Workshop Agenda

Wed 26th July 2:15 – 5:30 (break 3:45 – 4:00)

2:15 Overview of progress

2:30 – 3:15 De-Brief of DHS NSCD workshop 20th July 2006

3:15 – 3:45 Security Measurement Fundamentals

4:00 Break-Out 1: Review ICM Table and distil to a minimum generic set of measures, applicable to 'any' specialist domain

5:15 Report back

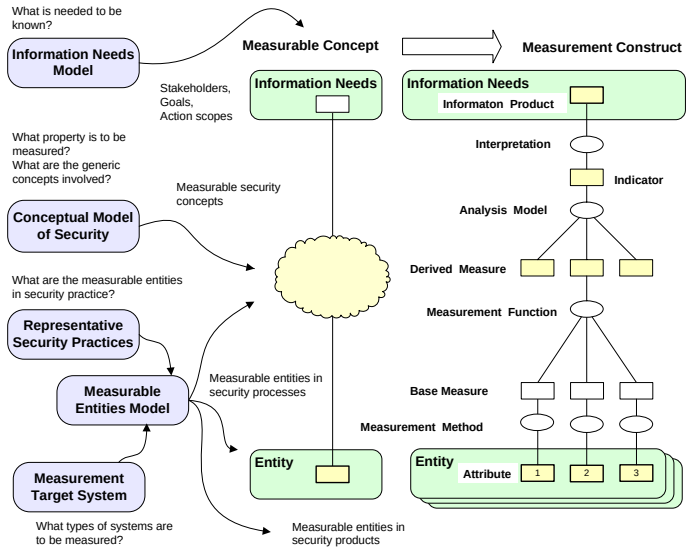
Objectives of Workshop

- **Discuss ICM Table distillation down to a 'generic essence' for security**
- **Discuss process/tasks to apply generic measures to a particular domain ('instantiate' the generic table) – take sw devlpt process as example domain (or other if preferred)**
- **Planning for development with specialists:**
  - **Map of relevant domains**
  - **How to engage efficiently and effectively**
  - **Relationships between domains**

Measurement Fundamentals

- PSM and ISO/IEC 15939:2002
  - Measurement construct
  - Measurement process
  - ICM table
  - Measurement specifications
- Measurement theory

Measurement Construct



Issues Arising in Security

- multiple specialties – varying 'semantics' – many types of measurements
- security is an emergent property – involves both technical and behavioral systems
- layered, dynamic, complex systems – decision-making agents at different levels
- concern about assurance and validation
  - How do we validate a measurement construct?
- threat environment changes; need 'flexible' constructs that respond to changing information needs
- security is a complex issue - will be contested at organization/ society level

Views of Security

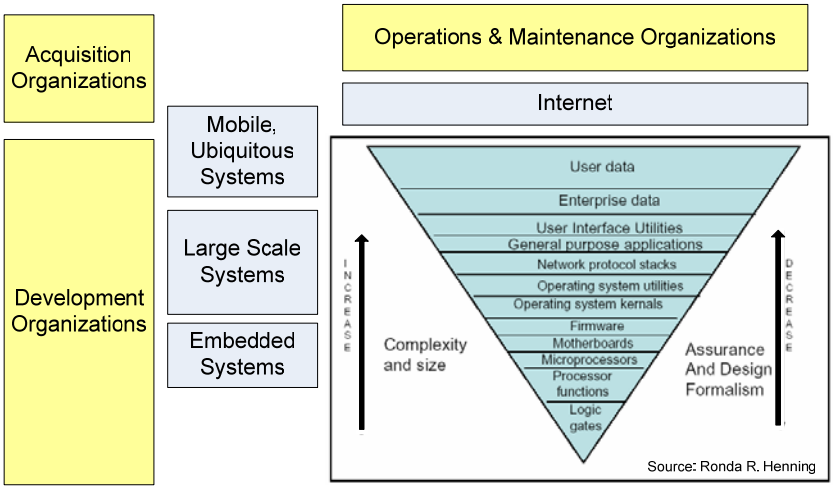
Scientific, 'impersonal' view:

- what are the undesired events?
- what are the threats, vulnerabilities, damages?
- how dependable is the system or service – to what extent can it be trusted?
- how can measurement principles, methods, tools be used to support the achievement of acceptable levels of these risks and to provide assurance?

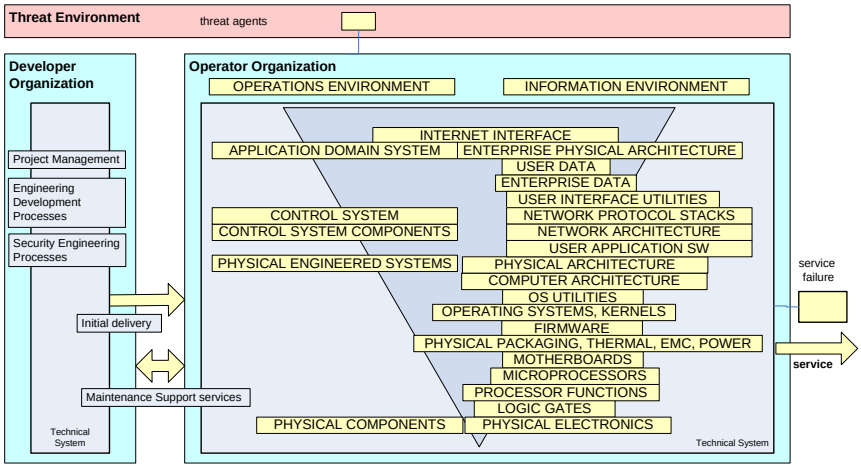
Behavioral, 'policy' view:

- how is risk distributed – who is exposed? who pays for damage?
- who decides on mitigation actions? who pays for mitigation?
- how can measurement principles, methods, tools be used to support the agreed policy, achievement of agreed policy outcomes?

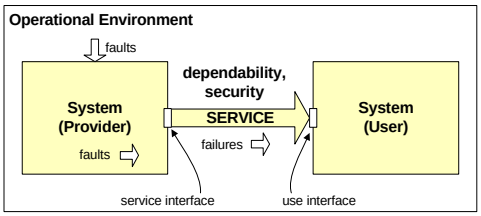
Organizational-Technical Context[1]



Organizational-Technical Context[2]



What is Security?



Definition	Dependability (of a system delivering a service)
1	The ability to deliver a service that can justifiably be trusted (implies that accepted dependence has to be justifiable)
2	The ability to avoid service failures that are more frequent and more severe than is acceptable (implies criteria for deciding whether a service is sufficiently dependable)

[Avizienis, A., et al., Basic concepts and taxonomy of dependable and secure computing, *IEEE Trans. Dependable and Secure Computing, 2004 1(1): p. 11-33]*

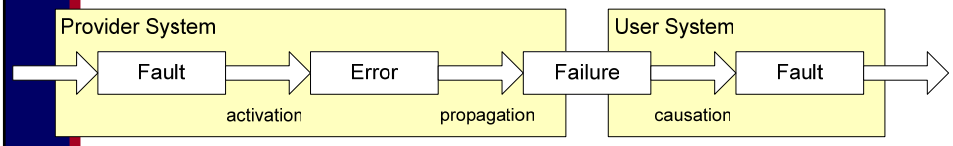
Aspects of Security

Security Property of a System	Associated Types of Service Failure
Confidentiality	unauthorized disclosure of information
Integrity	improper/unauthorized system alterations
Availability	service unavailable in a correct form, when required
Authenticity	a user not identified correctly – not who they claim to be
Non-repudiability	a neutral third party is unable to decide if a particular transaction or event did or did not occur

[Avizienis, A., et al., Basic concepts and taxonomy of dependable and secure computing, *IEEE Trans. Dependable and Secure Computing, 2004 1(1): p. 11-33]*

Faults, Errors and Failures

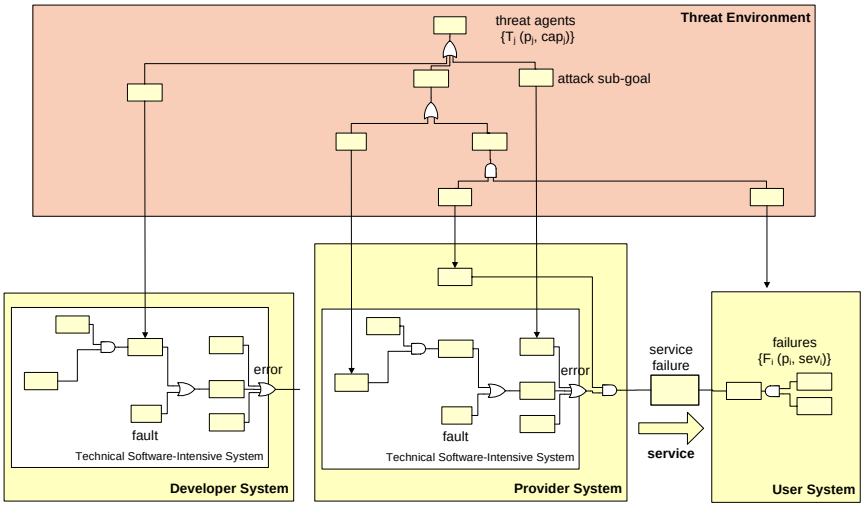
- ***A service failure implies that the provider system's external states deviate from the external states associated with the provision of a correct service. This deviation is called an* error**
- ***The adjudged or hypothesized cause of an error is called a* fault*. Faults may be located within the provider system and/or in its environment***



- ***'Reducing' failures, means 'reducing' faults and effect propagation paths***

[Avizienis, A., et al., Basic concepts and taxonomy of dependable and secure computing, *IEEE Trans. Dependable and Secure Computing, 2004 1(1): p. 11-33]*

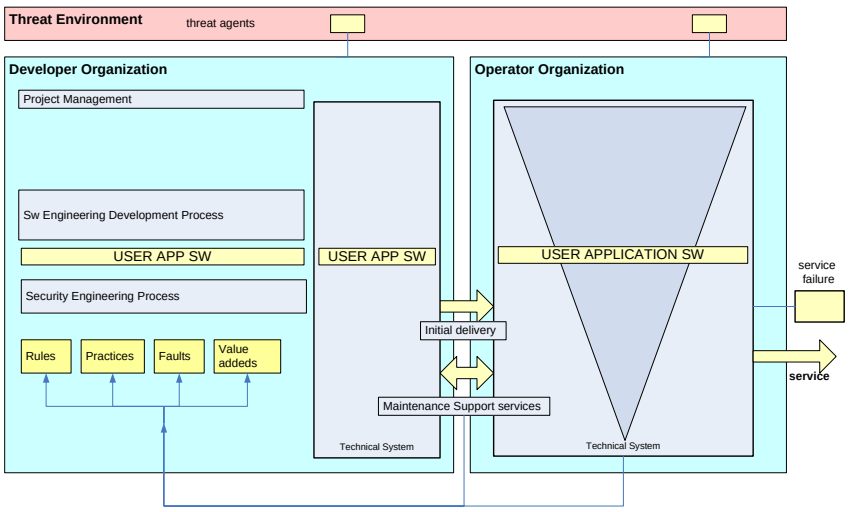
Threats, Faults and Failures In Organizational Context



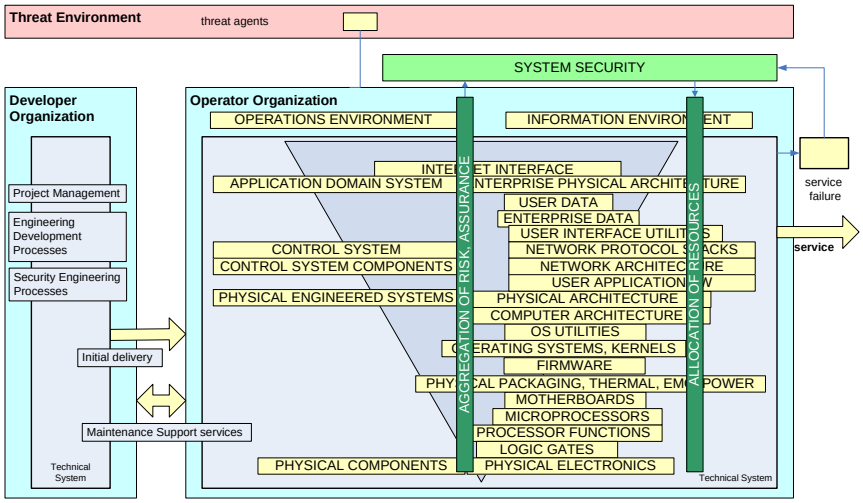
Achieving Security

- *Security properties are emergent properties of systems – security is achieved by a combination of many things*
  - *technical sw, hw, systems, networks, organizational*
- *Improving security means reducing the number of service failures we are concerned about, and/or reducing the severity of failures; and providing justifications for claims that we have achieved improvements (assurance)*
- *What are the main ways security is improved?*

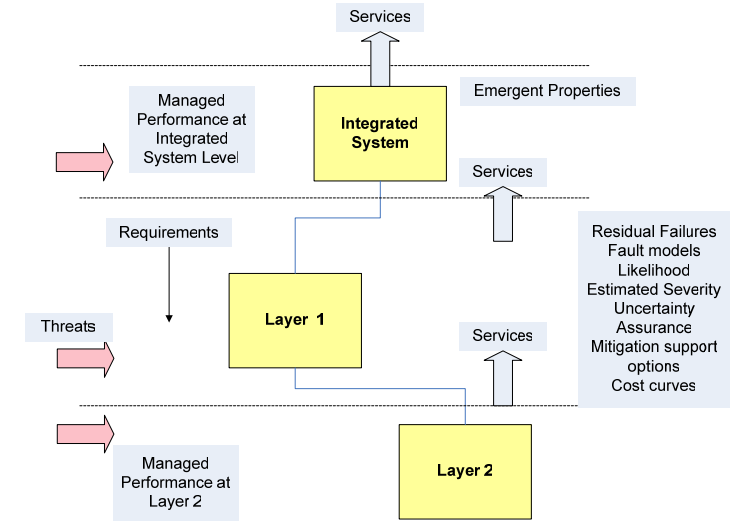
Horizontal Slice: improving performance of a specialist practice



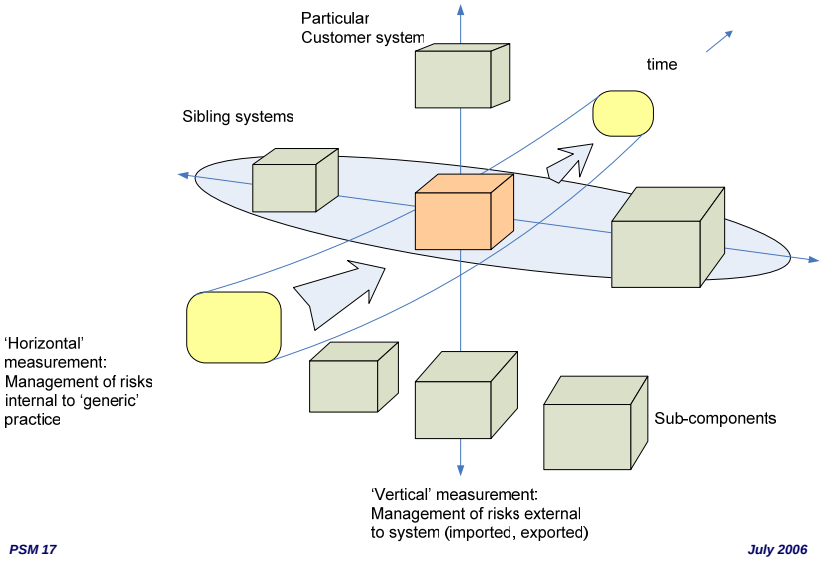
Vertical Slice: improving performance of a particular system



Aggregation of risk, allocation of trust



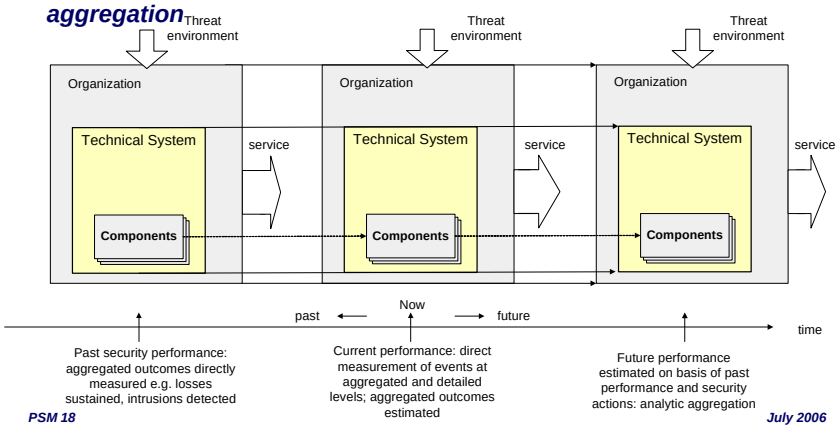
Value/Cost Trade-offs



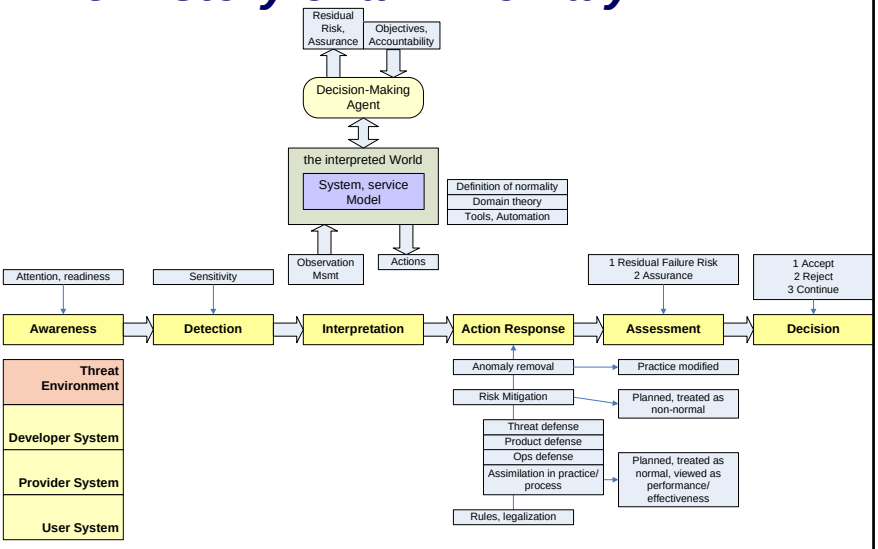
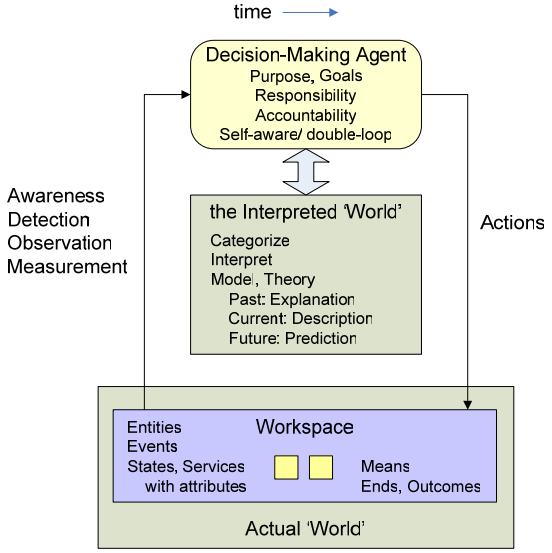
Prospective and Retrospective Views

Retrospective: more time to analyze, certainty that a particular scenario unfolded (may still be uncertainty about causes & effects), aggregated performance is measurable

Prospective: less time to analyze, uncertainty about scenario, aggregation



Life History of an Anomaly



Decision Maker Model