

**10TH INTERNATIONAL COMMAND AND
CONTROL RESEARCH AND TECHNOLOGY
SYMPOSIUM
The Future of C2**

**“Are Service Oriented Architectures
the Only Valid Architectural Approach for the
Transformation to Network Centric Warfare?”**

Topic: C4ISR Architecture

Date: June 2004

Presenter & Author: Jack Lenahan

Imagine-One Corporation

Office of The Chief Engineer

Space and NAVAL Warfare Systems Center

Charleston, South Carolina

Contact Information

Email – John.Lenahan@Navy.mil

Phone – 843-218-6080

Agenda

- **The issue addressed**
- **What are the basic NCW Infrastructure Architectural Requirements?**
 - **Reliability**
 - **Availability**
 - **Scalability**
- **What is an SOA?**
 - **Software Architecture**
 - **Highly Available (HA) Software Stack**
 - **HA + Disaster Recoverable (DR) Software Stack**
 - **Hardware Architecture**
- **What are other alternatives?**
 - **MOMS**
 - **GRIDS**
 - **EDA**
- **Quality of Service Architecture Rating Scale**
- **Conclusion**
 - **What solution meets the architectural requirements?**
 - **What does it look like?**

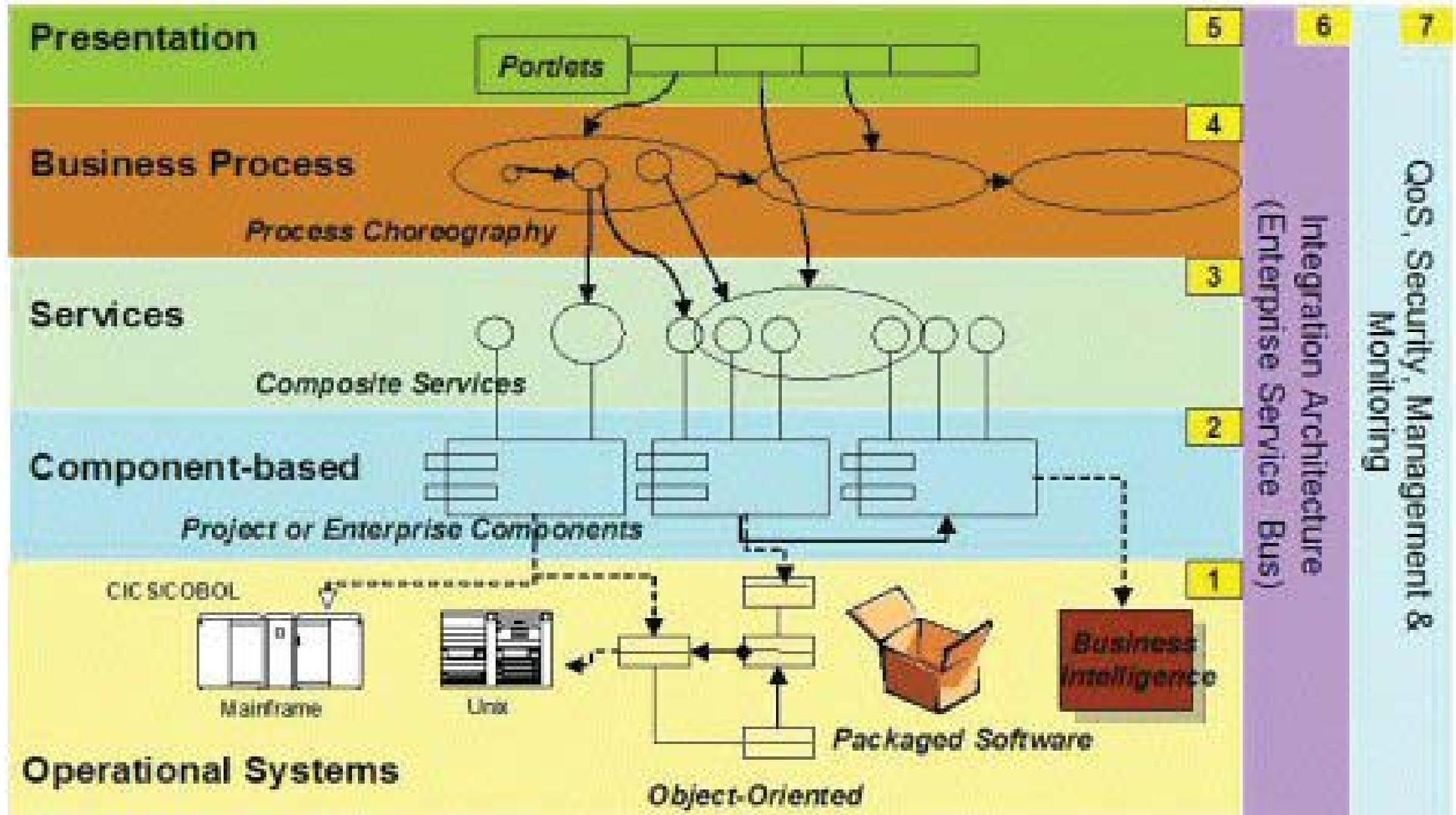
Issue Addressed

The use of a Service Oriented Architecture (SOA) as the dominant single architectural design paradigm of Network Centric Warfare (NCW) introduces architectural infrastructure stability risk levels which may be unacceptable in C4ISR mission frameworks.

Infrastructure Requirements

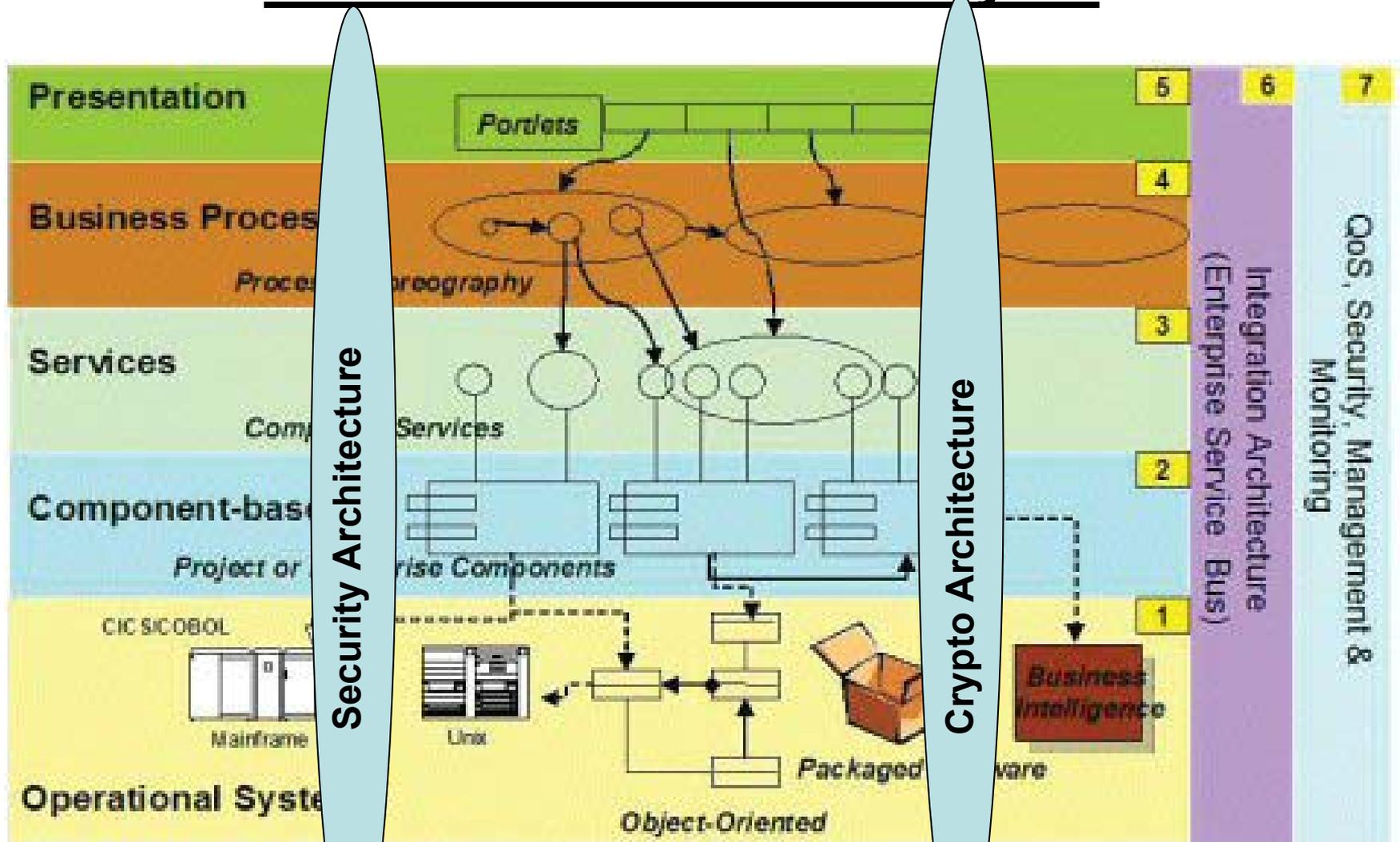
- **Reliability** - SOA software vendors must deliver software which will not fail between the start of the mission and the end of the mission regardless of mission duration.
- **Availability** – 5 nines - any component exceeding unavailability of 1.44 minutes per day violates quality of service at any level But this is in addition to and does not replace the primary availability requirement that no failures visible to the user can be tolerated during combat missions.
- **Performance** - The performance requirement is that no service can degrade below a pre-defined (hopefully tagged) SLA/QoS performance threshold. Performance must be monitored and if degradation is detected, re-routing of the service must occur transparent to the user.
- **No single points of failure can be tolerated in the hardware or software architecture stacks**

Software Architecture Layers



From: “Delving into Service-Oriented Architecture”, By [Bernhard Borges, Kerrie Holley and Ali Arsanjani](#) , used with permission of Jupiter Media – Copyright Owners

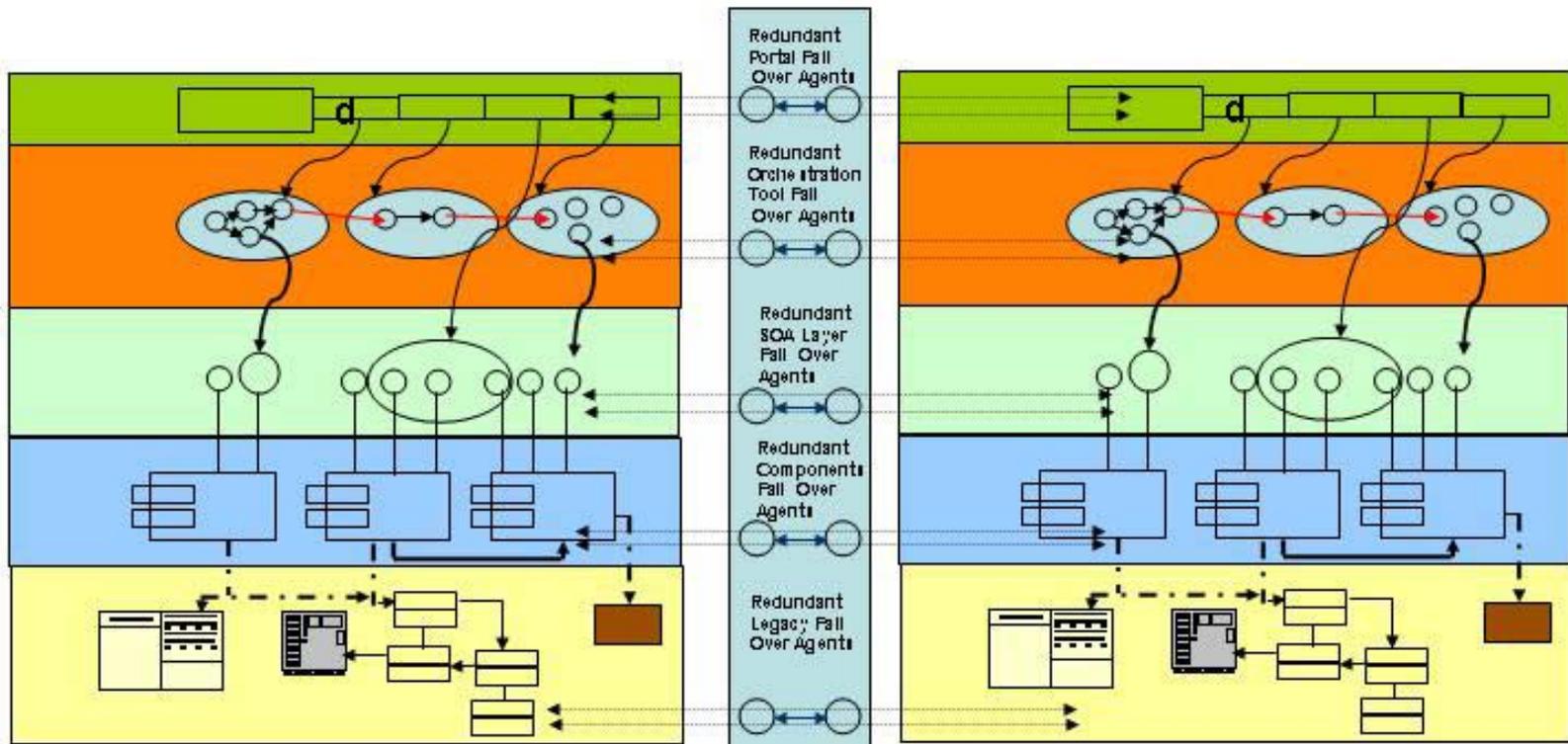
Software Architecture Layers



Modified by JL - From "Delving into Service-Oriented Architecture", By [Bernhard Borges](#), [Kerrie Holley](#) and [Ali Arsanjani](#), used with permission of Jupiter Media – Copyright Owners

Highly Available Software Stacks

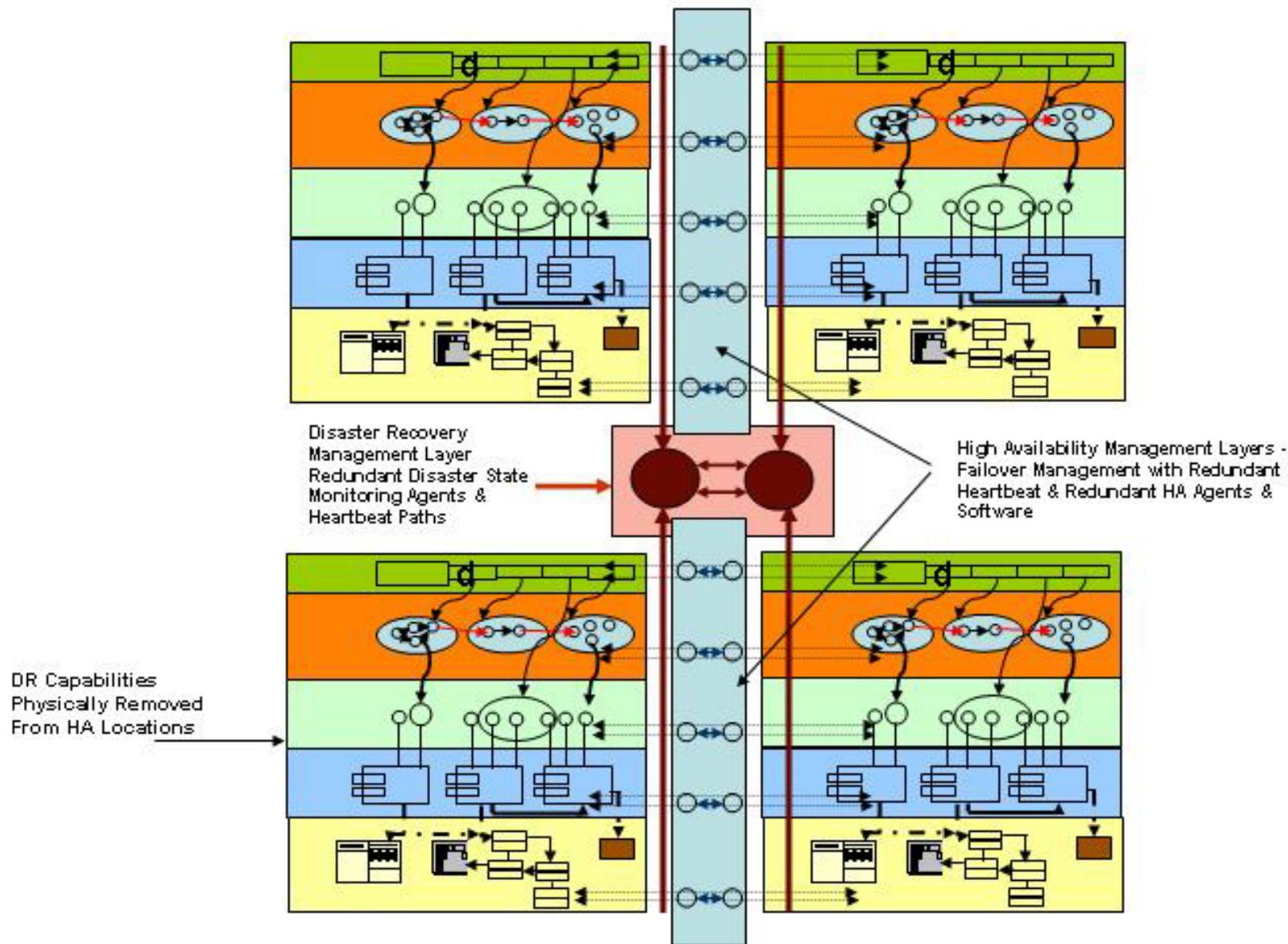
Full HA at All SW Layers – No DR



High Availability Layer Failover Management With Redundant Heartbeat, Redundant Failover Agents & Redundant HA Software

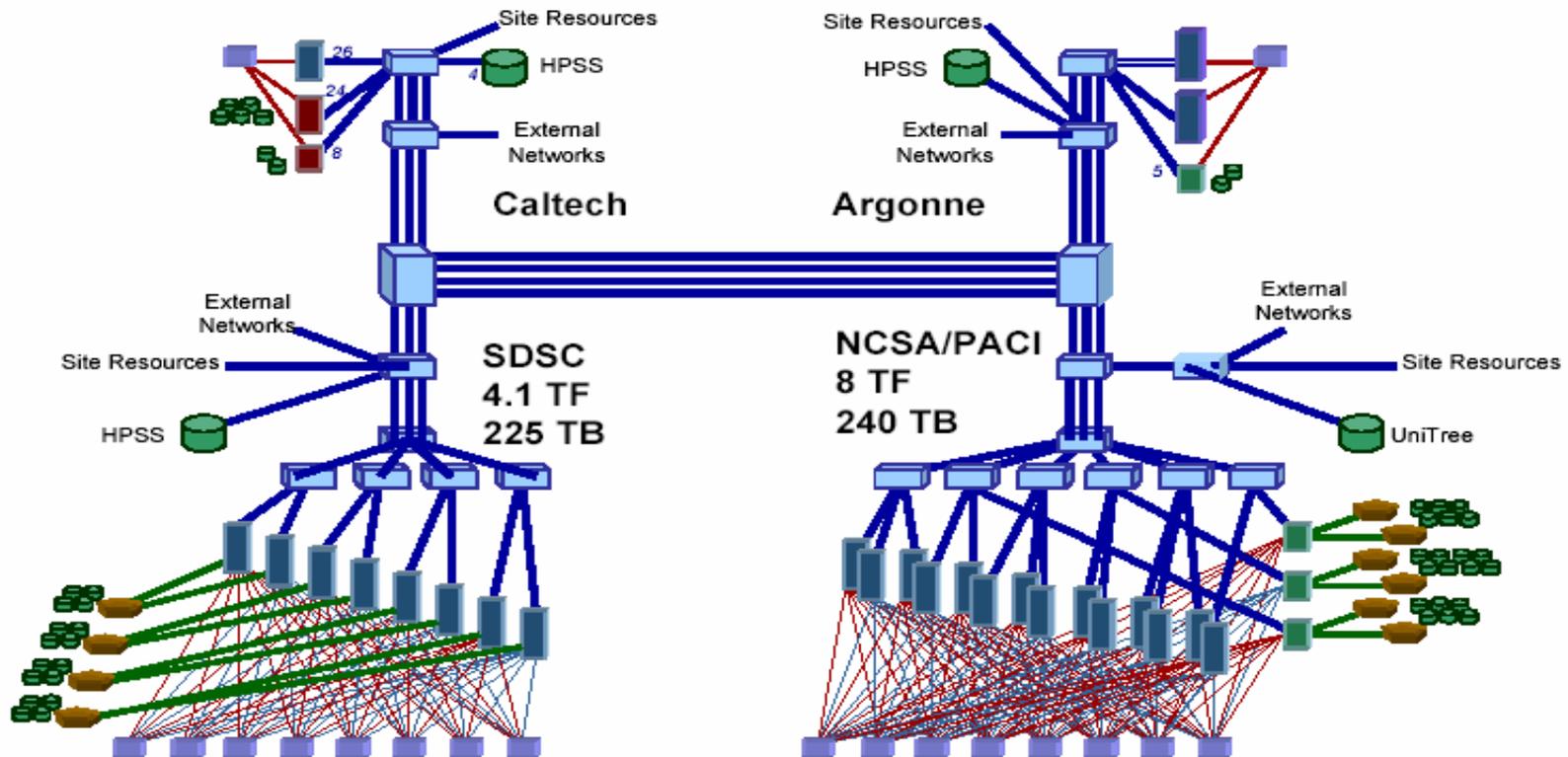
Highly Available – Disaster Recoverable Software Stacks

Full HA – With DR



Hardware Architecture

The 13.6 TF TeraGrid: Computing at 40 Gb/s



NCSA, SDSC, Caltech, Argonne

www.teragrid.org

GRID Architecture – A Complex Adaptive System which is scalable, highly available, disaster recoverable, and capable of dynamic program execution resource re-assignment.

Lenahan Levels of NCW Architectural QoS for Web Services Implementations

QoS Level	Capability or Capability Sets exposed as Web Services	State Recording	Simple State Recording with graceful fail over management by simple agents	Agent Monitoring of All Web Services in given C4ISR Architectural Orchestration or Choreography for Graceful Recovery of Services (Also applies to each service and its orchestration tool in a given FNEP being fully Stateful and agent monitored)	HA (All enabling software / hardware infrastructure layers (Listeners, Authentication SW, Firewalls, Single Sign-on Software, Directory and Naming Management, MOMS, Database Software, Redundant Directories, Redundant data, SAN, NIC, etc) for the entire orchestration set)	HA with Full DR - Clone Of HA Suites	HA/DR with guaranteed performance management (GRIDS Only with all 7 ISO Layers HA/DR)
1	Y	N	N	N	N	N	N
2	Y	Y	N	N	N	N	N
3	Y	Y	Y	N	N	N	N
4	Y	Y	Y	Y	N	N	N
5	Y	Y	Y	Y	Y	N	N
6	Y	Y	Y	Y	Y	Y	N
7	Y	Y	Y	Y	Y	Y	Y

Conclusion & Recommendation

- **Summary of The Analysis:**
 - That all levels of the model, including the communications and networking not depicted, must be highly available to support 5 nines availability, (one set of clones) and disaster recoverable (a second set of clones)
 - That all tools embedded in the SOA (particularly the choreography, orchestration, and single-sign-on software) must also be redundant
 - The HA/DR monitoring agents themselves must be HA/DR
 - Increased use due to new conflicts or surge deployments must not introduce degraded performance. This requirement almost by itself should be enough to justify the expense of a full GRID architecture as the underlying infrastructure of the SOA. We should not assume that an SOA will be performance scaleable in mission critical environments without a GRID.
 - No single points of failure can be tolerated. Simply stated, a break in any software component at any level will cause the service to be unavailable if HA/DR technologies are not implemented.
- **Conclusion:** a standalone SOA will be insufficient in terms of providing infrastructure stability. I am proposing that a highly available, disaster recoverable, GRID model (overlain with availability and performance monitoring agents) be implemented in order to sufficiently cover the reliability, performance, and availability issues needed for combat missions. A GRID infrastructure, with HA/DR monitoring of all components including the services and their sources themselves, should be selected to achieve this level of quality and availability.

**GRID Model of Multiple Executing FNEPs with Agent Monitors - Each FNEP Representing a Lenahan QoS Scale Value of 7 – Which means that all selected services in all architecture levels must be tagged as to HA/DR & GRID Compliance
(Modified from Original NASA Graphic)**

