OWL
Cyber Defense

OWL WHITE PAPER

UTILIZING THE ANSI/ISA 62443 CYBERSECURITY STANDARD TO DEFEND INDUSTRIAL CONTROL SYSTEMS

IEC 62443 is the global standard for the security of Industrial Control System (ICS) networks and helps organizations to reduce both the risk of failure and exposure of ICS networks to cyber threats.

The Security Landscape

As industrial control systems become more automated and increasingly digitized, the threat to the production systems comes from cyber attacks. 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 digital network, this is much more difficult. Your digital "gatekeepers" or firewalls have weaknesses and you're forced to go on lockdown to prevent hackers from accessing critical industrial 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 the secure Operational Technology (OT) networks and external monitoring systems to alert management to activity outside the acceptable norms.

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 IT 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.

US Department of Homeland Security Weighs In On Protecting ICS

In addition to the standards bodies, the US Dept of Homeland Security has also published a whitepaper describing Seven Strategies for Defending ICS systems. This paper recommends converting as many two way connections to one-way "pushes" of data from OT to IT using data diodes. Any data (i.e. software patches/updates) that need to enter a plant should also be done via a dedicated one-way connection and any remaining two-way connections (i.e. for remote command and control) should be a single purpose, single-port, locked-down tcp/ip connection. In short, by creating as many one-way connections as possible, the plant's digital footprint is reduced, thereby increasing the plant's cybersecurity posture. Precious resources can then be applied to the much smaller number of remaining two-way connections to identify and mitigate any threats found there.

Defense In Depth

A defense in depth strategy calls for using multiple measures to mitigate cybersecurity threats and attacks. A crucial element of "defense-in-depth" security, is the ability of data diodes to utilize a non-routable protocol break to move data across network segments/domains. Implementing data diodes to complement physical security ensures network segregation and enables the convergence of OT and IT for critical systems, and prevents unauthorized access to networks, databases, and storage.

Data Diodes

Data diodes provide a one-way data transfer that secures communication across network boundaries, ensuring a hardware-enforced, one-way data flow passing between OT and IT networks. Connecting the two "sides" of a data diode (source and

destination) are two diodes connected via a fiber optic cable. The one-way nature of the diodes 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 to the destination network. This process includes a protocol break and makes anonymous the source and destination IP addresses which is fundamental.

The hardware optical coupling system restricts data flow to one-direction. As such, protocol and application proxies have been specifically designed to compensate for breaking the bidirectional nature of some network protocols.

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

Kenexis Consulting Corporation performed a third-party validation to assess the capabilities of the Owl data diodes 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).

The validation exercise proved that the Owl OPDS system is capable of securing the network perimeter between the ICS and corporate network. The solution 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 system does not fully satisfy every security control identified in ISA-62443-3-3. Instead, it is designed to complement other security systems at the deployment site as part of a defense-in-depth strategy, that satisfies 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.

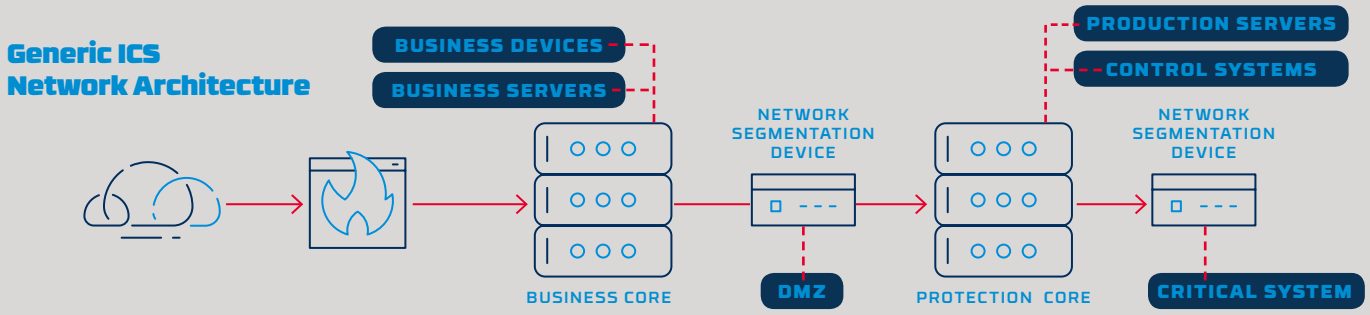
Due to varying recommended operating and deployment conditions, the Owl system performed better in some requirements than others. The system's capability security levels (SL) are displayed for each requirement.

- *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 system 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.

Generic ICS Network Architecture

While it is not possible to anticipate all ICS networks, it is possible to come up with a generic architecture that fits many different situations. This allows for some commonality between disparate systems, while still allowing for site and organization-specific versions of ICS network architectures to be developed. An example generic network architecture can be found below.



The generic ICS network architecture starts from the main corporate Internet firewall and the business core. One or more business device networks along with a collection of business servers hang off the business core network. In general, these business networks will consist of multiple subnets and there may be intermediate/distribution network infrastructure devices included in these networks depending on the size of the network. The business servers may also be behind some internal network segmentation devices for an added layer of protection. Between the business and production core networks, there should be some form of network segmentation device preventing the transmission of unnecessary or unwanted network traffic and the spread of malware in the event of an incident. Traditionally, these devices were firewalls, which have proven to be useful, although difficult to maintain. Over the last few years, a new class of network segmentation devices using hardware-enforced, one-way transmission has been introduced into the ICS environment.

The Owl system 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 system 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.

Use Cases

See attached use cases describing various implementations.