Ship Control System's Network Architecture, Communication Protocols and Message Authentication Options

Lead Author: John E. Messick, Jr., Co-author: Kerry Hansen

* Corresponding Author. Email: John.Messick@noblisMSD.com

Synopsis

There is a growing threat of cybersecurity attacks within shipboard machinery control systems (MCS). A major cyber security vulnerability in shipboard control systems is in the data message communication protocols. These message communication protocols currently do not have message authentication and verification using encryption methods, specifically message traffic of Programmable Logic Controller (PLC) data. This vulnerability makes these systems subject to man-in-the-middle cybersecurity attacks. PLCs struggle in terms of processing power with large amounts of string manipulations required for cryptographically secure hash values within data messages. This white paper will investigate shipboard MCS message data communications authentication options with respect to network architecture, communication protocols, and vendor equipment. The key objective is to investigate options for data message authentication for peer-to-peer control processors and control processors to operator consoles used in shipboard MCS. The approach will be to consider network architectures such as star, rings, bus, hot backup, and subnetworks and how these architectures influence the selection of vendor-specific equipment. The vendor-specific equipment often limits if not dictates communication protocols. Options for control data message authentication and verification are then limited by these design decisions. This paper will investigate the options both with hardware and software solutions with respect to shipboard control system network architectures and communications protocols.

Keywords: Operational Technology (OT), Network Architecture, Industrial Control Systems (ICS), Programmable Logic Controller (PLC), cybersecurity, Message Authentication, cryptography, communication protocols, SHA256

Author's Biography

John Messick has over 25 years designing shipboard control system projects. Recent activities involve designing strategies addressing cybersecurity, team member for a patent held by the U.S. Navy and author/co-author of four papers published by the American Society of Naval Engineers. He is currently the principal investigator for a Noblis Sponsored Research project titled 'Industrial Automation Cyber Security Message Authentication and Verification.'

1. Introduction:

Cyberattacks on critical infrastructure were rated as the fifth in a survey of risks most likely to increase in 2020, according to the 2020 World Economic Forum's Global Risk Report. (World Economic Forum. (2020)**.** Maritime infrastructure, which includes shipboard machinery control systems, is part of the global critical infrastructure. In 2019, for example, the United States Coast Guard (USCG) issued bulletins related to cybersecurity attacks on commercial vessels. On July 8, 2019, the USCG issued a Marine Safety Alert addressing a cybersecurity incident which exposed potential vulnerabilities onboard commercial vessels. According to the report, a shipboard network on a deep draft vessel was compromised (Inspections and Compliance Directorate, Safety Alert 06-19). On May 24, 2019, the USCG issued a Marine Safety bulletin informing the marine industry of recent email phishing and malware intrusion attempts targeting commercial vessels. This bulletin provided notice of reports of 'malicious software designed to disrupt shipboard computer systems' (Inspections and Compliance Directorate, MSIB Number: 04-19). Recent trends with remote maintenance and navigational technology have increased the need for ensuring the integrity in shipboard control system operational data transmission. Remote maintenance has become a trend as a result of COVID-19 responses from vendors supporting ICS equipment. The threat of cybersecurity attacks within shipboard MCS is a real and present danger.

Many shipboard MCS utilize commercial off the shelf industrial control systems. A large market share of Industrial Control Systems (ICS) and common shipboard MCS are known as Programmable Logic Controllers (PLC). These shipboard MCS typically have complex network architectures and use legacy communication

 https://doi.org/10.24868/10718

protocols. ICS communication protocols are based on Operations Technology (OT) rather than Information Technology (IT). This is a very important distinction for cybersecurity purposes. PLCs are typically smaller microprocessors designed to handle a specific operation of the shipboard and are distributed and networked together to share shipboard sensor data for shipboard conditions such as temperature, pressure, flow, and device status for engines, valves, and motors. Together, they are designed to control the propulsion, electrical distribution, and auxiliary systems of the shipboard along with many other fundamental operations.

IT implemented methods of message authentication and verification years ago using cryptographic methods. OT lags far behind and is limited in capabilities for message authentication and verification. This is because PLCs are limited in their ability to handle the complex operations related to cryptography without a significant impact on the performance of the microprocessor. Message traffic for OT requires a much faster response, often in the millisecond range or faster. This paper investigates the more common ICS network architectures, communication protocols, and existing technology options for OT data message authentication.

2. Shipboard Control Systems Network Architectures

Basic network architecture design decisions have significant impact on the options of message authentication based on current technology. There are several common basic OT network architectural concepts such as a ring or star topology, hot backup, client-server topology, and a serverless topology. One specific design decision which significantly affects the options of message authentication is whether the network architecture contains a client-server topology. An architecture that consists of hot backup for the microprocessors will also impact the options for message authentication based on the current technology available by most vendors of PLCs.

2.1. Ring Topology

A Ring topology consists of a network with the PLCs and operator consoles connected using two connections each to form a circular ring. Figure 1 Ring Topology depicts a simple ring architecture with fundamental backbone devices. Each device essentially communicates through every other device along the ring. There are several protocols used for OT networks that take advantage of the Ring topology. This white paper will build on this fundamental diagram to further explain the network architectures, communication protocols and message authentication options. Several vendors require a Domain Name System (DNS) server to implement an option for message authentication referred to as Transport Layer Security (TLS).

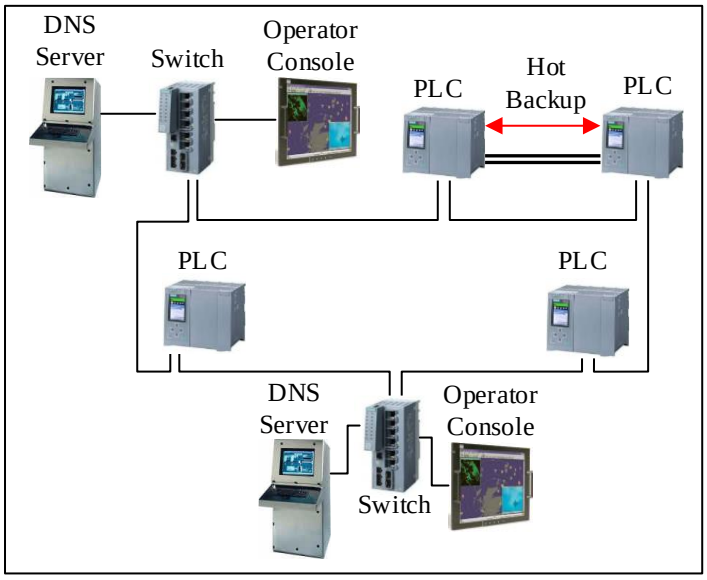

Figure 1 Ring Topology

 https://doi.org/10.24868/10718

2.2. Star Topology

A star topology consists of a network of communication devices connected to a single switch or group of switches. The group of switches are then typically connected in a mesh configuration to form the shipboard network. The star topology can be used as a method of segregating the operational networks. The below figure illustrates a fundamental star topology using two independent redundant Local Area Networks (LANs). This diagram implements redundant servers that can be used as certificate authorities for message data authentication purposes. Servers are a crucial component of several message authentication options for industrial shipboard control system protocols.

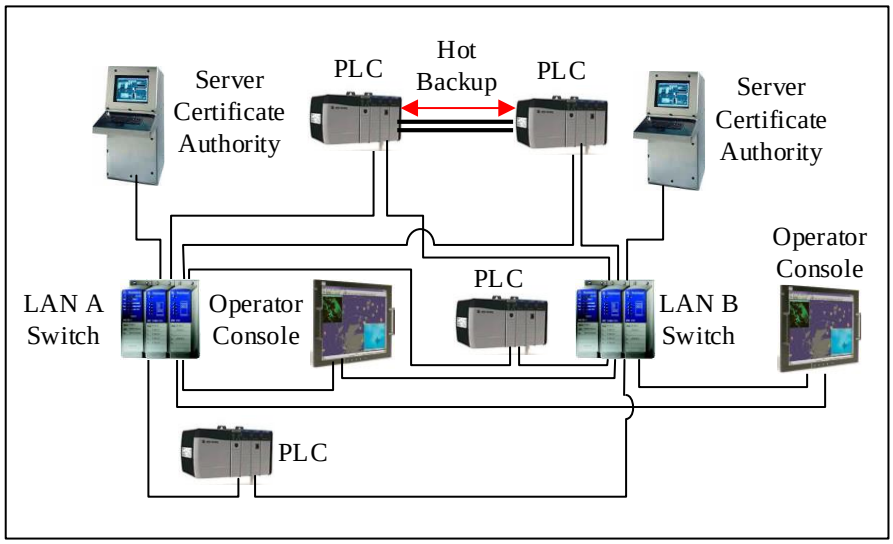

Figure 2 Star Topology with Redundant LAN

2.3. Hot Backup

Hot backup is when two microprocessors are synchronized and function as one microprocessor in a primary-backup configuration. Often, only one processor is 'visible' to the network. The switchover from primary to backup because of a fault is designed to be a bumpless transfer. The time requirement for the switchover and the method of the redundant communication devices residing on the network with identical configurations can cause authentication methods to be complicated. In some cases, ICS vendors make this a choice between redundancy and security.

2.4. Client-Server Topology

A client-server topology is popular with ICS, as indicated in both figures above. A server provides a mechanism for centralized data collection, security, and configuration management. The critical nature of a server dictates the need for redundancy. The implementation of server redundancy increases the complexity and potential failure modes of the overall shipboard control system. Some communication protocols such as OPC UA require a server-based topology. PLCs typically have a limited number of communication resources commonly referred to as connections. The use of a server for centralized communications allows the PLCs to transfer data to a single device, which then distributes the data to the shipboard's operator consoles. This option lends itself easily to message authentication options.

2.5. Serverless Topology

A significant distinction should be addressed between OT and IT network topologies. In IT topologies, serverless does not necessarily mean a server is not used. The servers are removed from the application layer; however, servers are still used at the cloud layer. Servers are completely removed from network topologies of serverless OT network architectures. This can be accomplished using a Multicast User Datagram Protocol (UDP). This allows for a connectionless protocol using sockets and therefore a one-to-many distribution of the message data. Multicast communications allow each PLC to transmit message packets to a group of operator consoles using a single message packet. Each operator console is independent of all other operator consoles. The implementation of multicast communications most likely requires developing custom communications software applications.

 https://doi.org/10.24868/10718

Multicast communication protocols in ICS applications are not typically offered in widely used third-party application development software. A bump in the wire or custom software-based message authentication option would also be necessary.

3. Equipment Vendor Selection

The vendor-specific equipment often limits if not dictates shipboard control system network topology, redundancy capabilities, and communication protocols. Some vendor equipment is designed to work best with a ring or bus network topology. Other vendor equipment operates optimally with mesh or star network topologies. The choice of vendor and topology lead to the options of communication protocols such as Profinet or EtherNet/IP. Next in the design decision are the protocol options for resiliency and redundancy. One option for a ring topology is the Media Redundancy Protocol (MRP). The MRP requires at least one Media Redundancy Manger and the other devices along the ring are clients. Another network redundancy option is Parallel Redundancy Protocol (PRP). The concept of PRP is based on communication devices connected to two independent networks with similar topology. A newer more resilient redundancy protocol is the High-availability Seamless Redundancy (HSR) protocol. The HSR protocol requires each communication device to have two connections and function as a bridge. The network topology using the HSR protocol is a ring or mesh and does not require dedicated switches. The availability of these network protocols is limited by not only the vendor chosen, but also the specific communications control devices and microprocessors selected.

4. Message Authentication and Verification Options

The options for securing data using message authentication and verification are significantly impacted by the ICS topology and communication protocols. Several options require the use of a server for certificate or key management. There are options currently available on the market for implementing control data message authentication and verification. These options have specific network topology and communication protocol requirements. Many of the options available also have restrictions and limitations with respect to the number of devices to authenticate and capabilities for redundancy. Furthermore, implementing message authentication could introduce latency in the communications response (NIST 2015). The corresponding latency often depends on the size, frequency, and quantity of the data blocks transferred. The following options are discussed further: Open Platform Communications Unified Architecture (OPC UA), Transport Layer Security (TLS), the use of Virtual Private Networks (VPN), bump in the wire hardware solutions, and software solutions integrated in the control and communications code of the microprocessors.

4.1. Open Platform Communications Unified Architecture (OPC UA)

The OPC UA is a platform-independent IEC62541 standard that enables the secure exchange of information in industrial systems. The OPC UA standard is a client-server or a publish-subscribe standard. The topology requires a server-based network. Vendors of industrial automation microprocessors often limit the number of potential clients the OPC UA server is capable of handling. Furthermore, to implement the standard, vendor-specific server application software is required to manage the security polices and certificates.

The OPC foundation further defines the following security features of OPC UA standard:

- **'Transport**: Numerous protocols are defined providing options such as the ultra-fast OPC-binary transport or the more universally compatible JSON over Websockets, for example.
- **Session Encryption**: Messages are transmitted securely at various encryption levels.
- **Message Signing**: With message signing, the recipient can verify the origin and integrity of received messages.
- **Sequenced Packets**: Sequencing eliminates exposure to message replay attacks.
- **Authentication**: Each UA client and server is identified through X509 certificates providing control over which applications and systems are permitted to connect with each other.
- **User Control**: Applications can require users to authenticate (login credentials, certificate, web token, etc.) and can further restrict and enhance their capabilities with access rights and address-space 'views.'
- **Auditing**: Activities by user and/or system are logged providing an access audit trail.'

(OPC Foundation 2022)

 https://doi.org/10.24868/10718

4.2. Transport Layer Security (TLS)

According to NIST Special publication 800-52 Revision 2, TLS 'is a layered protocol that runs on top of a reliable transport protocol—typically the Transmission Control Protocol (TCP),' (NIST, 2019). The fundamental principle is that the ICS data message is wrapped in the TLS layer providing authentication. This requires a client-server-based network architecture. TLS requires a certificate authority and key management. Several vendors require Domain Name System (DNS) servers. Some vendors restrict this option to TCP messages. It is currently not available in most cases for UDP. The use of certificates to authenticate ICS communication devices will also prevent the device from being hot swappable for quick replacement during a faulted module.

4.3. Virtual Private Network (VPN)

The concept of using VPNs is possible with some ICS vendor's latest communications devices. The technique is to create a VPN tunnel between two control stations. This typically requires the use of very specific communication modules. Remote access is a more common use for VPN security. Implementing a VPN for the purpose of secure peer-to-peer PLC communications requires a careful configuration of firewalls and network diagnostics. A VPN tunnel may not be available for some redundancy solutions such as hot backup for PLCs. Multicast UDP is not supported by most common VPN technologies but is currently available for PLC communication modules.

4.4. Bump-in-the-Wire Hardware Solutions

Solutions are available to place a device in proximity in front of an ICS communications physical connection port to handle message authentication. This method is commonly referred to as a 'bump in the wire.' This means every communications access point requires the device connection that handles the authentication and manages the certificates and keys used for encryption. Bump-in-the-wire authentication hardware devices are typically designed for specific ICS communication protocols. Several solutions are even available for legacy industrial communication protocols such as Modbus. This concept adds a level of complexity to the network topology. Some industrial communication protocols related to redundancy prevent the use of the bump-in-the-wire option. A careful evaluation of the response latency created by the added bump-in-the-wire device should be considered.

4.5. Message Authentication and Verification Software Solution

Another option for ICS message authentication is a software solution that encapsulates the PLC message data payload with a secure hash algorithm. One specific solution offers a custom communications algorithm at the application layer of the PLC. This option was investigated and published in a thesis authored by Dr. Kenneth Alan Fischer titled, 'Control System Data Integrity using a Variable-round Message Authentication Code with an Elliptic Curve Key Exchange Protocol.' The thesis defines the method as 'based on existing cryptographic algorithms such as the Secure Hash Algorithms (SHA), the Hash Message Authentication Code (HMAC) algorithms, the Elliptic Curve Diffie-Hellman Key Exchange algorithm, and a unique variant of an Elliptic Curve Cryptography (ECC) algorithm known as the Edward's Curve Digital Signature Algorithm (EdDSA).' (Fischer, K. A., 2017). This software solution is a two-part solution. The first part is the creation and verification of the secure hash using a variant of the HMAC-SHA256 algorithm. The second part of the solution is key management. One challenge with implementing a PLC-based message authentication and verification software solution is the trade-off between performance and security. The benefit of a purely software-based solution is that there is no impact on the network topology. Another benefit is this software solution is compatible with multicast UDP. The Key Exchange Protocol is a serverless network topology. The client-server strategy for managing the Key Exchange Protocol takes advantage of a dynamic client-server methodology. This dynamic methodology is based on a priority tree and whether the PLC has the key available for distribution.

 https://doi.org/10.24868/10718

5. Conclusions

Securing shipboard MCS using methods for message authentication and verification is necessary to protect against cybersecurity attacks. The strategies outlined in this paper are meant to maintain an air gap between the OT and the IT. New guidelines for ICS have addressed the need for proper message authentication. This paper investigated different network topologies and communication protocols for the purpose of defining options for message authentication. Specific options of ICS message authentication rely on network topologies. Most message authentication options are currently only available for specific ICS communication protocols. There is a challenge with implementing authentication while also incorporating redundancy. A shipboard MCS design needs to have a careful balance between performance, redundancy, and data message authentication. Communication protocols discussed were directly related to the network topologies. Communication protocols directly affect the options available for message authentication. Message authentication options discussed were OPC UA, TLS, VPNs, and a bump in the wire. A specific software option using a modified HMAC-SHA256 algorithm, and a Key Exchange Protocol was also discussed. The software solution at the application layer of a PLC that supports multicast UDP has been developed. Industrial automation vendors are currently actively developing new technologies for OT specifically for ICS. Hardware solutions could be years from actual implantation.

Acknowledgements

The author would like to acknowledge the inspiration for this paper is a direct result of the Noblis Sponsored Research project 'Industrial Automation Cyber Security Message Authentication and Verification.' The author would like to acknowledge the research by Kerry Hansen, a member of the Noblis Sponsored Research project team.

The author would like to acknowledge the input collected and inspiration from reviewing the dissertation 'Industrial Automation Cyber Security Message Authentication and Verification' authored by Dr. Kenneth Alan Fischer, chief of cybersecurity, SSTM Naval Surface Warfare Center Philadelphia Division.

References

Fischer, K. A. (2017). *Control System Data Integrity using a Variable-round Message Authentication Code with an Elliptic Curve Key Exchange Protocol. (*Publication No.10687303). Doctoral dissertation College of Engineering Villanova University. ProQuest Dissertations Publishing

Inspections and Compliance Directorate. (2019*). Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels* (Safety Alert 06-19). United State Coast Guard. Retrieved from https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/Alerts/0619.pdf

Inspections and Compliance Directorate (2019). *Cyber Adversaries Targeting Commercial Vessels* (MSIB Number : 04-19). United State Coast Guard. Retrieved from https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/MSIB/2019/MSIB_004_19.pdf

NIST, National Institute of Standards and Technology (2019) *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations.* (NIST Special Publication 800-52 Revision 2). U.S. Department of Commerce. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final

NIST, National Institute of Standards and Technology (2015) *Guide to Industrial Control Systems (ICS) Security*. (NIST Special Publication 800-82 Revision 2). U.S. Department of Commerce. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

OPC Foundation, (2017). *OPC Unified Architecture Part 1: Overview and Concepts*. (OPC 10000-1). Release 1.04. Retrieved from https://opcfoundation.org/developer-tools/specifications-unified-architecture/part-1-overview-and-concepts/

OPC Foundation, (2018). *OPC Unified Architecture Part 2: Security Model.* (OPC 10000-2). Release 1.04. Retrieved from https://opcfoundation.org/developer-tools/specifications-unified-architecture/part-2-security-model/

 https://doi.org/10.24868/10718

OPC Foundation (2022)**,** *About » OPC Technologies » Unified Architecture***.** https://opcfoundation.org/about/opc-technologies/opc-ua/

World Economic Forum. (2020). *Global Risk Report 2020*. 15th Edition.
Retrieved from https://www.weforum.org/reports/the-global-risks-report-2020/

Bibliography

Cisco Systems, Inc., Panduit Corp., and Rockwell Automation, Inc (2021). *Deploying CIP Security within a Converged Plantwide Ethernet Architecture. (NET-TD022A-EN-P).* Retrieved from https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td022_-en-p.pdf

Rockwell Automation, (2021). *CIP Security with Rockwell Automation Products. (SECURE-AT001B-EN-P).* Rockwell Automation. Retrieved from https://literature.rockwellautomation.com/idc/groups/literature/documents/at/secure-at001_-en-p.pdf

Siemens, (2021). *S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro, ET 200eco PN Communication Function Manual. (A5E03735815-AH, 05/2021).* Siemens AG. retrieved from https://support.industry.siemens.com/cs/document/59192925/simatic-s7-1500-et-200mp-et-200sp-et-200al-et-200pro-et-200eco-pn-communication?dti=0&pnid=14751&lc=en-US

Glossary

DNS – Domain Name Server
ECC - Elliptic Curve Cryptography
EdDSA - Edward's Curve Digital Signature Algorithm
HMAC - Hash Message Authentication Code
HSR – High-Availability Seamless Redundancy
ICS - Industrial Control System
IT – Information Technology
LAN – Local Area Network
MRP – Media Redundancy Protocol
OPC UA - Open Platform Communications Unified Architecture
PLC – Programmable Logic Controller
PRP – Parallel Redundant Protocol
OT – Operational Technology
TLS- Transport Layer Security
UDP – User Datagram Protocol
USCG – United States Coast Guard
VPN Virtual Private Network

Creative Commons Licences

 https://doi.org/10.24868/10718