

Major HCI Challenges Supporting the Dependability, Safety and Security of Evolving “On Demand” Enterprise Computing and Communications Services

Arthur S. Robinson S/TDC
O. Sami Saydjari - CDA



S/TDC system/technology
development corporation

First, a word about terminology:

- Enterprises understand the need for continuity in their mission critical services, despite stresses such as imperfections in system hardware, software and human-computer interactions; damage caused by both environmental stresses and physical attacks; and disruptions caused by both internal and external cyber attacks.
- In effect, they understand the need for service dependability, safety and security, but have not yet agreed on a single term encompassing all three attributes.



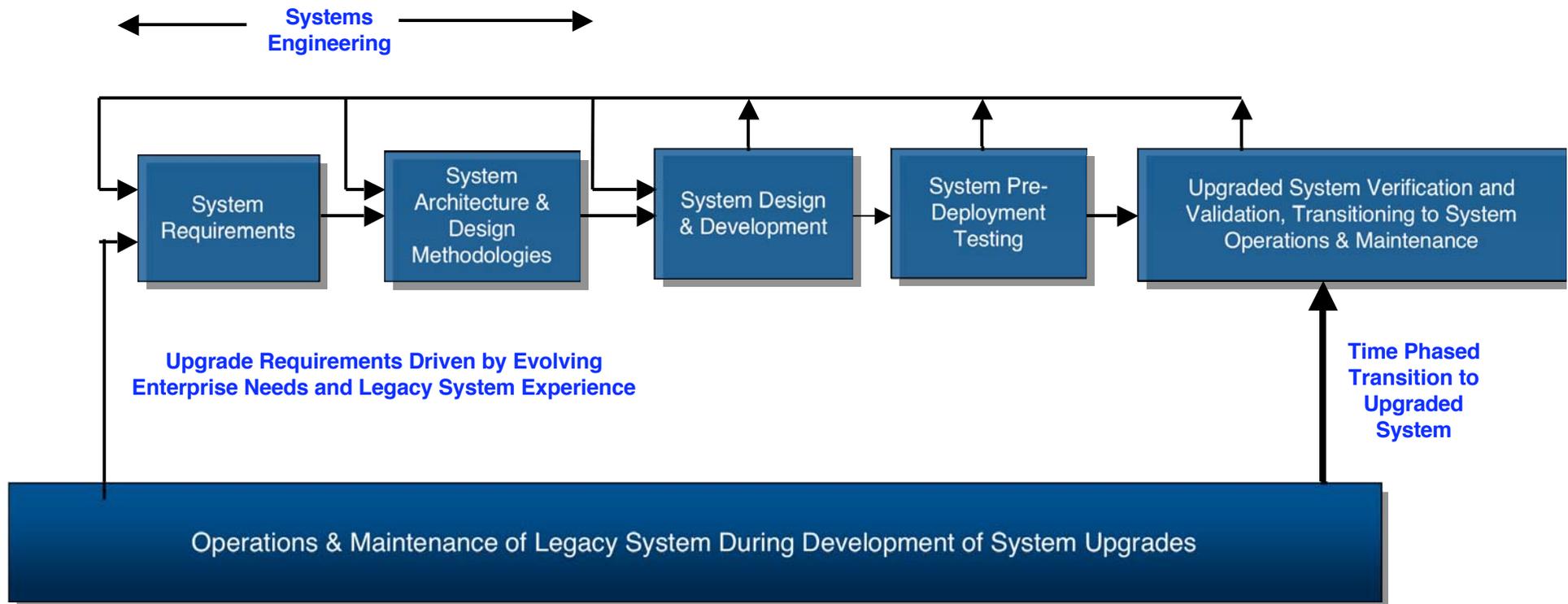
S/TDC system/technology
development corporation

- We have attempted to use “Enterprise Vulnerability Management” to describe the integrated management of Enterprise dependability, safety and security vulnerabilities, with limited acceptance to date
- Users appear to be more attracted to terminology such as “Enterprise Survivability”
- Since there is a major world need for processes that address all threats to mission continuity from an integrated perspective, we are continuing to use all three terms until consensus emerges on how best to describe their integrated effects



S/TDC system/technology
development corporation

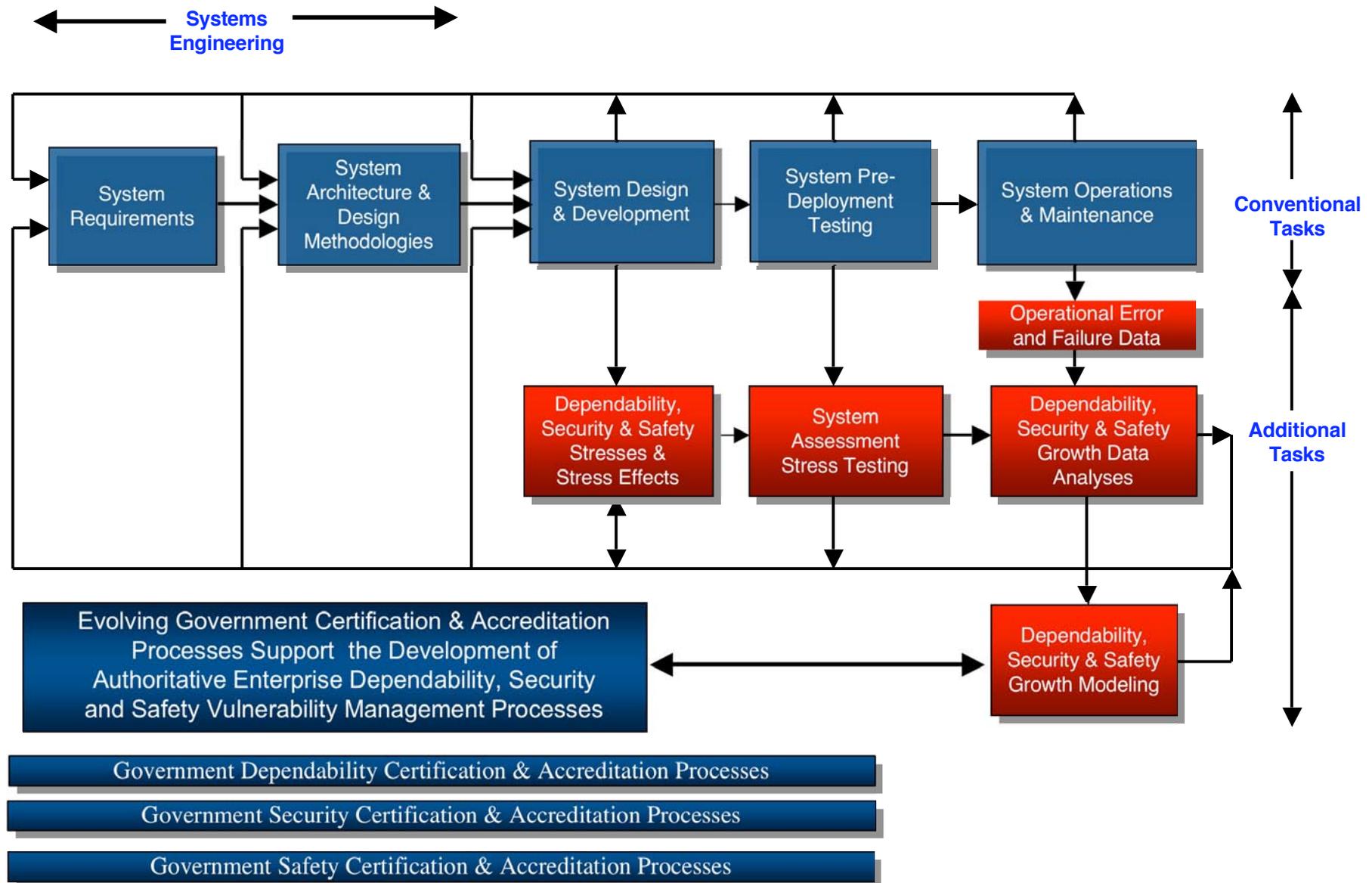
Current System Upgrade Processes Often Do Not Address Important Dependability, Safety and Security Issues



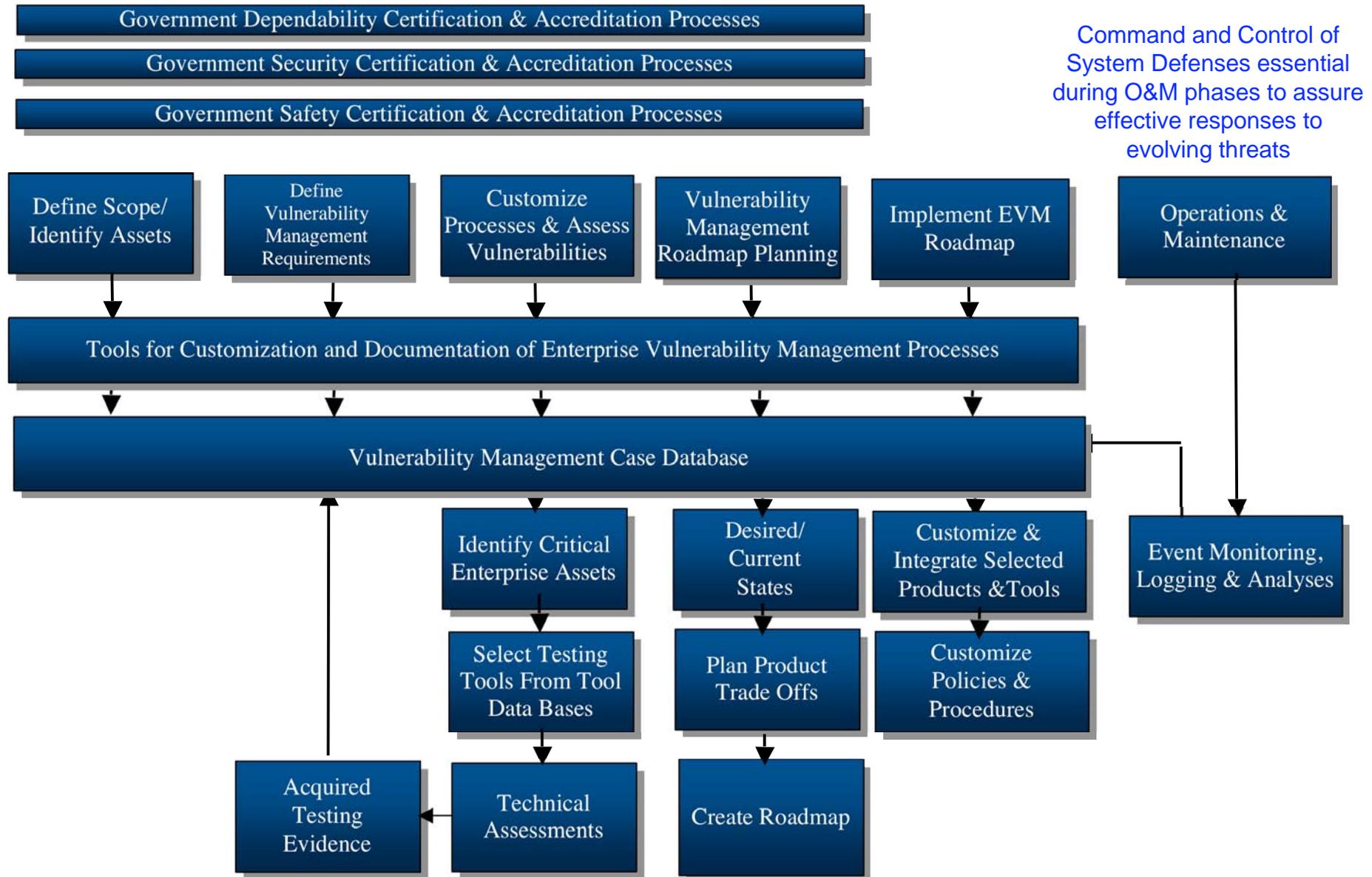
Typical upgrades focus on increasing profits and productivity by increasing demands on:

- Web Enabling
- Collaboration
- Distributed Commerce Transactions
- Outsourcing
- **Often without adequately addressing critical system dependability, safety and security issues!**

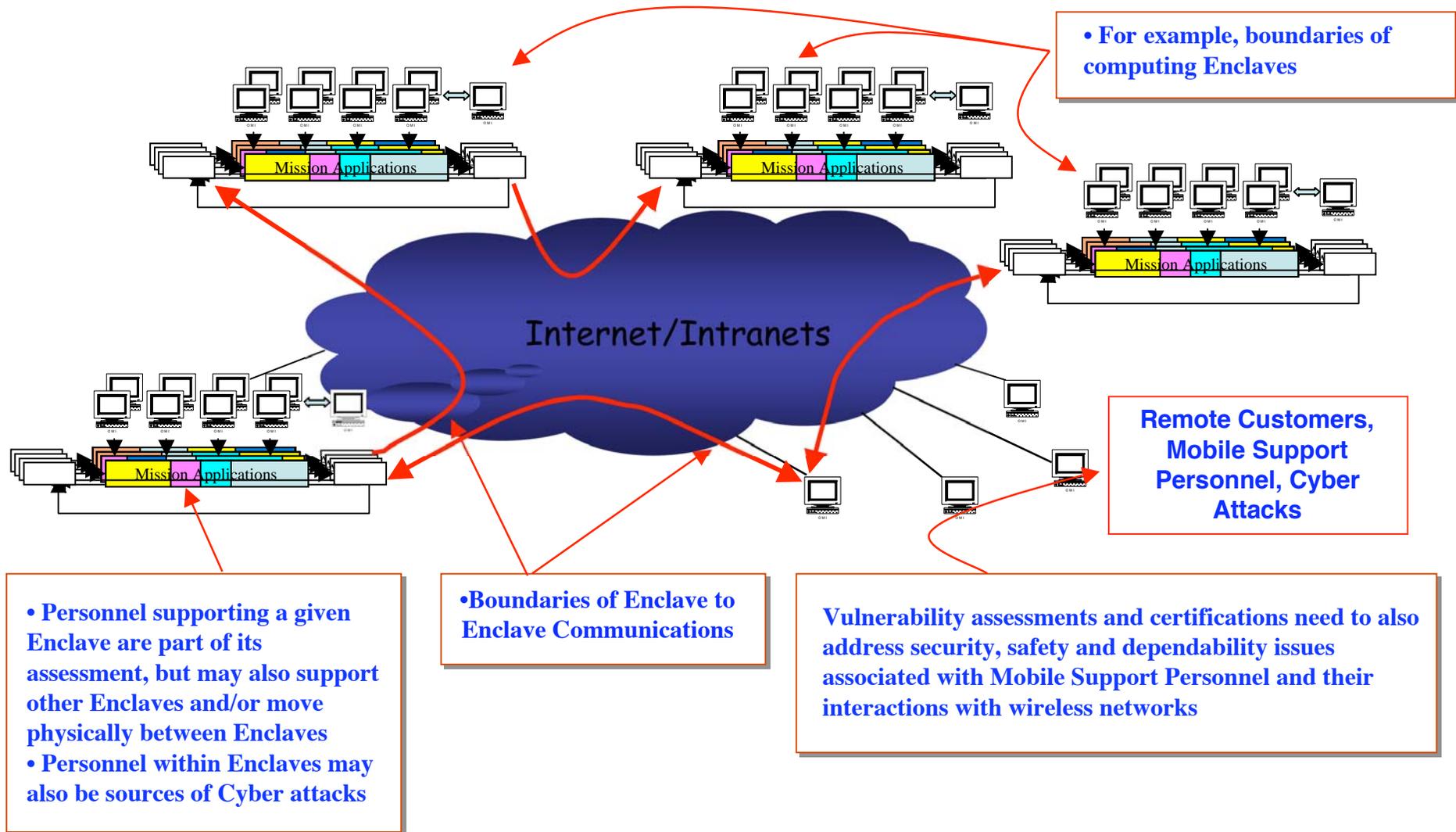
W.G. 10.4 Has Played a Major Role In Identifying the Additional Stress Testing Processes Needed to Assess & Mitigate the Combined Effects of Enterprise Dependability, Security, and Safety Stresses



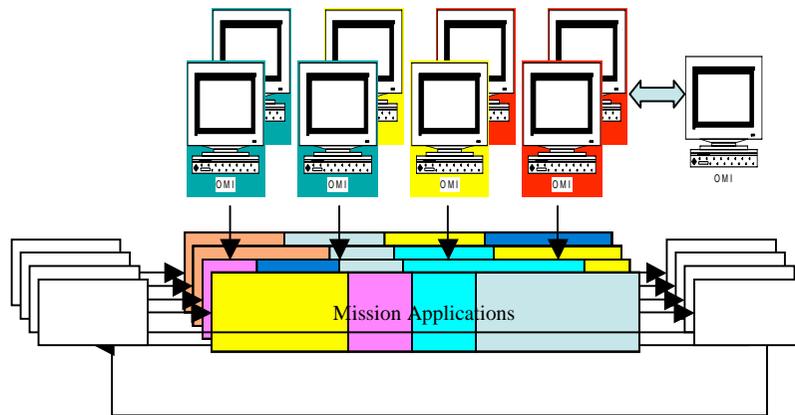
Approved Certification & Assessment Processes Can Be Used to Drive Enterprise Vulnerability Management (EVM) Planning & Implementation



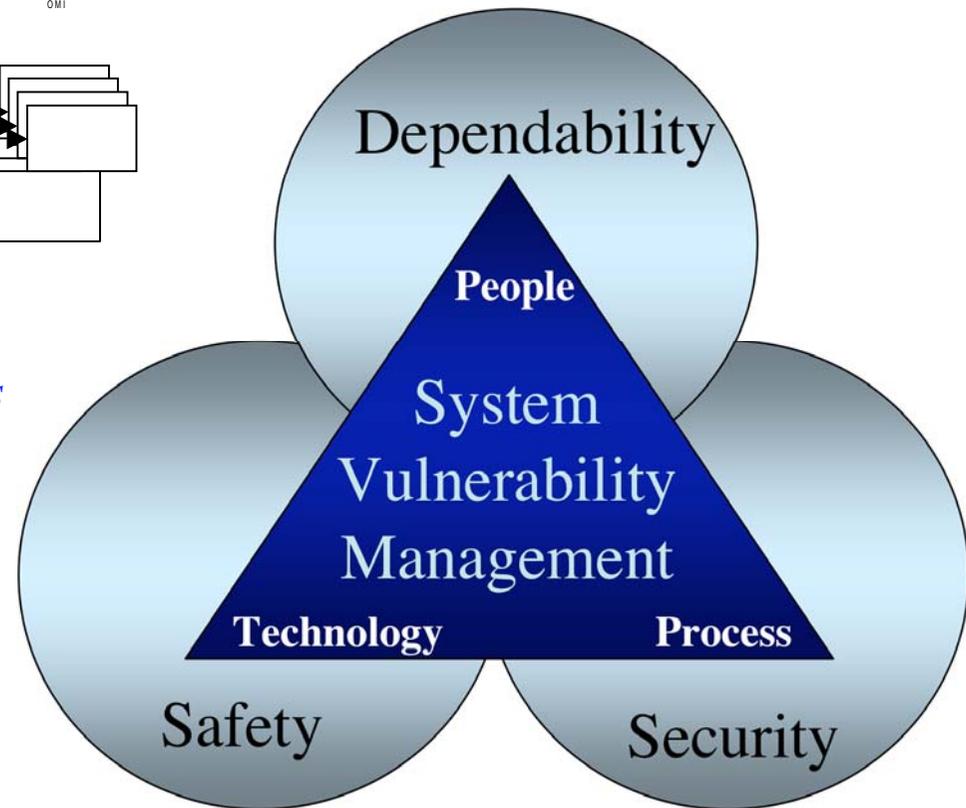
Evolving “On Demand” Architectures Will Depend on Linked Sequences of Services to Provide Required “End-to-End” Quality of Service (QoS) Capabilities



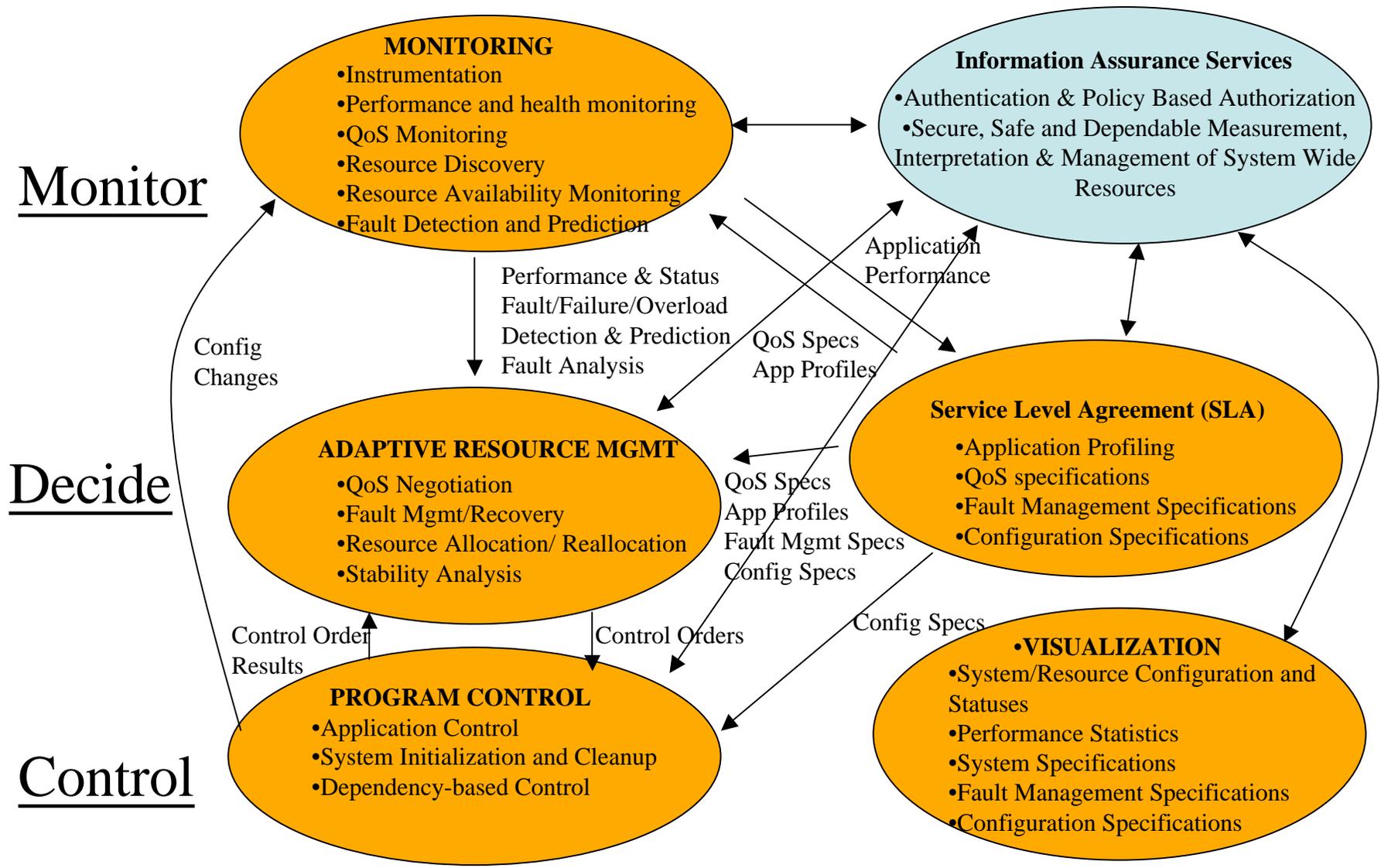
Need to Contend With Multiple Applications With Varying Security Requirements and Current System Benefit/Value, Competing for System Hardware, Software and Human Resources



*Increasing Levels of QoS Management Automation Will Enable Initial Reductions in People Support, **But System Designs Must Assure Human Understanding of Current System Status and Provide Means for Effective Human Participation in Detecting, Interpreting and Recovering From Continuously Evolving Levels of System Stresses***

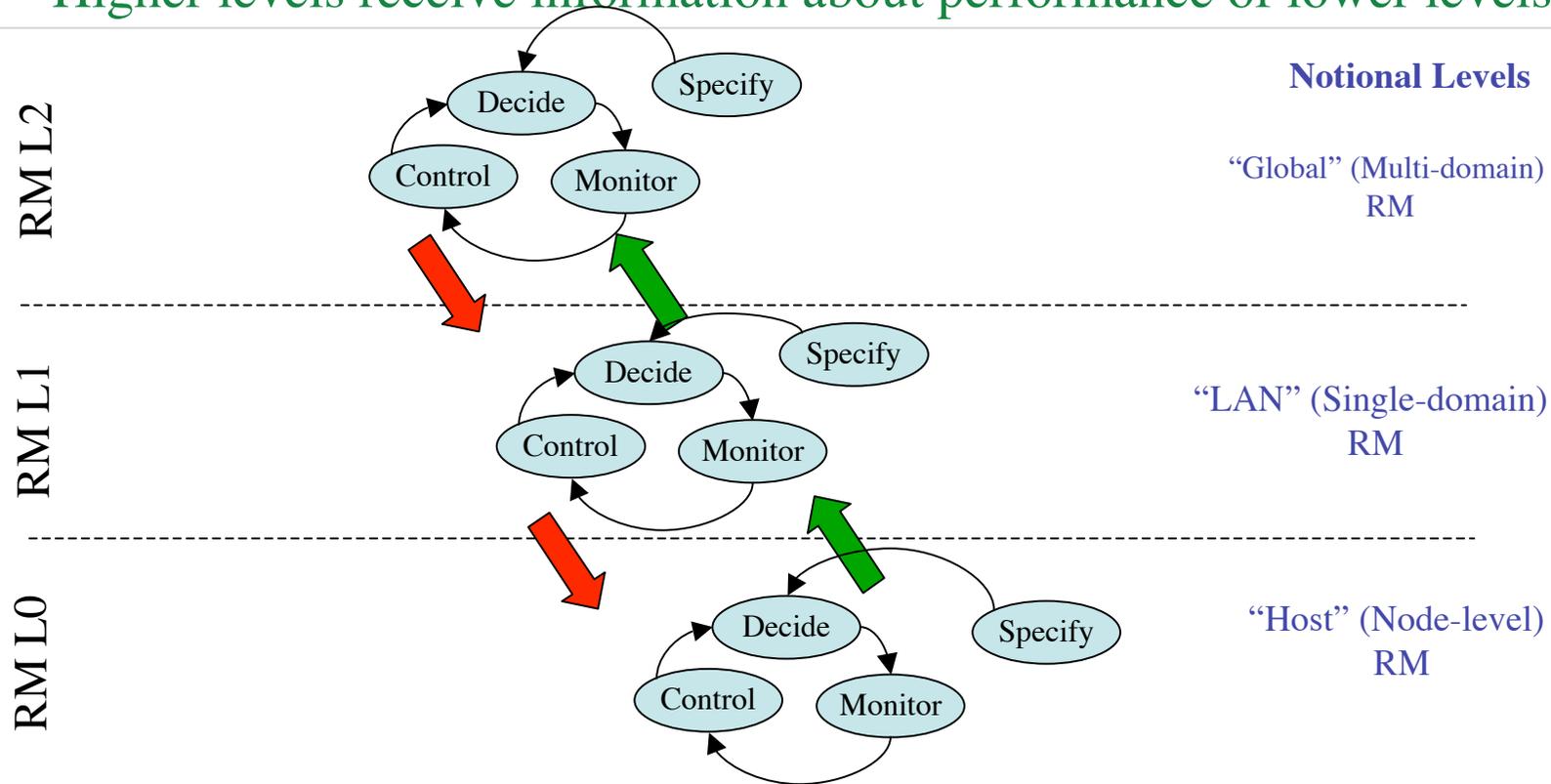


Broad Spectrum of Adaptive Resource Management Advances Under DARPA's "Quorum" Program Established Foundation for Current Industry-Wide Commitment to Providing End-to-End, QoS Controlled, "On Demand" Services



System-Wide QoS Management Will Utilize Multiple, Coordinated, Resource Management Levels

- Accepts directives from higher levels
- Provides status to higher levels
- Manages lower levels
- Higher levels receive information about performance of lower levels



Independent Stress Testing, Monitoring & Control Will Provide Metrics Guiding the Growth in System Performance, Dependability, Security and Safety

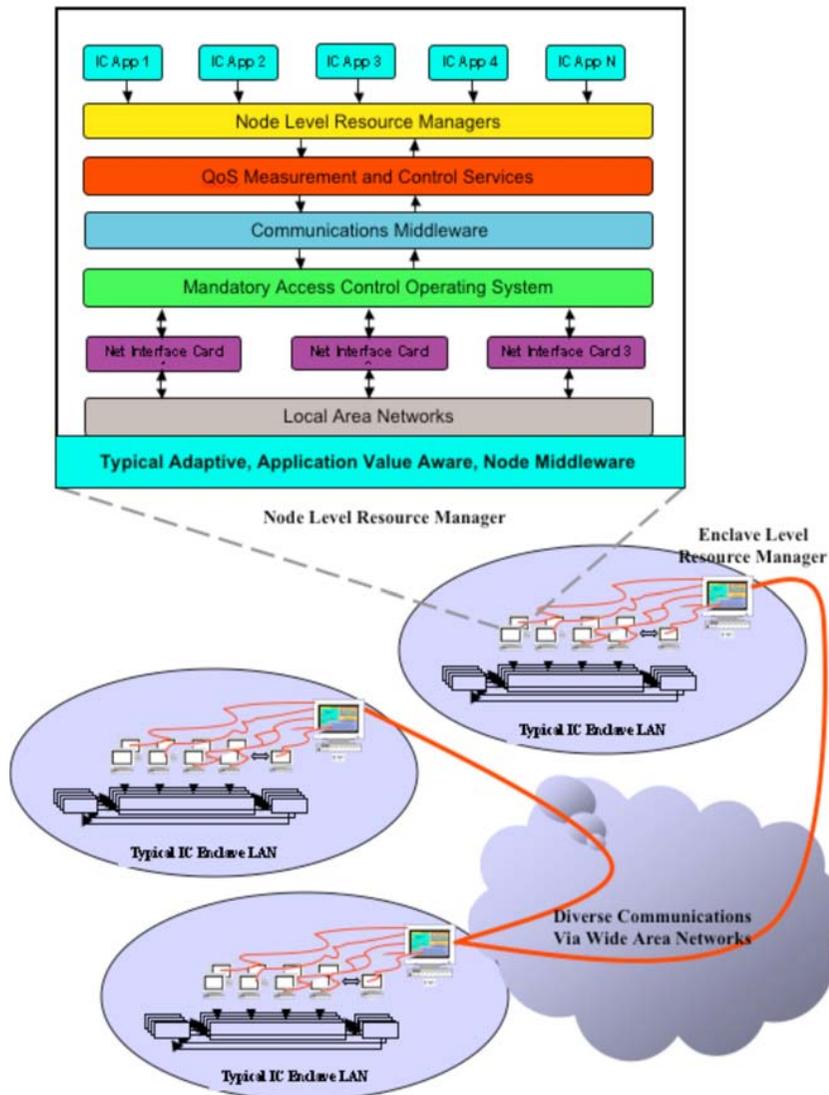


Fig. 1 Typical Secure & Dependable Wide Area System QoS Measurement and Control Spinal Cord

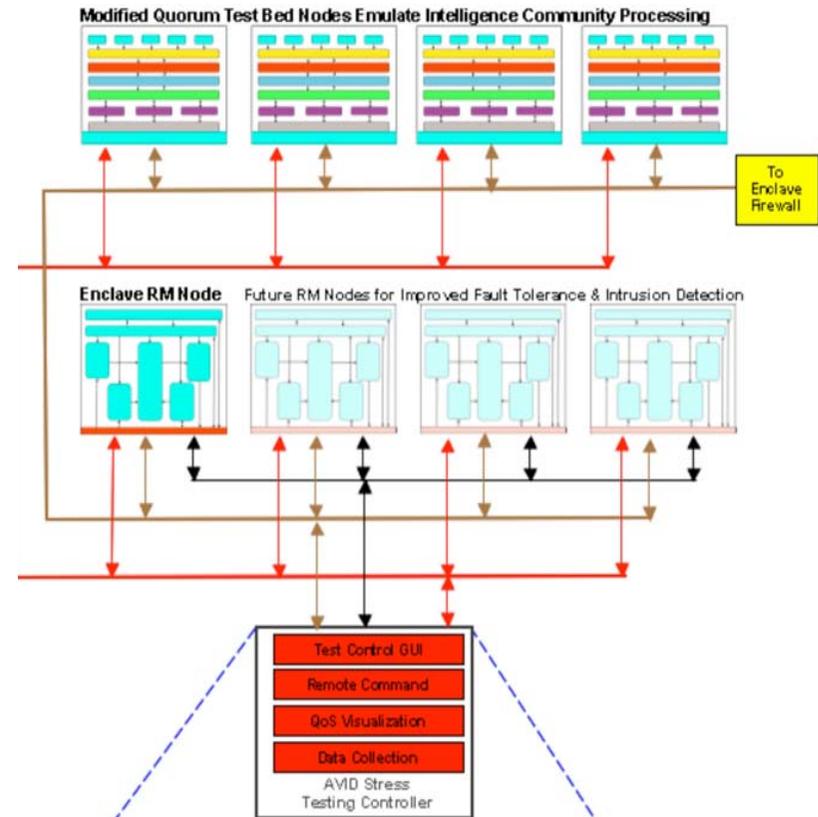
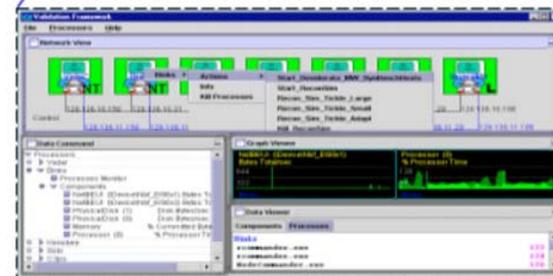
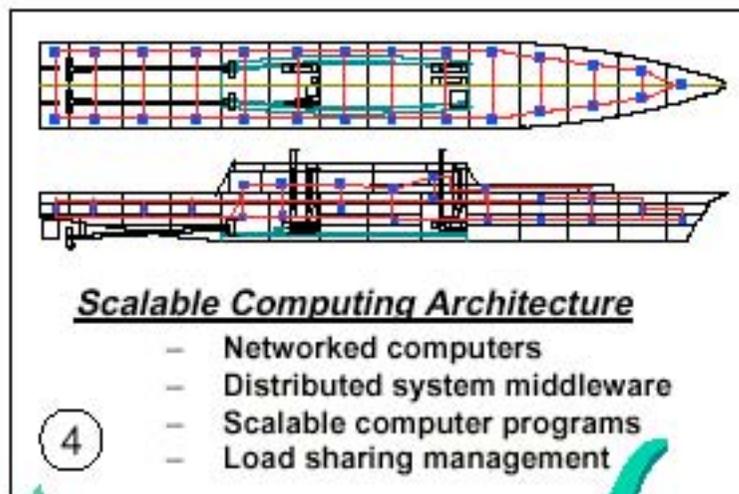
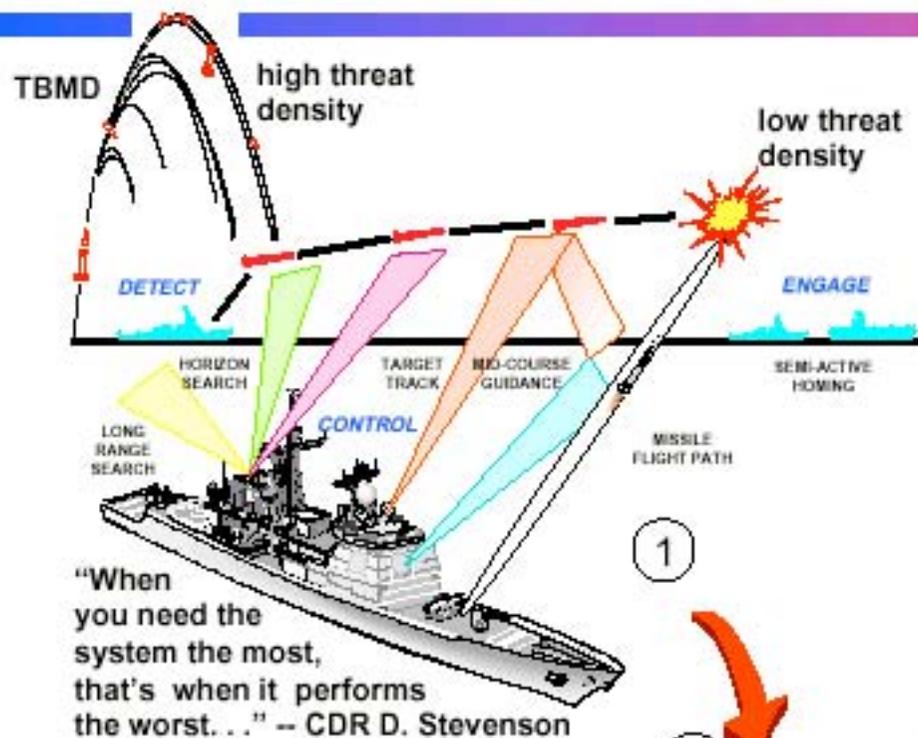


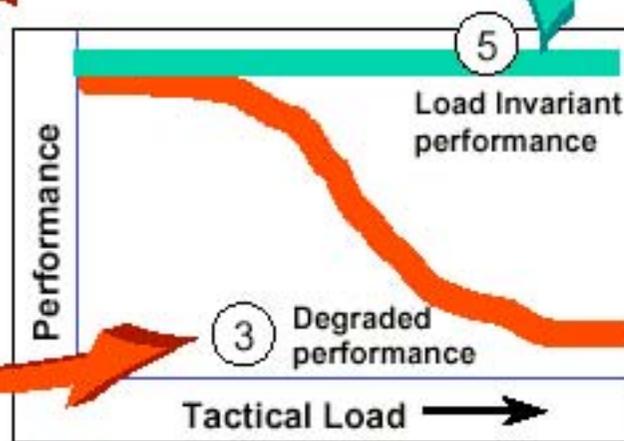
Figure 3 - AVID Stress Testing Enabled Test Bed

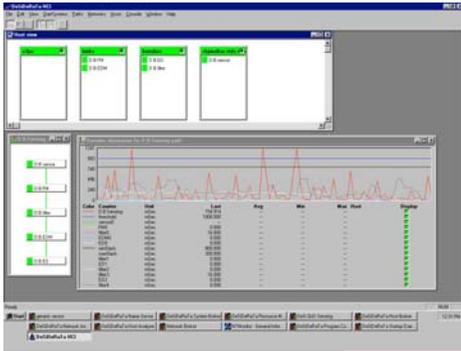


SCALABLE PERFORMANCE

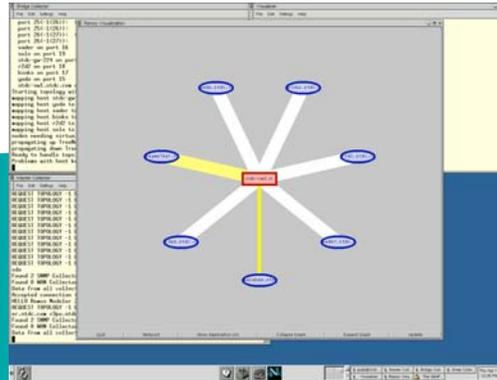


- Today's systems often exhibit degraded performance as tactical load increases
- Systems may be over-designed for worst case; this increases complexity & cost
- Scalability provides constant performance despite load & allows sharing of resources

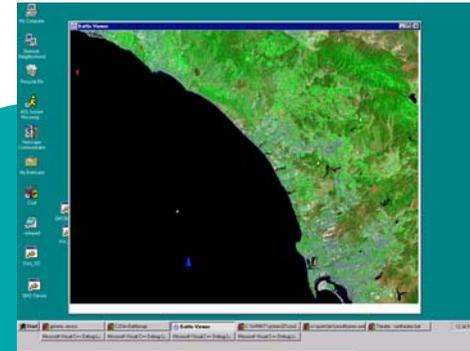




QoS Resource Manager

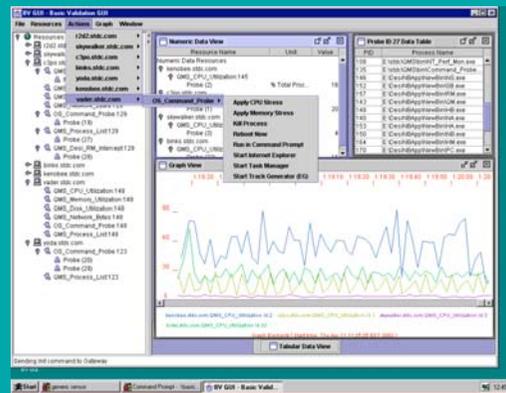


Network Resource Monitor



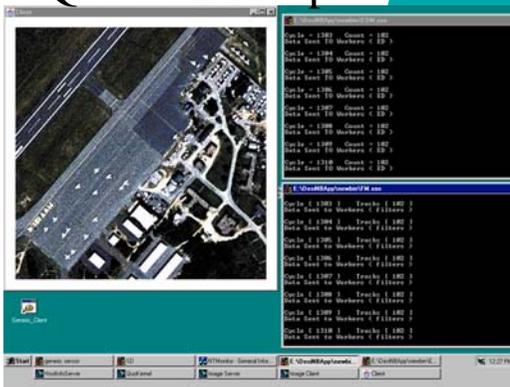
Mission Critical Application

“On Demand” Quality of Service (QoS) Management using QoS Metric Services (QMS)

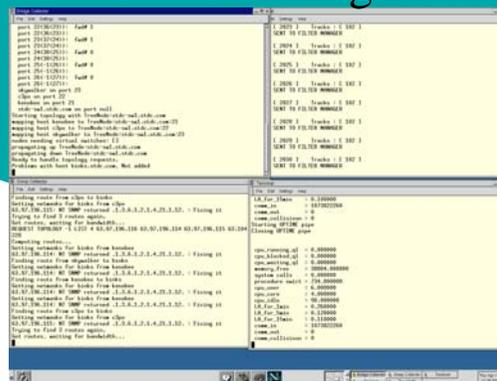


Sample QMS Application

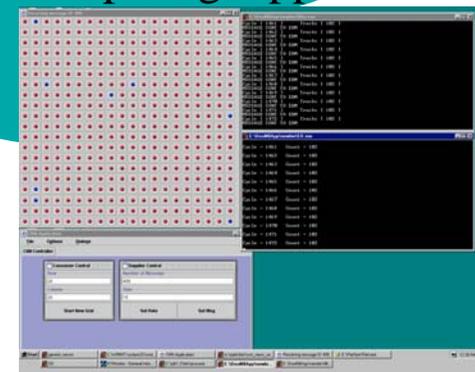
QoS Self Adaptation



Monitoring of System Resource Allocation Reasoning Processes



Competing Application



Resilient System Fall Back Modes Will Require Both Automated and Human Based Monitoring, Detection, Interpretation and Recovery Control Capabilities

The screenshot displays the DeSiDeRaTa HCI software interface. At the top, a blue banner contains the title. Below it, the application window has a menu bar (File, Edit, View, StartSystems, Paths, Networks, Hosts, Console, Window, Help) and a toolbar. The main area is divided into several panels:

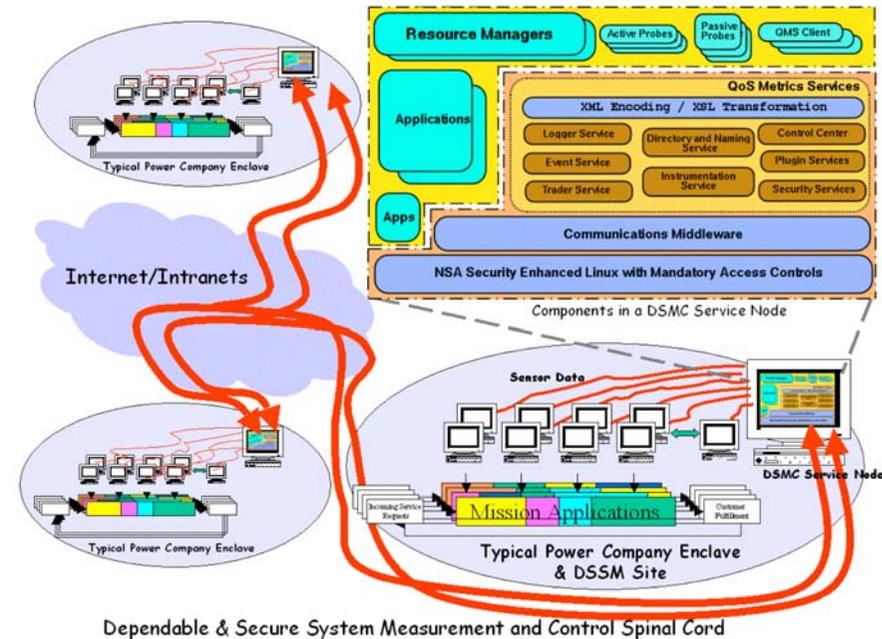
- Host view:** A window showing four host panels:
 - c3po:** Empty panel.
 - binks:** Contains 'D:B:FM' and 'D:B:EDM'.
 - kenobee:** Contains 'D:B:ED' and 'D:B:filter'.
 - skywalker.stdc.d:** Contains 'D:B:sensor'.
- D:B:Sensing:** A window showing a vertical stack of components: 'D:B:sensor', 'D:B:FM', 'D:B:filter', 'D:B:EDM', and 'D:B:ED'.
- Dynamic information for D:B:Sensing path:** A window containing a line graph and a table.

Color	Counter	Unit	Last	Avg	Min	Max	Host	Display
Red	D:B:Sensing	mSec	154.914	█
Blue	threshold	mSec	1000.000	█
Green	sensor0	mSec	█
Yellow	FM0	mSec	0.000	█
Cyan	filter0	mSec	16.000	█
Magenta	EDM0	mSec	0.000	█
Black	ED0	mSec	0.000	█
Grey	minSlack	mSec	800.000	█
Light Grey	maxSlack	mSec	200.000	█
Dark Grey	filter1	mSec	0.000	█
White	ED1	mSec	0.000	█
Light Blue	filter2	mSec	0.000	█
Light Green	filter3	mSec	16.000	█
Light Yellow	ED2	mSec	0.000	█
Light Cyan	filter4	mSec	0.000	█

The taskbar at the bottom shows the system is 'Ready' and includes various application icons such as 'generic sensor', 'DeSiDeRaTa Name Server', 'DeSiDeRaTa System Broker', 'DeSiDeRaTa Resource M...', 'DeSi QoS Sensing', 'DeSiDeRaTa Host Broker', 'DeSiDeRaTa Network An...', 'DeSiDeRaTa Host Analyzer', 'Network Broker', 'NTMonitor - General Infor...', 'DeSiDeRaTa Program Co...', and 'DeSiDeRaTa Startup Dae...'. The system clock shows 12:31 PM.

Also, Continuing Evolution of Cyber Attack Mechanisms and Tactics Will Require Effective Human Participation in Command and Control of Cyber Defenses, Including System Detection, Interpretation and Recovery Processes

- A coherent approach towards assuring their defense requires
 - Ability to provide visibility into the extent of the security attacks
 - Ability to counter the attacks through coordinated control of distributed system resources
- Security is another dimension of the end-to-end service guarantee
- Assured communications of measurement and control information between distributed system resources and their system security management facilities.
- Assured communications to distributed system resources of attack countermeasure control commands generated by the system security management facilities
- Capabilities must be survivable despite failures of individual Node, Group or Enclave defenses



"Dependable and Secure System Spinal Cords"

Cyber Command and Control

Human-Computer Interaction for
Strategic Decision Making

O. Sami Saydjari, CDA

6 July 2004

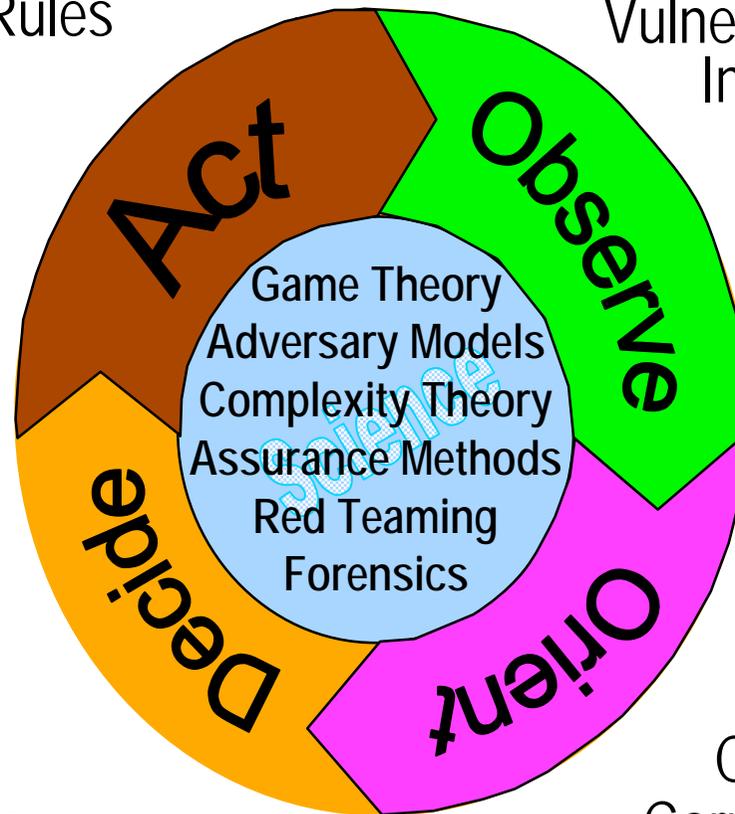
Problem and Premises

- Attackers are creative
- Missions and values are dynamic
- Defenders are creative
- Human brain recognizes patterns well
- Policies are limited to known

Command Cycle Feedback Loop

Change Firewall Rules
Disable Accounts
Retask Sensors

Vulnerability Assessment
Intrusion Detection
HUMINT



Rapid Response
Tactical Decisions
Strategic Decisions

Visualization
Cognitive Science
Correlation and Fusion

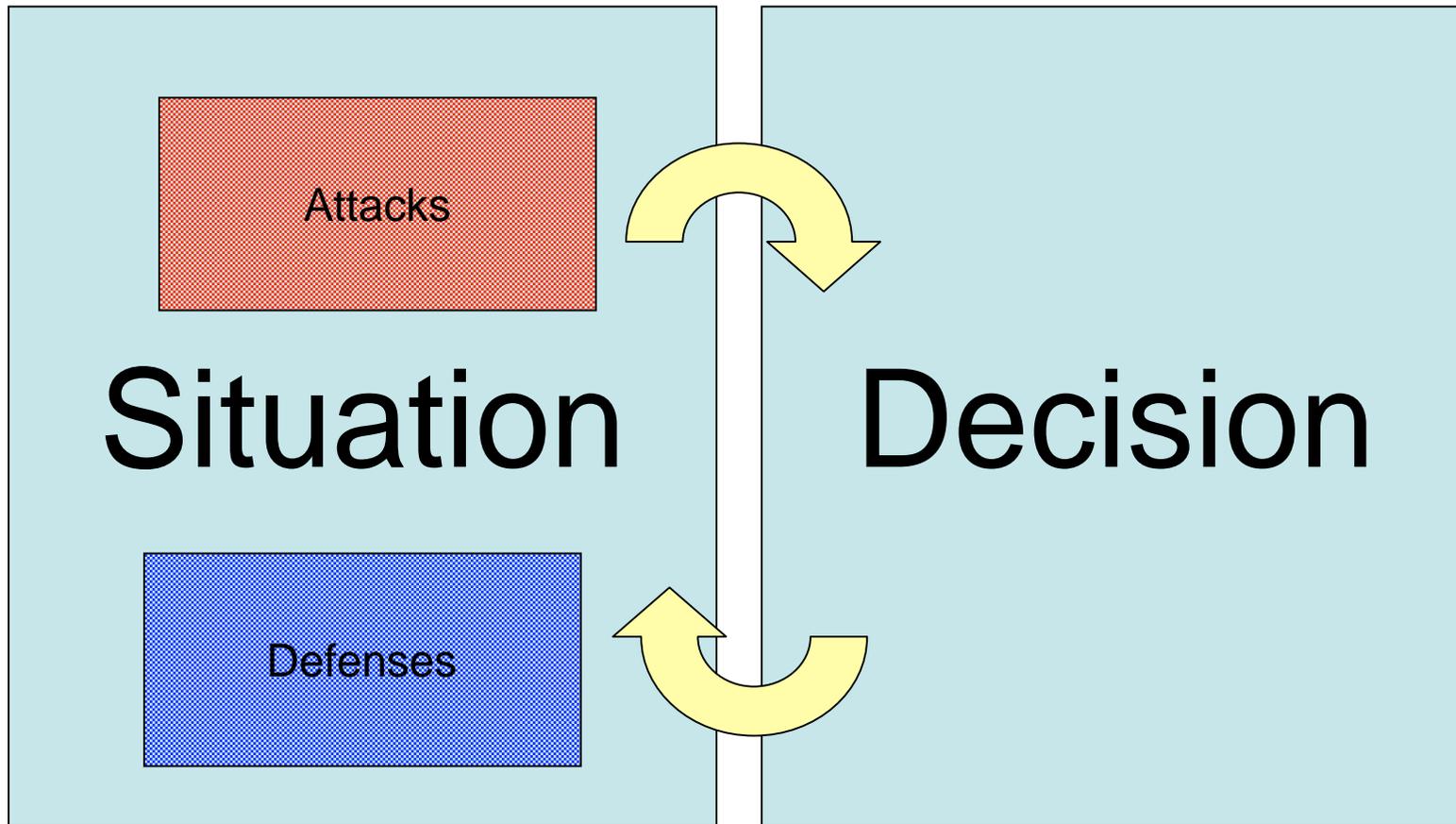
Command and Control

- Command
 - Decision-making process among possible actions given one's understanding of the situation.
- Control
 - Process of ensuring a command choice is correctly executed and has desired effect

Cyberspace Character

- Butterfly effects
- Super-human tempo
- Poorly understood interdependencies
- Attack-Defense asymmetry

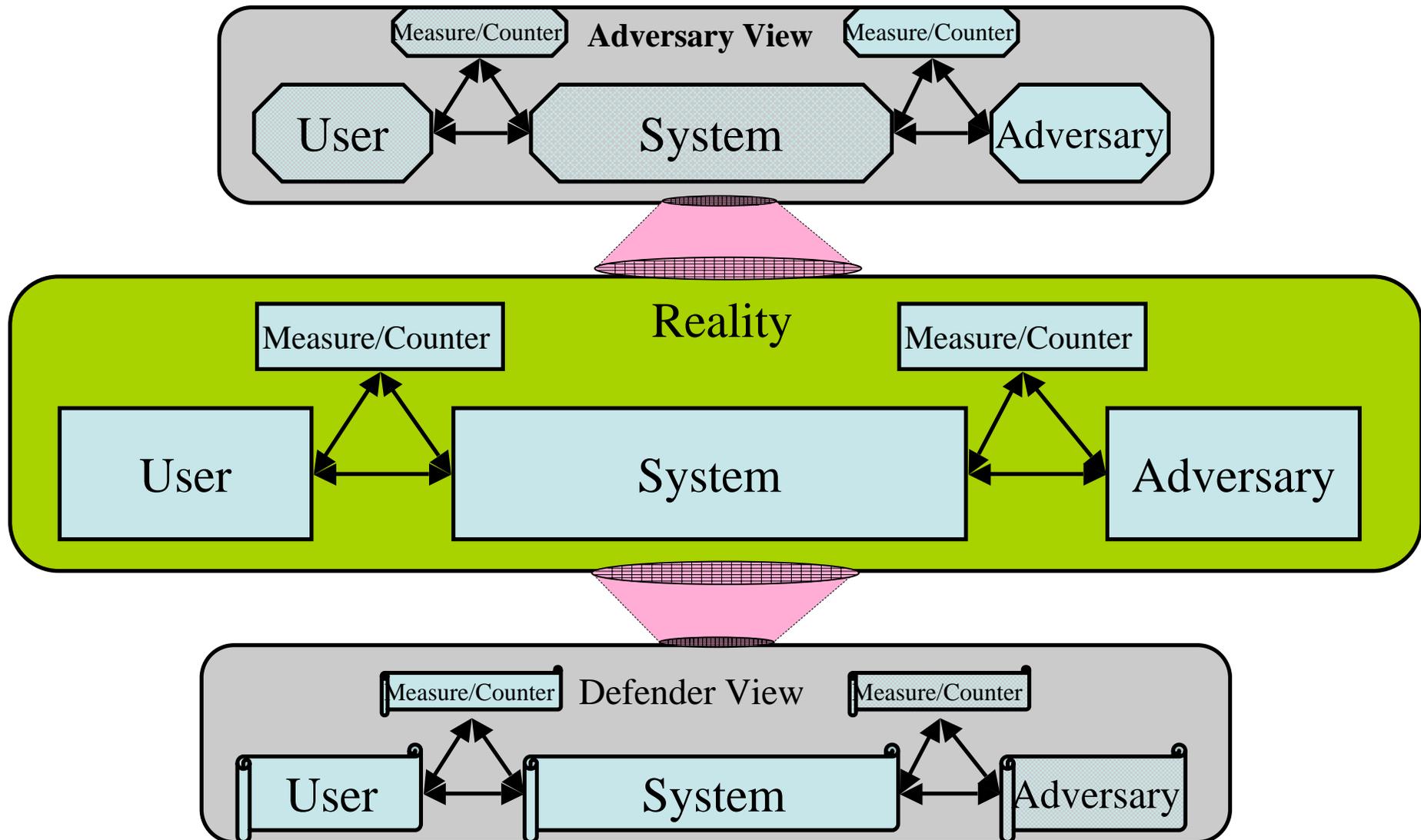
Basic Operation



Situation

- Model defense readiness
- Model attack status – multi-threads
 - Best guess on possible attacker plan
 - What is he doing, and where is he going
- Alert humans when decision is needed
- Status of defensive actions
- Delta to goal state (control)

Models Models Everywhere



Decision

- What are action options given the situation
 - Remind user in stressful situation of choices
 - Give less experienced users benefit
- Which have been most successful
 - In real situations
 - In simulations
- How long do decisions take to execute
- What are the consequences
 - On my mission
 - On attacker's goal
- What further information do I need
- Where is attacker headed?

Sample Cyber Command and Control Interface

The interface is divided into several functional areas:

- Enclave Monitors (Left Panel):**
 - Enclave Function Status:** A list of green buttons for 'Edit/View Plans', 'Distribute Plans', 'Distribute/Receive Reports', 'Send/Receive Email', and 'Browse Internet'.
 - Service Status:** A diagram showing a green circle connected to four green squares.
 - Daily Scan Results:** Two bar charts for 'Virus' (count 2) and 'Vuln' (count 5). The 'Virus' chart shows a total of 8 and the 'Vuln' chart shows a total of 11.
 - Heartbeat:** A line graph showing a regular oscillating signal between 10 and 50.
 - Alerts Per Minute:** A line graph showing a low, steady signal near the bottom of a scale from 0 to 200.
- Main Console (Top):** A navigation bar with tabs for 'Main Console', 'Task Schedule', 'Resources', 'Site Map', 'Network Topology', 'Sensor Alerts', 'Correlator Reports', and 'Trouble Tickets'. Below the tabs are buttons for 'Back', 'Forward', 'Refresh', 'Home', and 'Help'.
- Situation Monitor (Center):**
 - Indications and Warnings:** A list of red text items: '0805 Anomalous Filename scan & DB access', '0805 Anomalous connection from WS1 to DB', '0804 Stealthy IP address scan', '0802 Anomalous email from WOC to BR', and '0801 Stealthy scan on VPN from WOC'.
 - Possible Causes:** A list of red text items: 'Plan Corruption Attack', 'Plan Compromise Attack', and 'Adversary Reconnaissance'.
 - Impact:** A red text item: 'Plan corruption or compromise risks mission'.
- Response Planning and Execution (Bottom):**
 - Recommended Actions:** A list of blue text items with checkmarks: 'Review audit logs on anomalous host', 'Automated internal consistency check of plan', and 'Increase sensor sensitivities'.
 - Executing Actions:** A section with two progress bars under the heading '% Complete'. The first bar is for 'Vulnerability Scan' and the second is for 'Virus Scan'.
 - Buttons:** 'Details', 'Show Impact', and 'Do' (with a mouse cursor pointing to it).