T9070-BR-DPC-010/202-1

ORIGINAL

NAVSEA TECHNICAL PUBLICATION

DESIGN PRACTICES AND CRITERIA FOR THE ARCHITECTURE OF SHIPBOARD MACHINERY CONTROL SYSTEMS

PUBLISHED BY DIRECTION OF COMMANDER, NAVAL SEA SYSTEMS COMMAND

10 MAY 2016

LIST OF EFFECTIVE PAGES

Dispose of superseded pages in accordance with applicable regulations.

Dates of issue for original and subsequent revisions:

Original…………………………… 10 May 2016

TOTAL NUMBER OF PAGES IN THIS PUBLICATION IS 40, CONSISTING OF THE FOLLOWING:

Page No.

Title and A
i through vi
1-1
1-2 blank
2-1 through 2-2
3-1 through 3-4
4-1 through 4-17
4-18 blank
A-1 through A-3
A-4 blank
TMDER

TABLE OF CONTENTS

Chapter/Paragraph/Title **Page**

Chapter/Paragraph/Title **Page**

Chapter/Paragraph/Title **Page**

LIST OF FIGURES

Table Title Page

FOREWORD

The purpose of Design Practices and Criteria (DPC) Manuals is to provide ship design practices and criteria to personnel involved with the design, conversion, or modernization of U.S. Navy ships. This Manual is therefore part of a library of DPC Manuals. A listing of all DPC Manuals and other ship design documents can be found in the DPC Index (NAVSEA publication T9070-AE-DPC-010/001-1).

This manual was written to enhance commonality and affordability across all surface ship platforms and ensure reliable, maintainable, and survivable Machinery Control Systems (MCS) throughout the ships' lifecycles.

MCS hardware, software, and architecture deep dives identified 24 key elements of prior and current Navy MCS. These 24 key elements are identified as critical design decision points and have been examined for variation within the Fleet with respect to MCS Total Ownership Cost (TOC), performance, and survivability. The results of this examination identified the need for MCS variation reduction.

The Design Practices and Criteria for the Architecture of Shipboard Machinery Control Systems Manual includes architecture design requirements and alternatives for developing and specifying future shipboard MCS. The MCS architecture design specifications enable the designer (e.g., Ship Design Managers, MCS integrators, or In-Service Engineering Agents) to make judicious technical selections that provide the best value for the Navy. Use of this manual will decrease the overall MCS acquisition and life cycle costs on naval shipboard assets by utilizing common affordable MCS architectures that are reliable and maintainable. It is not the intent of this document to stand alone as a complete MCS specification. A complete shipboard MCS specification would address details beyond the architecture, as well as other Navy and Government standards, including, but not limited to, environmental specifications, testing, verification, and program-specific acquisition requirements such as Survivability, Information Assurance, Producability, Reliability, and Maintainability. As such, this manual is not a replacement of the Ship Work Breakdown Structure (SWBS) Section 202. NAVSEA requires all current and future Ship Design Teams to enforce this manual for any shipboard MCS specification.

For information pertaining to architecture of shipboard machinery control systems, please contact SEA 05Z, Dr. Edward Ammeen, commercial (202) 781-5195, email: edward.ammeen@navy.mil.

This manual is organized as follows:

Chapter 1, Scope

Chapter 2, Referenced Documents

Chapter 3, General Requirements

Chapter 4, Detailed Requirements

Appendix A, List of Acronyms and Definitions

TMDER INSTRUCTIONS

Ships, training activities, supply points, depots, Naval Shipyards and Supervisors of Shipbuilding are requested to arrange for the maximum practical use and evaluation of NAVSEA and SPAWAR technical manuals (TMs). All errors, omissions, discrepancies, and suggestions for improvement to NAVSEA and SPAWAR TMs shall be submitted as a Technical Manual Deficiency/Evaluation Report (TMDER). All feedback comments shall be thoroughly investigated and originators will be advised of action resulting there from.

The NAVSEA/SPAWAR Technical Manual Deficiency/Evaluation Report form, NAVSEA 4160/1 is included at the back of the TM.

The following methods are available for generation and submission of TMDERs against unclassified TMs:

For those with a Technical Data Management Information System (TDMIS) account, the most expedient and preferred method of TMDER generation and submission is via the TDMIS website at: https://mercury.tdmis.navy.mil/.

For those without a TDMIS account, generate and submit TMDER via the Naval Systems Data Support Activity (NSDSA) website at: https://mercury.tdmis.navy.mil/def_external/pubsearch.cfm. (TDMIS accounts may be requested at the NSDSA website at: https://nsdsa.nmci.navy.mil/, by submitting a Customer Service Request (CSR).)

When internet access is not available, submit TMDER via hardcopy to:

COMMANDER NAVAL SURFACE WARFARE CENTER
NAVAL SYSTEMS DATA SUPPORT ACTIVITY
4363 MISSILE WAY
ATTN: CODE 310 BLDG 1389 TMDERS
PORT HUENEME, CA 93043-4307

Additional copies of the TMDER form may also be downloaded from the Naval Systems Data Support Activity (NSDSA) website at: https://nsdsa.nmci.navy.mil/, by clicking on the blue tab labeled "Reference Docs/Forms".

TMDERs against classified/restricted TMs (includes all NOFORN) must be submitted using the hardcopy method cited above.

Urgent priority TM deficiencies shall be reported by Naval message with transmission to Port Hueneme Division, Naval Surface Warfare Center (Code 310), Port Hueneme, CA. Local message handling procedures shall be used. The message shall identify each TM deficiency by TM identification number and title. This method shall be used in those instances where a TM deficiency constitutes an urgent problem, (i.e., involves a condition, which if not corrected, could result in injury to personnel, damage to the equipment, or jeopardy to the safety or success of the mission).

Complete instructions for TMDER generation and submission are detailed on the NSDSA website at: https://nsdsa.nmci.navy.mil/, by clicking on the blue tab labeled "TMDER/ACN" and then clicking on the gray button labeled "TMDERs".

CHAPTER 1
SCOPE

1.1 SCOPE.

This manual covers architecture design requirements and alternatives for developing and specifying future shipboard Machinery Control Systems (MCS). Requirements that fall outside of the architecture of an MCS are not covered in this document.

1.2 PURPOSE.

The goal is to decrease the overall MCS acquisition and life cycle costs on naval shipboard assets by ensuring future MCS architectures meet the requirements of this manual. It is not the intent of this document to stand alone as a complete MCS specification. A complete shipboard MCS specification would address details beyond the architecture, as well as other Navy and Government standards, including, but not limited, to environmental specifications, testing, verification, and program-specific acquisition requirements such as Survivability, Information Assurance, Producability, Reliability, and Maintainability. In other words, this manual is not a one-to-one (1:1) replacement of the Ship Work Breakdown Structure (SWBS) Section 202. This manual is intended to be a set of requirements for defining architecture requirements when writing a complete MCS specification. As such, this manual should be referenced in part or whole when specifying a complete shipboard MCS. The author of any shipboard MCS specification should review the requirements and alternatives herein and utilize the most appropriate architecture solution in conjunction with other specifications and standards for the respective MCS application.

CHAPTER 2
APPLICABLE DOCUMENTS

2.1 GENERAL.

The documents listed in this section are specified in chapters 3 or 4 of this manual. This section does not include documents cited in other sections of this manual or recommended for additional information or as examples. While every effort has been made to ensure the completeness of this list, document users are cautioned that they must meet all specified requirements of documents cited in chapters 3 or 4 of this manual, whether or not they are listed.

2.2 GOVERNMENT DOCUMENTS.

2.2.1 Specifications, Standards, and Handbooks. The following specifications, standards, and handbooks form a part of this document to the extent specified herein. Unless otherwise specified, the issues of these documents are those cited in the solicitation or contract.

DATA ITEM DESCRIPTIONS

DI-IPSC-81436	-	Interface Design Description (IDD)

DEPARTMENT OF DEFENSE SPECIFICATIONS

MIL-PRF-32006	-	Programmable Controller, Naval Shipboard

(Copies of these documents are available online at http://quicksearch.dla.mil/.)

2.2.2 Other Government Documents, Drawings, and Publications. The following other Government documents, drawings, and publications form a part of this document to the extent specified herein. Unless otherwise specified, the issues of these documents are those cited in the solicitation or contract.

DEPARTMENT OF DEFENSE DOCUMENTS

DoD Instruction 8500.2	-	Information Assurance Implementation

(Copies of this document are available online at www.dtic.mil/whs/directives/.)

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

NIST SP 800-53	-	Security and Privacy Controls for Federal Information Systems and Organizations
NIST SP 800-82	-	Guide to Industrial Control Systems (ICS) Security

(Copies of these documents are available online at http://www.nist.gov.)

2.3 NON-GOVERNMENT PUBLICATIONS.

The following documents form a part of this document to the extent specified herein. Unless otherwise specified, the issues of these documents are those cited in the solicitation or contract.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC. (IEEE)

IEEE 1014	-	IEEE Standard for a Versatile Backplane Bus: VMEbus

(Copies of this document are available online at www.ieee.org.)

2.4 ORDER OF PRECEDENCE.

Unless otherwise noted herein or in the contract, in the event of a conflict between the text of this document and the references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

CHAPTER 3
GENERAL REQUIREMENTS

3.1 MCS.

The MCS shall be a layered system consisting of a Presentation Layer for graphical user interface, an Information Layer for data-centric logic, such as information and alarm processing, formatting, scaling, transfer of control logic, etc., a Network Layer for the transmission of data from the Presentation Layer throughout the Control Layer and out to the field devices, and a Control Layer for the input, processing, and output of external system and field device data and signals (see Figure 3-1).

NOTE

The Presentation Layer (or GUI) will not be addressed in this architecture document, as it will not contain any logic and will act solely as the graphical portion of the HMI, independent of the MCS architecture. The Presentation Layer and the Information Layer make up the HMI.

NOTE

MCS is a large distributed system that interfaces with and provides control and monitoring to many shipboard systems. If a ship system implements a local control capability outside the boundaries of the MCS, there shall be consultation with the MCS and Network Technical Warrant Holders (TWHs) prior to initial and final design.

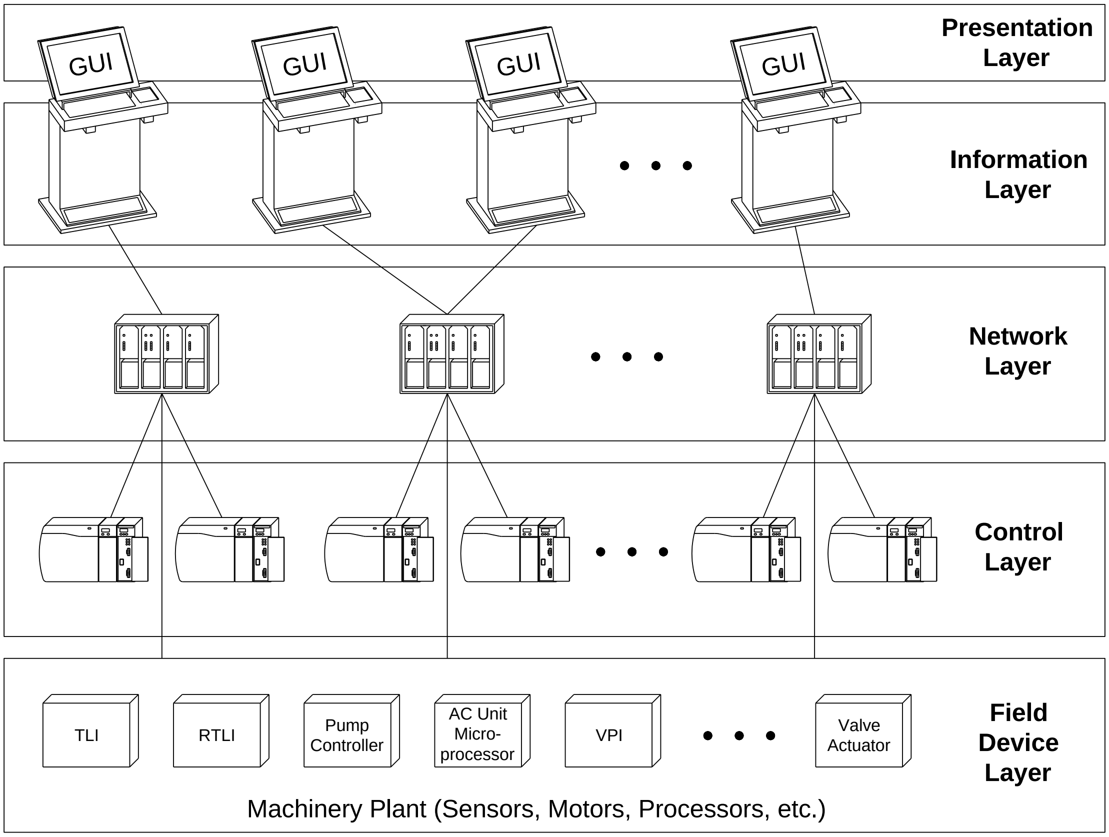


Figure 3-1. MCS Architecture.

3.2 MODULARITY.

The Information, Control, and Network Layers shall be modular in design with independent software modules that drive their respective layer's functionality.

3.2.1 Interface. Each software module within each layer shall contain well-defined boundaries documented by interface design documentation in accordance with Interface Design Document (IDD) Data Item Description (DID) DI-IPSC-81436.

3.3 REDUNDANCY.

A scheme(s) for duplicating critical MCS components or functions shall be implemented based on survivability and reliability analysis with respect to power, HMI, the inherent redundancy of the controlled system, and alternative (such as local) control and monitoring capabilities. The analysis shall consider MCS size, space limitations, and any other overall ship design constraints.

NOTE

A usability and survivability analysis may indicate that redundancy is not required at all for some non-critical components or where there is mechanical redundancy in the ship or in other situations.

3.3.1 Power. The MCS shall have a zonal or individual source(s) of uninterruptable backup power that maintains MCS equipment in accordance with program/platform specific requirements and Concept of Operations (CONOPS).

3.3.1.1 Backup Type. The shipboard zones or individual sources of backup power shall be determined through survivability analysis.

3.3.1.2 Redundancy Scheme. The power redundancy scheme shall consider the effect on MCS availability.

3.3.2 User Interface. The MCS shall have multiple HMIs capable of providing identical monitoring and control by an operator. The quantity and location of HMIs shall be determined through usability and survivability analysis.

3.3.3 Hardware. The MCS shall provide redundant control and monitoring hardware for signals or functions designated as mission-critical.

3.3.3.1 Redundancy. The redundant control and monitoring hardware shall be determined through reliability and survivability analysis and implemented in accordance with the Control Layer requirements herein. The level of redundancy shall meet the level of redundancy in the system being controlled and monitored.

3.3.4 Evaluation. A cost/benefit analysis of the redundancy scheme(s) chosen shall be completed and documented.

3.4 CONFIGURABILITY.

The MCS shall have the ability to configure certain dynamic variables (e.g., alarm settings and set points within a predefined range) without compiling computer code, uploading files, and reinstalling the MCS application.

3.5 SECURITY.

The MCS architecture shall implement a security capability through analysis of threats which shall drive the control system implementation details on all MCS devices, both physically and with respect to cyberwarfare, to mitigate those threats and the impacts of attacks.

3.5.1 Analysis. The analysis shall identify assets (e.g., control consoles/HMIs, backbone network, control processor, communication interfaces, I/O, network, etc.) and threats, both accidental and malicious (e.g., APT, threats on system availability, integrity, and authenticity), to the MCS and identify mitigation considerations.

3.5.2 Considerations. The MCS shall consider, at a minimum, the following security measures:

(a) Physical security shall consider, but not be limited to:

(1) Proper signage of equipment

(2) Locked enclosures for primary control elements

(3) Enclosures with intrusion detection

(4) Obstructed or removed external ports

(b) Network security shall consider, but not be limited to:

(1) Disabling unused ports

(2) Port-based security

(3) Media Access Control (MAC) based security

(4) Disabling unused services and protocols

(5) Default security parameters

(6) Secure network protocols

(7) Intrusion detection

(c) Controller (PLC) security shall consider, but not be limited to:

(1) Password authentication

(2) Login failure lockout

(3) Password failure lockout

(4) Code protection

(5) Control firmware validation

(6) Digital signatures

(d) Console/computing security shall consider, but not be limited to:

(1) User access

(2) Application white-listing

(3) Operating system patching

(e) Application security shall consider, but not be limited to:

(1) Virus scanning

(2) Secure coding standards

(3) Application authentication

(f) System security shall consider, but not be limited to:

(1) Virus scanning

(2) Change logs

(3) User authorization

(4) Password standards

(5) Vendor default modifications

(6) Disabling or removal of unused ports

(7) Protocols

(8) Software features

(9) Information Awareness (IA) training

(g) External interface security shall consider, but not be limited to, firewalls.

(h) Supply chain security shall consider, but not be limited to, U.S. parts only.

3.5.3 Implementation. The MCS design shall be implemented in consideration of the above security measures and in accordance with NIST Special Publications 800-53 and 800-82 and DoD Instruction 8500.2.

3.5.4 Evaluation. After an MCS design is complete and before it is implemented, a security evaluation of that design shall be completed. An evaluation method shall be chosen to identify areas of insufficient security as well as to provide a method by which MCS designers may evaluate and subsequently improve the overall security of the MCS as the MCS assets and subsequent threats evolve. The evaluation shall document the security measures considered for implementation and how each determination was made whether to implement (and how) for each security measure considered.

3.6 SUPPORTABILITY.

The MCS architecture shall address obsolescence through analysis and use of commercial or Government off-the-shelf equipment (COTS/GOTS) versus specialized, uniquely designed hardware.

3.7 COMPONENT CABLING.

The MCS shall utilize the most efficient combination of copper and fiber cabling derived from platform/system requirements for transmitting data between I/O units, control processors, and network components based on installation and life cycle maintenance costs.

3.7.1 Field Device Cabling. The MCS shall utilize hardwire (e.g., 4 – 20 milliamp, 0 – 10 volt) or copper cabling for transmitting data between I/O units and field devices. Fiber optic cabling shall not be used for MCS-to-field device connections to eliminate interruptions in communication to MCS due to vibration.

3.7.2 Cable Installation. All cable shall be installed in accordance with Navy and program-specific standards and specifications.

CHAPTER 4
DETAILED REQUIREMENTS

4.1 INFORMATION LAYER.

The Information Layer shall act as a platform for applications that utilize and manipulate MCS data through interaction with users through a Presentation Layer.

NOTE

Alarm management and processing will not be addressed in this architecture document as it will be dependent upon specific applications; it is independent of the MCS architecture.

4.1.1 Consoles. The Information Layer shall include local and remote consoles, or HMIs, to control and monitor the multiple systems and subsystems within and that interface with the MCS. Each console shall have the HMI hardware to control and monitor all systems and subsystems, including monitoring the MCS for system health and administration. Each console shall provide software configurability (i.e., systems controlled/monitored, level of control, etc.) for controlling and monitoring specific ship systems and subsystems, including the MCS itself.

4.1.1.1 Local Consoles. Local Consoles shall be co-located (i.e., in the same compartment or adjacent control room for that compartment) with the equipment being controlled and monitored by that Local Console.

4.1.1.2 Remote Consoles. Remote Consoles shall be installed in the ship's Central Control Station (CCS), secondary CCS, and distributed across the ship in accordance with program-specific requirements to remotely monitor and control local and distributed ship systems.

4.1.1.3 Data Logging. Alarm Logs, Data Logs, Event Logs, Diagnostic Logs, Bell Logs, and any other data used post processing shall be stored and manipulated on hardware and software independent of, but accessible by, the MCS.

4.1.2 Transfer of Control. The Information Layer shall include functionality to arbitrate and move the control and monitoring roles from HMI to HMI across different consoles/GUIs.

4.2 NETWORK LAYER.

The Network Layer shall provide communication of data and signals within the MCS, including all data and signals between the Control Layer and the Information Layer, as well as any interface for data or signals coming into or going out of the MCS to and from external systems and field devices.

NOTE

Within the Network Layer section, there shall be consultation with the Network TWH prior to the design and use of network switches.

4.2.1 Information Consumption Methodology. The Network Layer shall employ a Producer/Consumer methodology for independently transmitting MCS information to and from devices.

4.2.2 Communication Scheme. The Network Layer shall implement a Unicast or Multicast communication scheme to transmit information from the HMIs to the Control Layer. The Network Layer shall not include centralized Tag Servers on intermediary hardware in the field that act as mediators between HMI consoles and controllers in the field.

4.2.2.1 Passive Listening. Passive listening shall be precluded by creating a federated interface for third party control and monitoring (i.e., do not use Multicast on defined and tested interfaces.).

4.2.3 Network Configuration. The network shall be dedicated to MCS data transmission. When the MCS has a connection to other equipment, systems, or networks, the connection shall be implemented through well-defined boundaries, non-restrictive of firewalls.

4.2.3.1 Field Device to I/O Unit. The field devices shall be configured in a single-connection, ring, dual ring (i.e., each node connected to two survivably separated rings), star (each node homed to a single I/O connection), or dual star (i.e., each node is homed to at least two separate I/O units) configuration back to the respective I/O unit.

4.2.3.1.1 Single Connection. The single connection configuration shall be used when a dedicated point-to-point connection is necessary (see Figure 4-1).

NOTE

Hardwire point-to-point, non-networked, non-computer processed command backups outside of the MCS architecture, such as Emergency STOP commands for rotating equipment, may be required in the event of a major casualty.

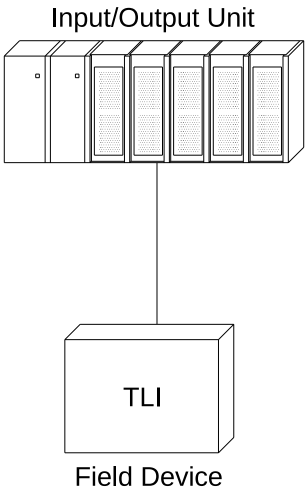


Figure 4-1. Functional Depiction of a Notional Single Connection from an I/O Unit to a Field Device.

4.2.3.1.2 Ring. The ring configuration shall only be used in non-mission-critical networks when there are three field devices or less, or when every field device depends on every other field device to operate (see Figure 4-2). The ring configuration shall not be used in mission-critical networks.

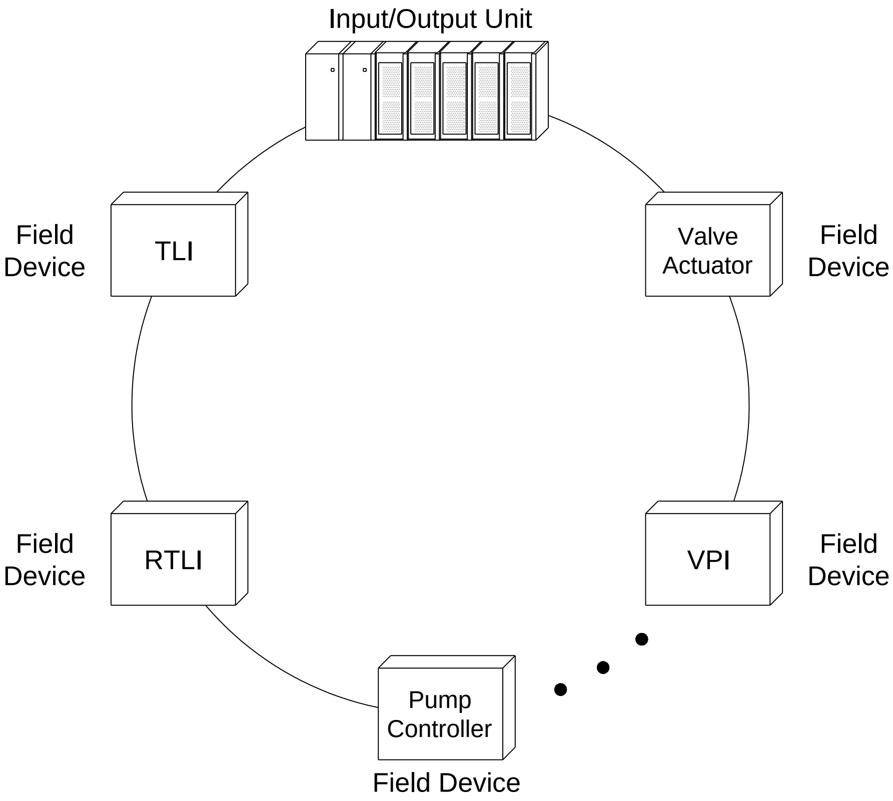


Figure 4-2. Functional Depiction of a Notional Ring Topology from an I/O Unit to Field Devices.

4.2.3.1.3 Dual Ring. The dual ring configuration shall only be used in mission-critical networks when there are three field devices or less, or when every field device depends on every other field device to operate (see Figure 4-3). The dual ring configuration shall not be used when there are more than three field devices or when field devices can act independently of each other.

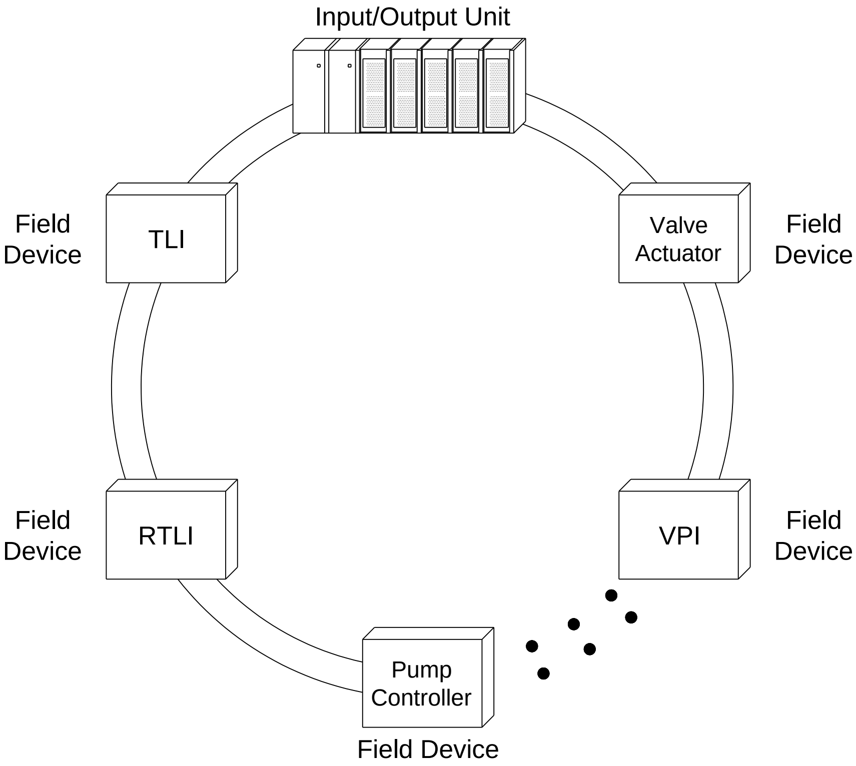


Figure 4-3. Functional Depiction of a Notional Dual Ring Topology from an I/O Unit to Field Devices.

4.2.3.1.4 Star. The star configuration shall be used when the number of field devices is four or more (see Figure 4-4).

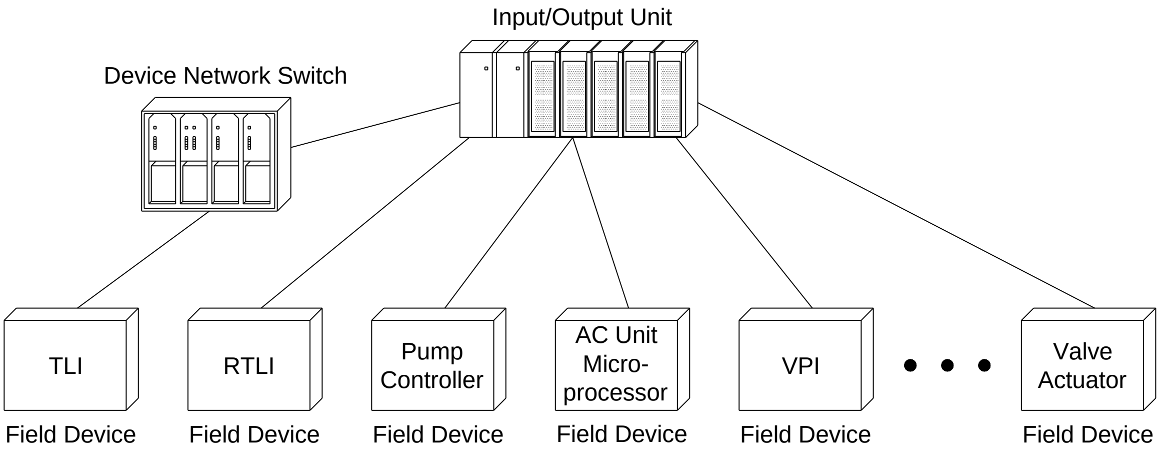


Figure 4-4. Functional Depiction of a Notional Star Topology from an I/O Unit to Field Devices (Direct and through a Network Device Switch).

4.2.3.1.5 Dual Star. The redundant star configuration shall be used when redundancy is required for mission-critical field devices (see Figure 4-5).

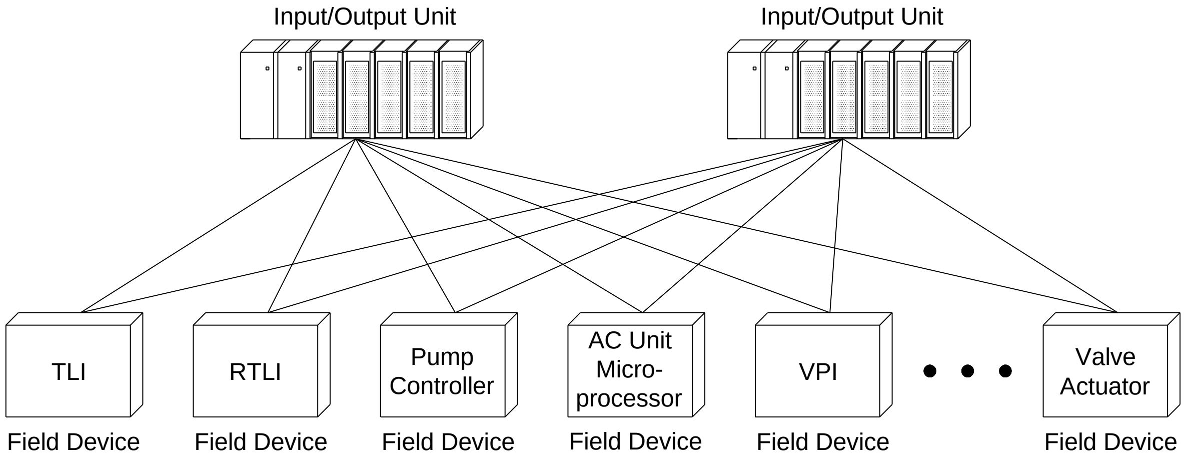


Figure 4-5. Functional Depiction of a Notional Dual Star Topology from I/O Units to Field Devices.

4.2.3.2 I/O Unit to PLC/Control Processor. The I/O units shall be configured in a ring, dual ring (i.e., each node connected to two survivably separated rings), star (each node homed to a single switch), or dual star (i.e., each node is homed to at least two separate switches) configuration back to the respective Group's processor.

4.2.3.2.1 Ring. The ring configuration shall only be used in non-mission-critical networks when there are three nodes or less, or when every node depends on every other node to operate (see Figure 4-6). The ring configuration shall not be used in mission-critical networks.

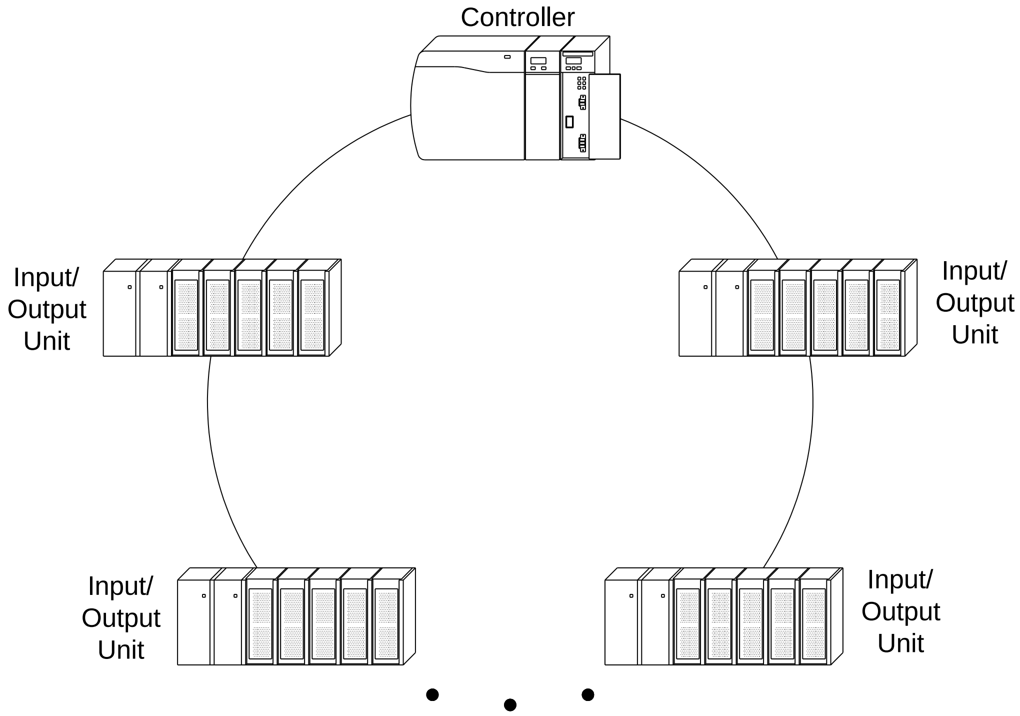


Figure 4-6. Functional Depiction of a Notional Ring Topology from a PLC/Control Processor to I/O Units.

4.2.3.2.2 Dual Ring. The dual ring configuration shall only be used in mission-critical networks when there are three nodes or less, or when every node depends on every other node to operate (see Figure 4-7). Shipboard systems, such as conveyors and elevators, are candidates for dual ring topologies as every I/O unit and sensor suite depends on every other I/O unit and sensor suite to operate the system as a whole. The dual ring configuration shall not be used when there are more than three nodes or when I/O units and sensors can act independently of each other.

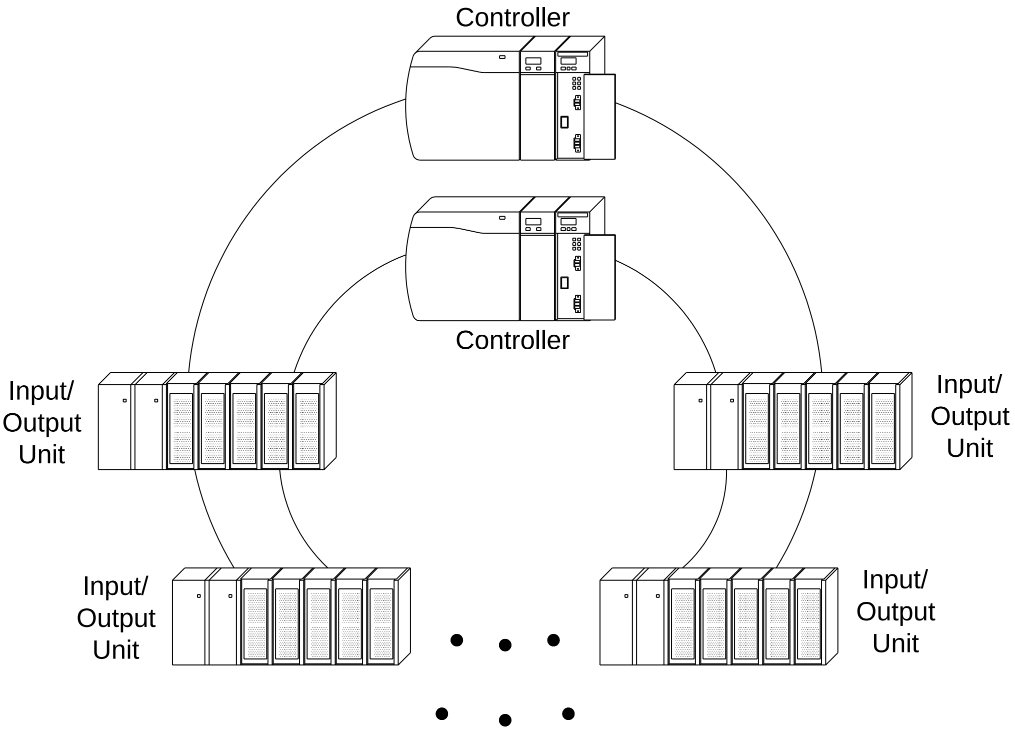


Figure 4-7. Functional Depiction of a Notional Dual Ring Topology from PLC/Control Processors to I/O Units.

4.2.3.2.3 Star. The star configuration shall be used when controller (i.e., PLC or VME) redundancy is not required, when industrial network switches that possess a minimum of 20 years mean time between failures (MTBF) at 60 °C are utilized, and when copper cabling is used between the network switches and nodes (see Figure 4-8). The star configuration shall not be used when controller redundancy is required or when fiber optic cabling is used.

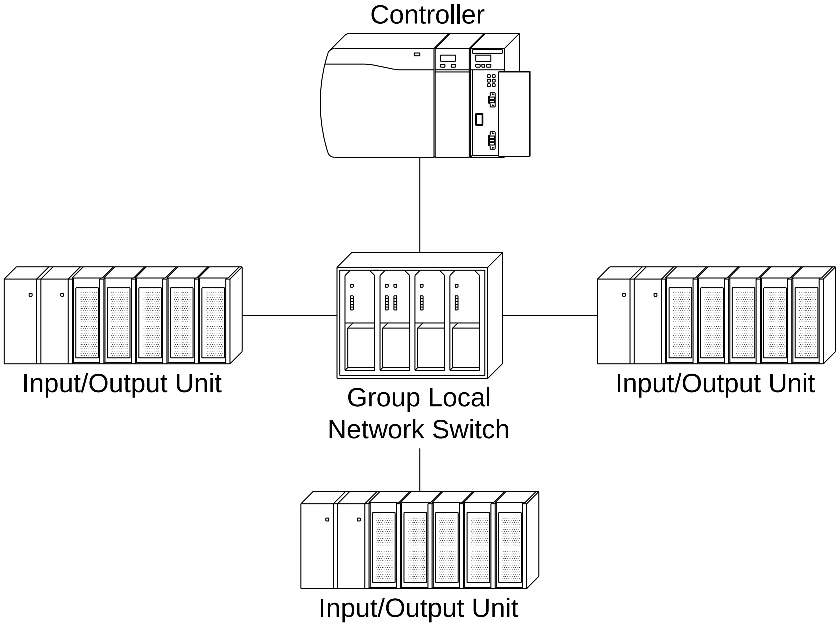
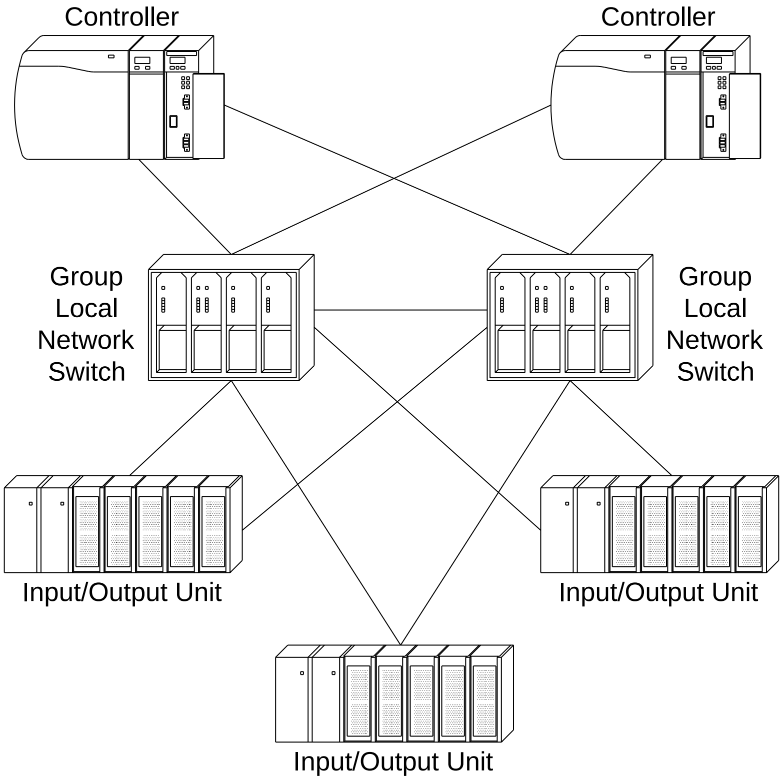


Figure 4-8. Functional Depiction of a Notional Star Topology from a PLC/Control Processor to I/O Units.

4.2.3.2.4 Dual Star. The redundant star configuration shall be used when controller (i.e., PLC or VME) redundancy is required, or fiber optic cabling between switches and nodes is required (see Figure 4-9).



NOTE: This dual star is depicted with dual controllers but that part of the redundancy is not required.

Figure 4-9. Functional Depiction of a Notional Dual Star Topology from PLC/Control Processors to I/O Units.

4.2.3.3 PLC/Control Processor to PLC/Control Processor. Group processors shall be configured in a ring, dual ring (i.e., each node connected to two survivably separated rings), star (each node homed to a single switch), dual star (i.e., each node is homed to at least two separate switches), mesh (every node is connected to every other node), or dual mesh (every node is connected to every other node twice) configuration.

NOTE

The PLC/control processor to PLC/control processor section is specific to the processor-to-processor configuration, which is independent of the core ship-wide network configuration. The core ship-wide network configuration is not subject to these requirements.

4.2.3.3.1 Ring. The ring configuration shall only be used in non-mission-critical networks when there are three nodes or less, or when every node depends on every other node to operate (see Figure 4-10). The ring configuration shall not be used in mission-critical networks.

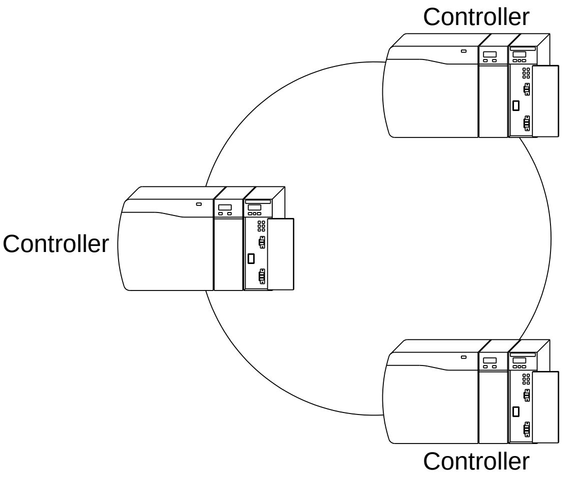


Figure 4-10. Functional Depiction of a Notional Ring Topology from PLC/Control Processors to other PLC/Control Processors.

4.2.3.3.2 Dual Ring. The dual ring configuration shall only be used in mission-critical networks when high network survivability is required, when incorporation of new network devices after implementation is highly probable, and when a logical segmentation of the network is required (i.e., segment separate user groups/systems into separate broadcast domains (e.g., Virtual Local Area Networks [VLANs]/subnets) while still allowing Unicast/Multicast communication between them) (see Figure 4-11).

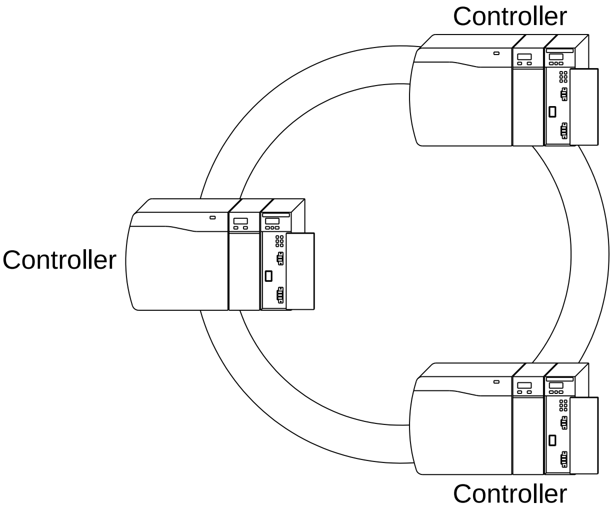


Figure 4-11. Functional Depiction of a Notional Dual Ring Topology from PLC/Control Processors to other PLC/Control Processors.

4.2.3.3.3 Star. The star configuration shall be used when controller (i.e., PLC or VME) redundancy is not required, when industrial network switches that possess a minimum of 20 years MTBF at 60 °C are utilized, and when copper cabling is used between the network switches and nodes (see Figure 4-12). The star configuration shall not be used when controller redundancy is required or when fiber optic cabling is used.

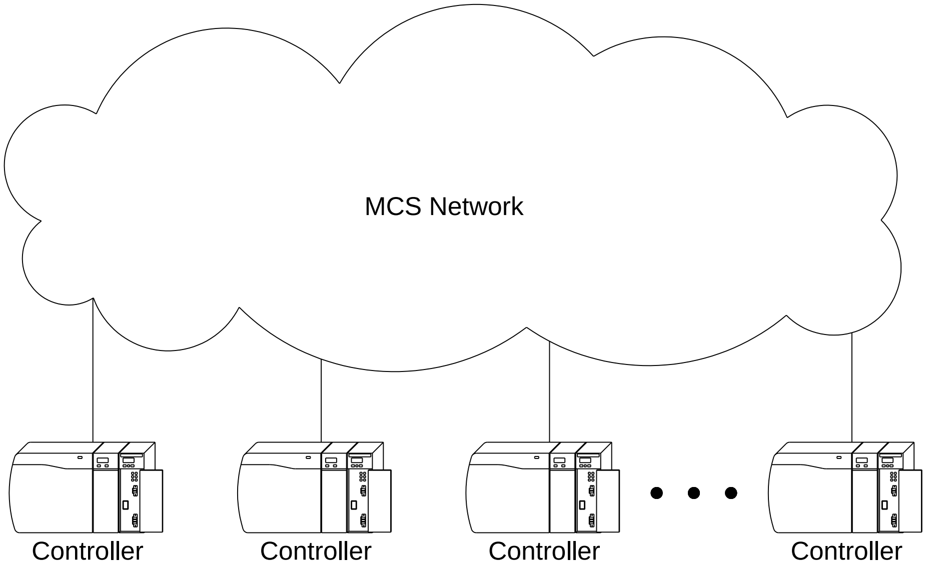


Figure 4-12. Functional Depiction of a Notional Star Topology from PLC/Control Processors to other PLC/Control Processors.

4.2.3.3.4 Dual Star. The redundant star configuration shall be used when controller (i.e., PLC or VME) redundancy is required, or fiber optic cabling between switches and nodes is required (see Figure 4-13).

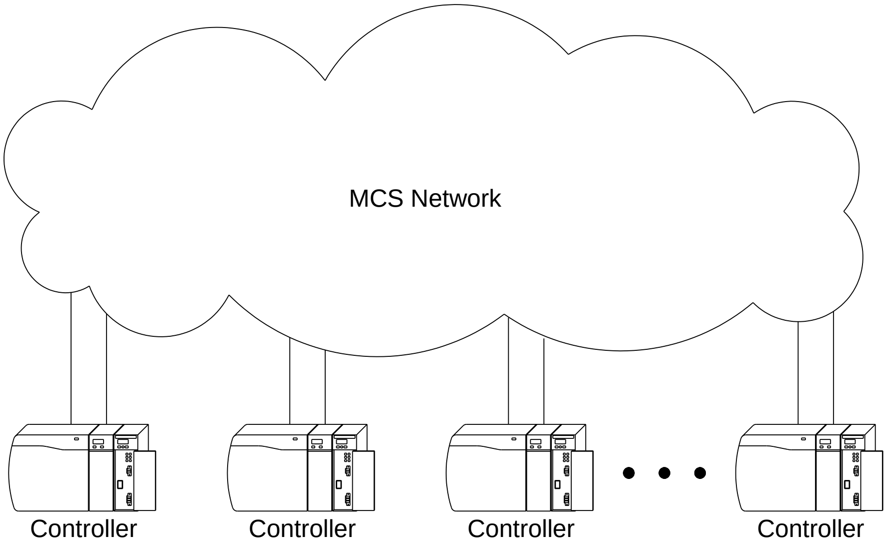


Figure 4-13. Functional Depiction of a Notional Dual Star Topology from PLC/Control Processors to other PLC/Control Processors.

4.2.3.3.5 Mesh. The mesh configuration shall be used when cloud processing (e.g., roving, de-centralized, virtual PLC, PC-based control) is utilized at the controller level (see Figure 4-14).

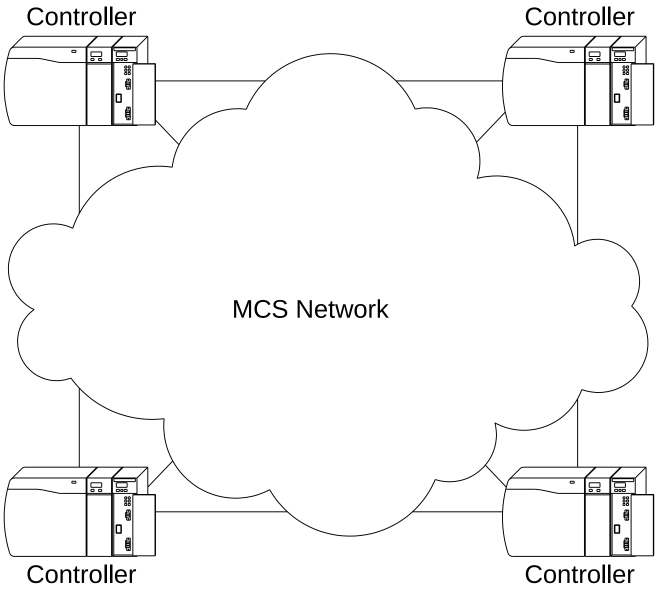


Figure 4-14. Functional Depiction of a Notional Mesh Topology from PLC/Control Processors to other PLC/Control Processors.

4.2.3.3.6 Dual Mesh. The dual mesh configuration shall be used when cloud processing (e.g., roving, de-centralized, virtual PLC, PC-based control) is utilized at the controller level; survivability, availability, and maintainability are a priority; and when cost is not a large factor (see Figure 4-15).

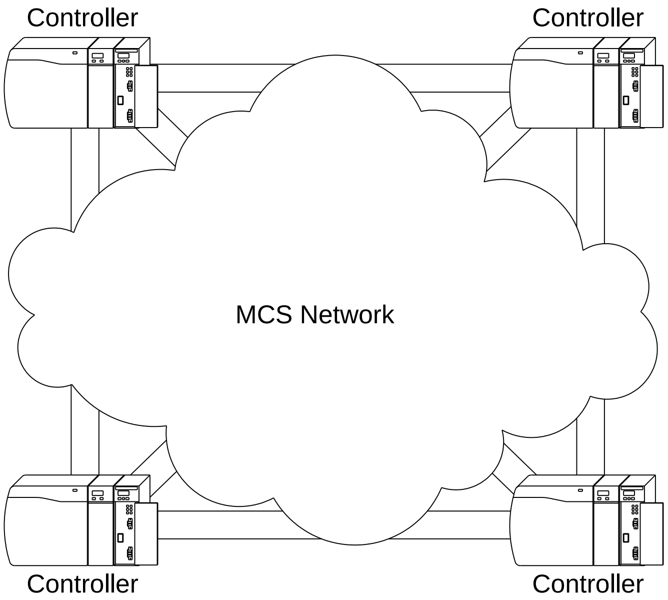


Figure 4-15. Functional Depiction of a Notional Dual Mesh Topology from PLC/Control Processors to other PLC/Control Processors.

4.2.3.4 HMIs. The HMIs shall be configured as remote and local workstations, as required by each system being controlled and monitored and in accordance with program/platform specific requirements and CONOPS.

4.2.3.4.1 Remote. Remote HMIs shall be configured to transmit and receive data and information to and from PLCs/control processors over the network through group local network switches (see Figure 4-16).

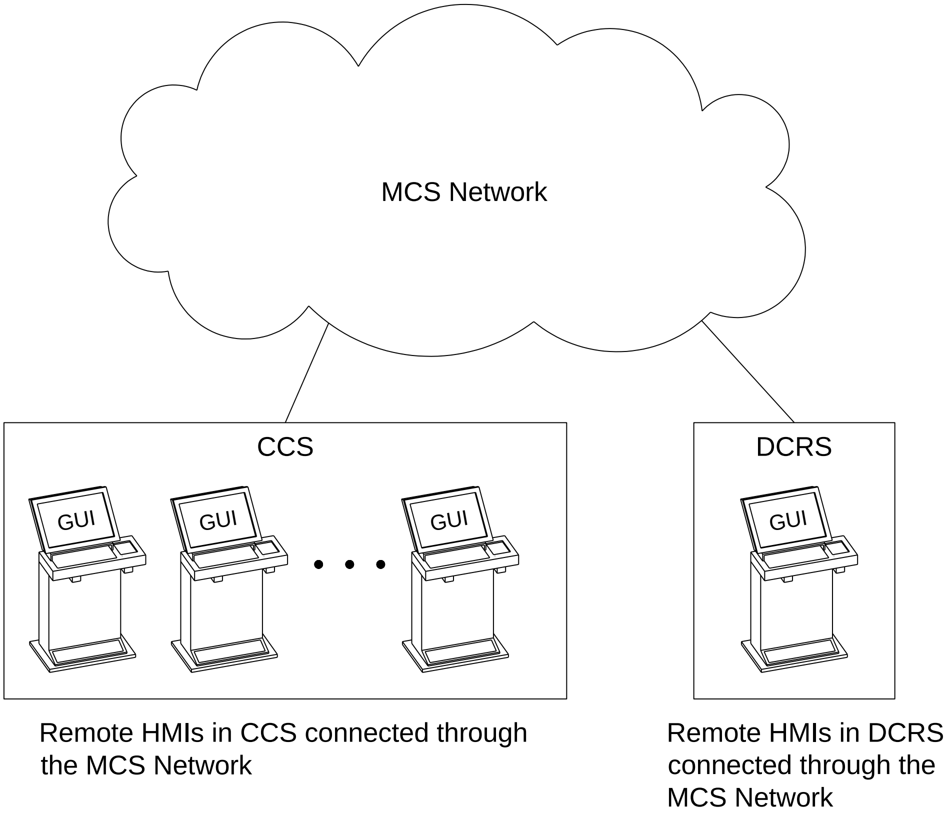
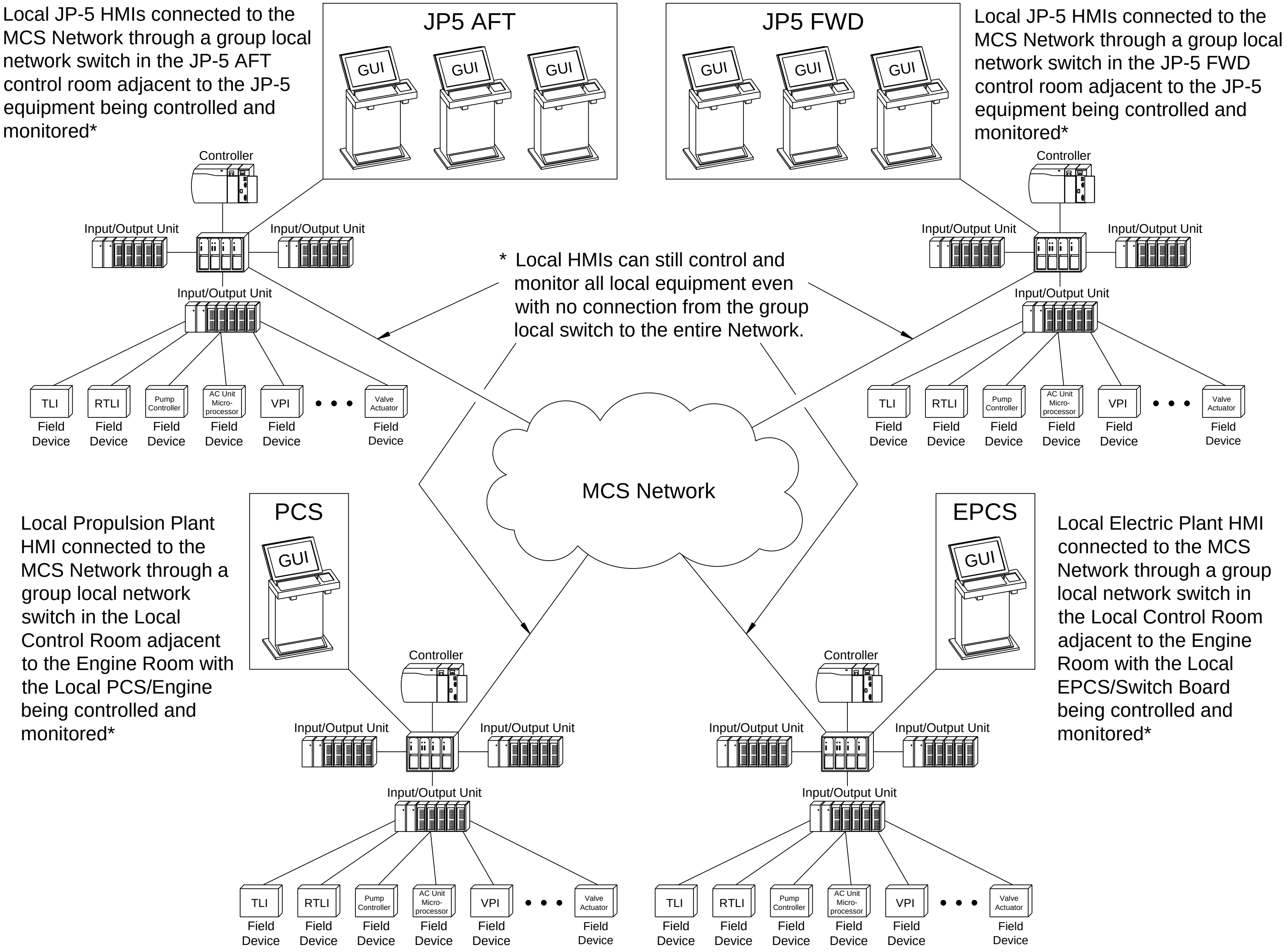

MCS Network
CCS
GUI
GUI
GUI
DCRS
GUI
Remote HMIs in CCS connected through the MCS Network
Remote HMIs in DCRS connected through the MCS Network

Figure 4-16. Functional Depiction of Notional Remote Connections from HMIs to the MCS Network.

4.2.3.4.2 Local. Local HMIs shall be co-located (i.e., in the same compartment or adjacent control room for that compartment) with the local equipment being controlled and monitored to transmit data and information to and from PLCs/control processors through the group local switch in the same compartment as the PLC/control processor controlling/monitoring the respective equipment (see Figure 4-17).



Local JP-5 HMIs connected to the MCS Network through a group local network switch in the JP-5 AFT control room adjacent to the JP-5 equipment being controlled and monitored*

Local JP-5 HMIs connected to the MCS Network through a group local network switch in the JP-5 FWD control room adjacent to the JP-5 equipment being controlled and monitored*

* Local HMIs can still control and monitor all local equipment even with no connection from the group local switch to the entire Network.

Local Propulsion Plant HMI connected to the MCS Network through a group local network switch in the Local Control Room adjacent to the Engine Room with the Local PCS/Engine being controlled and monitored*

Local Electric Plant HMI connected to the MCS Network through a group local network switch in the Local Control Room adjacent to the Engine Room with the Local EPCS/Switch Board being controlled and monitored*

Figure 4-17. Functional Depiction of Notional Local Connections through the MCMS Network.

4.2.3.4.2.1 Propulsion. Local Propulsion HMIs that control and monitor propulsion machinery shall be co-located (i.e., in the same compartment or adjacent control room for that compartment) with the prime mover being controlled and monitored by that HMI.

4.2.3.4.2.2 Electric Plant. Local Electric Plant HMIs that control and monitor electric plant machinery shall be co-located (i.e., in the same compartment or adjacent control room for that compartment) with the prime mover being controlled and monitored by that HMI.

4.2.4 Protocols. The Network Layer shall utilize the following protocols at various layers of the MCS to enable the transmission of data and information.

4.2.4.1 Field Devices to I/O Units. First party protocols (i.e., hardware native protocols) or hardwired signals shall be used to transmit data and information between field devices and I/O units.

4.2.4.2 I/O Units to PLC/Control Processor. ControlNet, EtherNet/IP, Profibus PA, Profibus DP, or ModBus TCP shall be used to transmit data and information between remote I/O units and PLC/control processors.

4.2.4.3 HMI to HMI. IP Multicast or TCP/IP shall be used to transmit data and information between HMIs.

4.2.4.4 HMI to PLC/Control Processors. IP Multicast or TCP/IP shall be used to transmit data and information from HMIs to PLC/control processors.

4.2.4.5 PLC/Control Processors to HMI. IP Multicast shall be used to transmit data and information from PLC/control processors to HMIs.

4.2.4.6 PLC/Control Processor to PLC/Control Processor. For communication over the MCS Network Layer, IP Unicast or IP Multicast shall be used to transmit data and information from PLC/control processors to PLC/control processors.

NOTE

Network Layer latency will not be addressed in this architecture standard as it will be dependent upon specific applications; it is independent of the MCS architecture.

4.3 CONTROL LAYER.

The Control Layer shall provide a direct connection with machine systems or interface to an external system's embedded controller or external control system via distributed clusters of collocated processing and I/O units (i.e., Groups) for controlling, monitoring, and processing machine systems' information.

4.3.1 Location. Groups shall be situated as close as practical to the equipment being controlled and monitored, and be within a single fire zone boundary. Groups shall be distributed with locations determined through both survivability analysis, as well as cost effectiveness, with respect to installation, testing, and life cycle maintenance.

4.3.1.1 Propulsion. Groups that control and monitor propulsion machinery shall be co-located (i.e., in the same compartment or adjacent control room for that compartment) with the prime mover being controlled and monitored by that Group.

4.3.1.2 Electric Plant. Groups that control and monitor electric plant machinery shall be co-located (i.e., in the same compartment or adjacent control room for that compartment) with the prime mover being controlled and monitored by that Group.

4.3.2 Sparing. The Control Layer architecture shall provide sparing capacity for future growth. Sparing capacity, as defined by platform/system requirements, shall be implemented within the MCS architecture defined herein.

4.3.3 Control Processing Technology. The Control Layer shall utilize PLCs (in accordance with MIL-PRF-32006) or VME (in accordance with IEEE 1014) technology, but not a combination of both, in one MCS. This does not preclude an interface from MCS to the technology not chosen; it only restricts the use of mixed technologies within an independent MCS.

NOTE

Non-MCS CPUs that interface to the MCS should not be installed on valves (i.e., smart valves), unless direct MCS or ship system requirements cannot be met without direct valve-to-valve communication or the additional functionality in the valve's CPU increases the capability of the Group(s) (controlling and monitoring the valve) beyond that of what the Group's control processing technology can perform. For example, if a smart valve is specified into a system specification for interaction with MCS, the smart capability (beyond remotely opening and closing the valve) should show how it directly increases the performance of the control and monitoring beyond that of the Group's control processing technology.

4.3.4 MCS Controller Redundancy. The Control Layer shall utilize hot backup when redundancy is required at the PLC or VME controller.

NOTE

Control Layer latency will not be addressed in this architecture document as it will be dependent upon specific applications; it is independent of the MCS architecture.

APPENDIX A
LIST OF ACRONYMS AND DEFINITIONS

A.1 LIST OF ACRONYMS.

ACRONYM	MEANING
APT	Advanced Persistent Threat
CCS	Central Control Station
CONOPS	Concept of Operations
COTS	Commercial Off-the-Shelf
CPU	Central Processing Unit
DLC	Device Level Controller
DCRS	Damage Control Repair Station
ECS	Engineering Control System
EPCS	Electric Plant Control System
GOTS	Government Off-the-Shelf
GUI	Graphical User Interface
HMI	Human-Machine Interface
IA	Information Awareness
I/O	Input/Output
MAC	Media Access Control
MCMS	Machinery Control and Monitoring System
MCS	Machinery Control System
MPCMS	Machinery Plant Control and Monitoring System
MTBF	Mean Time Between Failures
OIP	Operator Interface Panel
PC	Personal Computer
PCS	Propulsion Control System
PLC	Programmable Logic Controller
RTLI	Radar Tank Level Indicator
TLI	Tank Level Indicator
TWH	Technical Warrant Holder
VME	Versamodule Eurocard
VPI	Valve Position Indicator

A.2 DEFINITIONS.

A.2.1 Advanced Persistent Threat (APT). An APT is a network attack in which an unauthorized person gains access to a network and stays there, undetected, for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization. APT attacks target organizations in sectors with high-value information, such as national defense, manufacturing, and the financial industry.

A.2.2 Communication Scheme. The method (e.g., Point-to-Point, Broadcast, Multicast, etc.) used to transmit information over a network from human-machine interfaces (HMIs) to equipment on a network.

A.2.3 Connection. See Interface (see A.2.12).

A.2.4 Control Processing Technology. Technology used for processing information within an MCS (i.e., a microprocessor-based piece of auxiliary machinery would not be considered part of the MCS, but rather interfaced with the MCS).

A.2.5 Cyberwarfare. Politically motivated hacking to conduct sabotage and espionage. Actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption. It is a form of information warfare sometimes seen as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation. The fifth domain of warfare, as a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain in warfare which has become just as critical to military operations as land, sea, air, and space.

A.2.6 Graphical User Interface (GUI). A type of user interface that utilizes a combination of images and text to present data to the end user and allows the end user to monitor status, issue commands, and acknowledge alarms.

A.2.7 Group. A Group is a Programmable Logic Controller (PLC) or Versamodule Eurocard (VME) central processing unit (CPU), a local network switch (if applicable), and one or more Input/Output (I/O) units usually located within the same compartment or same survivable zone (fire or flooding zone of the ship). A Group is generally in close proximity to the field devices or Device Level Controller (DLC) being controlled and monitored. A Group generally supports all signals from a subsystem, or set of subsystems where feasible. The I/O units connect the PLC/VME CPU to and from field devices (e.g., valves, pumps, other embedded local controllers, indicators, switches, etc.).

A.2.8 Hardwired. Direct point-to-point wiring where each signal is transmitted over one unique signal path. No signal path is considered hardwired if it is used to transmit more than one signal; for example, multiplexed signals are, by definition, not hardwired.

A.2.9 HMI. The component where interaction between humans and machines occurs. The HMI provides a system of displays (i.e., GUIs) to monitor and control the engineering plants. HMIs can be traditional sit-down type, stand-up type, or simple bulkhead-mounted Operator Interface Panels (OIPs).

A.2.10 Hot Backup. A redundant pair of controllers which seamlessly switch control from one controller to the other during definable failure modes. The primary processor controls are switched to the backup processor without any noticeable variation in the processes or states or alarms (i.e., bump-less) except for the alarms associated with identifying the switchover event. The mechanisms and software for this operation are achieved within MCS controller hardware.

A.2.11 Information Consumption Methodology. The method (e.g., Client/Server, Producer/Consumer, Publish/Subscribe) used to transmit information from a controller (i.e., PLC or VME controller) to a GUI/HMI (i.e., display device).

A.2.12 Interface. An interface is where two or more separate systems communicate under limited capacity, where data is maintained in separate locations, and a one-to-one physical connection links the two systems.

A.2.13 MCS. A system that remotely and locally controls and monitors distributed and local machinery for the purposes of shipboard propulsion, electrical, auxiliary, and damage control functions. MCS is also synonymous with Engineering Control System (ECS), Machinery Control and Monitoring System (MCMS), and Machinery Plant Control and Monitoring System (MPCMS), and these terms can be considered interchangeable.

A.2.14 Network Configuration. The association of a network (i.e., standalone or attached) to other networks and, if attached, the type or degree of association (i.e., interfaced or integrated) to the other network(s).

A.2.15 Node. A point in a network topology at which lines intersect or branch; a connection point, either a redistribution point or a communication endpoint.

Ref: NAVSEAINST 4160.3 NAVSEA S0005-AA-GYD-030/TMMP

NAVSEA/SPAWAR TECHNICAL MANUAL DEFICIENCY/EVALUATION REPORT (TMDER)

INSTRUCTIONS: Continue on 8 ½" x 11" on page if additional space is needed.

1. Use this report to indicate deficiencies, problems and recommendations relating to publications.
2. For **CLASSIFIED** TMDERs see OPNAVINST 5510H for mailing requirements.
3. For TMDERs that affect more than one publication, submit a separate TMDER for each.
4. Submit TMDERs at web site https://nsdsa.nmci.navy.mil or mail to: **COMMANDER, CODE 310 TMDERs, NAVSURFWARCENDIV NSDSA, 4363 MISSILE WAY BLDG 1389, PORT HUENEME CA 93043-4307**

1. PUBLICATION NUMBER	2. VOL/PART	3. REV/DATE OR CHG/DATE	4. SYSTEM/EQUIPMENT ID

5. TITLE OF PUBLICATION	6. REPORT CONTROL NUMBER (6 digit UIC-YY-any four: xxxxxx-10-xxxx)

7. RECOMMEND CHANGES TO PUBLICATION

7a. Page #	7b. Para #	7c. RECOMMENDED CHANGES AND REASONS

8. ORIGINATOR'S NAME AND WORK CENTER	9. DATE	10. ORIGINATOR'S E-MAIL ADDRESS	11. TMMA of Manual (NSDSA will complete)

12. SHIP OR ACTIVITY Name and Address (Include UIC/CAGE/HULL)	13. Phone Numbers: Commercial (___) ___-____ DSN ___-____ FAX (___) ___-____

FOLD HERE AND TAPE SECURELY
PLEASE DO NOT STAPLE

INCLUDE COMPLETE ADDRESS

USE
PROPER
POSTAGE

FOR OFFICIAL USE ONLY

COMMANDER
CODE 310 TMDERs
NAVSURFWARCENDIV NSDSA
4363 MISSILE WAY BLDG 1389
PORT HUENEME CA 93043-4307

FOLD HERE AND TAPE SECURELY
PLEASE DO NOT STAPLE