# MARITIME SECURITY

## White Paper

BAYSHORE NETWORKS
INDUSTRIAL AND IT NETWORK SECURITY

BAYSHORE NETWORKS
INDUSTRIAL AND IT NETWORK SECURITY

# Introduction

Since the first canoe was dugout over 8000 years ago the flow of goods and people over the world's oceans and seas has been fundamental to advancing the world's economy. As with other methods of transportation, maritime vessels are frantically adopting new technology to improve navigation, propulsion, safety, and traffic management. The Operational Technology (OT) space is critical for the operation of vessels and is dependent on Industrial Control Systems (ICS) and SCADA systems, which have become enticing targets for hostile actors.

Attacks on maritime vessels and key infrastructure components has promoted the US Coast Guard to publish advisories1 and bulletins2 and the European Union has issued advisories and even a formal analysis of this space3.

# Problem Statement

Many maritime Industrial Control Systems (ICS) in service are similar to land based applications (building management, power, manufacturing, etc) and yet are susceptible to more security issues.

The key difference with seafaring vessels is hostile actors typically have easier physical access to ICS devices and the network in which they operate.

There are two main areas to improve ICS security on maritime vessels:

i. **Remote access (typically satellite based)**
ii. **Local network access**

The goal is to increase security while not disturbing legitimate functionality and ensuring installed security devices provide their protective function independently and in parallel to Programmable Logic Controllers (PLC).

Security devices must be rugged and operate under harsh conditions, endure strong vibrations, and withstand above normal temperature conditions for general computing devices. Additionally, power consumption must be minimized because security devices will most likely be installed in low power consuming fanless enclosures.

# Introduction to Solution Components

Bayshore Networks, Inc. created OTfuse to address these exact challenges. OTfuse introduces strong security measures and operates via a transparent bridge mode at runtime. OTfuse can be seamlessly integrated into existing environments with no disruptions. It will operate in the standard model for transparent bridges where upon a dynamic table of MAC Addresses is maintained. The OTfuse appears invisible to the network as it utilizes two network ports to transmit and receive in unidirectional fashion. Due to these traits, the introduction of OTfuse to an environment seeking deep security can go virtually undetected, and a strong security posture is achieved with very little effort.

## OTfuse addresses multiple requirements:

- **It is focused on protecting ICS devices that are at risk on the network.**
- **It protects itself because it is installed on a local network susceptible to the same hostile elements as the ICS devices.**
- **It supports, at a hardware level, a fail open state so outages (i.e. loss of power, hardware failure, etc) causes no operational disruptions to legitimate operations**

OTfuse is an innovative approach to the generation of enforceable security policies. Its learning engine is specifically designed to provide highly focused security rules in the generated policy. Rules are constructed based on learned traffic encountered in the protected environment and surpasses what any generic set of rules could achieve given the unique possibilities with ICS communication protocols. The effectiveness of generic rules is generally nullified because in multiple environments running the same exact ICS communications protocol there can be highly customized and modified variants.

To be truly effective, products operating in this space need to understand operational ranges of values such that threshold, or out of range, violations are detected and handled accordingly based on customer needs.

## OTfuse allows the customer two choices in handling violations:

- **raise alerts, or notifications, yet allow traffic to flow**
- **actively block traffic flows**

While OTfuse effectively operates in this learning mode and generates security rules and a policy that is subjective, experts can make modifications of these rules via a web based graphical user interface (GUI).

Bayshore Networks also provides generic rulesets based on known best practices. These can be included in a given security policy or ignored altogether. One example of these pre-built rulesets is the Line of Sight use case. In this case write functions are not allowed and communications are enforced to be read only at a native protocol function level. Typically this is coupled with allowing traffic from specific segments of the network with the added granularity of function code enforcement. Secure remote access use cases often pursue this protection so remote operators are allowed access to a given network but only to utilize read function codes to a specific target ICS machine or range of machines.

# Application of Solution

Deploying OTfuse is simple and requires minimal configuration. Setup and management is performed via a virtual network interface.

### Once installed OTfuse provides 6 layers of protection:

i. **Reconnaissance activity detection and blocking**
ii. **Protocol level protection**
iii. **Denial of Service (DoS) protection**
iv. **Remote access protection**
v. **Firewall capabilities**
vi. **Network Segmentation**

# Reconnaissance Activity

Hostile actors physically onboard a vessel can have easy access to the network and the time needed to perform reconnaissance. This creates an imperative to stop, or at least report and/or raise alerts on detected reconnaissance activity at the lowest of network levels, as close to the actual protected ICS devices as possible.

OTfuse specifically attempts to detect reconnaissance activity by focusing on two common early steps hostile actor's reconnaissance activity:

i. **Checking if a given host is alive on the network**
ii. **Discovering the listening and open ports on some potential target device (i.e. port scan)**

Detection of port scan activity is critical because it must be effective in protection for OTfuse itself and any protected ICS device. Moreover, this detection has to be intelligent enough to detect sophisticated port scanning techniques such as the "slow and low" port scans.

## Protocol Level Protection

OTfuse provides native protocol security. There are many different ICS communication protocols with their own rules and structures. OTfuse has a deep understanding of each protected protocol. This enables OTfuse to provide deeper protection than a basic firewall or simple deep packet inspection (DPI) allows.

One core tenet that drives OTfuse's design is that entire network flows need to be analyzed. When a scan is performed for anomalies or threats both request and response data must be scrutinized. Analyzing one half of network flows is not sufficient for adequate protocol level protection.

For example, in Modbus/TCP standard and normal communications requires matching function codes be present in a request response pair. It is not possible to enforce and/or analyze that aspect of the specification, on live traffic, if a security device only looks at unidirectional traffic.

## DoS Protection

Blocking and/or detecting DoS attacks at a protocol level is very important and relevant to the security of the maritime vessel. The aspect of this happening at the native protocol level, and not the typical TCP level, is critical because the traffic is radically different between those 2 types of DoS. For example stopping a DoS attack at a Modbus/TCP or DNP3 level is radically different than stopping a SYN Flood attack. The security device in place needs to natively understand how an attacker would manipulate traffic at Layer 7 in order to be effective. OTfuse comes protects against this exact use case.

## Remote Access Protection

To provide remote access protection the security solution must restrict access to what a remote entity can do based on the segment of the network where actions are sourced. Typical Virtual Private Network (VPN) solutions allow for, and facilitate, unrestricted network access once a remote tunnel has successfully been setup. This is unacceptable in a maritime environment as this introduces unnecessary risk. OTfuse policies can be structured such that it understands the source range of IP addresses and only allows specific operations sourced from any entity in that source range.

## Firewalling Capabilities

Standard firewall capabilities are inherently part of OTfuse. A policy can be set to the quintessential “deny all” after all other rules in a policy have been processed. Given the mode of operation being a transparent bridge this is very powerful as a policy combining network 5-tuple data can be combined with protocol level elements for a solid white-list approach. Anything outside of the white listed elements would simply be blocked by OTfuse.

## Network Segmentation

OTfuse easily creates network segmentation by using very simple rules in the security policy. This capability provides the standard ability to allow communications from specific segments of the network, it can be coupled with other elements, such as time of day ranges or protocol type, to allow for flexible segmentation.

## Benefits of Solution

One of the undeniable benefits of OTfuse is it seamlessly inserts into the target network avoiding the challenges of restructuring the target network via IP address changes. This is achieved due OTfuse’s transparent bridge run time mode. This seamless insertion allows detection of existing attack operations that may be taking place at the time of installation.

OTfuse introduces a strong security posture on the 6 layers of protection presented earlier. This includes restricting remote user activity at a deeply granular level.

## Looking at lower operational levels within OTfuse one of the true benefits is the fact that it can learn:

- **network traffic (5 tuple)**
- **protocol data (i.e. function codes, set point values, ranges of set point values, etc)**
- **behavioral elements (i.e. within some time range specific function codes are utilized from specific areas on the network)**

Automated learning yields highly subjective, intelligent and enforceable policies that can natively protect a given environment based on real world activity.

# Future Direction

The future of OTfuse is to approach zero touch autogenerated security policies based on very specific Machine Learning (ML) algorithms. These automated but adaptive policies will get more accurate over time based on learned data and behavioral aspects within the data itself.

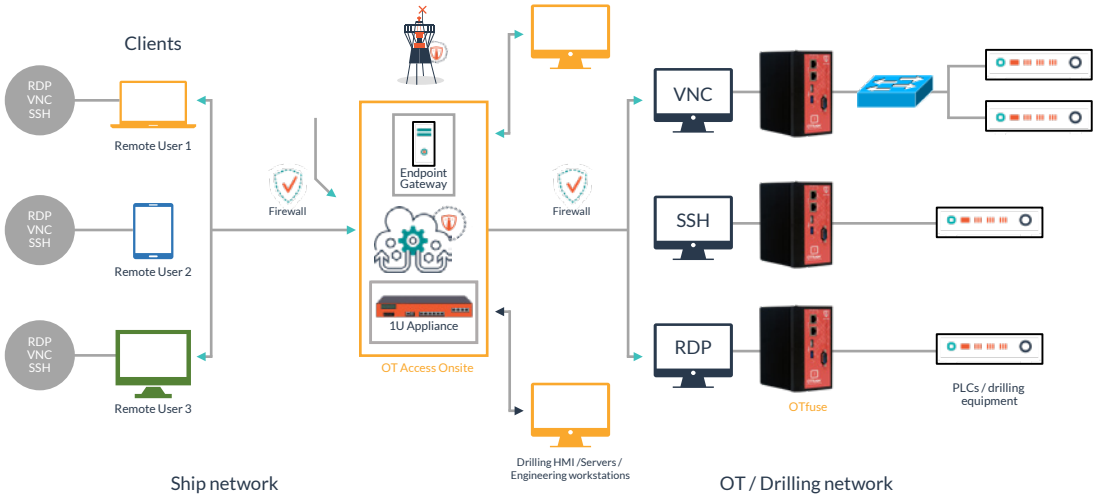
These processes need to be optimized to perform within standalone devices with limited computational horsepower due to size and power consumption restrictions.

# References

**https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/Alerts/0619.pdf**
**https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/MSIB/2019/MSIB_004_19.pdf**
**https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1/at_download/fullReport**

# Maritime Deployments:

## OT Access Onsite and SCADAfuse






BAYSHORE