Testability of Complex, Middleware-Based Systems

Douglas Wells*, The Open Group
Amar Vadlamudi, S/TDC

d.wells@opengroup.org
http://www.opengroup.org/AR

Current State of Technology: Theory vs. Practice*

- Small islands of theoretical results, separated by an ocean of unknowns
- Industry is mired in many separate swamps of proprietary technology separated by tall opaque walls topped by barbed-wire fences of IPR issues
- Occasional forays to acquire research results and drag them behind the walls
- A few rays of hope:
  - Aegis Open Architecture (OA)
  - Weapon Systems Open Architecture (WSOA)

(*)The opinions expressed herein are attributable only to one or more of the authors.

Goals of Position Paper and Presentation

- Explain the problem of testing
  - Describe testing physics of an example problem
  - Propose some relevant research problems
- Convey information about requirements for a shipboard weapons system infrastructure
  - Describe an accessible, real-world problem
  - Discuss the desired, long-term solution
  - Describe a possible short-term solution (paper)
- Indirect goals
  - Initiate discussion of difficulties of deploying real-time, dependable applications
  - Foster creation of knowledge, technology and tools to ensure success of future systems

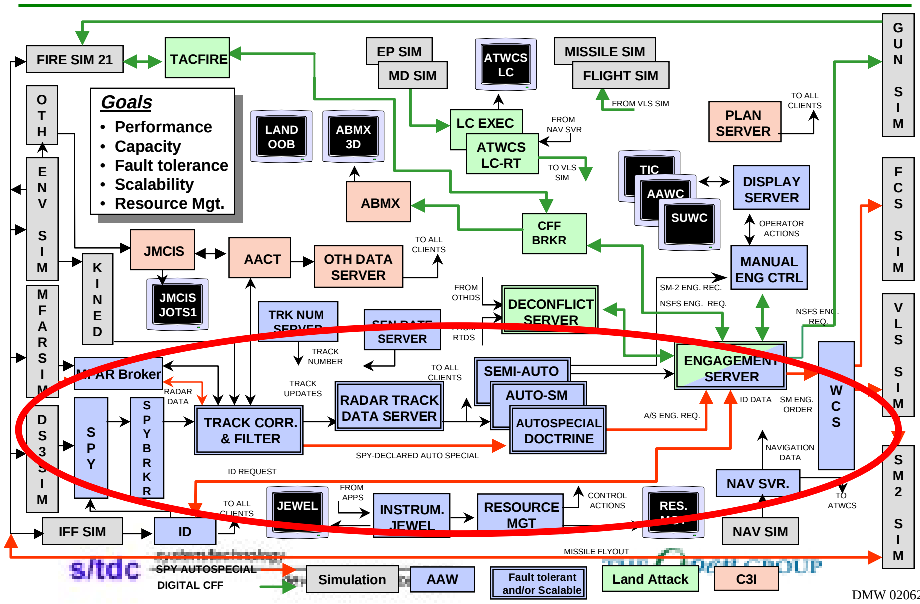
s/tdc system/technology development corporation

THE Open GROUP

DMW 020626

DEMO 99 FUNCTIONAL BLOCK DIAGRAM

(From NSWC HiPer-D Project)

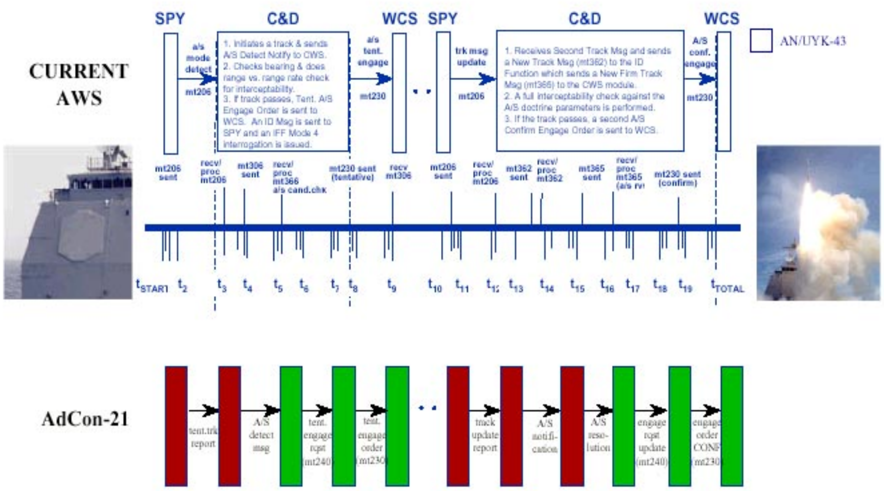


s/tdc system/technology development corporation

THE Open GROUP

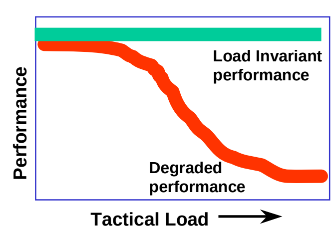
DMW 020626

Why DD-21 Needs Assured Response: SPY Radar Auto-Special Time-Line



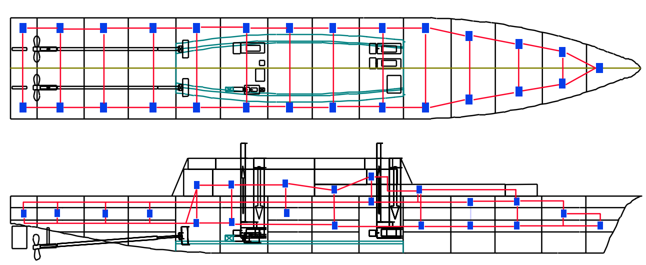
SCALABLE PERFORMANCE

(Content from NSWC HiPer-D Project)



Scalable Computing Architecture

- Networked computers
- Distributed system middleware
- Scalable computer programs
- Load sharing management



DMW 020626

System Goals for Shipboard Weapons Systems

- Functional goals
  - Achieve mission goals
  - Scale system performance per requirements
  - Dynamically adapt system configuration
    - Maximize mission-specific application-level metrics, such as number of tracks processed
  - Maintain Auto-Special Response capability
  - Use COTS-based computing infrastructure
- Assurance goals (trustworthiness)
  - Satisfy initial functional goals
  - Satisfy evolving, life-cycle functional goals
  - Achieve certification
    - Convince a third-party (U.S. Navy) that system will satisfy functional requirements

Some Physics within System Assurance

- Some systems must be trustworthy
  - Trustworthiness is associated with particular QoS parameters such as dependability and timeliness
  - "Safety-critical" implies high values for certain application-specific QoS parameters
- Trustworthiness is an emergent property of a component and its dependencies
  - Hardware
  - Software
  - Environmental
- Trustworthiness usually derives from
  - Proof chains, and/or
  - Testing

More Physics within System Assurance

- Testing is part of the scientific process of verifying a hypothesis
- Characterization is not testing
- Testing a particular system configuration can only validate that particular configuration
  - — although one can separately assert (and test) theories about "modes" of operation

Thus:

- Reducing testing while maintaining assurance is almost always good and is usually very, very cost effective in the real world

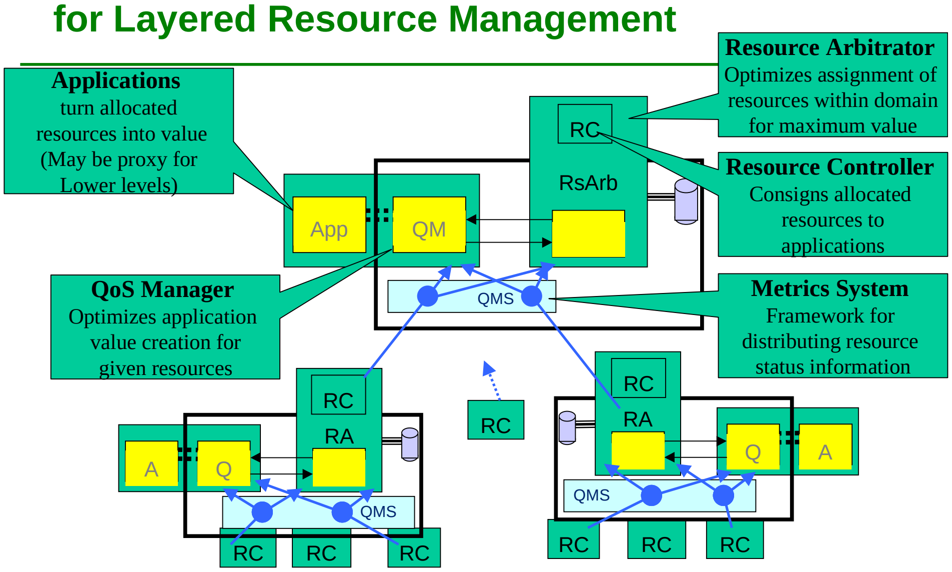
The Long Term Vision

- Desire to reason about system behavior to:
  - — verify correct operation of current configuration
  - — predict future performance changes resulting from resource or load configuration changes
  - — convey assurance about a trustworthy system
  - — minimize system management by humans
  - — effectively accommodate evolving mission requirements, hardware trends, and software upgrades
- Based on dynamic, run-time system models
  - Models used to predict future system behavior

The Long Term Vision (cont'd)

- (Re-)use common manageability mechanisms
  - Information models, such as DMTF's CIM
  - Repositories, such as The Open Group's Pegasus CIM Object Manager (CIMOM)
  - Extensible instrumentation and control frameworks, such as are in S/TDC's QoS Metrics Services (QMS)
- (Re)-use common resource management mechanisms via application-specific policies components based on common, well-understood strategies, such as
  - Control theoretic
  - Boyd Cycle (OODA)

A Functional Architecture for Layered Resource Management



Dependability Issues

- "Normal" dependability fault sources
  - Computer hardware failure
  - Network component failure
  - Software component failures
  - Environmental insults
- Real-time application-derived sources
  - Timing faults
- Battle damage sources
  - Loss of hull compartment
    - Lose all components in compartment
  - EMF attacks
    - Lose many components simultaneously

Complications

- Applications are inter-dependent
  - For example, Auto-Special path depends on sensor DSP, track manager, gyro position
- Use of shared resources
  - Comm links between hull compartments are limited to reduce damage impact (a la firewalls)
- Use of multiple FT strategies
  - FT strategies hidden within reused components
  - Different strategies for different fault sources
- Huge number of potential configurations
- Dynamically updated hardware and software

Implications on Design

- Traditional real-time determinism is not likely to be a characteristic of eventual system
  - Systems too complex
  - Conflicts with goal of component reuse
  - Exception: safety-critical subcomponents
  - Predictability is likely to be crux
- System must characterize itself automatically
  - Perhaps continual self-characterization of interesting configurations during “slack” periods
  - Adapability must be considered normal operating behavior, not just a reaction to abnormal environmental insults

Potential Dependability Research Areas

- Investigate interaction of multiple managed QoS parameters with current strategies
- Consider that multiple FT algorithms might have to operate concurrently
- Investigate application-level QoS parameters
- Identify stable, robust operating regions of common fault-tolerance strategies
- Investigate non-linear application behavior

More Potential Research Areas

- Investigate interaction between multiple FT strategies on an execution path, e.g., transducers.
- Develop methods for dealing with partially specified information, including probability information, e.g. Kalman filters
- Extend causal ordering concepts to resolve race conditions, a la Karnaugh maps

- Industry and research community can work together to ascertain realistic values of FT strategy QoS parameters

s/tdc system/technology development corporation THE Open GROUP

DMW 020626

Conclusions

- Improved capability to reason about system performance would increase system assurance for some real-time systems
- There is a wide gap between current research and industry needs—but it can be bridged
- An open shipboard weapons system would provide a rich problem space for research investigations into real-time, fault-tolerant mission-critical applications
- Exhaustive testing is not THE answer, although it will be a part of the answer

s/tdc system/technology development corporation THE Open GROUP

DMW 020626

Testability of Complex, Middleware-Based Systems

For more information:
http://www.opengroup.org/AR/
Mail: d.wells@opengroup.org

s/tdc system/technology development corporation

THE Open GROUP

DMW 020626