OHIO UNIVERSITY

Raytheon
Customer Success Is Our Mission

Toward Certification of Adaptive Distributed Systems

John M. Slaby, Lonnie R. Welch, Paul R. Work

OMG's Workshop on Distributed Object Computing for Real-time and Embedded Systems

July 10-13, 2006 - Arlington, VA USA

DARPA Distribution Statement “A” (Approved for Public Release, Distribution Unlimited)

The Challenge

- Much of the early work on adaptive, distributed systems has focused on the hard problems of the technology

- As we have come closer to transitionable solutions, we have discovered that some of the hardest problems are not in the technology itself, but in the challenges of certifying these dynamic systems

- We need to come up with new ways of approaching certification that will satisfy the needs of the certification community but are meaningful in the context of these new dynamic, adaptive systems

DARPA Distribution Statement “A” (Approved for Public Release, Distribution Unlimited)

Certification of Dynamic and Adaptive Systems

- First of all, the certification activity is a continuum that begins with the establishment of requirements for the system.

- On large production systems there are often many (> 6) certification activities:
  - Technical Certification of Individual Software Builds and System "Deliveries"
  - Software Safety Reviews
  - Weapon Safety Reviews
  - Security Evaluations
  - Technical Readiness Assessment (a/k/a TECHEVAL)
  - Operational Readiness Assessment (a/k/a OPEVAL)

- The certification processes focus on specific requirements and need sufficient information to make the proper assessment

The Problem

In large scale dynamic and adaptive systems, the ***methods, techniques, and tools*** for certification are ***still in the research phase***, while ***the need is in the production phase***

The Multi-Layer Resource Management (MLRM) Landscape

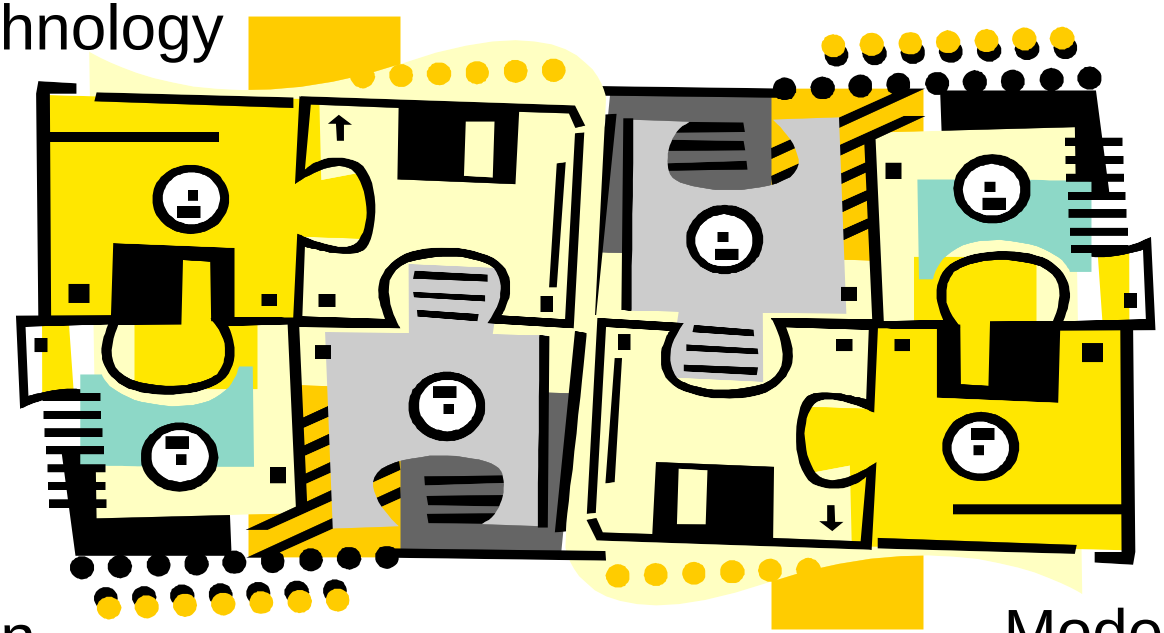
Raytheon

OHIO UNIVERSITY

Resource Allocation and Control Technology

Fault Tolerance Technologies

Reconfiguration and Redeployment Technology



Allocation Algorithms

Deployment & Configuration Technology

Model Driven Development Technology

DARPA Distribution Statement “A” (Approved for Public Release, Distribution Unlimited)

Meeting the Certification Challenge

- Working to help Certification Agents understand the Multi-Layered Resource Management approach, become familiar with it, and develop confidence in the processes and results available for analysis

- Becoming involved with research programs on the development of the analytical (and simulation) tools and techniques necessary for the generation of the results and support analysis of the results

- Working with the large production systems' processes to shape and align the required changes for both the system developer's and the certifier's processes for adaptive systems

Our “Recipe”

- Establish Theoretical Foundation for Technology
- Develop Reference Implementation
- Perform Experimentation and Analysis for Evaluation and Validation

Establish A Theoretical Foundation

- Multi-Dimensional Bin-Packing with Constraints
  - Any single algorithm provides insufficient guarantees to certify on its own
  - Create multiple algorithms that can be proven to be independent
  - As a suite, the solution can then be proven to be highly reliable

DARPA Distribution Statement “A” (Approved for Public Release, Distribution Unlimited)

Develop Reference Implementation

- Resource Allocation and Control Engine (RACE) and Redeployment and Configuration (ReDaC)
- Network Performance Monitor
- Policy-Based Risk Adaptive Access Control (RAdAC) Filter

Perform Experimentation and Analysis for Evaluation and Validation

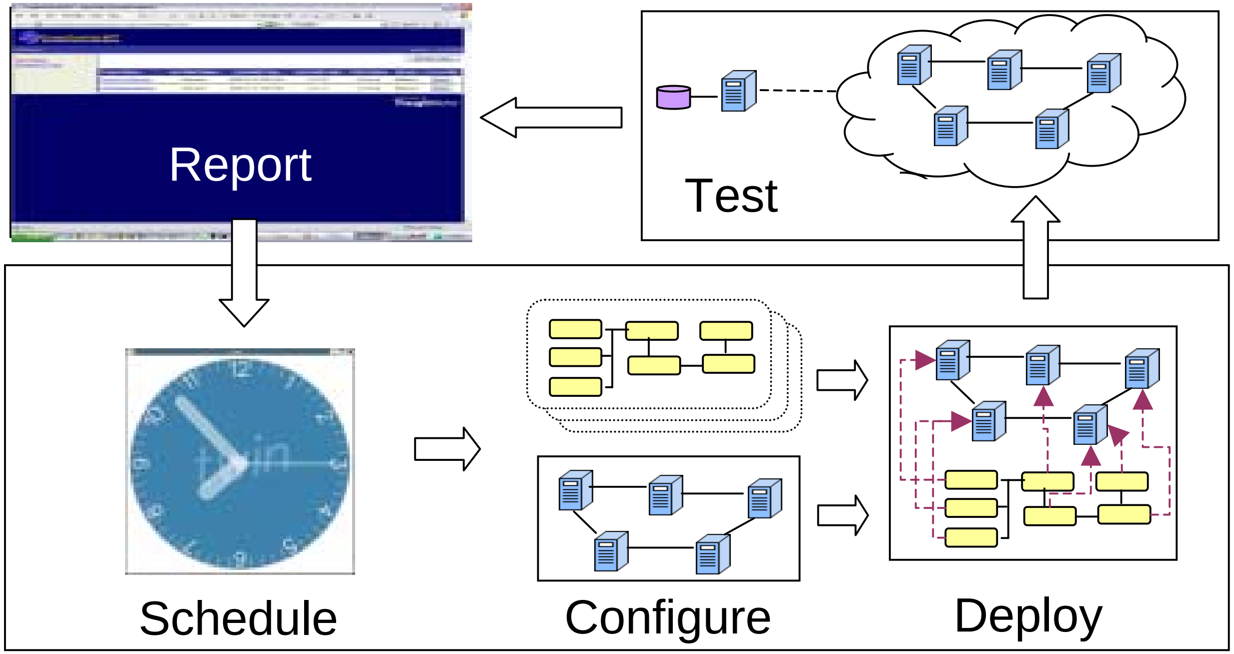
Gate Tests

- Guarantee that a Multi-Layered Resource Management (MLRM) approach will find good resource allocations when they exist.
- Provide assurances that a system implementing an MLRM approach will perform better than when it is not operating under MLRM control.
- Insure that an MLRM approach promptly detects changes and promptly responds to changes in resource status and in resource demands.
- “Guarantee” that individual components of the MLRM perform correctly.

DARPA Distribution Statement “A” (Approved for Public Release, Distribution Unlimited)

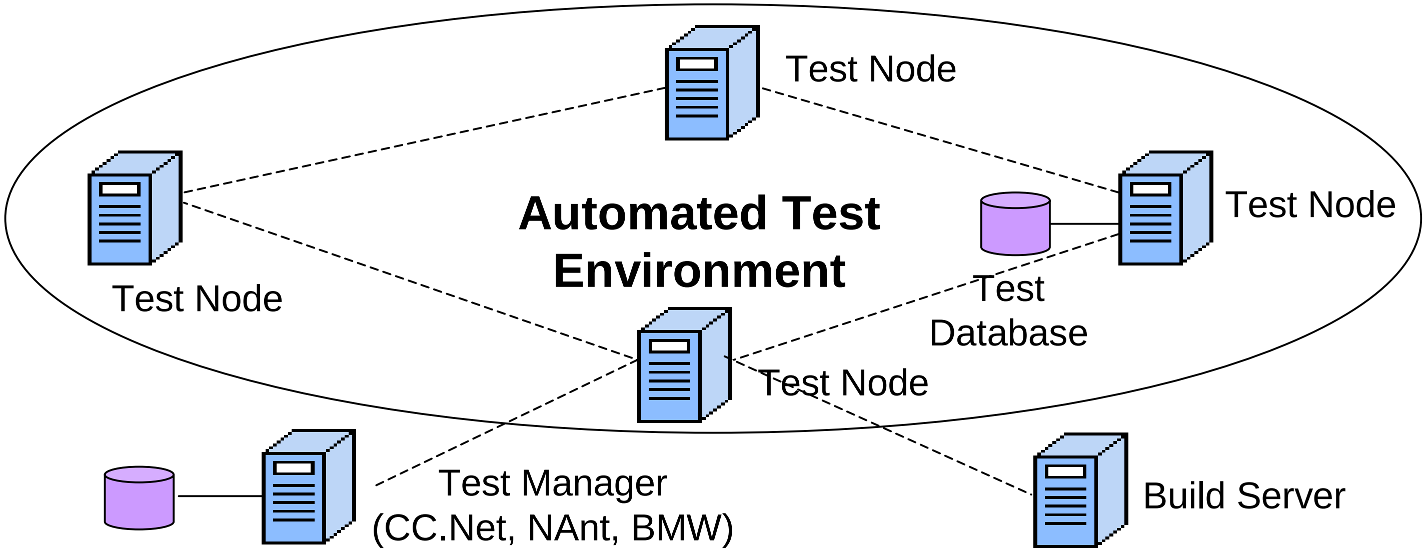
Continuous Integration with Test-Based Development Approach - 1

- Highly automated testing
- Producing large amounts of focused evidence
- In a broad set of scenarios
- Establishing a high level of confidence in the viability of alternate certification techniques for dynamic systems



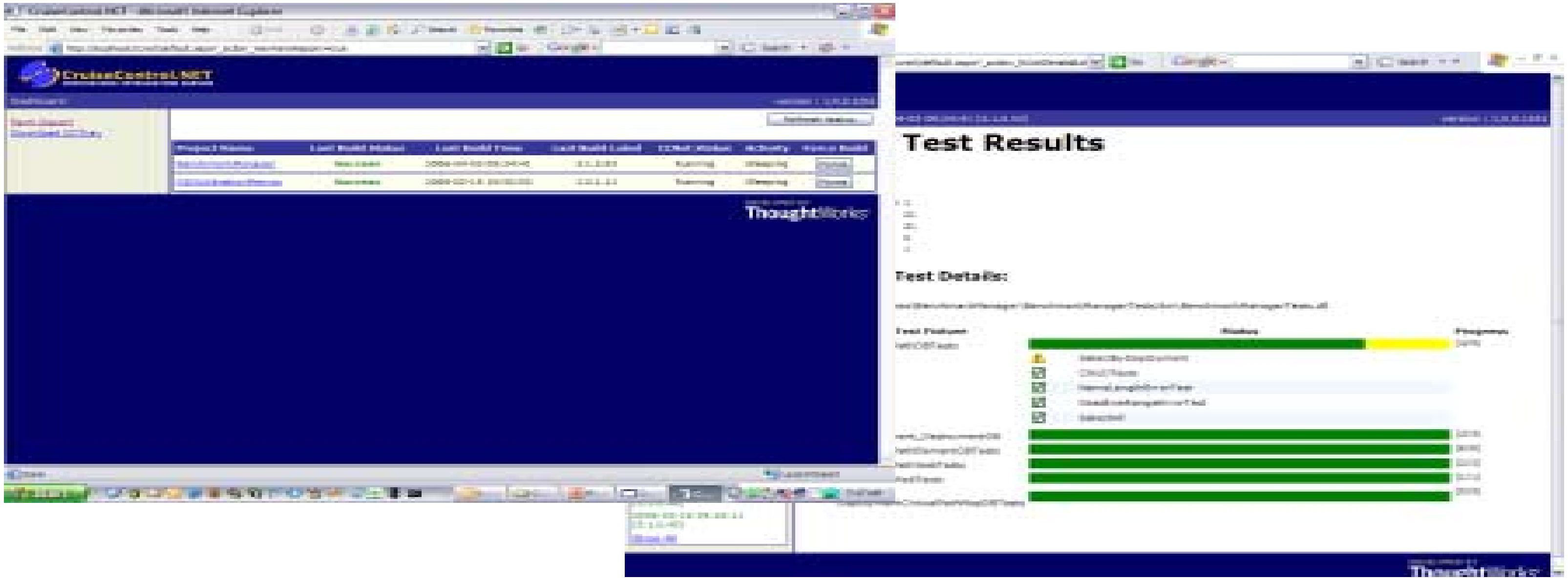
Continuous Integration with Test-Based Development Approach - 2

- Goal is to establish a **testing strategy** that can help in the certification of **dynamic systems** (e.g. MLRM) where current methods are not viable
- Strategy is to perform **automatic, continuous tests** that are a combination of both **known scenarios** (those addressed by current deterministic solutions) **and random**, unpredictable scenarios
- Because testing is automated, a large body of evidence can be collected **to support analysis**
- Ideally, control **tests** (against static solutions) would be **run in parallel**



DARPA Distribution Statement “A” (Approved for Public Release, Distribution Unlimited)

Continuous Integration with Test-Based Development Approach - 3



- **Current work in provides a starting point** for the automated testing
- **Requires a change in the testing mindset**, which impacts what is collected and how it is used
- Stability of all software in the testing environment becomes critical in order to run continuous, unattended tests
- **Trends** that might not otherwise be observed in ad hoc, manual testing **become obvious in continuous testing** environments
- Automation **reduces errors in testing and enables comprehensive test suites** to be built up over time, providing more and more complete and repeatable evidence generation

Analysis and Certification

- Z. Tan, “Certification of Instrumentation Techniques for Resource Management of Real-time Systems ,” *Ph.D. Dissertation*, Ohio Univ., 2005.

- M. Delaney, L. Welch, D. Juedes, C. Liu, “RMBench: CORBA Benchmarking Services for Resource Management Middleware,” *OMG RTES Workshop*, 2004.

- W. Leal, F. Drews, C. Liu, L. Welch, “Toward Model-Based Verification of Adaptive Allocation Managers,” *Workshop on Model-based Development of Embedded Systems*, 2004.

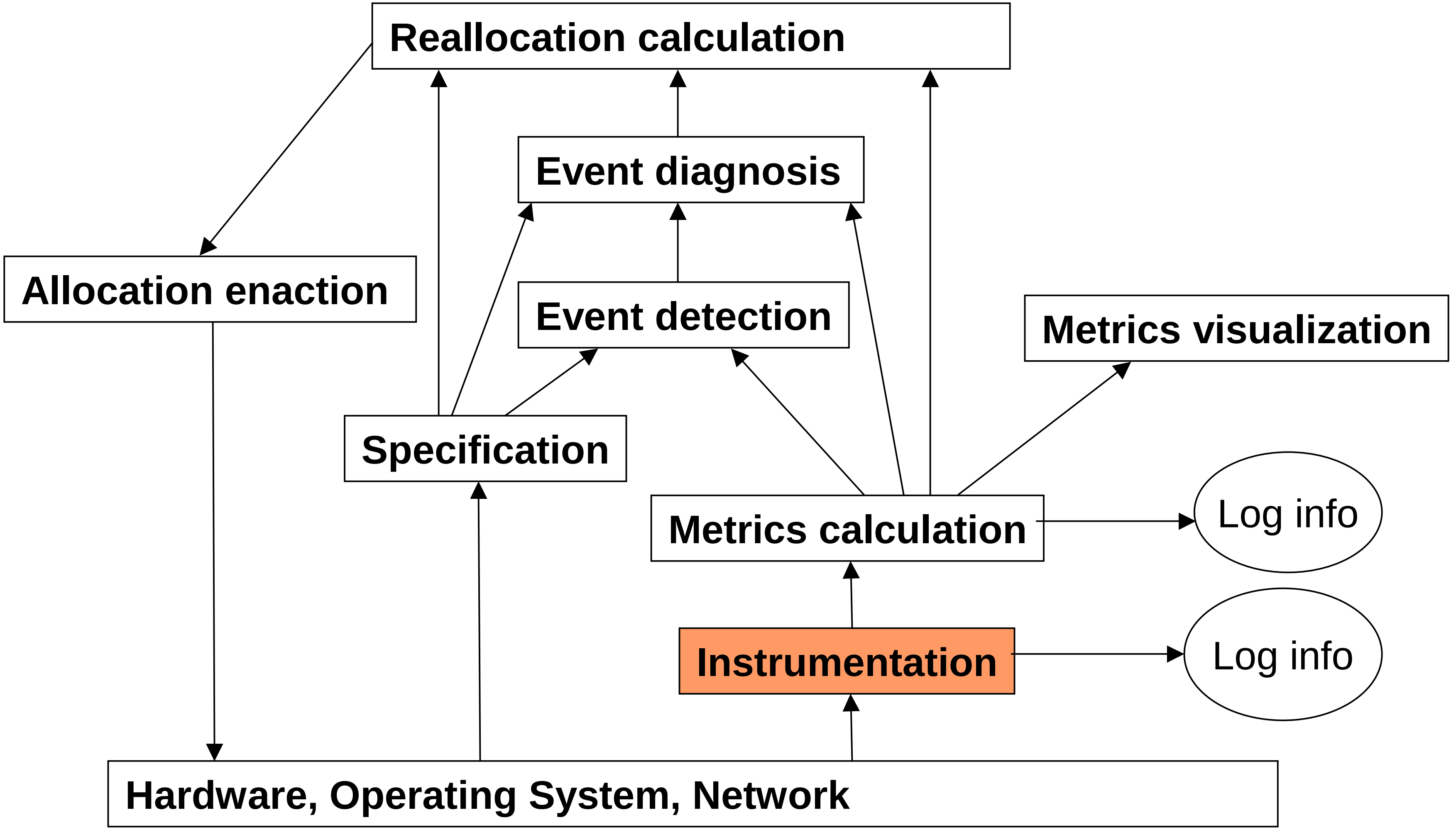
- Z. Tan, L. Welch, C. Bruggeman, D. Chelberg, D. Fleeman, and D. Parrott, “Automatic Profiling Architecture for Dynamic, Distributed Real-time Systems.” *Int. Conf. Parallel & Distrib. Proc. Tech. & Appns.*, 2003.

- E. Huh, “Certification of Real-Time Performance for Dynamic, Distributed Real Time Systems,” *Ph.D. Dissertation*, Ohio University, 2002.

Questions?

Backup

Certification Context



DARPA Distribution Statement "A" (Approved for Public Release, Distribution Unlimited)

Certification Properties

- Bounded Precision
- Bounded Uncertainty
- Bounded Intrusiveness
- Assured Timeliness

Components Certified

- Task start time
- Task stop time
- Host CPU utilization
- Deadline violation detection