Fault Tolerance in a Real Time Weapon Control System

- **Authors and Reviewers**
  - James G. Shumate 410-682-1716
    james.g.shumate@lmco.com
  - Ralph W. Edwards 410-682-0805
    ralph.edwards@lmco.com
  - George H. Goetz 410-682-2286
    george.goetz@lmco.com
  - Jennifer L. Houston-Manchester 410-682-0793
    jennifer.houston-manchester@lmco.com
  - Ben Skurdal 410-682-0590
    benjamin.skurdal@lmco.com

- **Address**
  Lockheed Martin
  MS2 Littoral Ships and Systems
  2323 Eastern Blvd.
  Baltimore, Maryland 21220
Lockheed Martin
Littoral Ships & Systems

History - LS&S is part of the MS2 (Maritime System & Sensors) organization. MS2 is 13,000 people strong and supports more than 500 programs for US and nearly 50 international customers.

LS&S Lines of Business

- Launching Systems
  - MK41 Vertical Launching System (VLS)
  - Non-Line of Sight LS (NLOS)
  - Electromagnetic Launching System
  - Terminal High Altitude Area Defense (THAAD)

Domain Experience

- Fault Tolerance in DRE Systems
- Control Systems
- Open Architecture
- Distributed, R-T Embedded Applications

Littoral Combat Ship (LCS)

Ship Systems
The Domain

- Launching Systems
  - Configurations
    - 1-122 weapon cells in single or modular form
  - Weapon Control Systems (11)
  - Launch Sequence Control
  - Availability, Reliability & Safety

- Drive for Open Architecture
  - Total Ship Computing Env.
  - Reduce Cost & Time to Market
  - Open Business Practices

- Domain Knowledge Required
  - Fault Tolerance Principles
  - Network Architectures and Protocols
  - Distributed, Real Time Embedded Applications
Fault Tolerance Attributes

- Fault Tolerance
  - Redundancy
    - Hardware, Software, Both
  - Failover, Recovery
    - Manual, Automatic
  - Redundant Communications
- Styles – How and when to achieve state coherency
  - Passive
  - Active
  - Stateless

- Quality Attributes
  - Availability
    - Tightly Coupled with:
      - Safety
      - Maintainability
      - Reliability
- Tactics
  - Detection
  - Recovery (Failover)
  - Prevention
FT in Real Time Applications

- **Driving Requirements**
  - Real Time Responses
  - Size
  - Cost
  - Complexity
  - Distribution

- **Open Architecture Readiness**
  - Standards Organization
  - Vendors – Tools and MW
  - Customer Requirements
  - Contractors - adaptability

- **Single Point of Failure**

![Diagram showing a client, Ethernet switch, application, and some other server with single points of failure.](image-url)
Example Redundancy Strategy

Context View

- Redundant Ethernet Switches.
- Multiple points of failure supported.
- Existing interfaces (IDS).

"Open Architecture Naval Warfare Systems requires component replication as the primary way to achieve a fault tolerant system."
Middleware Standards and COTS Products

COTS

- RTI DDS
- LynxOS
  - RTOS – POSIX
  - NTP
- Linux

Open Source

- TAO (CORBA)
- Spread
- MEAD
- DDS (OCI)
- FT HA (OCI)

Benefits

- Standards-based
- Quality of Service

Limitations

- Cost, Complexity, Portability, support

Emerging Standards - Spread

- Reliable Multicast
- Scalable Group Services
- Membership Services
- Message Ordering
  - Total Order of Messages
Transforming the Current Launching Systems Solution

**Benefits:** Reduced All
- **FT SLOC:** 6600 to (950 + COTS)
- **# Requirements:** 366 to 10
- **Failover Time:** 100 ms to 10 ms
- **Recovery Time:** 50 ms to 5 ms

- Application isolated from transport mechanisms
- FT MW layer supports redundant transmission and arbitration
- Spread provides synchronized exchange of state
- Distributive MW used for application communications
- Flexible Configurations
Challenges and Solutions

- **General Solution and Attributes**
  - Independent of the Application
  - Easy to use and to extend
  - Standard Communications
  - Small Footprint

- **The LM Solution**
  - Real Time Failover through Active Redundancy
  - State Coherency to 10-millisecond resolution
  - Redundant Network Coordination
  - Dynamic Recovery Scheme
  - Remote Monitoring
  - Scalable