

End-to-End Intrusion Response in Control

Systems

Presented to the EPRI Enterprise Infrastructure
Security Program
San Diego, CA August 28, 2001

David Lounsbury
Open Group Advanced Research

<http://www.opengroup.org/ar>

d.lounsbury@opengroup.org

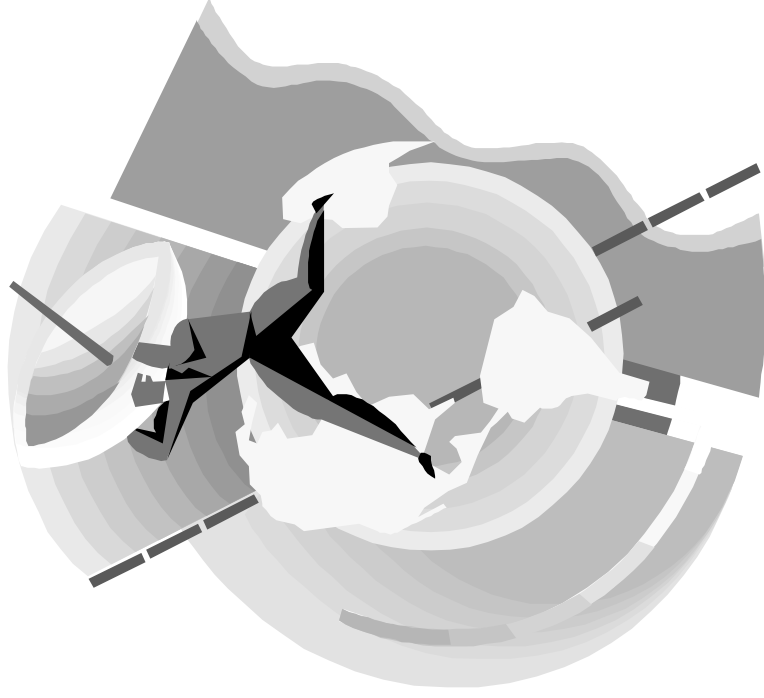
THE *Open* GROUP

with

system/technology

s/tdc

development corporation



Intrusion Detection

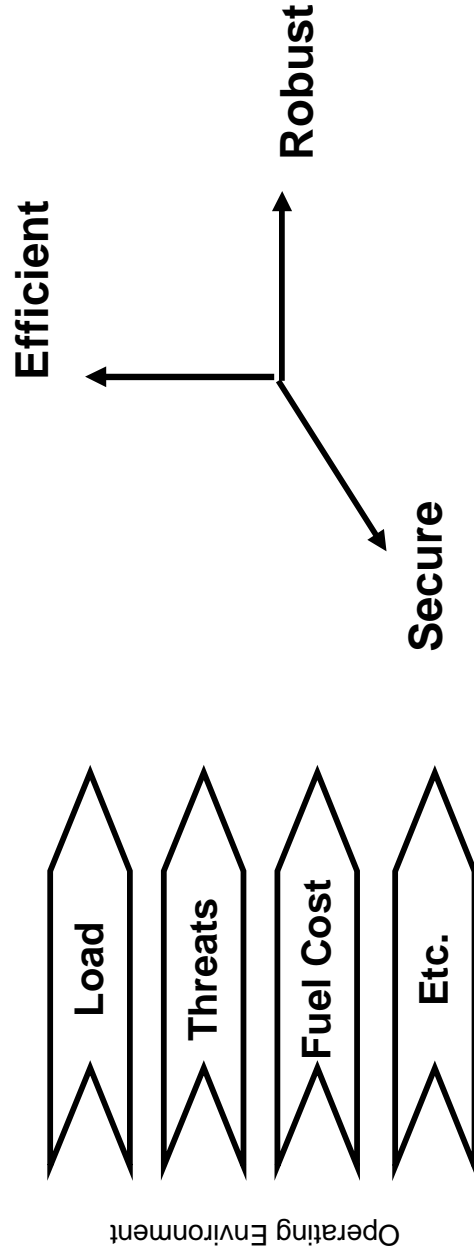
- Significant progress made in both intrusion detection and intrusion response by commercial and Government (DARPA) efforts.
- Majority of effort has been on protection in Internet or Command & Control environments.

Intrusion Response

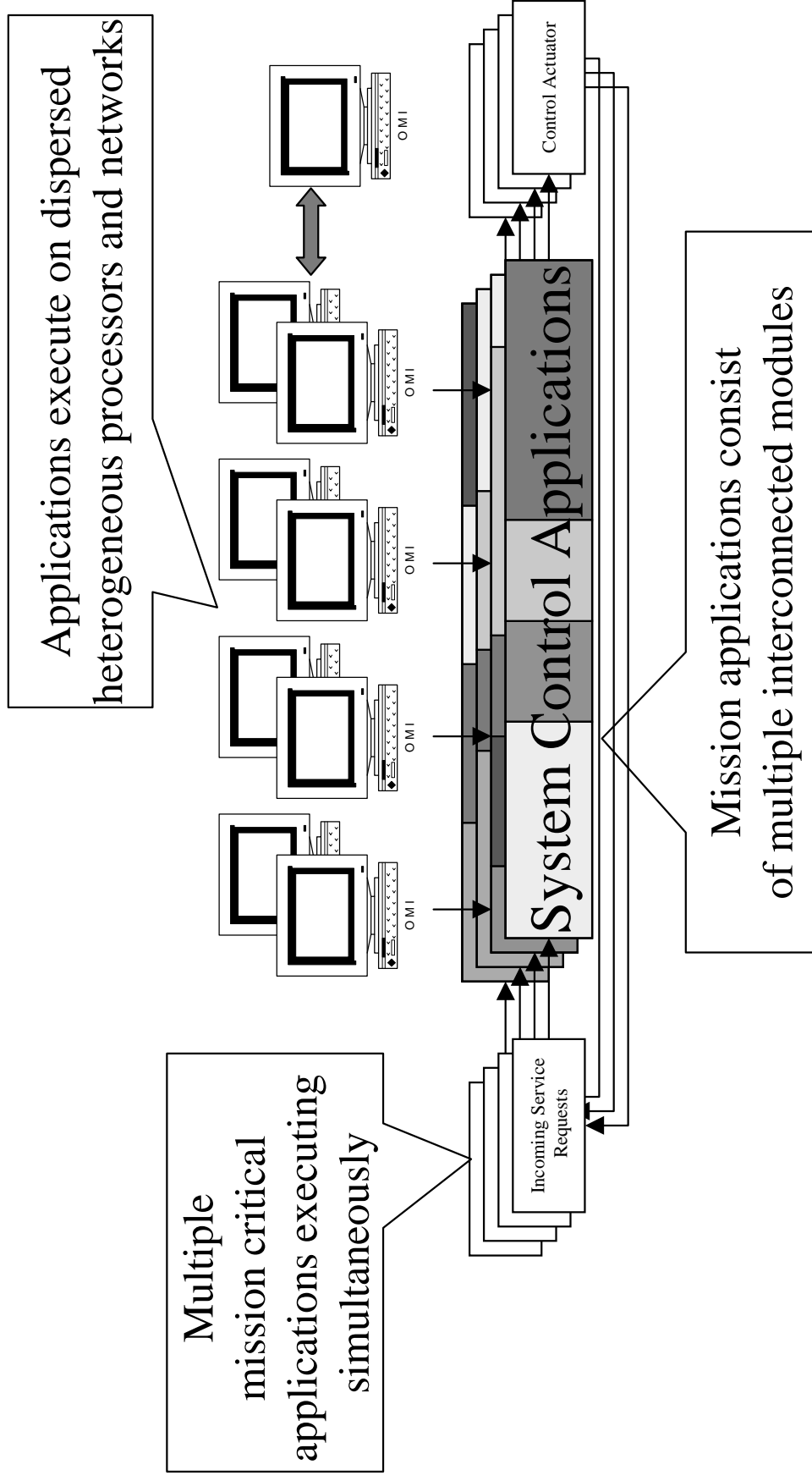
- Many components and techniques are available to respond to known or potential IT system and network intrusions:
 - Operating System security features
 - Firewalls
 - VPNs, link encryption
 - Administrative best practices
 - Emerging secure OS features

Security Management

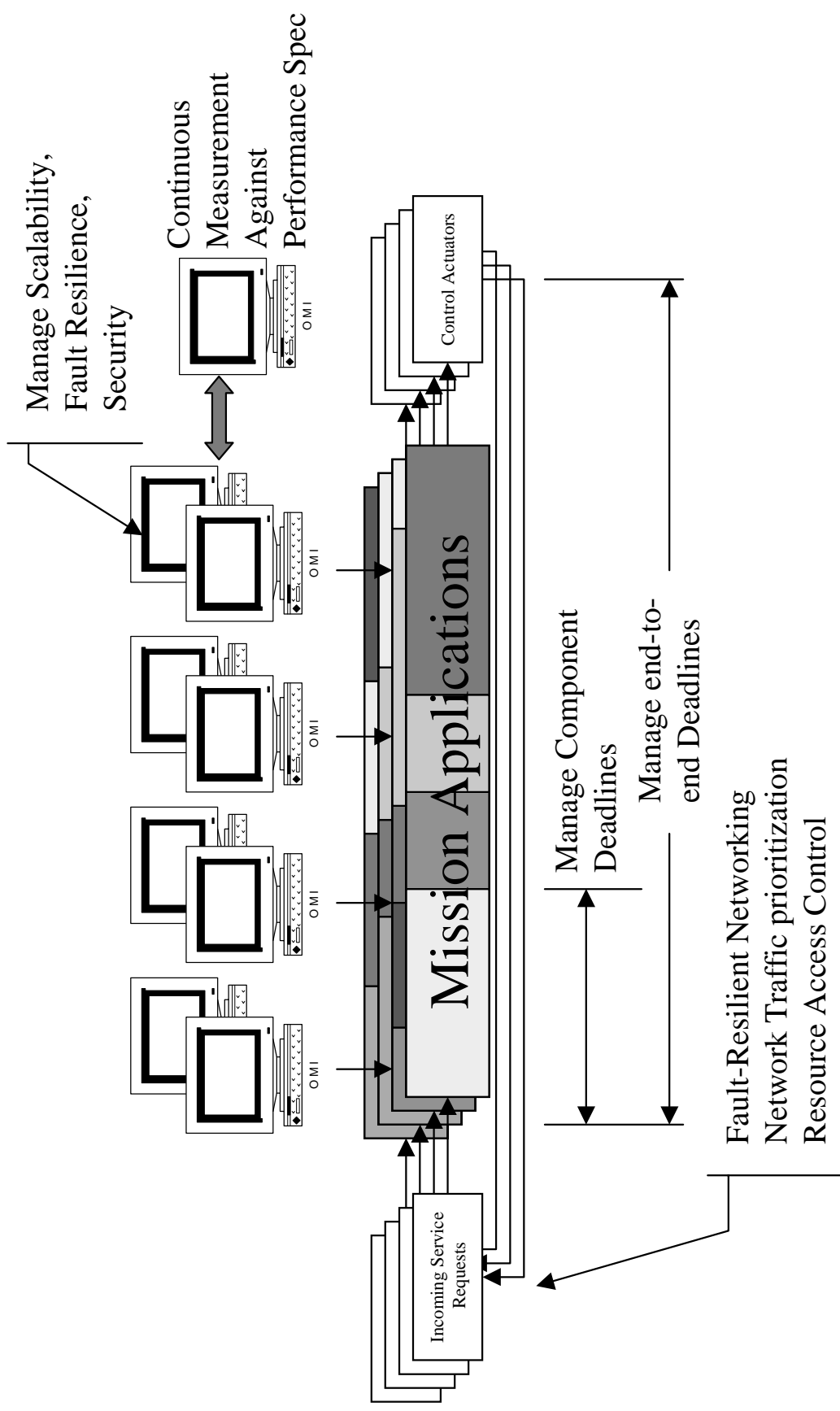
- Challenge is how to apply these techniques to large-scale, distributed, multi-partner, real-time control environments in a way that optimizes business results in a dynamic operating environment.



Notional System Control Environment

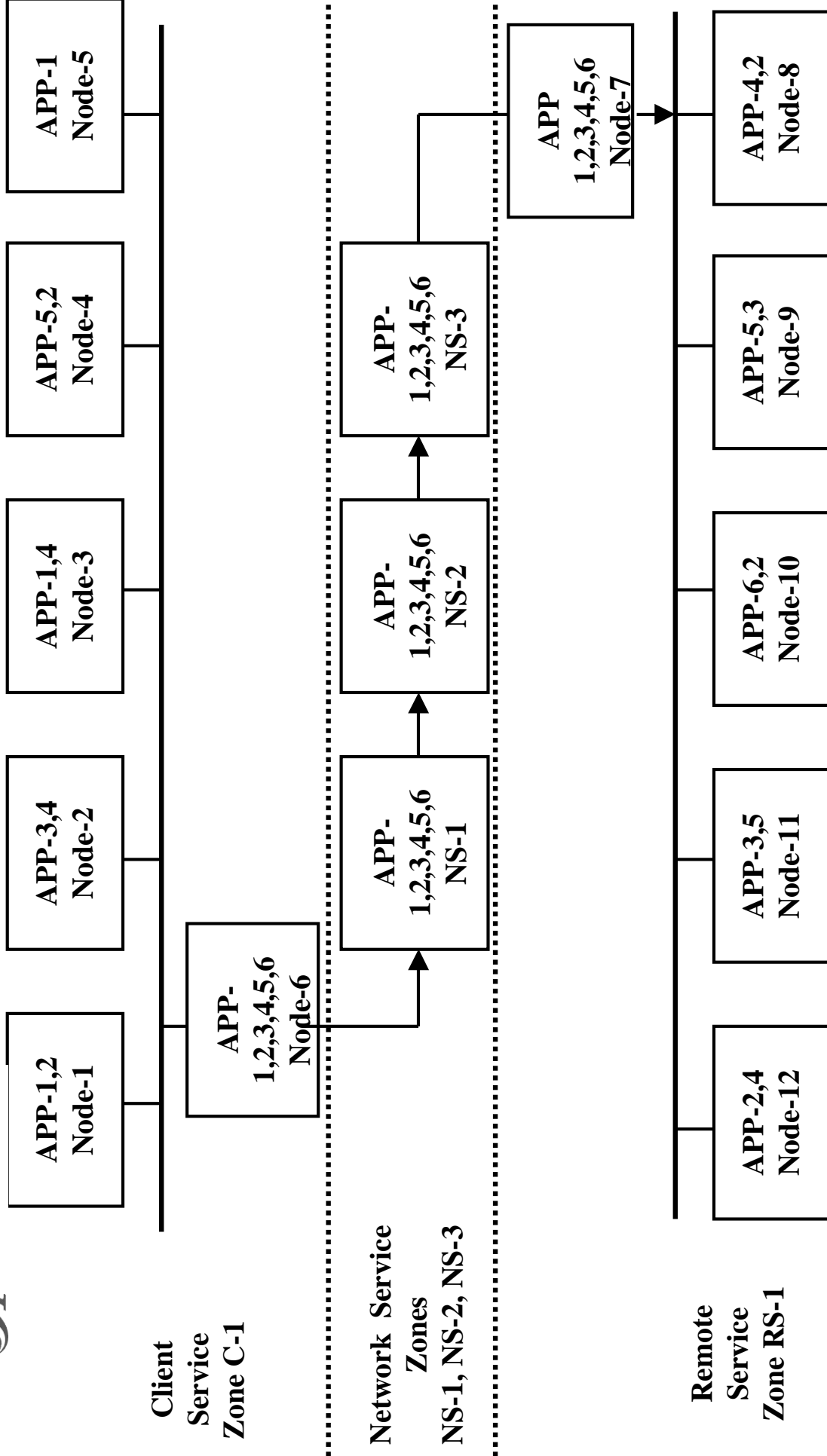


Managed System Control Environment



EXAMPLE - Multiple Applications Competing for End to End Computing & Network Services

THE *Open* GROUP



Security as End-to-End Quality

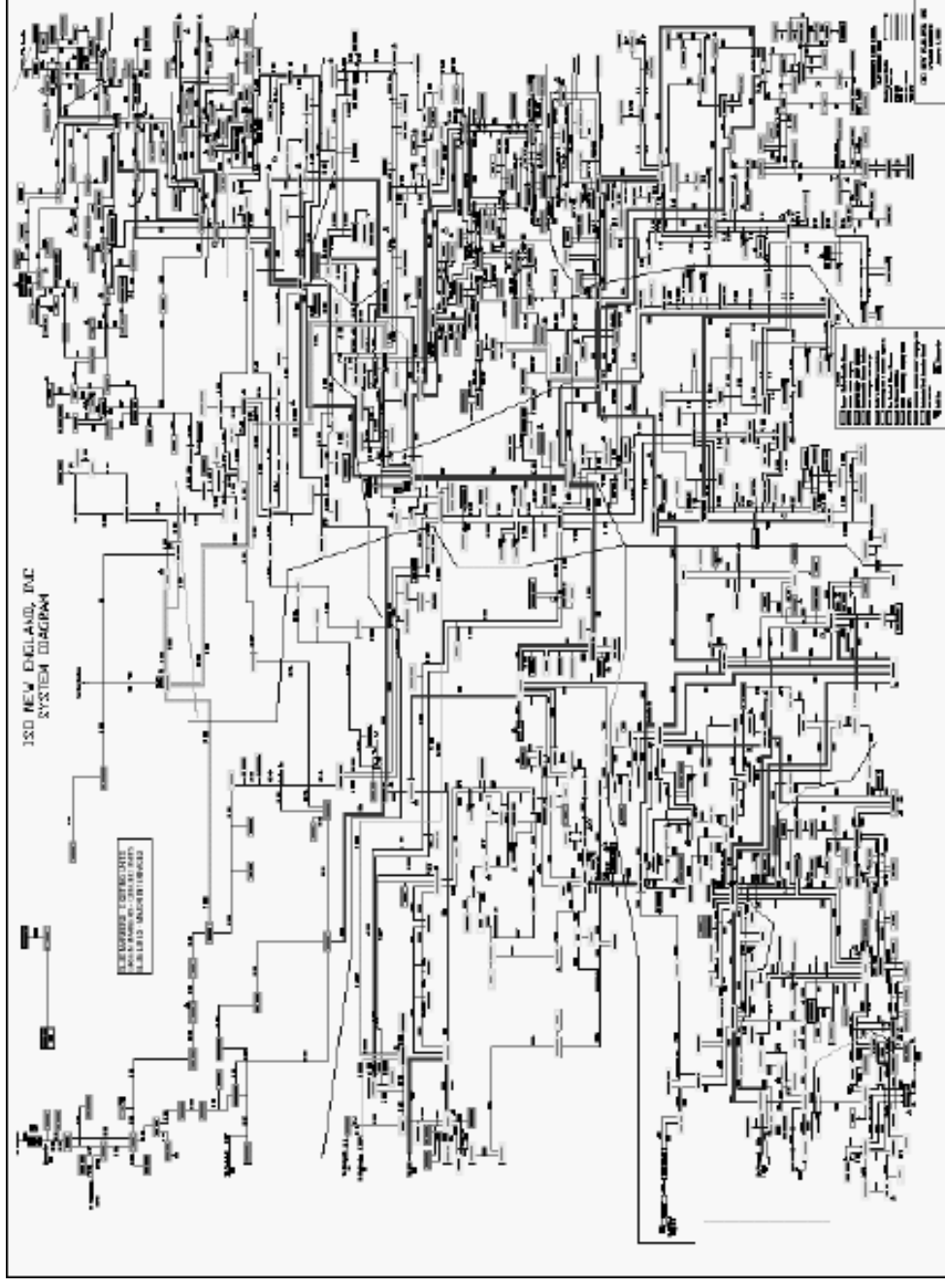
- Security just another dimension of end-to-end Quality of Service (QoS) guarantees
 - Must be part of process, not an add-on product
 - Must support (not interfere with) system operation
- Critical commercial systems and public infrastructure systems face diverse and continuously-evolving security threats
- 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

The bad news...

- Your system is only as strong as the weakest link
 - Stitching together two proprietary or incompatible security solutions introduces a weak link
- Your system is only as strong as your weakest partner
 - Y2K taught many of us to be aware of the interdependencies of our systems
- Spending more money to patch up the weak points will not fix the problem

Speaking of Links and Partnerships...

- Each color a partner (15)
- Each line a network link
- Each box a site to be protected
- **Any security solution must support this level of networking and resource sharing to meet business goals**



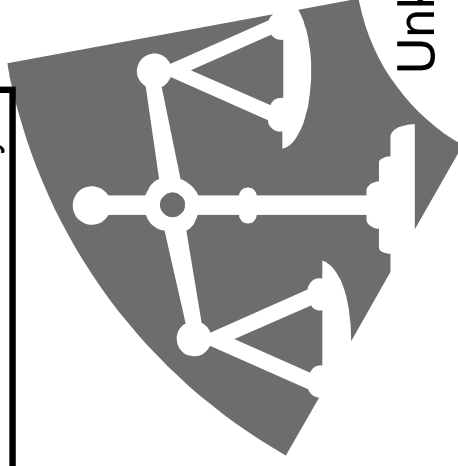
Source: ISO New England

THE *Open* GROUP

Shared Resources and Security

Known rewards

Reduced costs
Rapid Reconfiguration
Operational Flexibility



Unknown risks

Denial of service
Financial loss
Network Damage

- ❑ Sharing networks is the foundation of Utility business
- ❑ Use of shared network resources and public network infrastructures a reality in business functions
- ❑ Economics of shared networks in multi-partner environment creates strong business incentive for use in control systems
 - *IF risks can be managed*
- ❑ **Security architecture must anticipate the use of shared (and therefore vulnerable) network resources**

Dependable and Secure Links

- Ensuring that the chain of overall system security is built with trusted links of secure mechanisms
 - Secure Operating Systems +
 - Intrusion Detection +
 - Secure Measurement and Control Capabilities +
 - Secure Middleware and Resource Manager +
 - Security Best Practices and auditing
- =
- A complete security package
- Without each link in this chain of trust – failure is inevitable

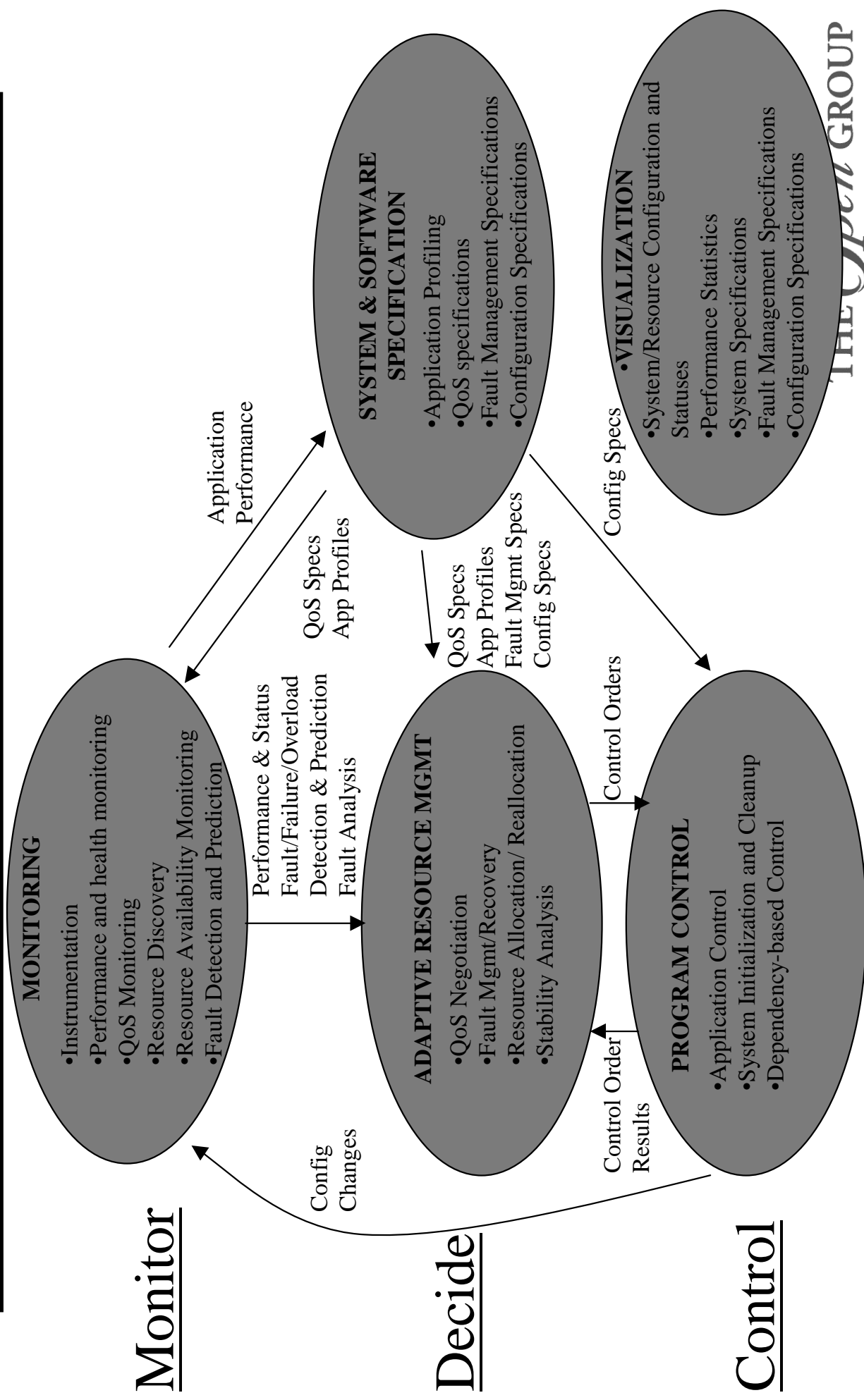
A Proposed Approach

"Dependable and Secure System Spinal Cords"

- 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
- "Autonomic Response" to protect access to critical system control resources in response to security threats

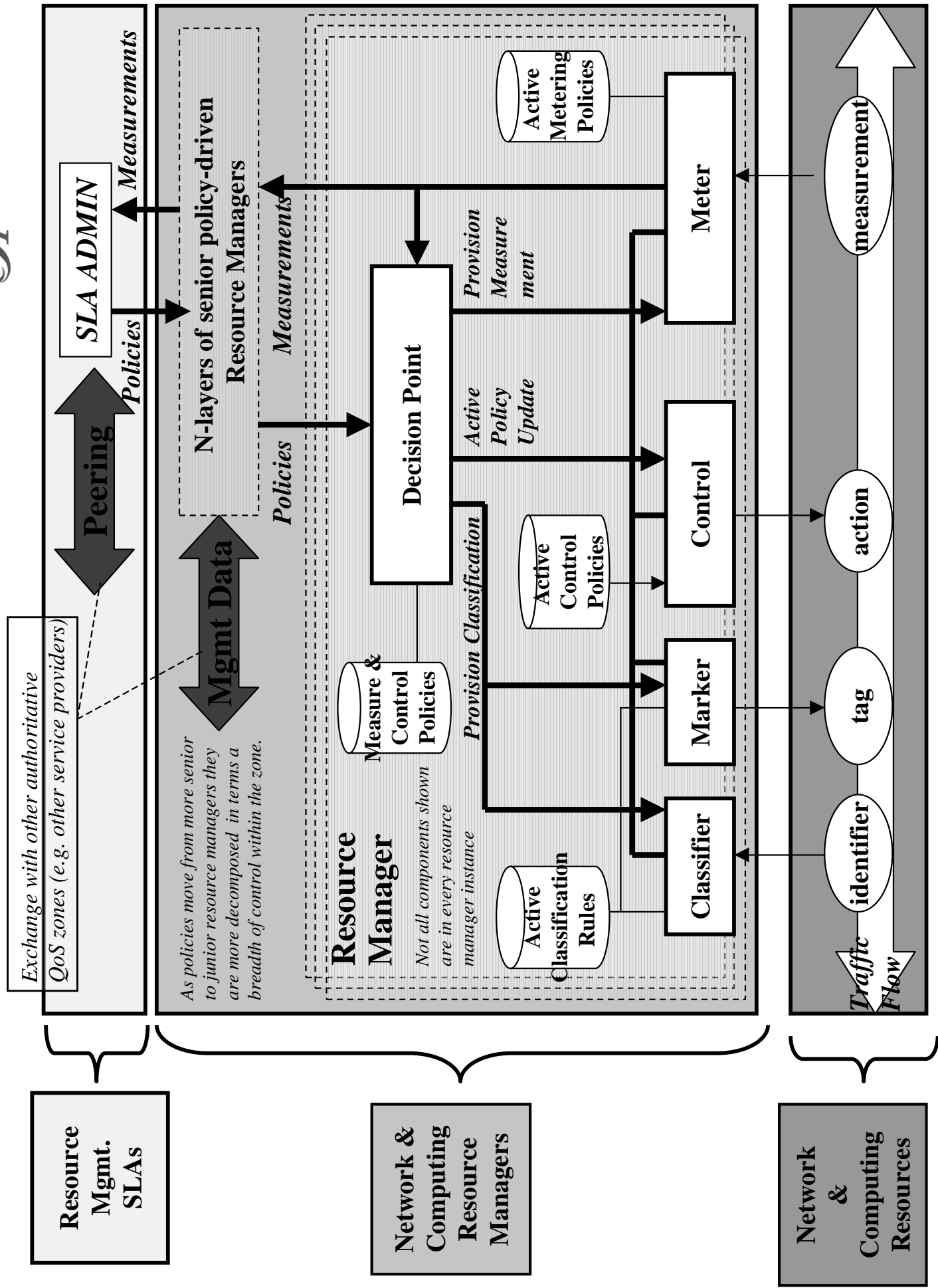
Core Resource Management

Capabilities



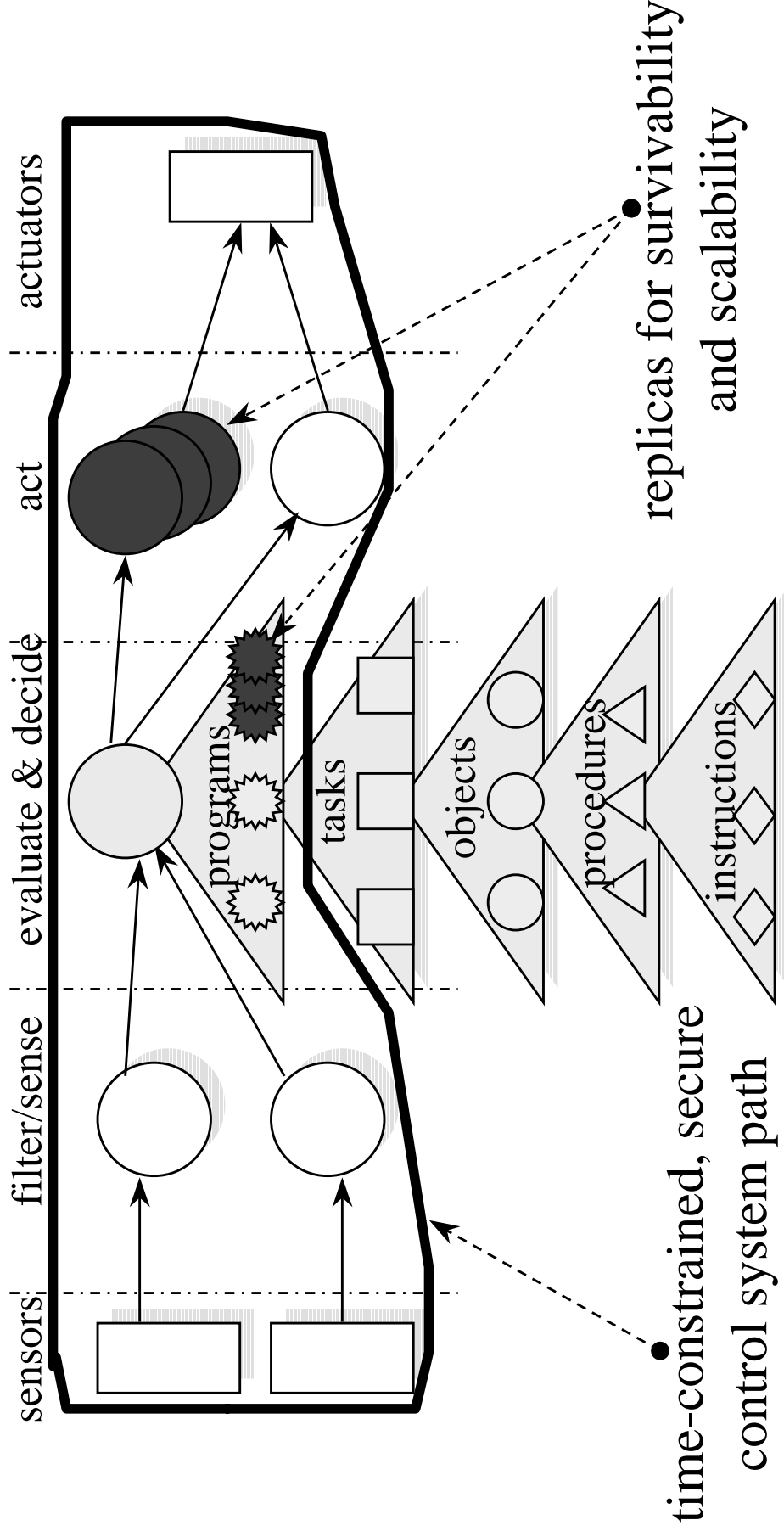
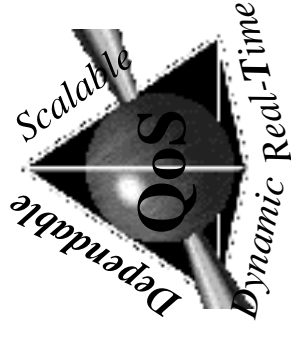
QoS Task Force - MID-LEVEL COMPONENT MAP

THE *Open* GROUP





RM Example: DeSiRaTa



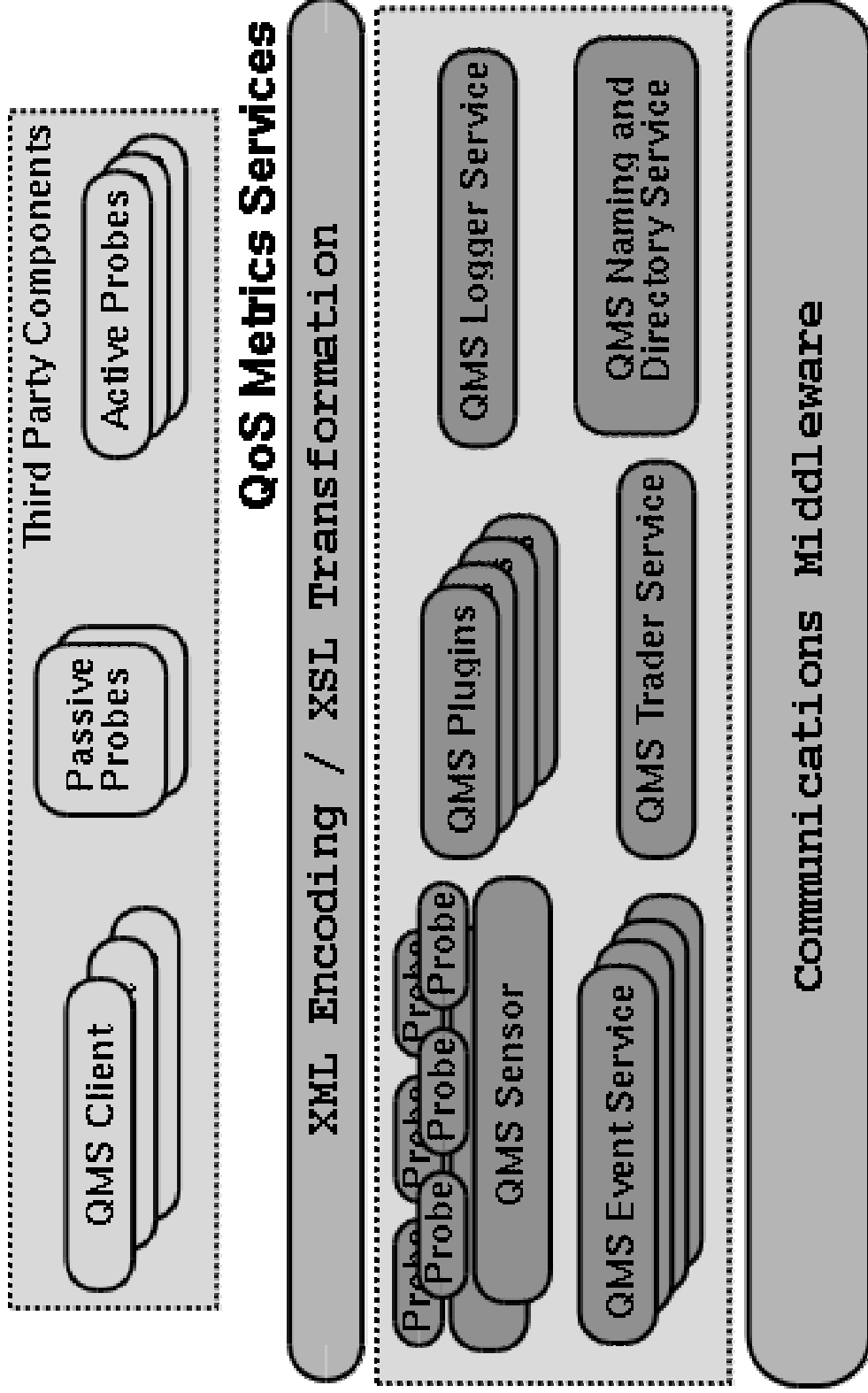
Slide courtesy of Lonnie Welch, Ohio U.

DeSiDeRaTa - Principal Attributes

- Manages end-to-end latency among competing distributed real-time applications
 - Automatic load distribution among scalable replicas
- Provides failure monitoring and recovery for survivability
- Schedulability (admission control) of new tasks
- Stability Analysis

QoS Metrics Services

Framework for Scalable, Secure Distributed Metrics



QoS Motivation and Attributes

- ❑ Correct resource management decisions depend on obtaining correct QoS metrics data
- ❑ Ease of data collection key obstacle in bringing new applications under Resource Management control
- ❑ Management of multiple QoS dimensions requires instrumentation from the same sources driving distinctly different policies
 - Cpu load relates to application latency as well as complexity of encryption algorithm used
- ❑ Service must supply QoS metrics data to a dynamic set of consumers from a dynamic set of suppliers while satisfying the following requirements
 - **Minimally intrusive**
 - **Near Real Time in performance**
 - **Distributed**
 - **Extensible**
 - **Composable**
 - **Survivable**
 - **Standards-based**

s/tdc system/technology

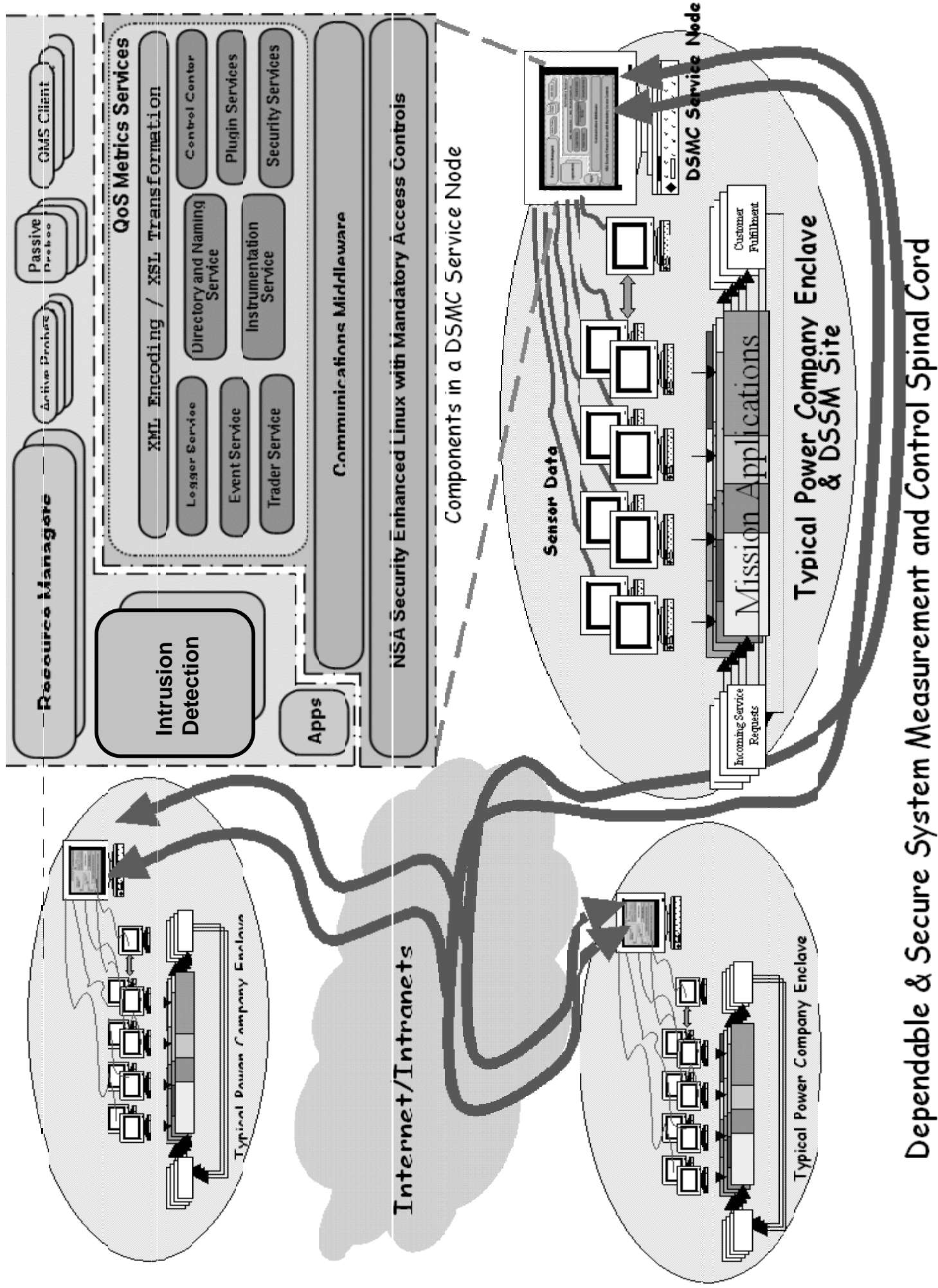
development corporation

THE *Open* GROUP

Some DARPA ID&R Efforts

- **Fault-Tolerant Networks** - <http://www.darpa.mil/ito/research/ftn/>
 - Ensure the continued availability and graceful degradation of the network infrastructure under partially successful attacks, maximizing the residual capacity available to legitimate users.
 - Ensure the fault-tolerance and secure survivability of critical network services;
 - Thwart denial-of-service attacks by constraining an attacker's resource consumption; and
 - Trace and contain attacks as close to the source as possible.

- **Active Networks** - <http://www.darpa.mil/ito/research/anets/>
 - “Smart Packets” - fundamental change in how packets travel through network
 - Authentication forms basis for dynamic access control
 - Separate traffic and administrative functions based on types and policy
 - Fault-Tolerance Mechanisms Based in Network



Dependable & Secure System Measurement and Control Spinal Cord

Possible First Steps

- Reference Architecture for scalable security backbone
 - Driven by business requirements
- Security components survey
- Establish testbed for security technologies
- Identify “low-hanging fruit” - what existing components and protocols can be easily modified (or wrapped) to begin migration to security architecture

A Starting Point

- Potential Technologies
 - SE Linux & TrustedBSD
 - QoS Metrics Services
 - Quorum QoS Resource Managers
 - Amaranth
 - DeSiDeRaTa
 - Adaptive Communication Environment (ACE)
 - The Ace ORB (TAO) - real-time middleware
 - CIM, WBEM and AIC Standards
- Definite need for
 - Certificate Authorities
 - Transport Layer Security
 - Security Policy Engines
 - Public Key Infrastructure

Active Loss Prevention

- The Open Group launching forum on Active Loss Prevention
 - Address trust and risk issues associated with electronic trade
 - Develop strategies to actively counter financial loss resulting from security breaches
 - Build consensus among technical, IT management, legal, and regulatory interests
- Initial meeting Amsterdam, October 22-26
 - See <http://www.opengroup.org/amsterdam2001/>
- Other meeting highlights:
 - Wireless Security Workshop - Mobile Management Forum
 - Safety Critical Software - Real-Time & Embedded Forum
 - Service Level Agreements - QoS Task Force