Open Group - Vulnerability Management (OG-VM) Initiative

an integrated approach to strengthening continuity of mission critical system services and protecting against catastrophic losses

by
assessing and mitigating system dependability, security and safety vulnerabilities

Background Notes:

• Interest generated by earlier, proprietary, S/TDC presentations on “Enterprise Vulnerability Management” led to current Open Group interest in developing an Open, non proprietary, approach to the problem that will facilitate cooperative government, industry and academia participation in addressing critical System Vulnerability Management issues

• While we have tentatively called this an Open Group Vulnerability Management (OG-VM) Initiative, suggestions for other names are welcome - e.g. Open System Vulnerability Management; Open Architecture Vulnerability Management, etc. Could be characterized as a subset of System Risk Management

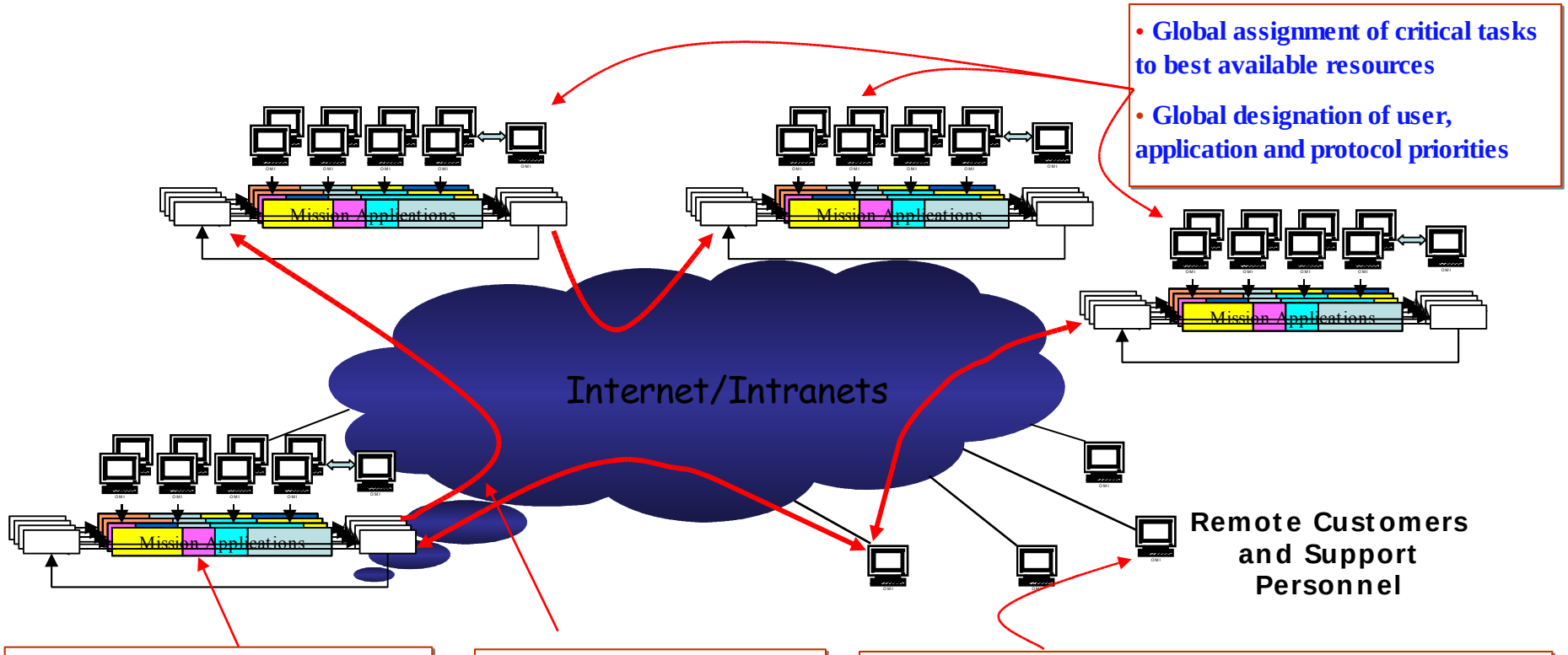
The Weakest Link

- As Government and Industrial Systems evolve to remain competitive, changes focused on improving productivity are often accompanied by substantial, hidden, increases in system dependability, security and safety vulnerabilities

- Vulnerabilities are introduced both within organizations and in the organization's increasing dependence on chains of supporting, distributed, application and communication services

Evolving Systems Need Open, Holistic, End to End, Vulnerability Management!

Need for Both Vulnerability Management and Adaptivity in Each Link of the End-to-End Chain Supporting Mission Critical System Services



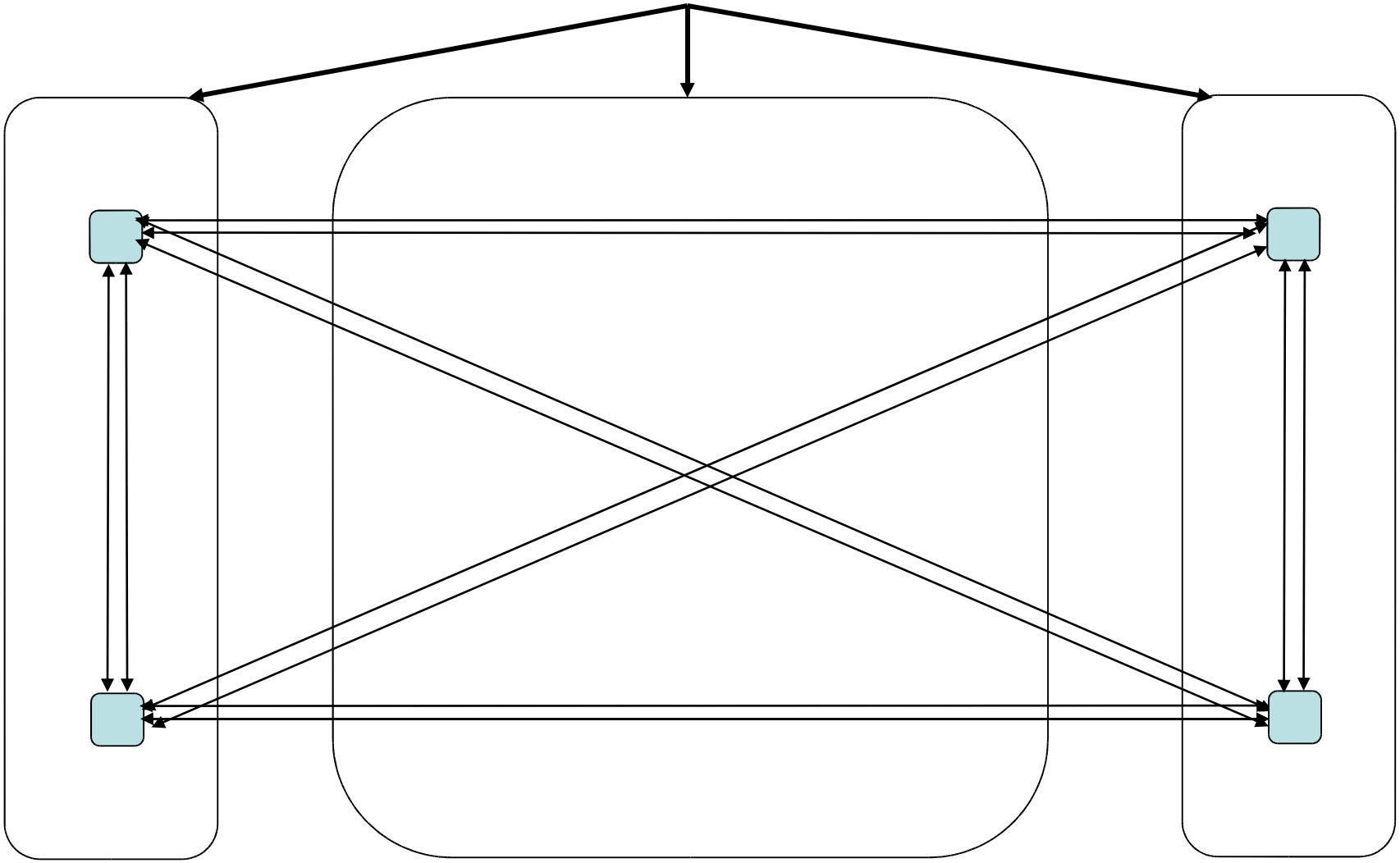
- Global assignment of critical tasks to best available resources
- Global designation of user, application and protocol priorities

- Prioritization of users and applications within sites
- Site resource management and control based on specification and monitoring of required QoS

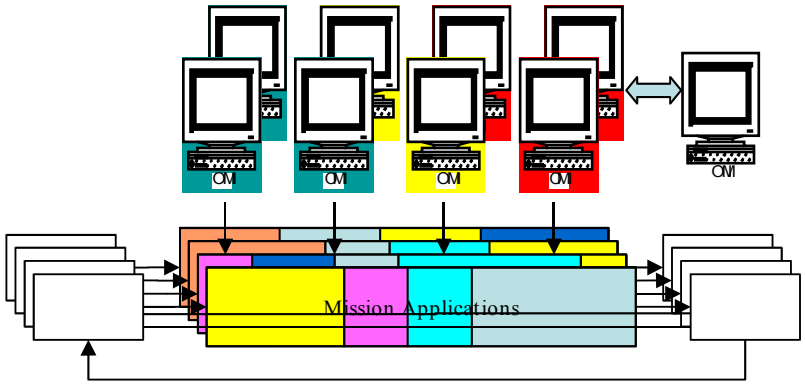
- Prioritization of critical traffic on networks

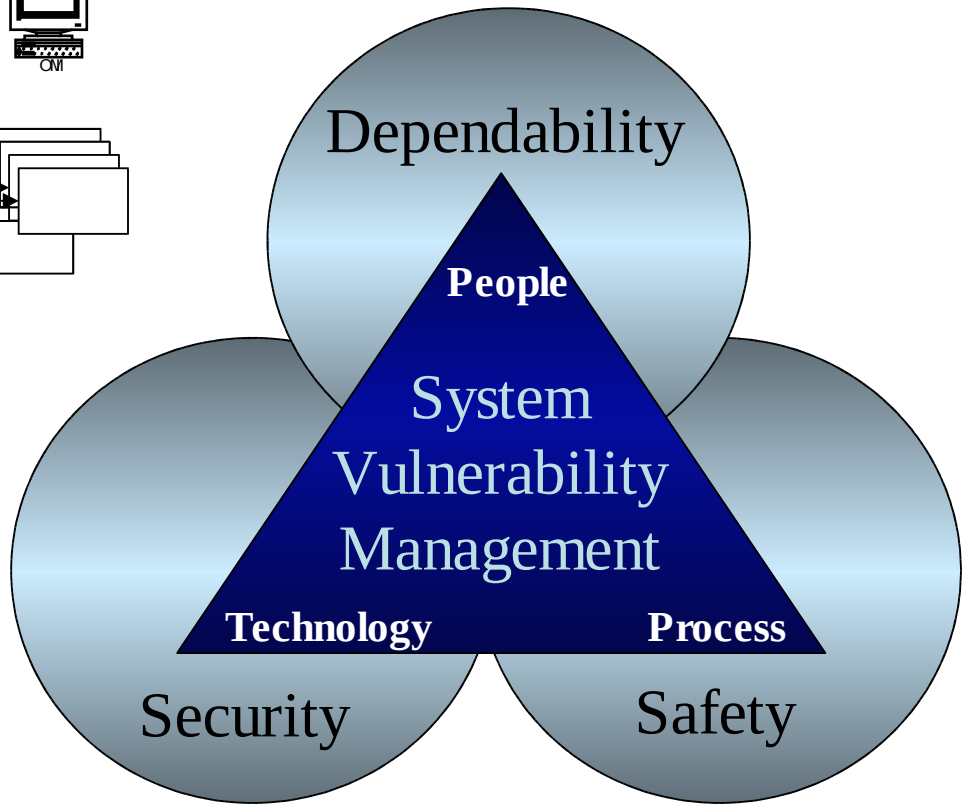
- Global visibility and control over specification and measurement of both required end to end QoS and QoS required from each critical site and network link
- Capability of using redundant links to enhance end to end performance, availability and survivability

Vulnerability Management Solutions Are Likely to Require Extensive Redundancy in Both Computing and Communications Services Links



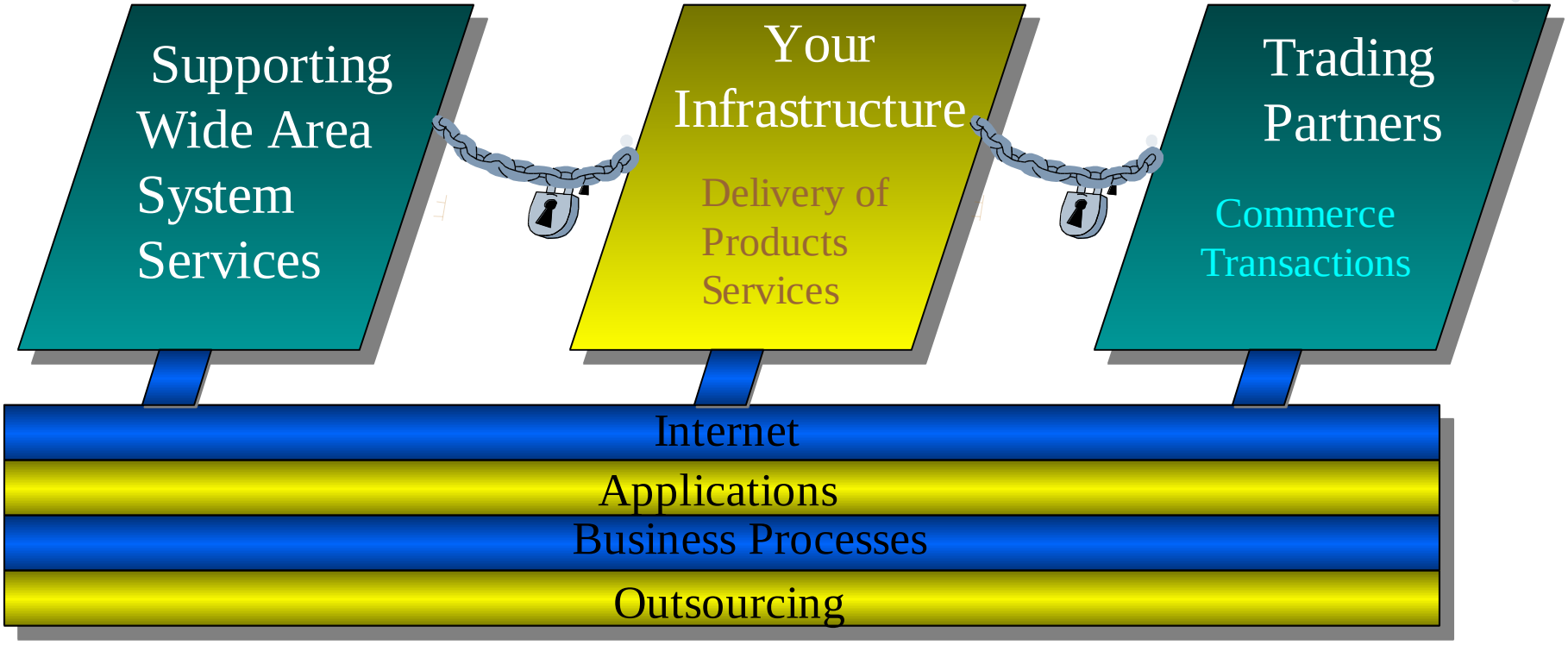
Need to Contend With Multiple Applications With Varying Security Requirements and Current System Benefit/Value, Competing for System Hardware, Software and Human Resources





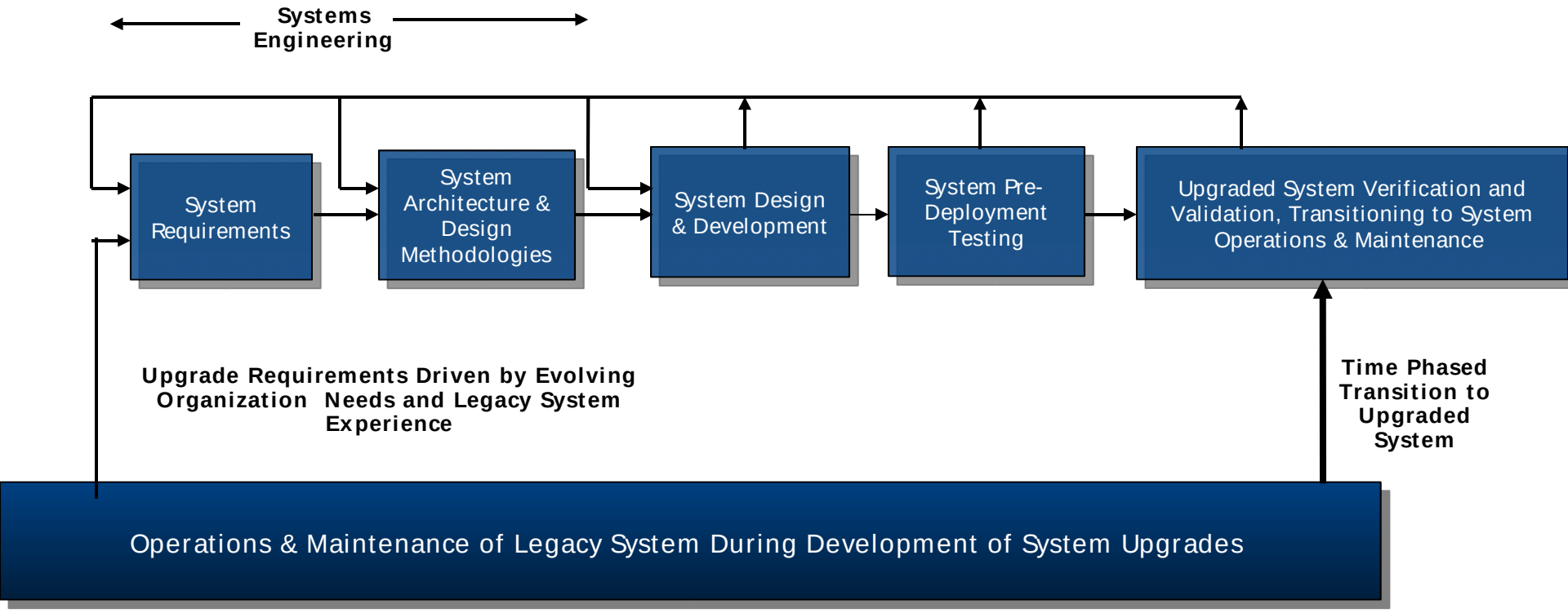
Interdependent elements of End-to-End System Vulnerability Management!

Typical Linked Mission Critical System Services



End-to-end services are only as strong as the weakest link in the chain!

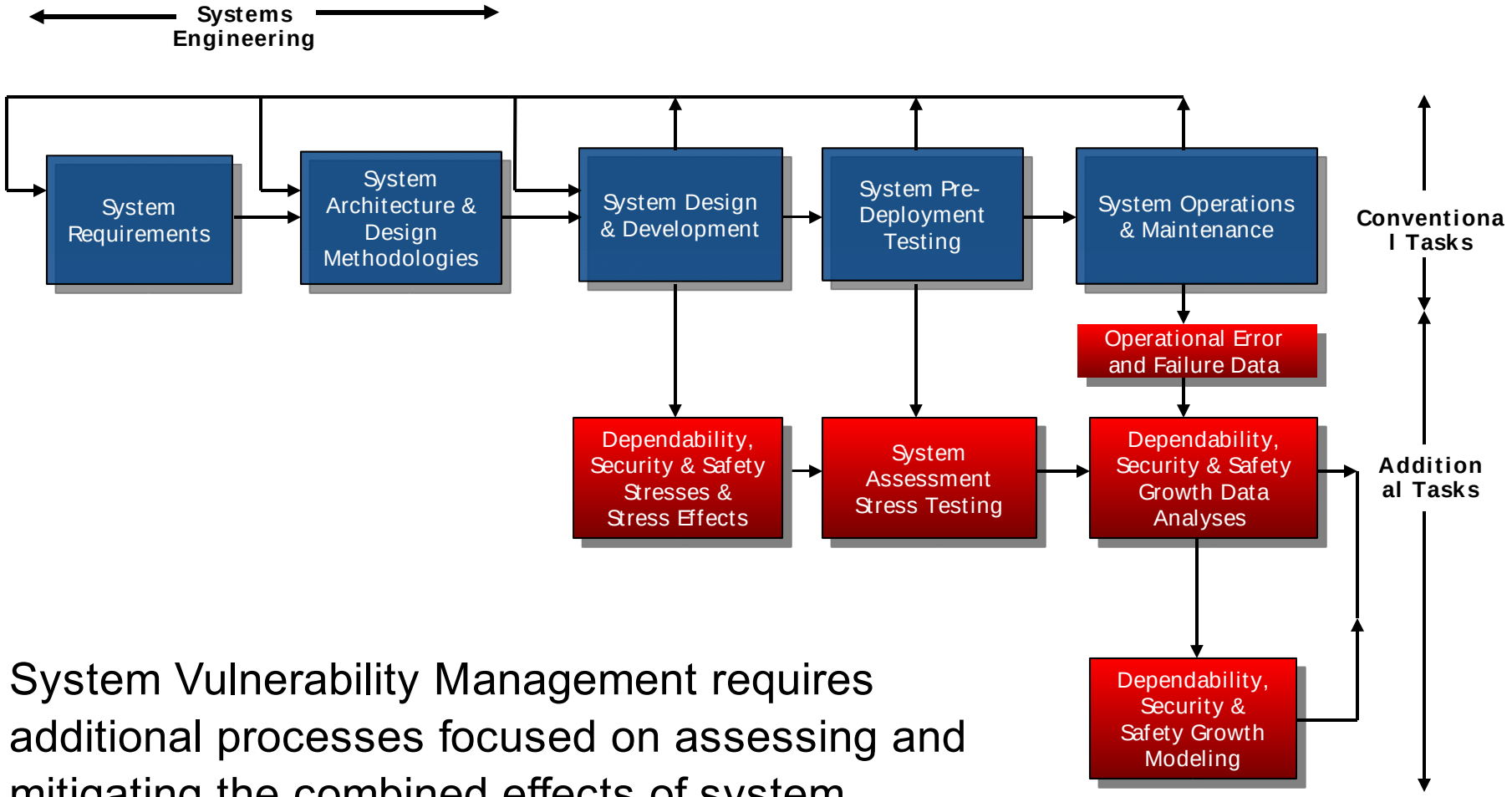
Conventional System Upgrade Processes Often Do Not Address Important Vulnerability Management Issues



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

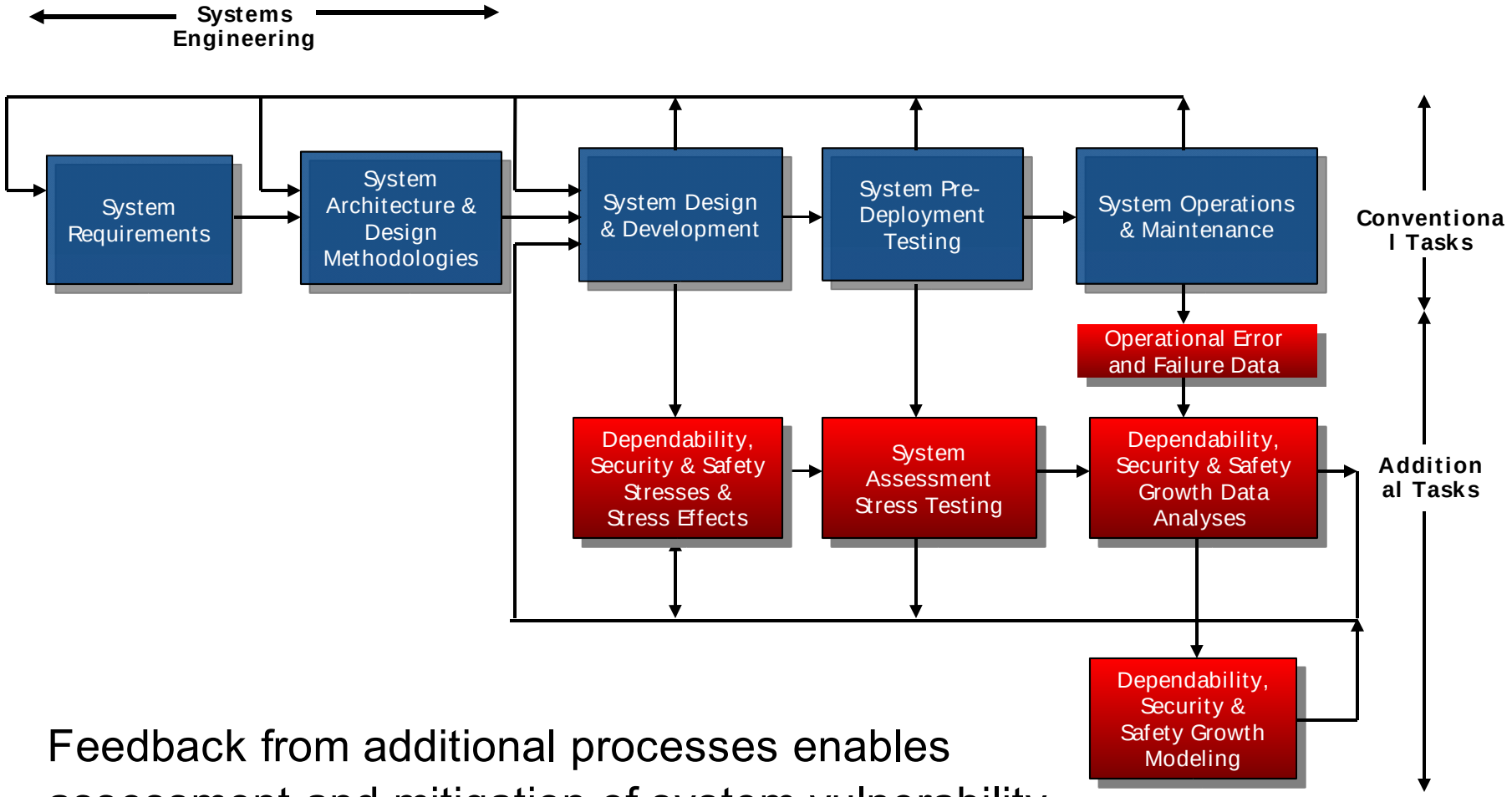
- **Web Enabling**
- **Collaboration**
- **Distributed Commerce Transactions**
- **Outsourcing**
- Usually, without adequately addressing critical vulnerability management issues!

Additional Processes Enable System Vulnerability Management



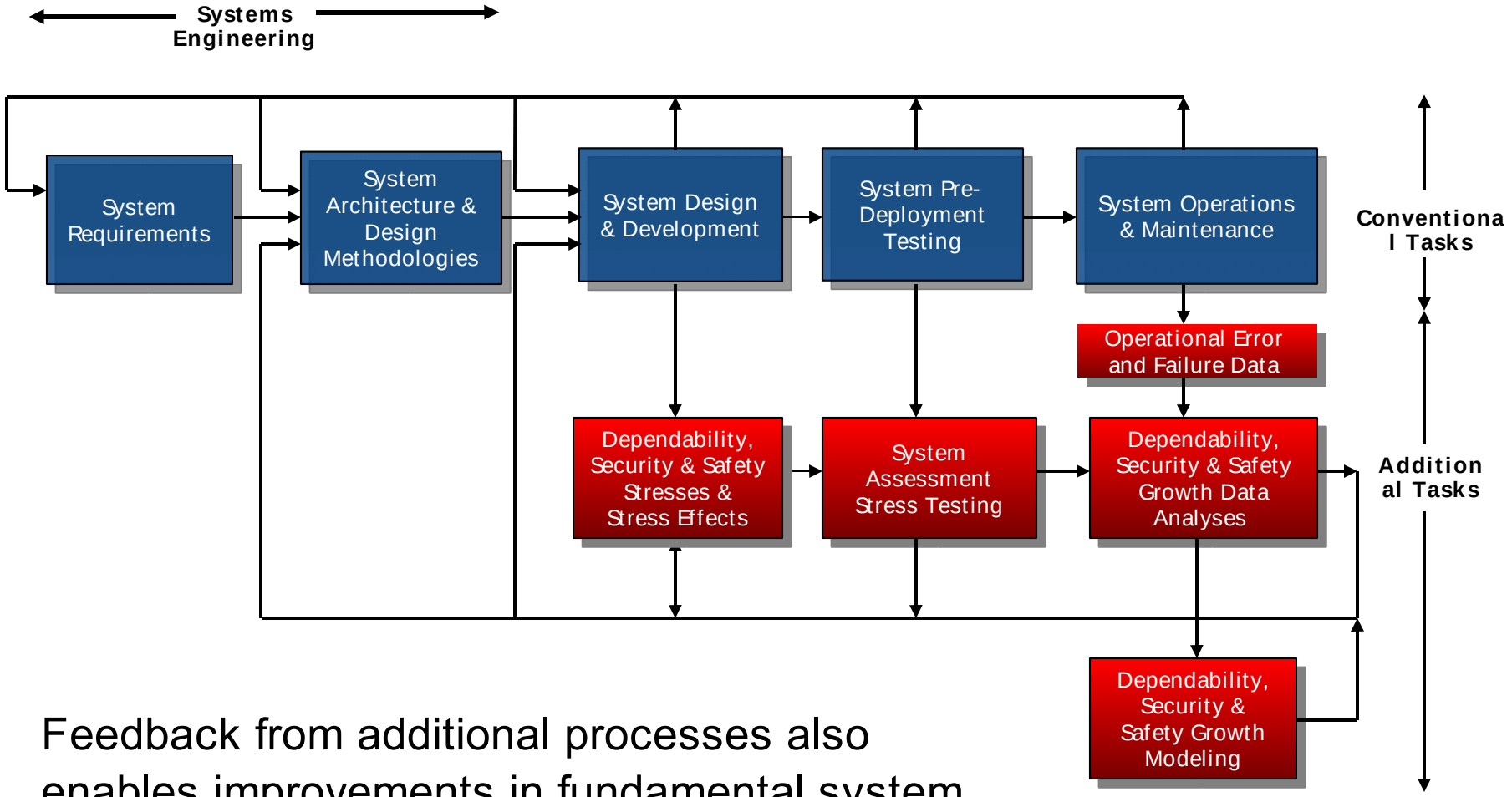
System Vulnerability Management requires additional processes focused on assessing and mitigating the combined effects of system dependability, security, and safety stresses

Feedback Enables Detection and Correction of System Vulnerability Management Deficiencies



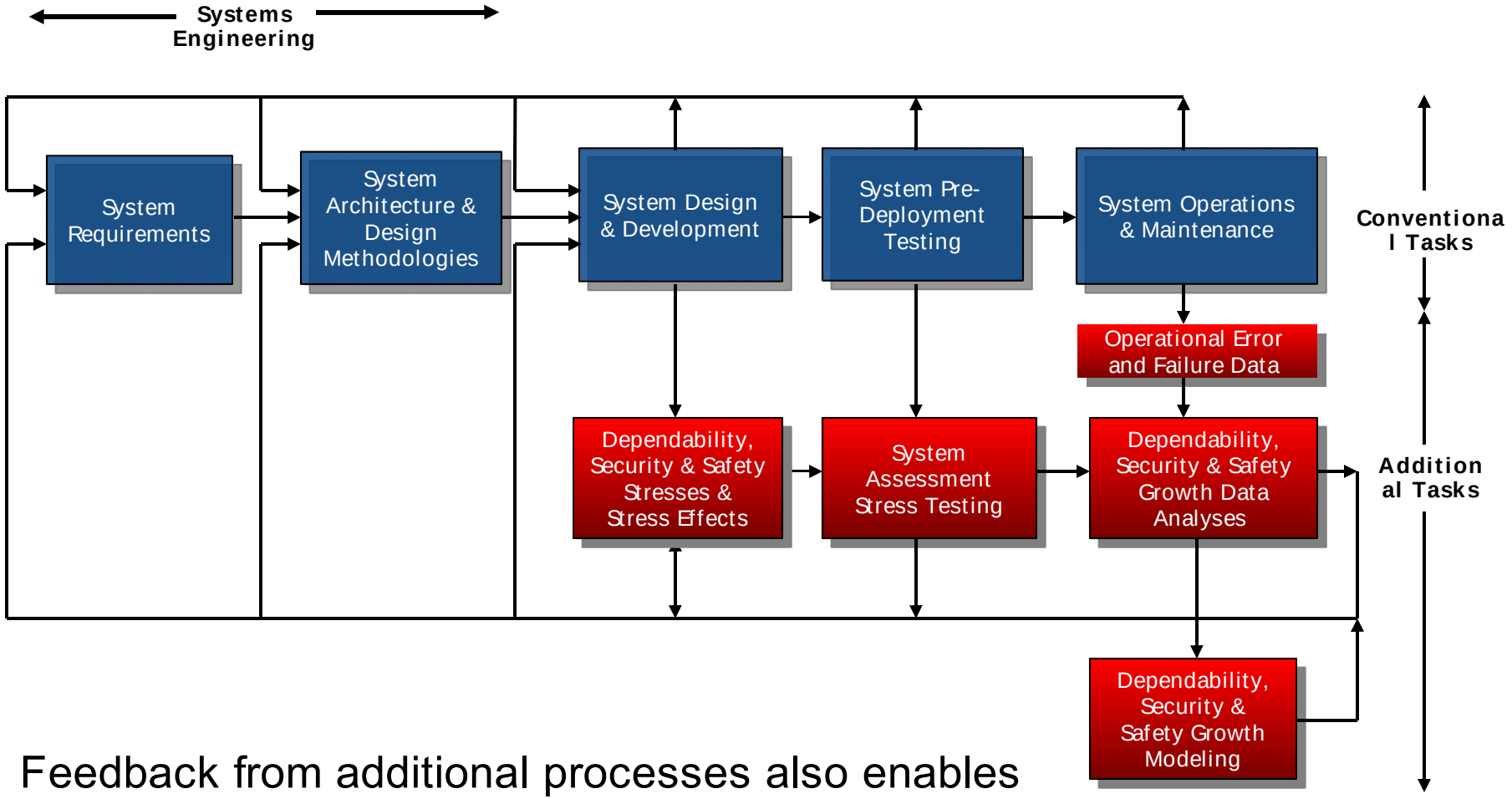
Feedback from additional processes enables assessment and mitigation of system vulnerability deficiencies

Feedback Also Enables Improvements in System Architecture and Design Methodologies



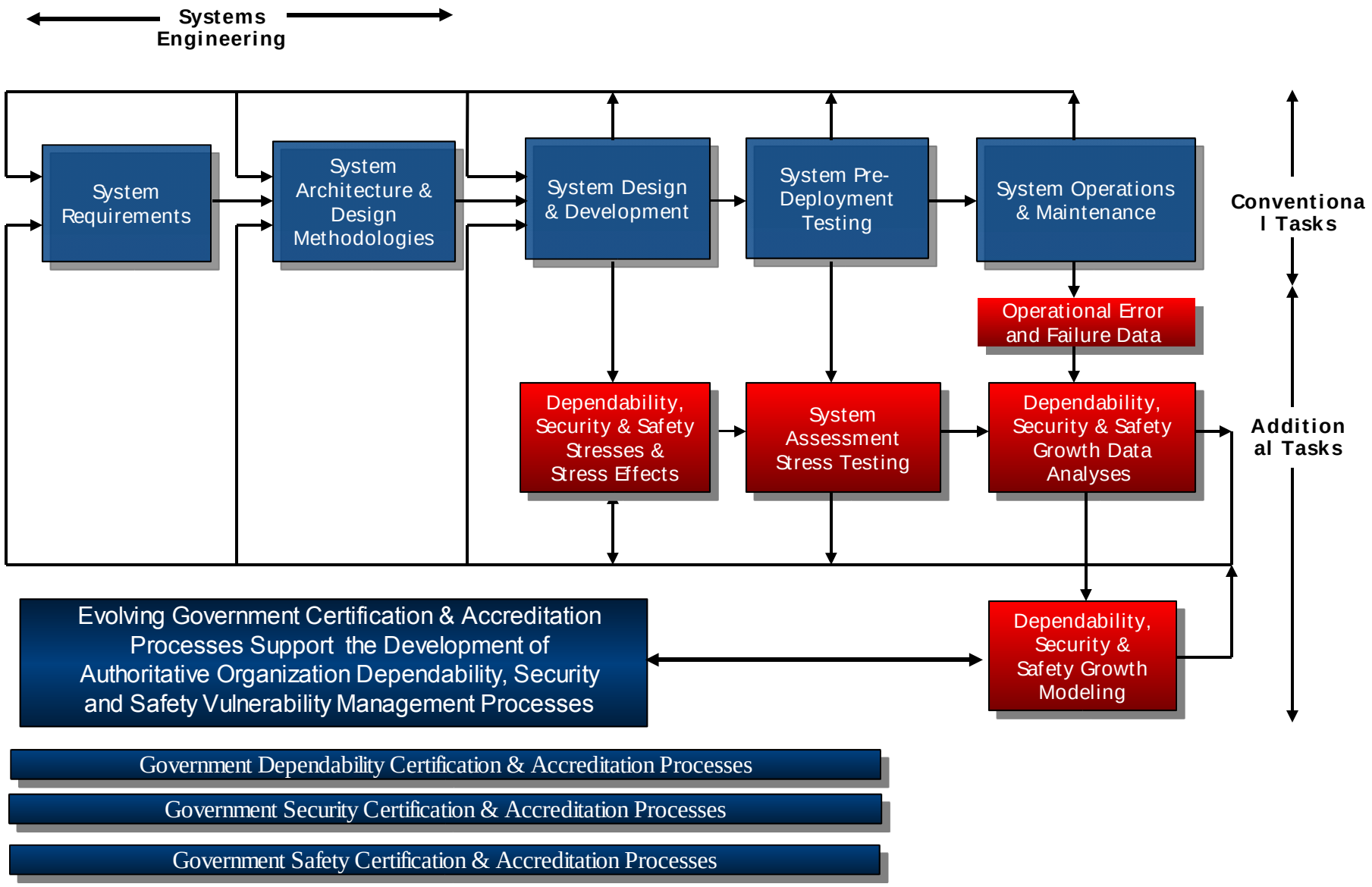
Feedback from additional processes also enables improvements in fundamental system architecture and design methodologies

Feedback Also Enables Detection and Correction of System Requirements Deficiencies



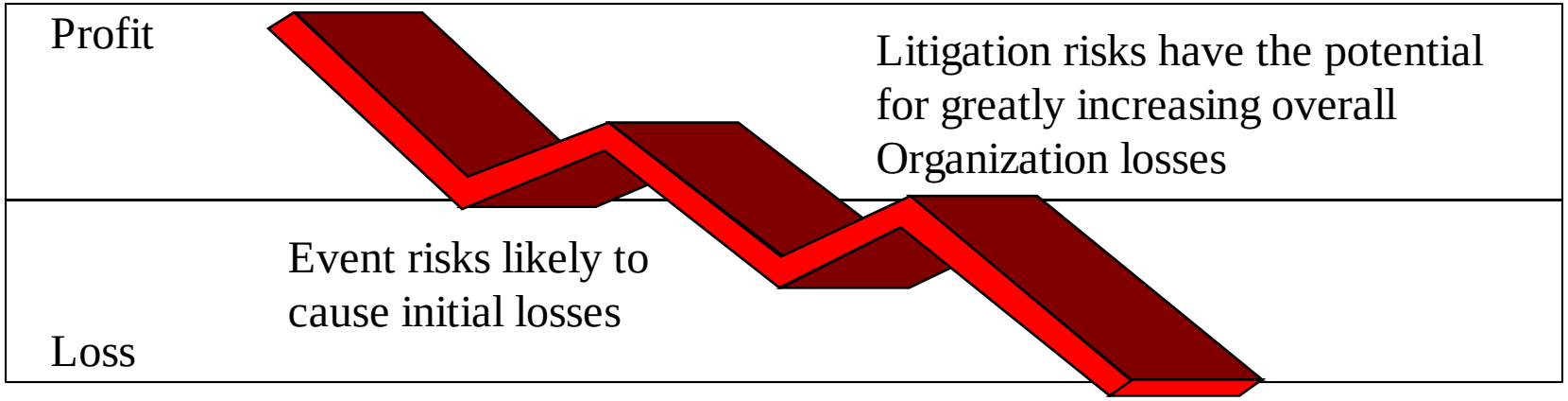
Feedback from additional processes also enables detection and correction of deficiencies in system vulnerability management requirements

Evolving Government Standards Support The Open Group's Vulnerability Management Framework



Must Face Two Levels of Organization Risks

- Initial risk of losses due to events that defeat dependability, security or safety defenses, plus
- Second risk of additional losses due to litigations claiming that Organization management failed to provide adequate system vulnerability defenses
- Lessons learned in the development of system safety cases can be extended to the development of vulnerability management cases that provide the foundation for protecting management against litigation liabilities



The best legal defense is proof that Management has implemented Vulnerability Management Best Practices!

Developing Open Group Vulnerability Management Cases

• Case approach evolved to modify costly and complex safety processes initially required by the nuclear industry

Safety Case: ***"A documented body of evidence that provides a demonstrable and valid argument that a system is adequately safe for a given application and environment over its lifetime."***
(Adelard - Bloomfield)

• Extended by The Open Group to dependability, security and safety to support overall vulnerability management of Organization mission critical system services

Elements of Safety Case Methodology

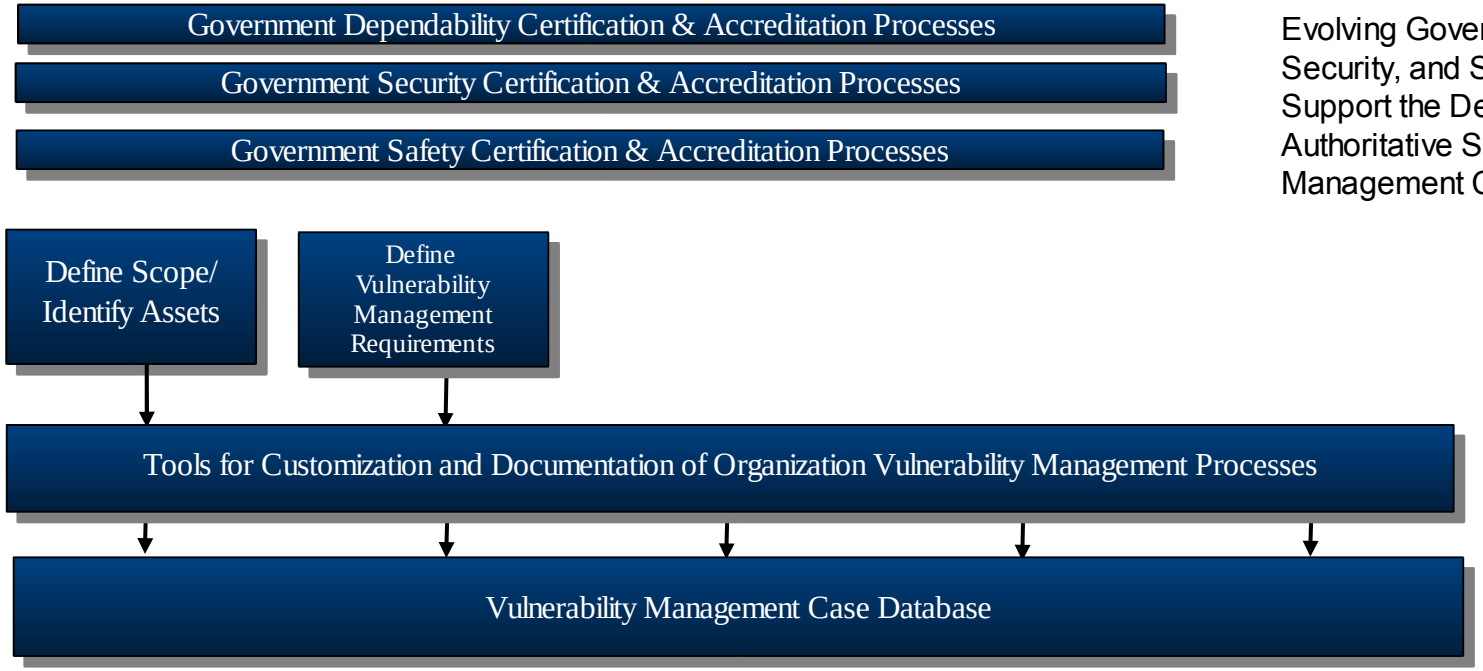
Provides mechanisms for participation by major system stakeholders (e.g. system/subsystem developers, end users, procuring and certification authorities).

Evolves from initial estimates of system hazards and hazard handling mechanisms through both pre-deployment and post deployment system validation. Includes Safety Case as an integral part of system life cycle processes.

Top level system safety case, with subsidiary safety cases for subsystems and traceability between subsystem and system levels.

Safety case links system design, development, operations and maintenance documentation into a unified whole, supporting system safety claims.

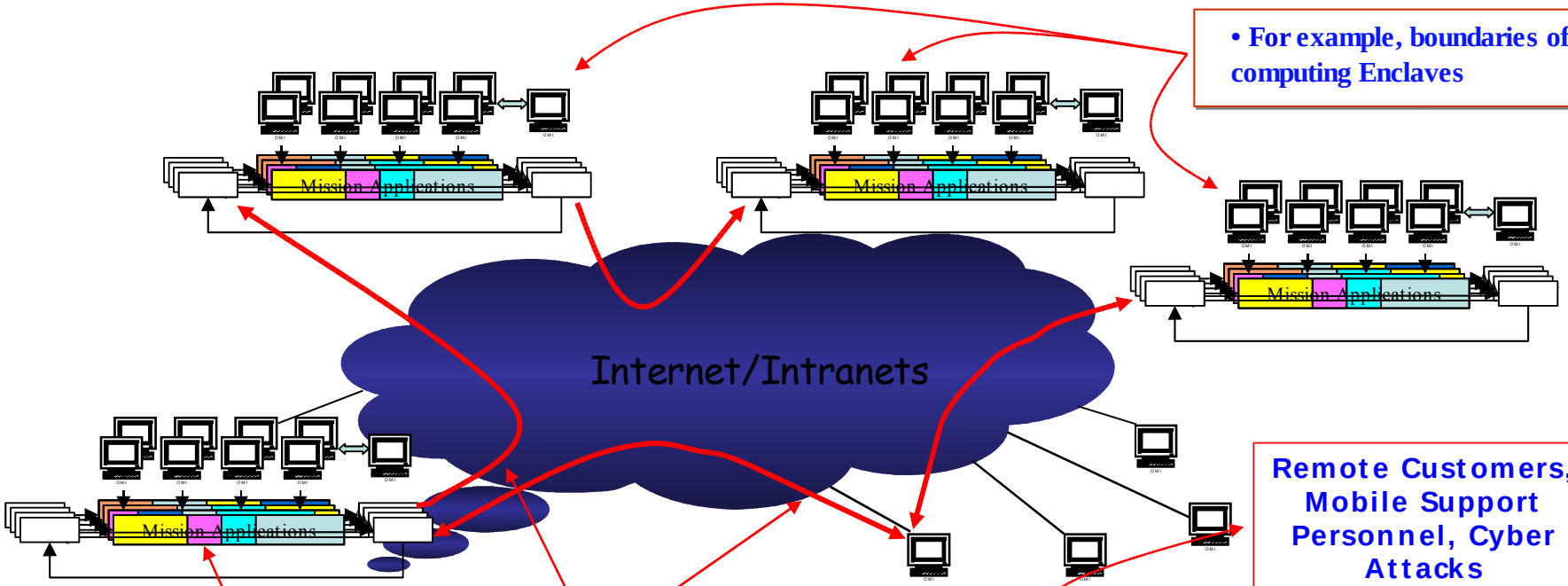
Vulnerability Management Cases Supported by System Assessment and Mitigation Processes



Evolving Government Dependability, Security, and Safety Processes Support the Development of Authoritative System Vulnerability Management Cases

Initial steps involve adapting government Certification and Accreditation guidelines to System constraints

To Certify and Accredit Each Link in the End-to-End Chain Supporting Mission Critical System Services, Each Link's Boundaries Have to be Defined



- For example, boundaries of computing Enclaves

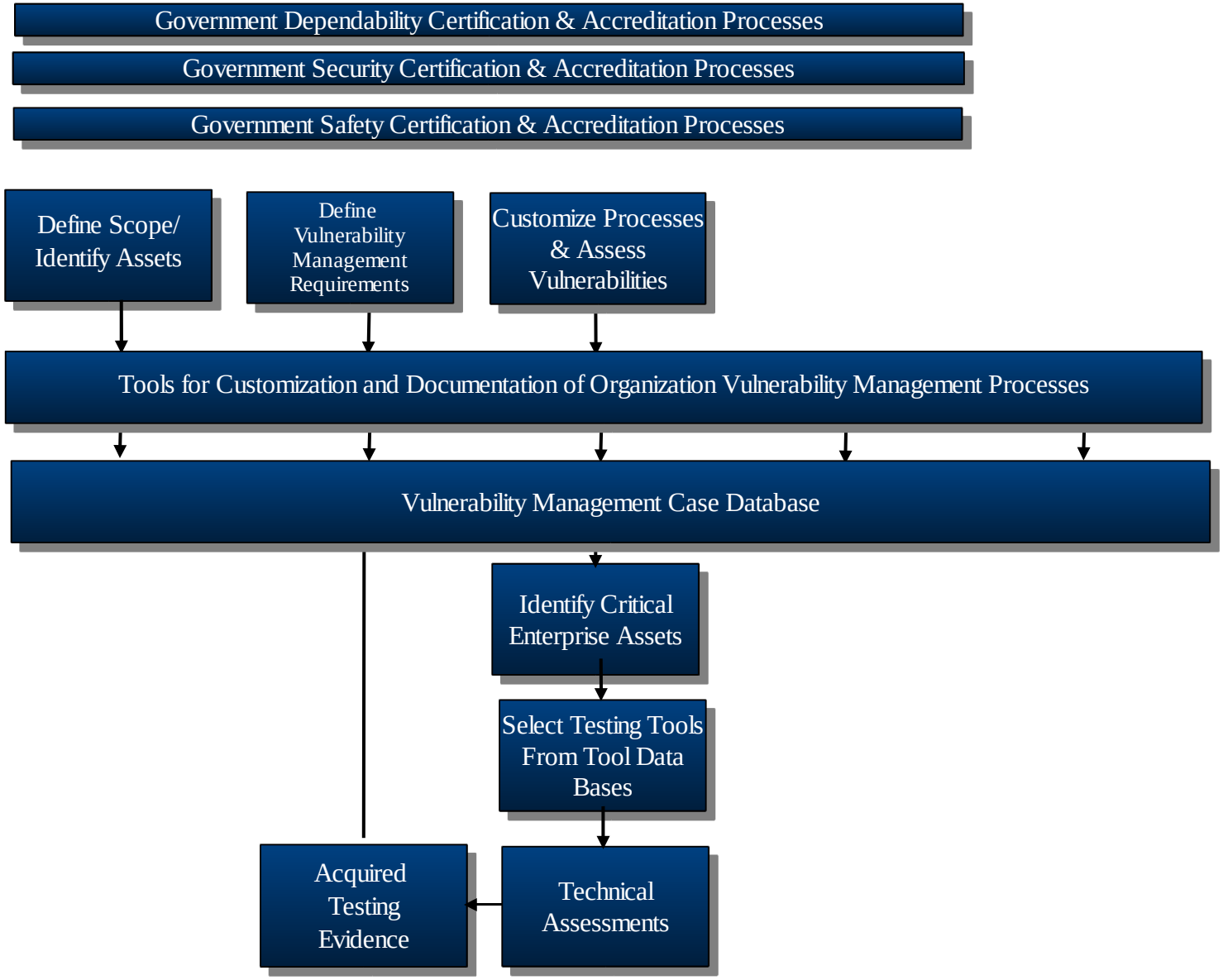
Remote Customers, Mobile Support Personnel, Cyber Attacks

- Personnel supporting a given Enclave are part of its assessment, but may also support other Enclaves and/or move physically between Enclaves
- Personnel within Enclaves may also be sources of Cyber attacks

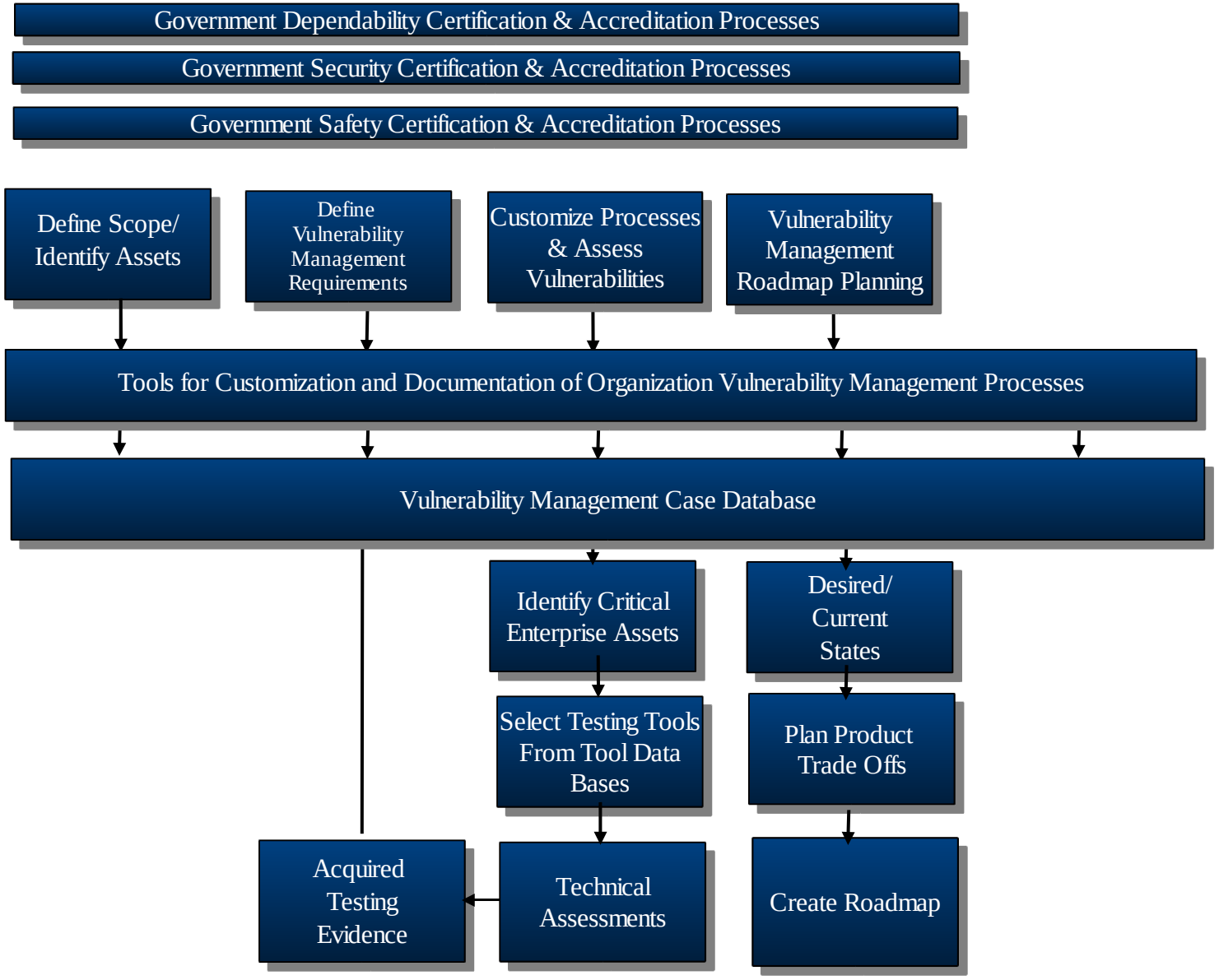
- Boundaries of Enclave to Enclave Communications

Vulnerability assessments and certifications need to also address security, safety and dependability issues associated with Mobile Support Personnel and their interactions with wireless networks

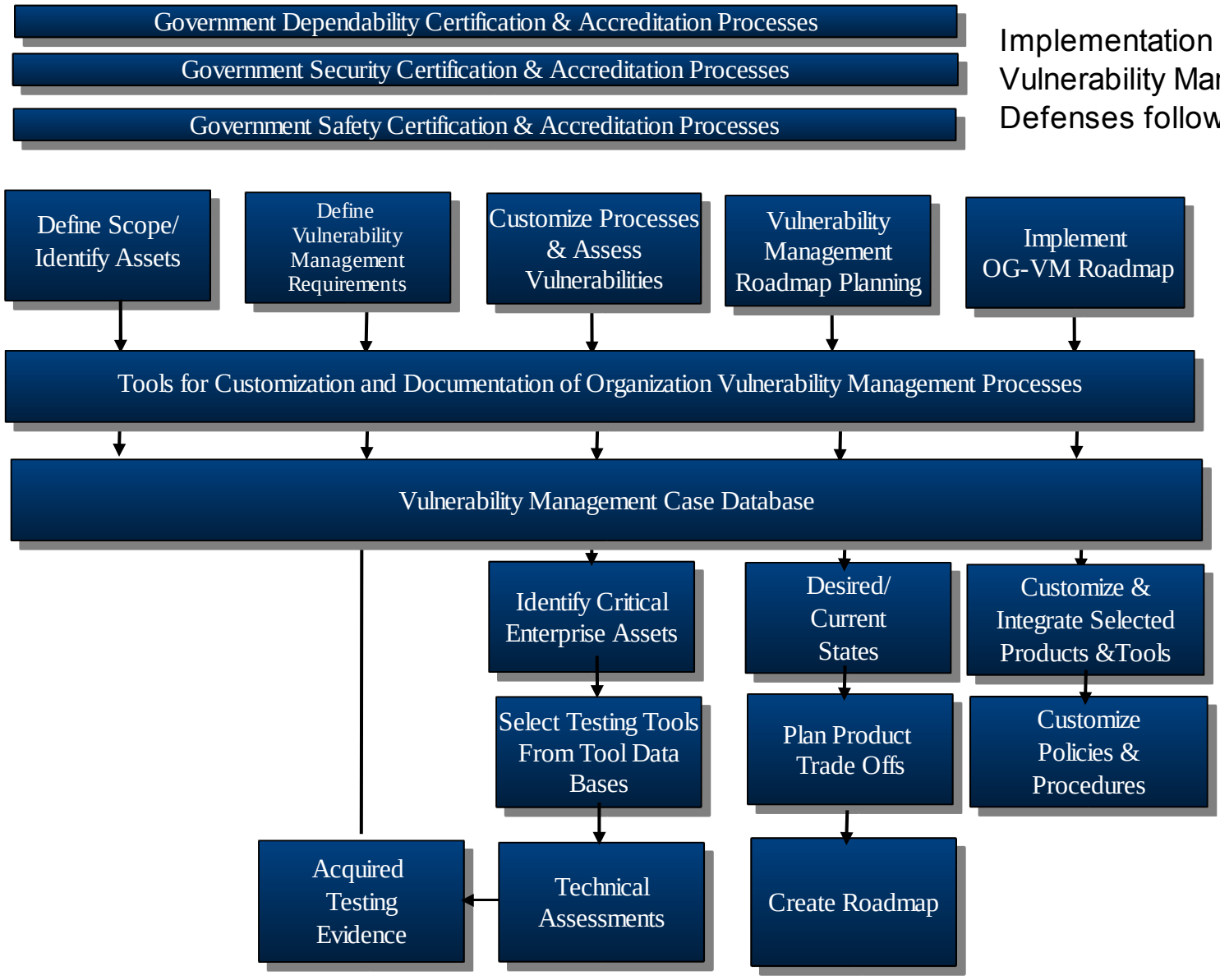
Assessment Process Then Identifies Current System Vulnerabilities



Identified Vulnerabilities Drive Development of Vulnerability Mitigation Roadmap Plans

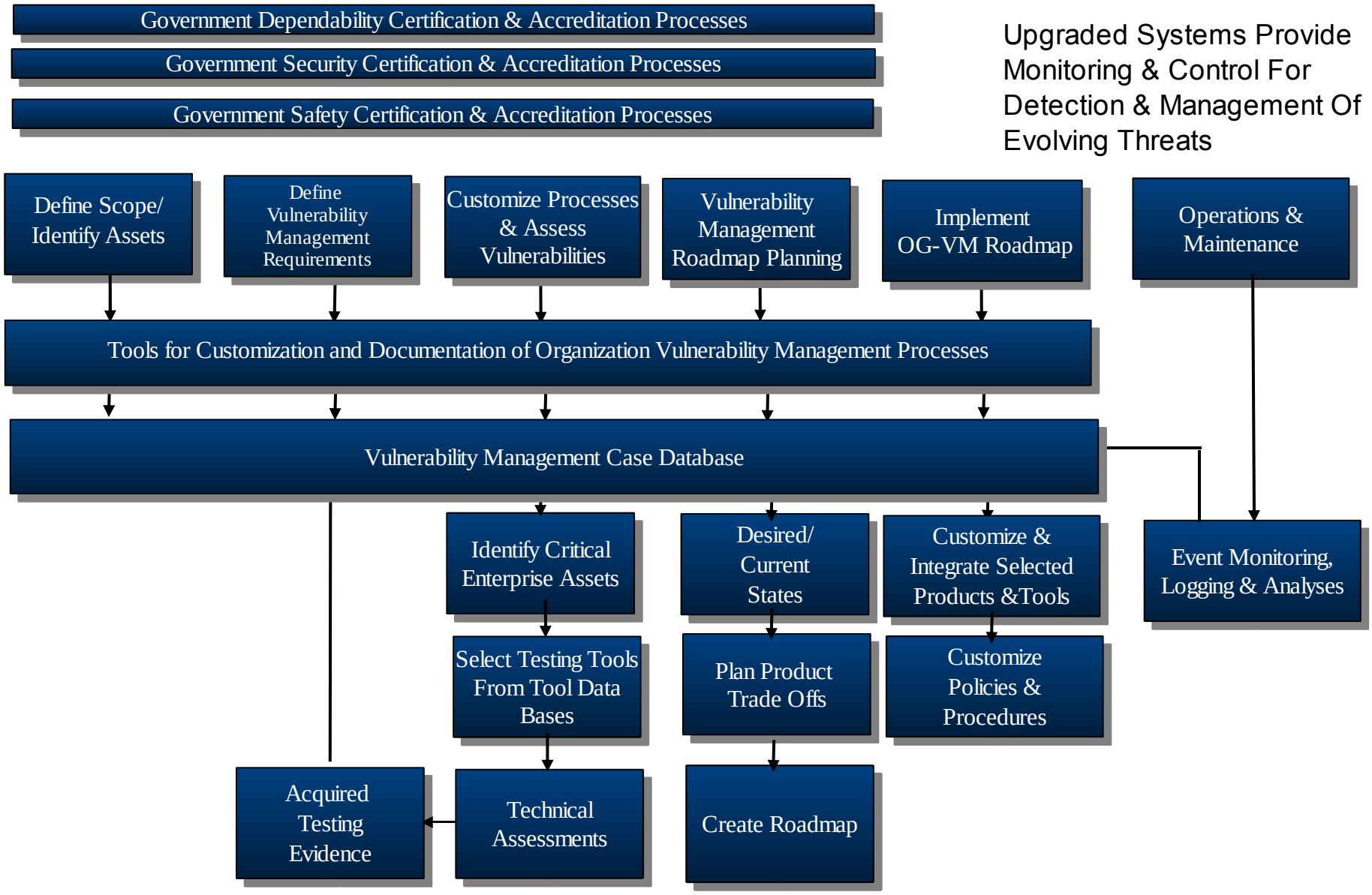


Roadmap Plans Drive Implementation of Vulnerability Management Capabilities



Implementation of System Vulnerability Management Defenses follows Roadmap Plan

Open, Standards Based, OG-VM Processes Include Provisions for Continuous Organization Vulnerability Management Monitoring and Control



An interesting point of departure for Open Group Vulnerability Management discussions could be provided by a review of NIST Special Publication 800-26, “Security Self-Assessment Guide for Information Technology Systems”.

While our understanding is that this guide will be updated to include changes being introduced in SP 800-53, SP 800-53A and SP 800-37, the System Questionnaire in Appendix A provides interesting insights into the classes of self assessment questions that are being considered.