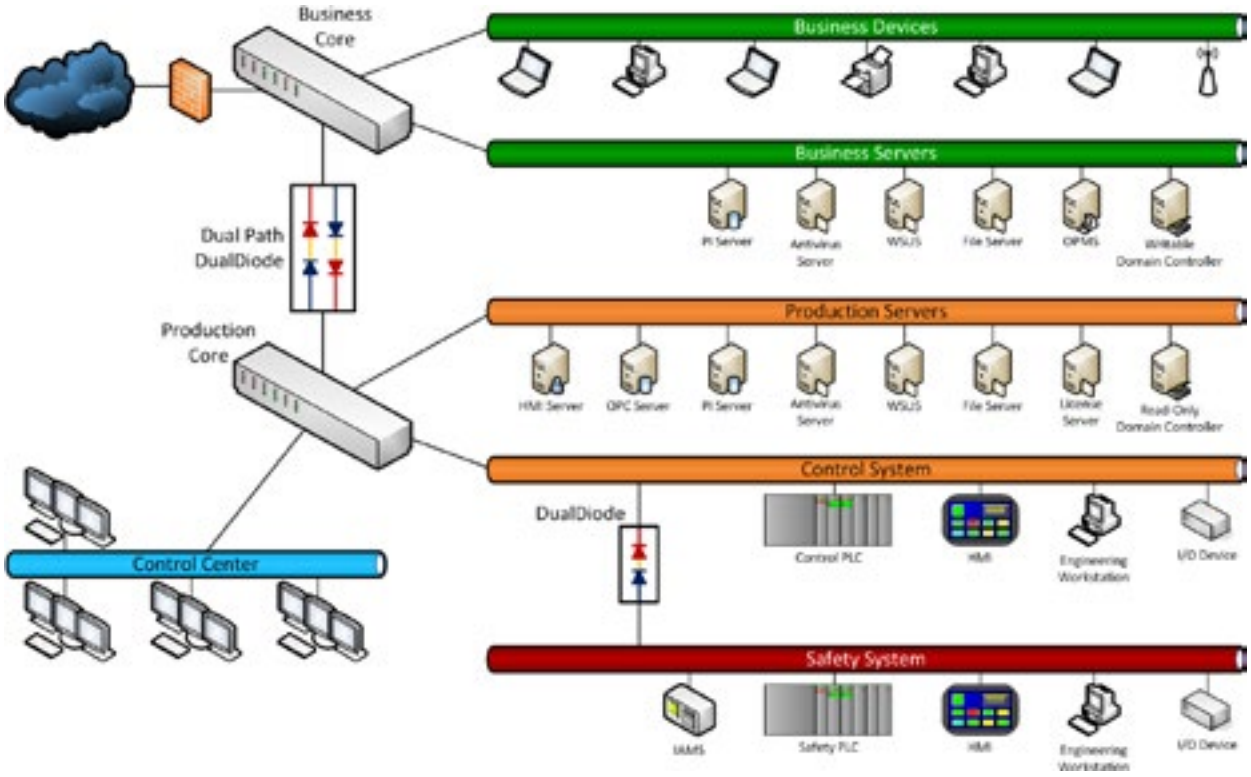
The Owl CSS has a wide variety of applications. Implementations that show the range of the systems include a chlorine truck loading station at a chemical/pharmaceutical manufacturer and an automotive manufacturing assembly line. The truck loading station architecture is based upon a single, large facility with a centralized control center and integrated safety systems to prevent the hazardous release of chlorine gas. The automotive assembly line architecture is based upon a large number of small robotic work cells with a single vehicle inspection station that, if it failed, would result in a large financial cost due to the downtime.

Use Case 1: Chlorine Truck Loading Station

After installing a chlorine truck loading station for new production capabilities, a pharmaceutical company needed a means to monitor loading and unloading operations with a centralized control center. The data needed to be available to both the business and logistics systems for inventory tracking and billing purposes.

The system architecture includes an integrated SIS that communicates with the loading/unloading control system over the network. The control system monitors the condition of the SIS and reports that information to the operator via the human-machine interface (HMI). In addition, an instrument asset management system (IAMS) calibrates and monitors the SIS sensor components and reports its data to systems within the production networks. In this design, the network segmentation device between the business and production network is an Owl Dual Path DualDiode device and the one between the production network and the safety system is an Owl DualDiode device. The OPTS, OSTS, and OV^{2}S are additional applications to aid with information consolidation and network monitoring.

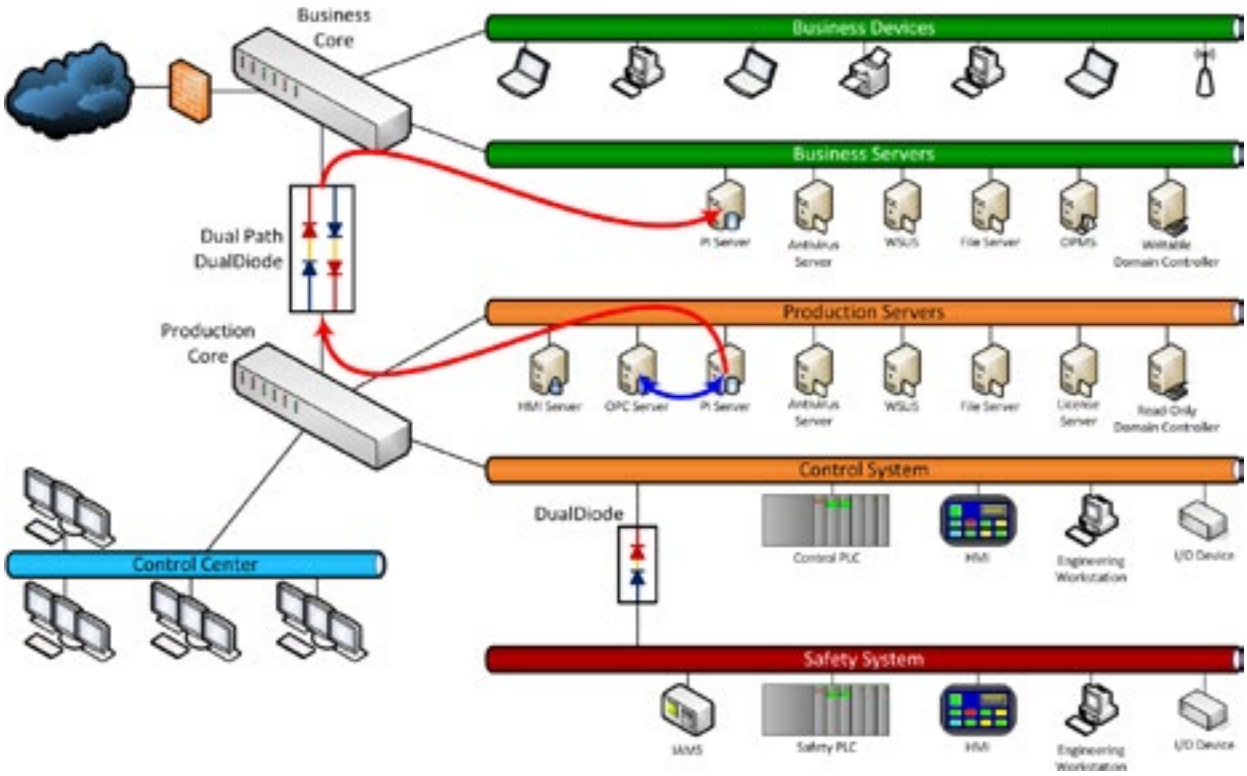
Chlorine Truck Loading Use Case Architecture



Data Historian Update with Owl PI Transfer Service (OPTS)

Facilitating a data historian system, the pharmaceutical company employs OSIsoft PI. First, the PI server reads OPC server data on the production network. Then, OPTS is used to transfer that data across the Dual Path DualDiode to the business network's corresponding PI server.

Chlorine Truck Loading Use Case: Owl PI Transfer Service (OPTS)

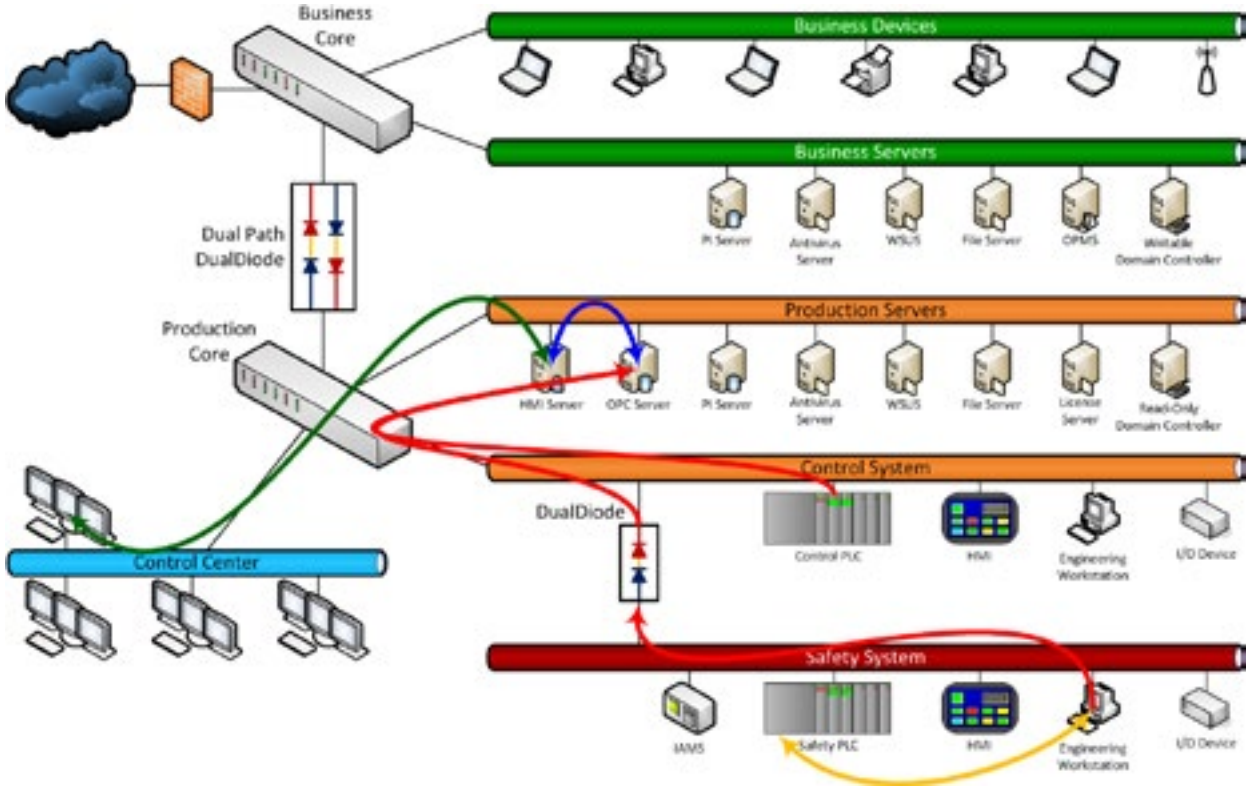


Consolidating Data with Owl OPC Server Transfer Service (OSTS)

To communicate with control center HMI systems, the programmable logic controllers (PLCs) employed in the truck loading station control system and safety systems are configured to use OPC. To consolidate information from multiple sources, including control and safety system PLCs, the production network is equipped with an OPC server. Operators in the control center are then able to use HMI servers to pull information from the OPC server.

The OSTS system on the engineering workstation in the safety system network is configured for information transfer across the zone boundary since the safety PLC is located behind the DualDiode device. The production network's OPC server then reads the values sent from the other side of the DualDiode device, making the information available to local operators at the truck loading station and HMI operators at the control center. Using discrete wiring, the control PLC is also hardwired to the safety PLC to back up the local OPC data consumption.

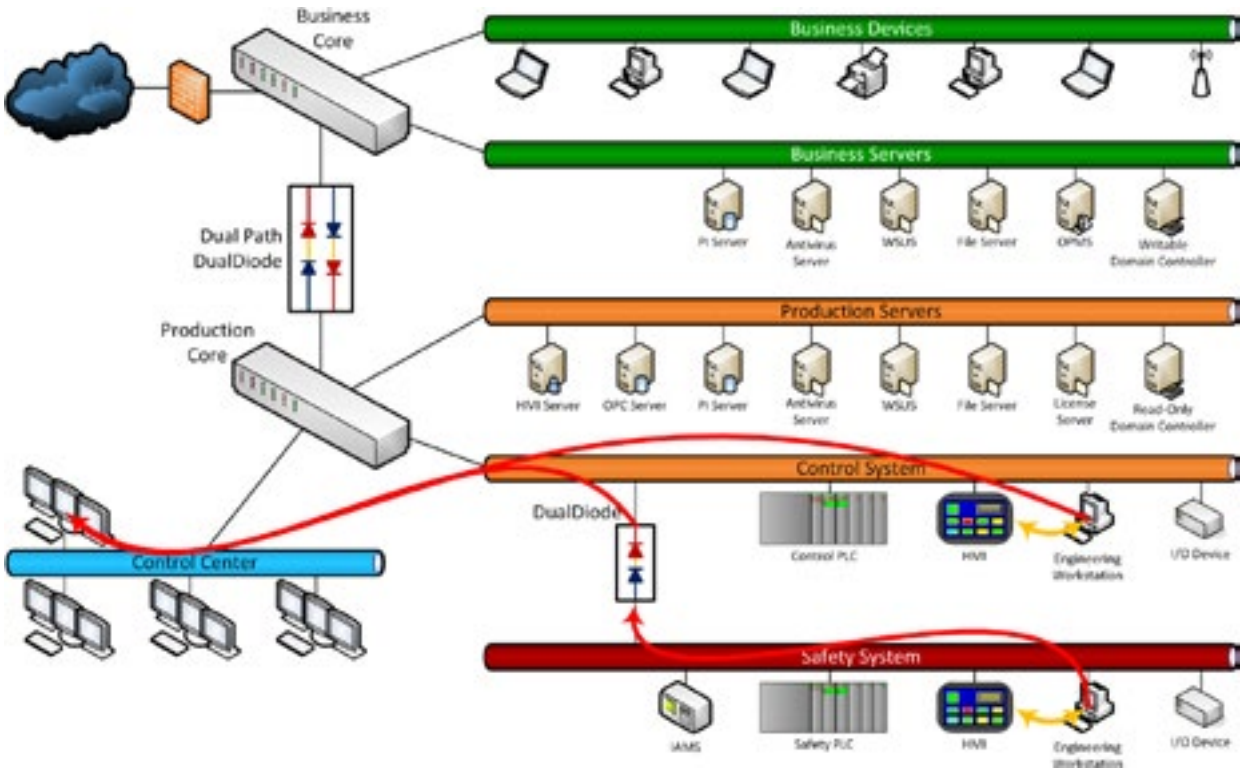
Chlorine Truck Loading Use Case: OPC Server Transfer Service (OSTS)



Remote Observation with Owl VirtualScreen View Service (OV²S)

For monitoring of the control and safety systems at the chlorine truck loading station during operation, the centralized control center employs both the OPC server method for data collection and a virtual screen view of the control system HMI and safety system HMI. Using both methods allows a local operator's actions to be verified by both the data received and the actions seen on screen. This ensures that the operator's actions are consistent with standard operating procedures. In addition, it increases the overall reliability of the system by providing redundant observation.

Chlorine Truck Loading Use Case: Owl VirtualScreen View Service (OV²S)



Patch Management Using Owl Secure Software Update Service (SSUS)

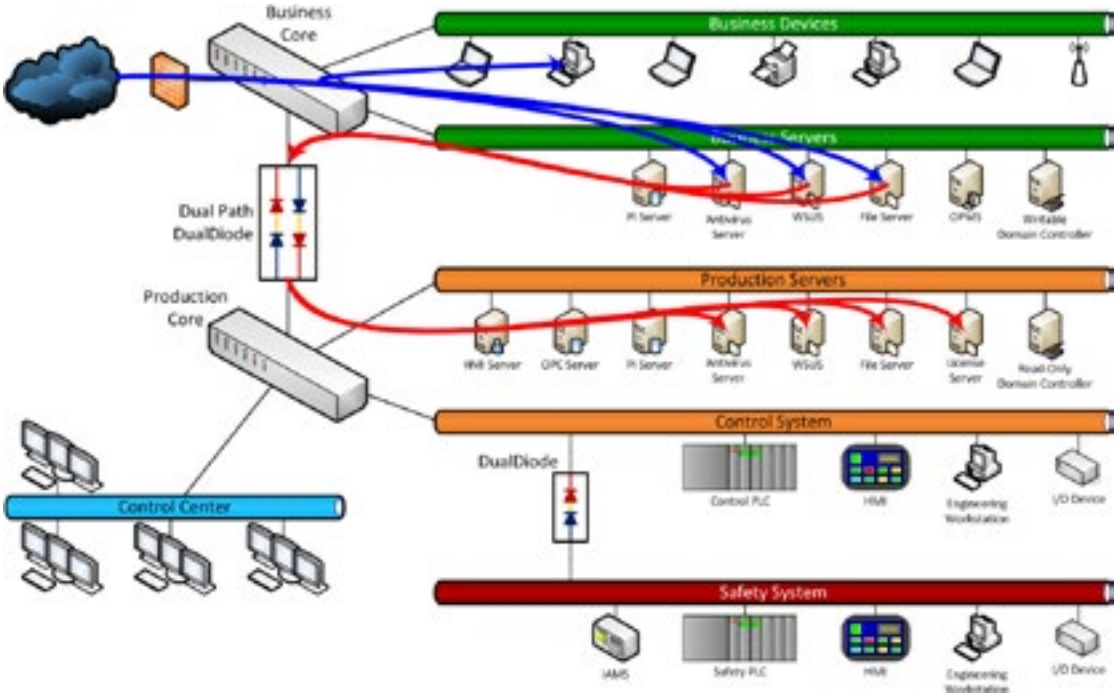
This architecture achieves patch management using the Owl SSUS system to cross the business to production zone boundary. Patch management refers to all system updates in the production network, including, but not limited to:

- Microsoft® Windows® OS updates and patches;
- Antivirus updates, patches, and definition files;
- Production application updates and patches;
- Production device firmware updates; and
- Licenses for production applications.

The same basic steps will be used for most of the types of files being brought into the production network from the business network. The difference is generally where the files will end up after they have been moved across the zone boundary. Any relevant files will be downloaded from the Internet to a business system and/or server along with a hash value (MD5, SHA1, etc.) for integrity checking and virus scanning. The files will then be copied to the SSUS system where they will be validated before being copied over to the production network. Once inside the production network, the Microsoft Windows operating system (OS) files will be moved to the Windows Server® Update Service (WSUS) system, antivirus files will be moved to the antivirus server, license files will be moved to the license server, and all other files will be moved to the production file server.

Due to the one-way nature of the SIS DualDiode system, it is necessary to move the relevant files from the production servers to the SIS network via a protected universal serial bus (USB) memory stick. This memory stick will only be used to transport files across the SIS to production network zone boundary. In the event that the engineering workstation of other devices within the safety system become compromised, the one-way nature of the DualDiode product should reduce the possibility of data being exfiltrated or systems being used as Bastion hosts for additional attacks on the system. Those types of connections usually require a back channel to be established between the system and a command and control (C&C) server of some sort. Without the reverse communication path, the back channel will generally die. Also, since the DualDiode has been pre-configured to only allow forward communications to a select group of systems on specific ports, it is unlikely that the compromised host could exfiltrate data to a C&C server on the Internet.

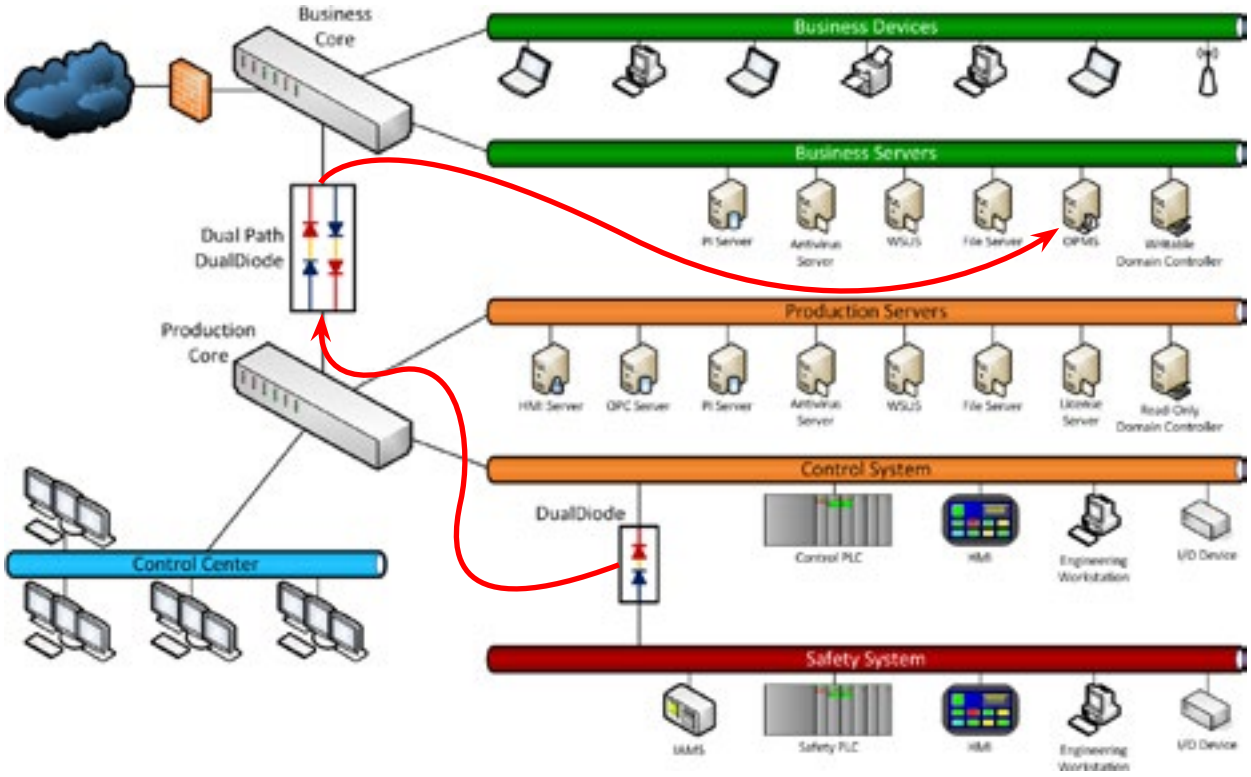
Chlorine Truck Loading Use Case: Patch Management Using SSUS



Network Monitoring Using Owl Performance Management Service (OPMS)

The OPMS enables users at the pharmaceutical manufacturer to manage electronic perimeter defense solutions surrounding the chlorine truck loading station with timely system operating data. Performance, system health, and application status may be examined nearby or remotely via a web-based interface, monitoring and displaying log file information. OPMS allows privileged administrators the ability to oversee the health and effective throughput of a single perimeter solution, multiple application instances on a single system, or multiple discrete systems.

Chlorine Truck Loading Use Case: Network Monitoring Using OPMS



Use Case 2: Automotive Manufacturing Assembly Line

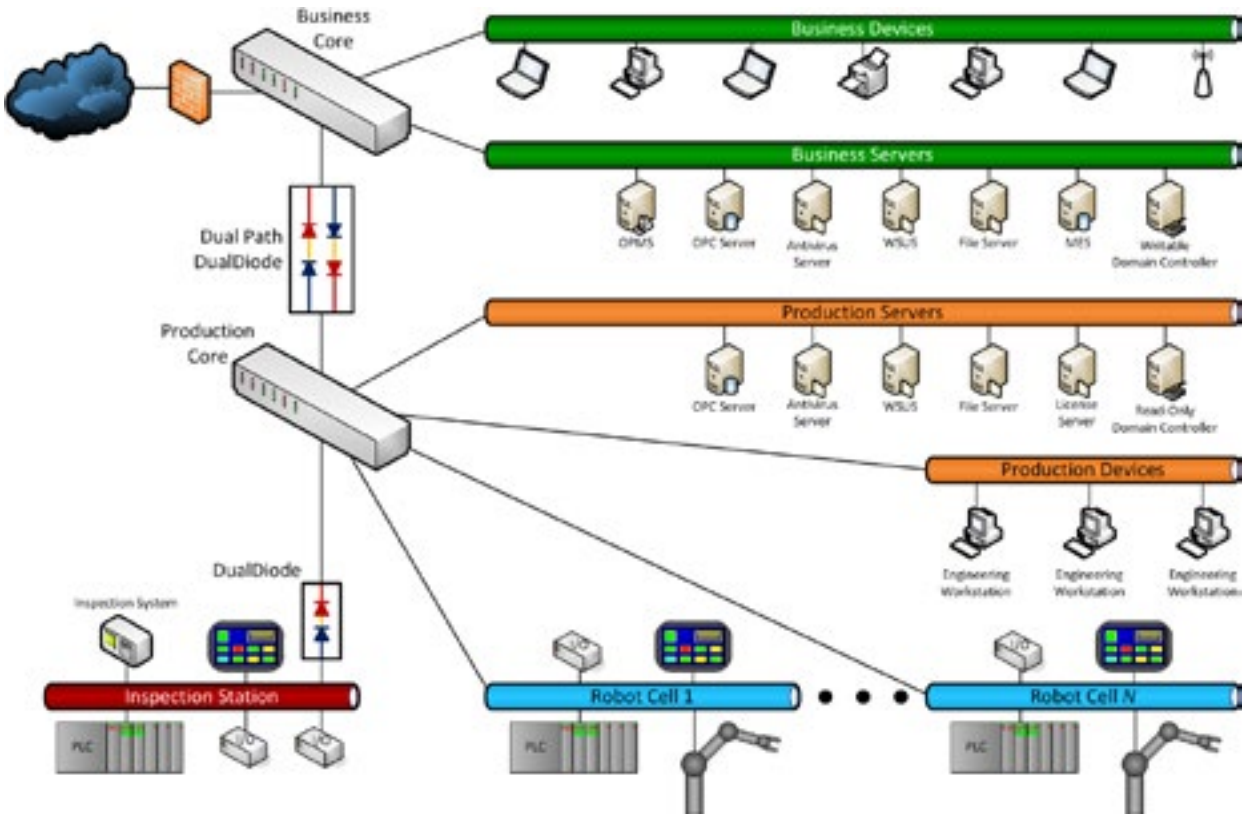
The automotive manufacturing installation required greater security for the assembly line control system to prevent system failure and financial loss from downtime.

For one section of the assembly line, an inspection station is used to validate that the vehicle under construction meets the design specifications to within a specified tolerance level. Due to the extra cost associated with the inspection station, this operation is generally conducted by a single station. The inspection station represents a single point-of-failure to the process, so the automotive manufacturer regards this as a critical system that needs to operate with a high degree of availability. The inspection system creates reports in both a machine-readable extensible markup language (XML) format and a human-readable text-based report.

The company uses OPC for most of its higher-order data collection. After the data is consolidated in the business network, a manufacturing execution system (MES) collects the OPC data and combines that with the XML inspection reports to generate overall manufacturing reports for each vehicle and for the overall assembly line detailing things like number of defects per vehicle needing attention and the number of defected vehicles per shift.

In this design, as in the chlorine truck loading station, the network segmentation device between the business and production network is an Owl Dual Path DualDiode device and the one between the production network and the inspection station is a DualDiode device. The inspection station is being protected from the other systems on the network due to its need for very high reliability and its relative criticality to the overall process. The OPTS, OSTS, and OV^{2}S are additional applications to aid with information consolidation and system monitoring.

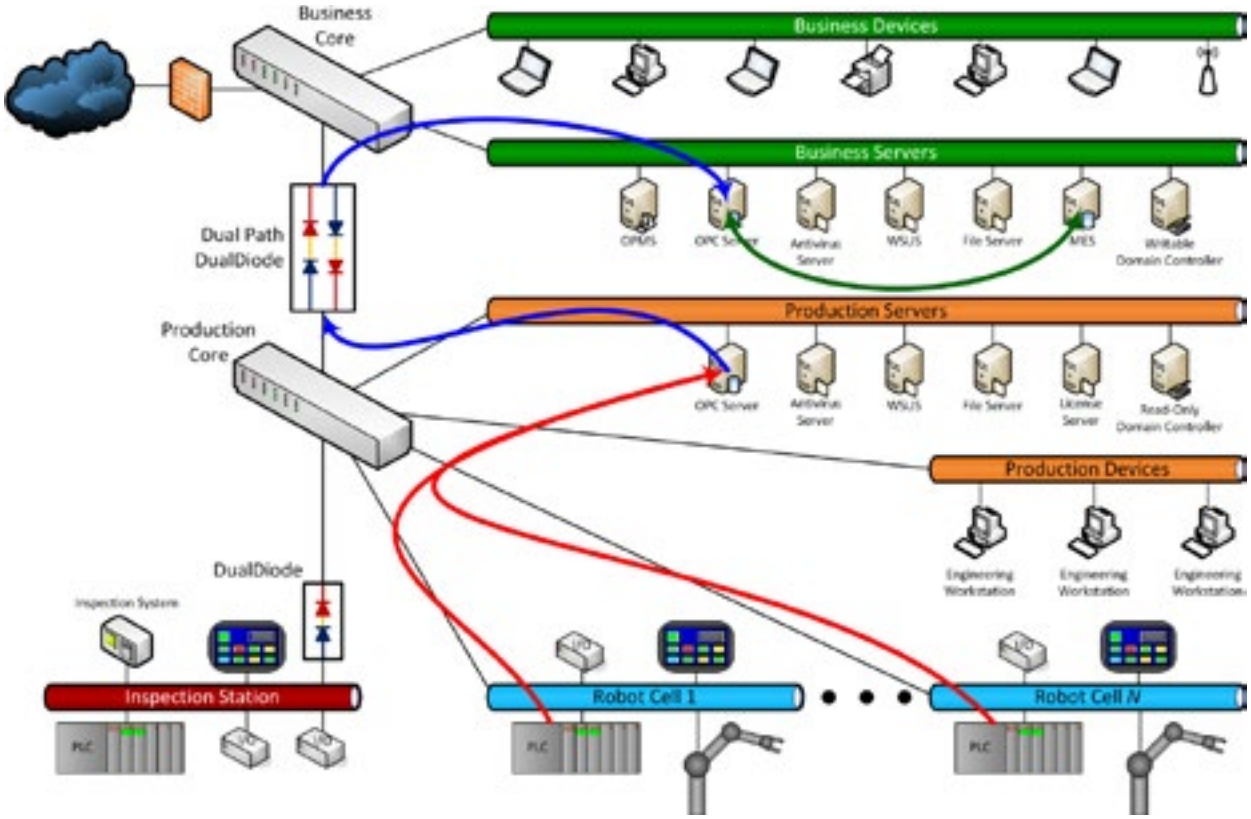
Automotive Manufacturing Assembly Line Use Case Architecture



Consolidating Data with Owl OPC Server Transfer Service (OSTS)

All PLCs are configured to use OPC, allowing the robotic work cells and the inspection station to communicate with the production OPC server. OSTS connects to the production OPC server and moves the OPC data to the business network's OPC server. OSTS duplicates the production OPC server across the production to business zone boundary. Using this OPC data, the MES system is able to calculate individual work cell efficiency, overall line efficiency, mean time between failures for equipment, tool wear, and other key performance indicators (KPI).

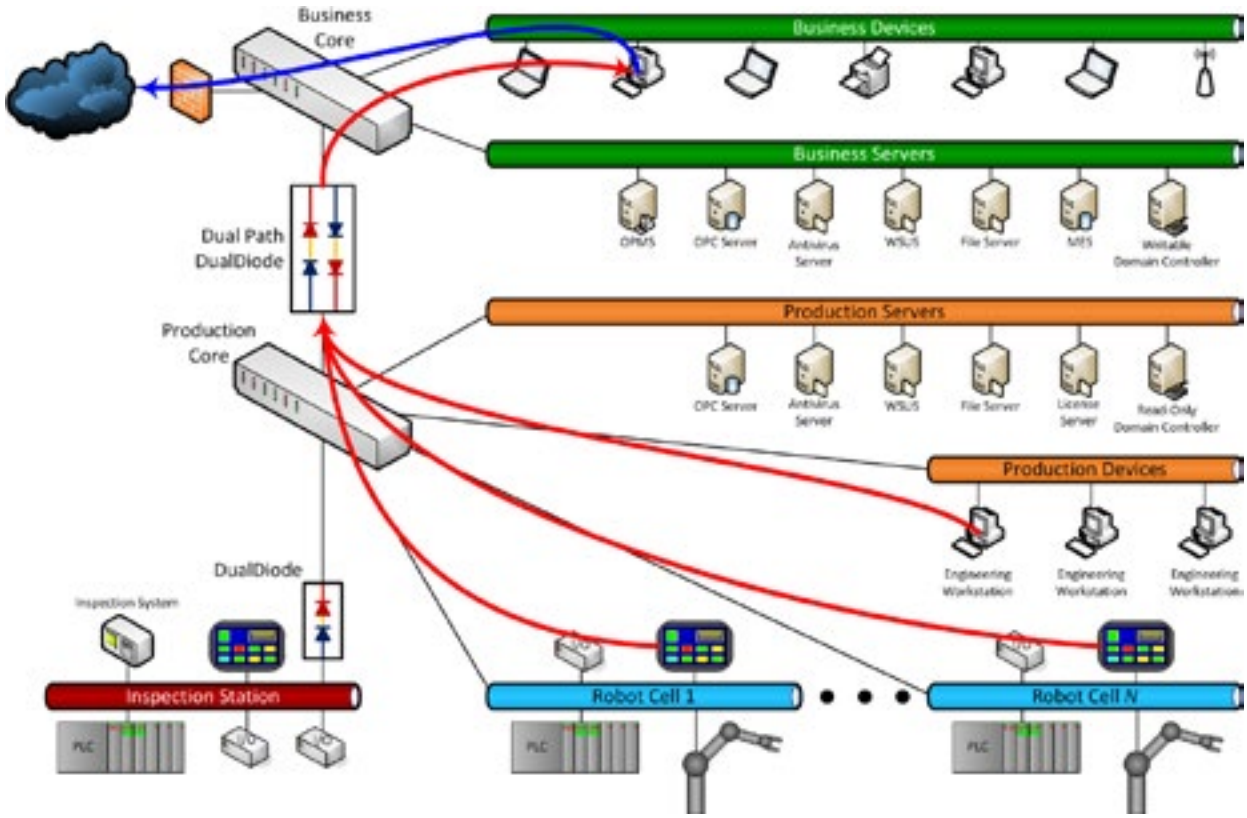
Automotive Manufacturing Use Case: OPC Server Transfer Service (OSTS)



Remote Observation with Owl VirtualScreen View Service (OV²S)

Automotive manufacturers generally maintain only a few moderately skilled engineering staff at each facility, concentrating the highly skilled staff in one location. This being the case, remote maintenance can be facilitated by allowing engineers to view an operator's screen to search for possible issues. To do this, the remote engineer logs into the local facility's business network using a remote virtual private network (VPN) tunnel from their corporate location. Once on the business network, OV²S has replicated the production device HMI servers to a business network display, which allows engineers to view the operator's actions in real-time. This allows remote engineers to improve the uptime for work cells by decreasing the repair time.

Automotive Manufacturing Use Case: Owl VirtualScreen View Service (OV²S)



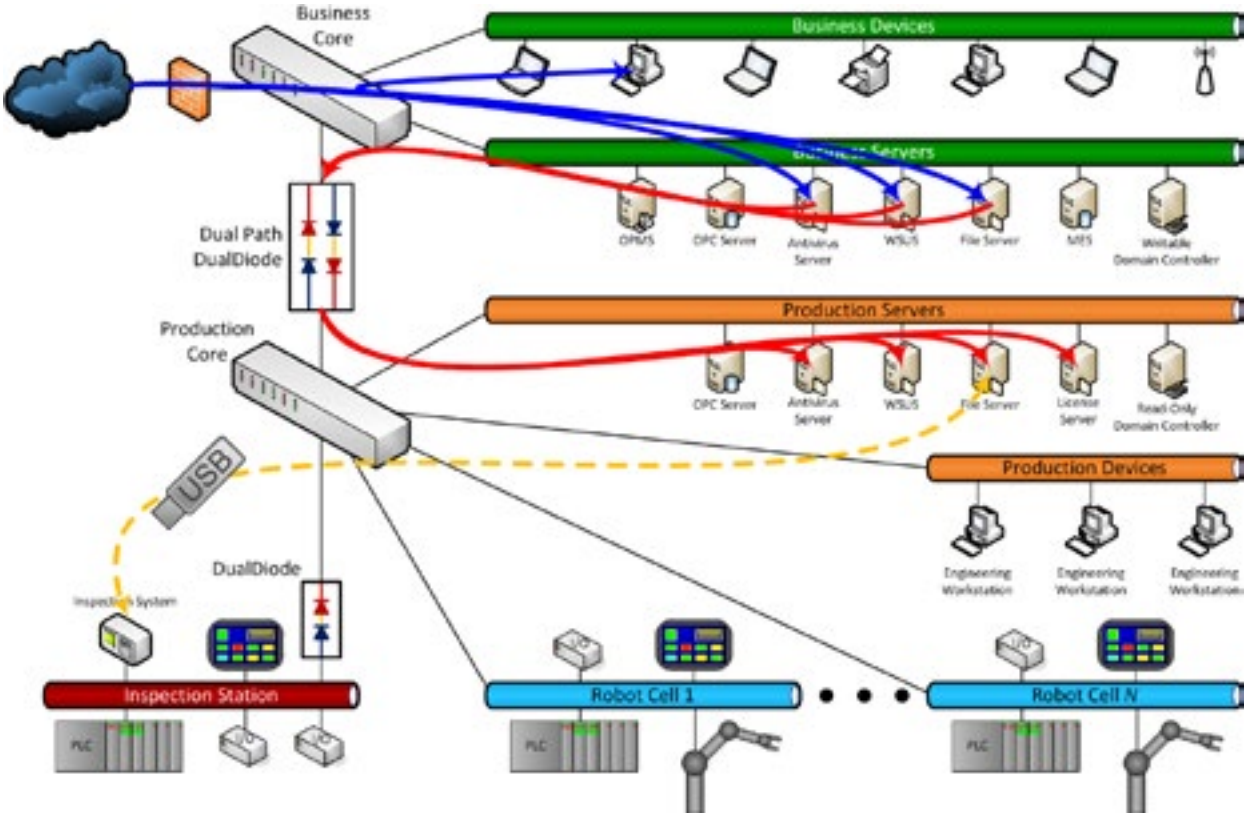
Patch Management Using Owl Secure Software Update Service (SSUS)

Similar to the chlorine truck loading station, by using Owl SSUS the system can achieve patch management across the business to production boundary. Patch management encompasses all updates to the system in the production network.

The same basic steps are used for most file types being moved from the production to the business network. The difference is generally the file's destination after moving across the boundary. Relevant files will be downloaded to a business system or server from the Internet, along with a hash value (MD5, SHA1, etc.) to allow for integrity checking and virus scanning. Next, the files will be copied to the SSUS system, undergoing validation before being copied to the production network. Once inside the production network, the Microsoft Windows operating system (OS) files will be moved to the Windows Server® Update Service (WSUS) system, antivirus files will be moved to the antivirus server, license files will be moved to the license server, and all other files will be moved to the production file server.

Due to the relatively regular (5-10 years) retooling of automotive manufacturing plants, it can often be the case after installation and certification that inspection stations go untouched until the line is retooled. Should files need to be moved into the station, a protected USB memory stick brings it in from the production server. This memory stick only transports files across the inspection station and production network boundary.

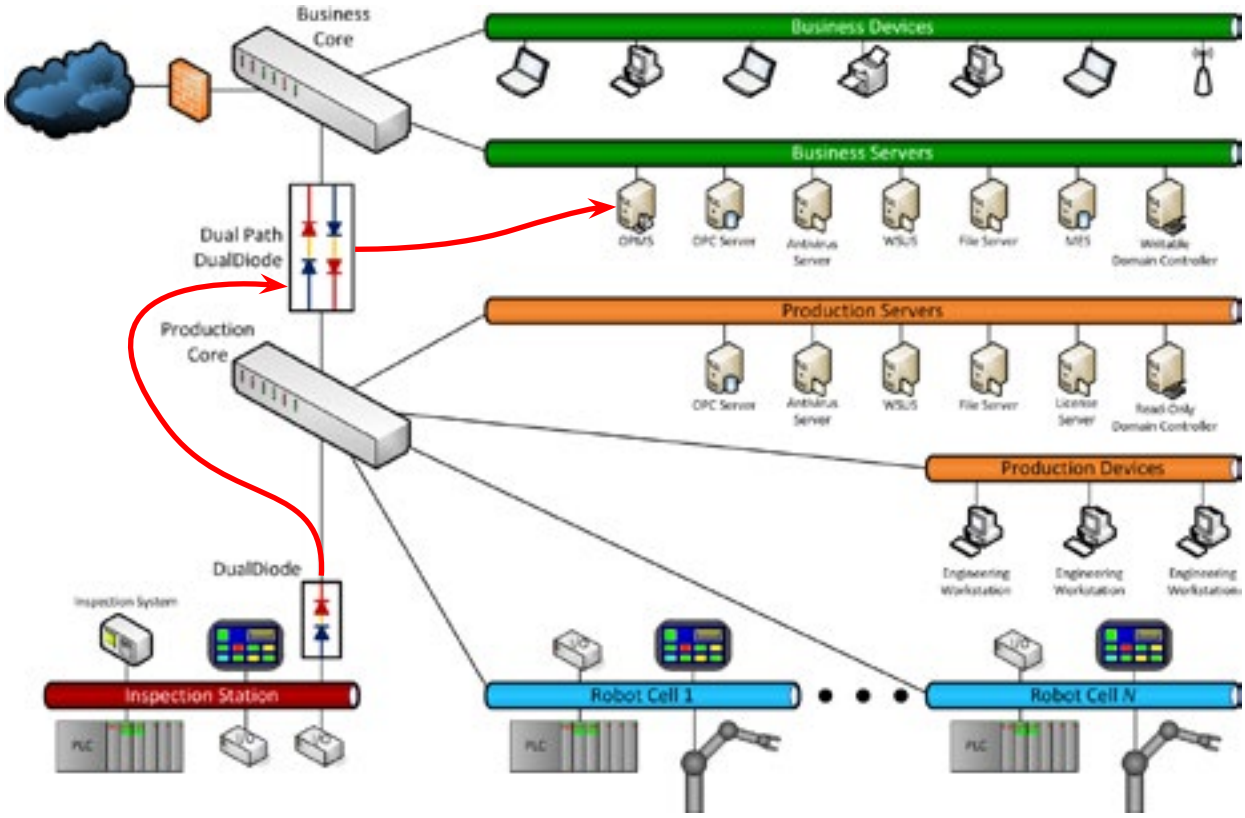
Automotive Manufacturing Use Case: Patch Management Using SSUS



Network Monitoring Using Owl Performance Management Service (OPMS)

Utilizing OPMS, automotive manufacturers monitoring the assembly line are able to manage the electronic perimeter defense solutions with timely system operating data. Performance, system health, and application status may be examined nearby or remotely via a web-based interface, monitoring and displaying log file information. OPMS allows privileged administrators the ability to oversee the health and effective throughput of a single perimeter solution, multiple application instances on a single system, or multiple discrete systems as part of the assembly line.

Automotive Manufacturing Assembly Line Use Case: Network Monitoring Using OPMS



About Owl

Owl Computing Technologies® is the leading source for next-generation cybersecurity. Owl's DualDiode Technology™, a proprietary data diode, has been successfully deployed in solutions across government, military, and critical infrastructure networks. Owl's hardware-enforced technology enables secure, reliable, and robust information sharing for streaming data files of all sizes and data types.

