Practical Software and Systems Measurement

A foundation for objective project management

Measurement of Safety & Security Processes

PSM TWG Meeting
28 July 2004 / 13:45 – 17:30

Paul Caseley, John Murdoch

Objectives of the Workshop

- ***To develop an agreed framework/ approach to security measurement for PSM***
- ***To pool/ generate ideas for security measurement***
- ***To develop initial proposals for security measurement additions to PSM***

Workshop Format

Agenda (½ day)

Introduction – status of work

1. ***Update inputs, related programs etc.***
2. ***Review proposed framework/ approach to security***
3. ***Brainstorm security measurements***
4. ***Develop strawman PSM security additions***
5. ***Plan for next step, update to v3.0 of White Paper***

Conclusion – workshop outbrief

Workshop Background

- ***Work on safety measurement started at the TWG meeting, March 2003, White Paper (v2.0) February 2004***
- ***iCMM/CMMI materials for an Application Area in Safety & Security Assurance (published Jan 2004)***
- ***Much activity in information security, network security, homeland security; DoD, federal systems, commercial***
- ***Standards***

Intended Output

1. *Updated inputs, related programs etc*
2. *Agreed framework/ approach to security measurement*
3. *Brainstorm output: measurement ideas and concepts*
4. *Agreed initial proposals for PSM security additions*
5. *Plan for next step, update to v3.0 of White Paper*

1. Inputs and Related Programs

Measurement PSM/ ISO 15939

- current 'official' version
- current developments in the TWGs – safety, systems

Information Security

- ISO/IEC 17799:2000 Code of Practice for Information Security Management
- BS 7799-2:2002 Information Security Management Systems
- OCTAVE^{SM} (SEI) Operationally Critical Threat, Asset and Vulnerability Evaluation

Information Technology Security Techniques, Evaluation Criteria

- ISO/IEC 15408 Common Criteria (NIST)
- Evaluation against criteria of IT systems and components
- Evaluation Assurance Levels
- DoD aspects (e.g. PKI, KMI systems)

Practical Software and Systems Measurement

DoD Directives e.g. DoDD 8500.1

- Information Assurance; policy, responsibilities, scope
- Equivalent Federal Laws etc.

Costing Secure Systems (USC-CSE)

- Extensions to COCOMO, CoSysMO

Maturity Models

- SSE-CMM (ISSEA, NIST) System Security Engineering
  - ISO/IEC 218287
- iCMM/CMMI Safety & Security AA (FAA/DoD, Jarzombek, Ibrahim)

Certification and Accreditation

- NIST SP 800 – 26, 30, 37, 53, 55, 60
- NIST SP 800-55 Security Metrics Guide for Information Technology Systems – example metrics
- NIACAP National Information Assurance Certification & Accreditation Process

NIST CSP (Computer Security Division)

- FASP Federal Agency Security Practices
- FITSAF Federal Information Technology Security Assessment Framework, levels, criteria
- Checklists for settings and options selections for hw & sw

DISA (Defense Information Security Agency)

- Checklists (e.g. Application Security Checklist: Identification and Authentication – APP 0120 thru APP 0160)

SPC Security Engineering

- Security Threat Assessment, Modeling
  - **Threat Trees (SPC)**
- Information Security Policies
  - Content, Management, Implementation, Benchmarking

Practical Software and Systems Measurement

Security and Systems Engineering

Safety & Security Integration

Donald Firesmith SEI TN, survivability, defensibility

System Interoperability

Layered reference models (LISI)

Reference architecture models (DoD)

Commercial Organizations

SecMet (Security Metrics Consortium)

Academic/ Professional Specialist Research & Practices

Specialist engineering areas e.g. crypto, PK systems, computer security specialties, real time embedded systems, sw eng

e.g. IEEE HASE Conferences

2. Initial Questions

- ***Which important inputs are being overlooked?***
- ***What is the role of PSM in security engineering and management?***
- ***What is the added knowledge/ capability that the PSM Project brings to an already very active field?***
- ***How should we apply PSM principles to the security field?***
- ***How should we go about developing PSM measurement guidance materials?***
- ***Which important 'initial questions' are being overlooked?***

PSM Contributions

- ***Integrate security measures with other measures (safety, TPMs, project measures)***
- ***Integrate measures across different aspects of security (IS, IT, network, physical)***
- ***Serve the security measurement needs of emerging kinds of systems?***

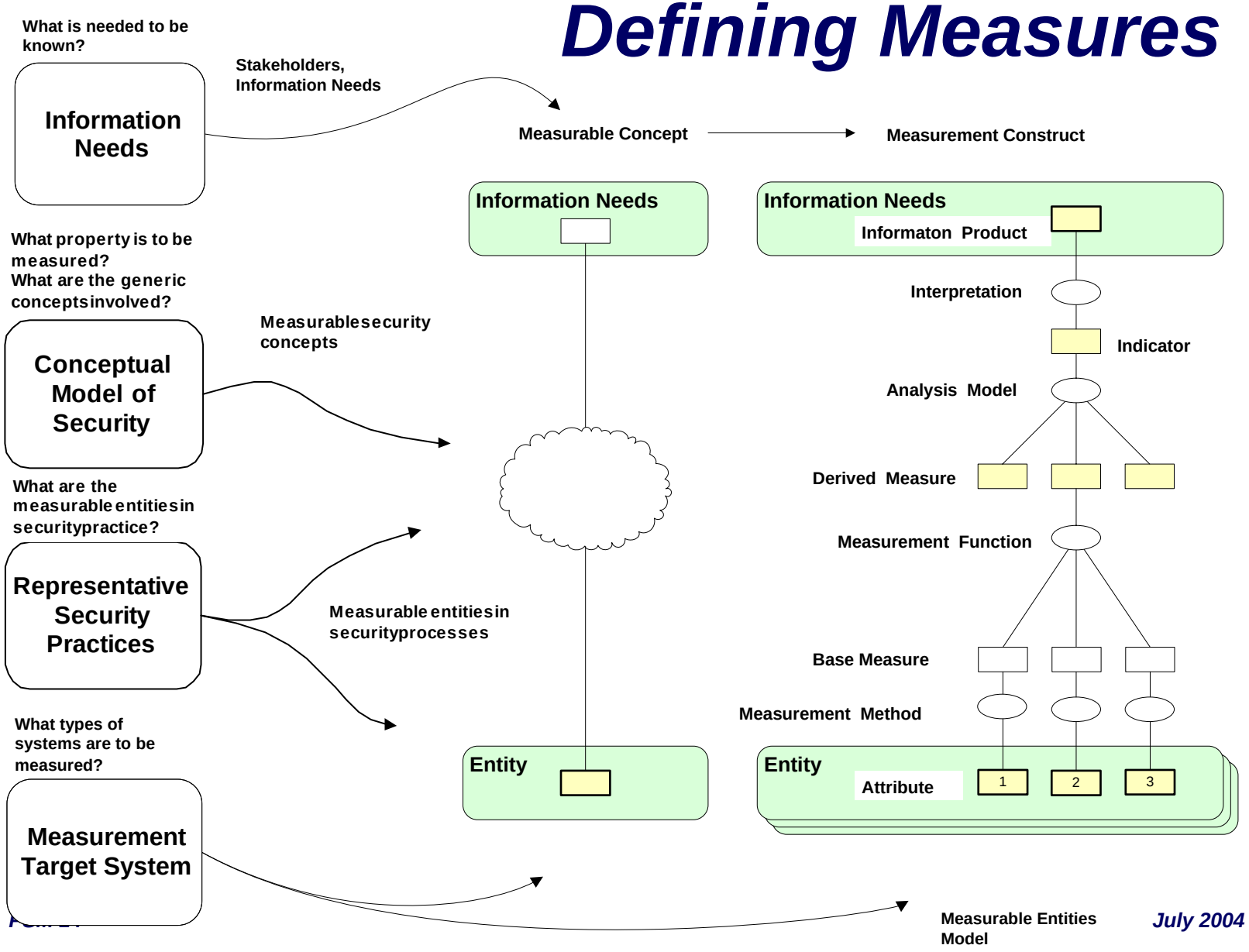
Features of Security Measurement

- ***Diversity of target systems, implies diversity of base measures, increasingly networked systems***
- ***Development of audit and certification in IS and IT***
- ***Existing commercial/ industrial measurement practices in IS, IT***
- ***Need some flexibility in measurement to respond to evolving risks***

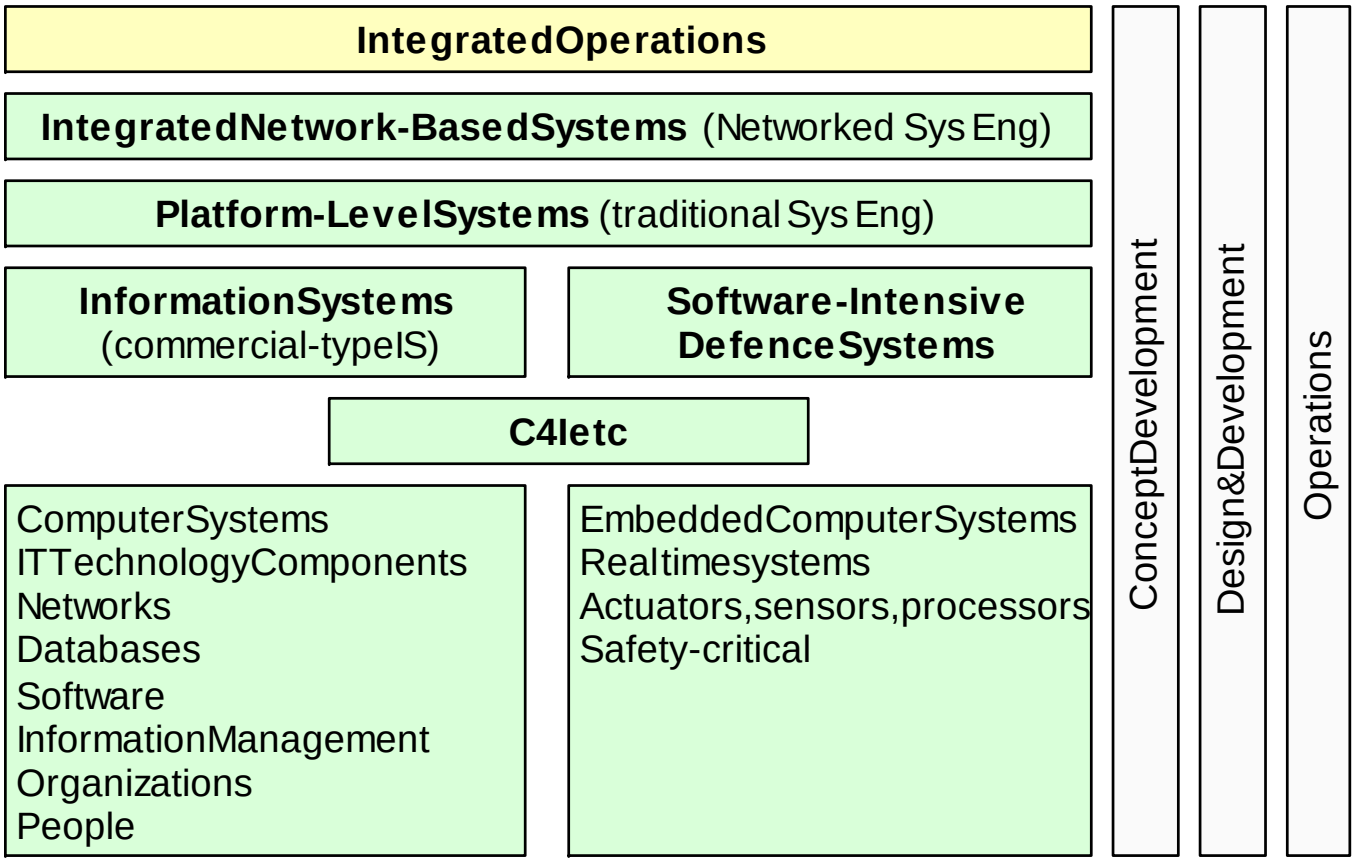
Security Msmt Strategy for PSM

- ***Develop general security measurement guidance i.e. an 'entry point' for security measurement***
- ***Integrate measurement practice across different areas of security***
- ***Integrate with other performances (safety, survivability etc); applicable to new kinds of systems***
- ***PSM Proposed Approach: single security measurement framework plus categorization of measure types; link to existing security practices where they exist***

Defining Measures



Measurement Target Systems



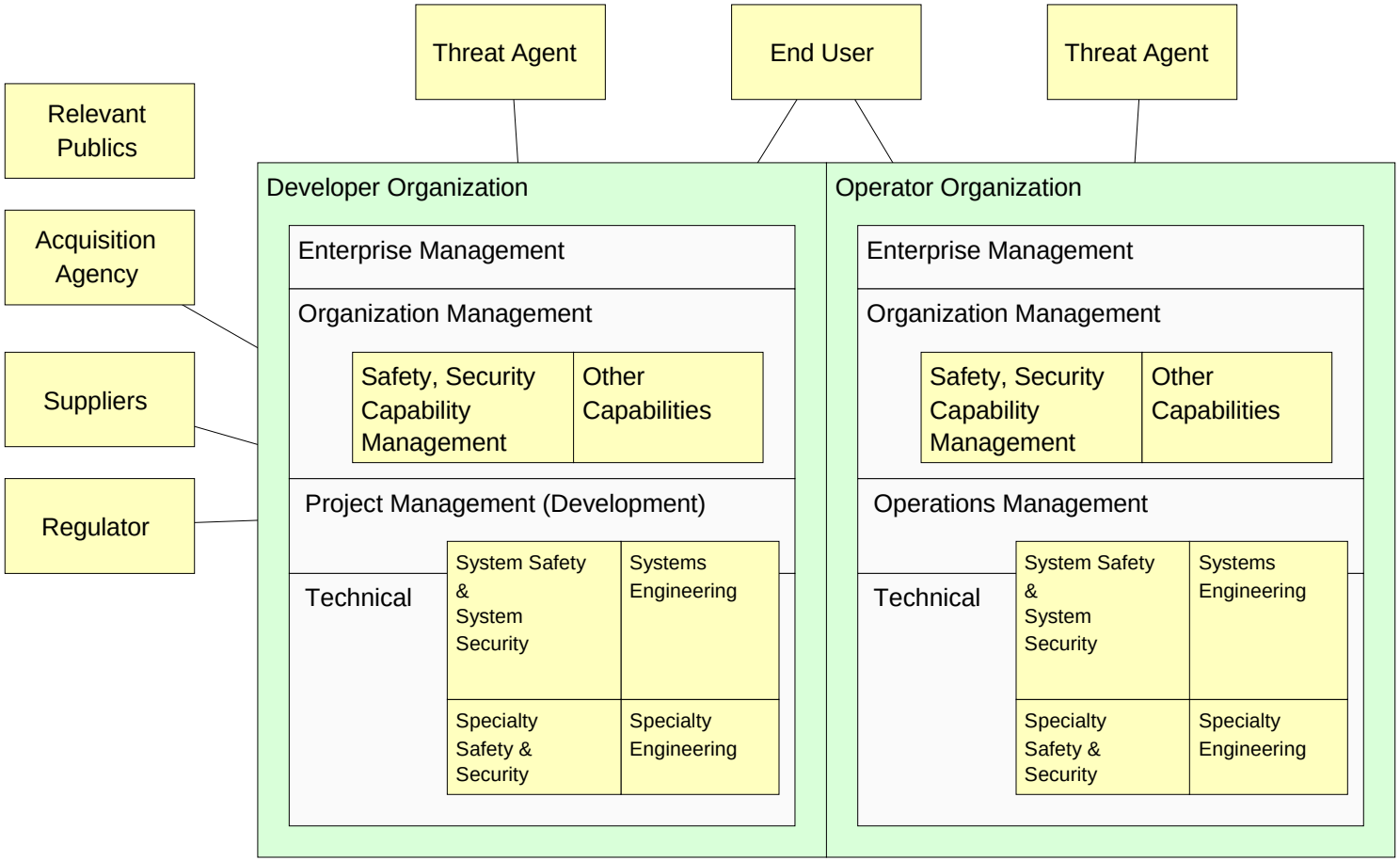
System Technologies

- *IT – widespread use of commercial components; Common Criteria*
- *Accepted use of un-trusted networks*
- *People aspects of IS security*
- *Emerging systems – networked physical systems*
- *We are aware of the vulnerabilities of current IS technologies, but wish to exploit networked systems increasingly in defence and civil applications*
- *Inter-operability generates potential vulnerabilities*
- *System architecture, interoperability models provide bases for security assessments*

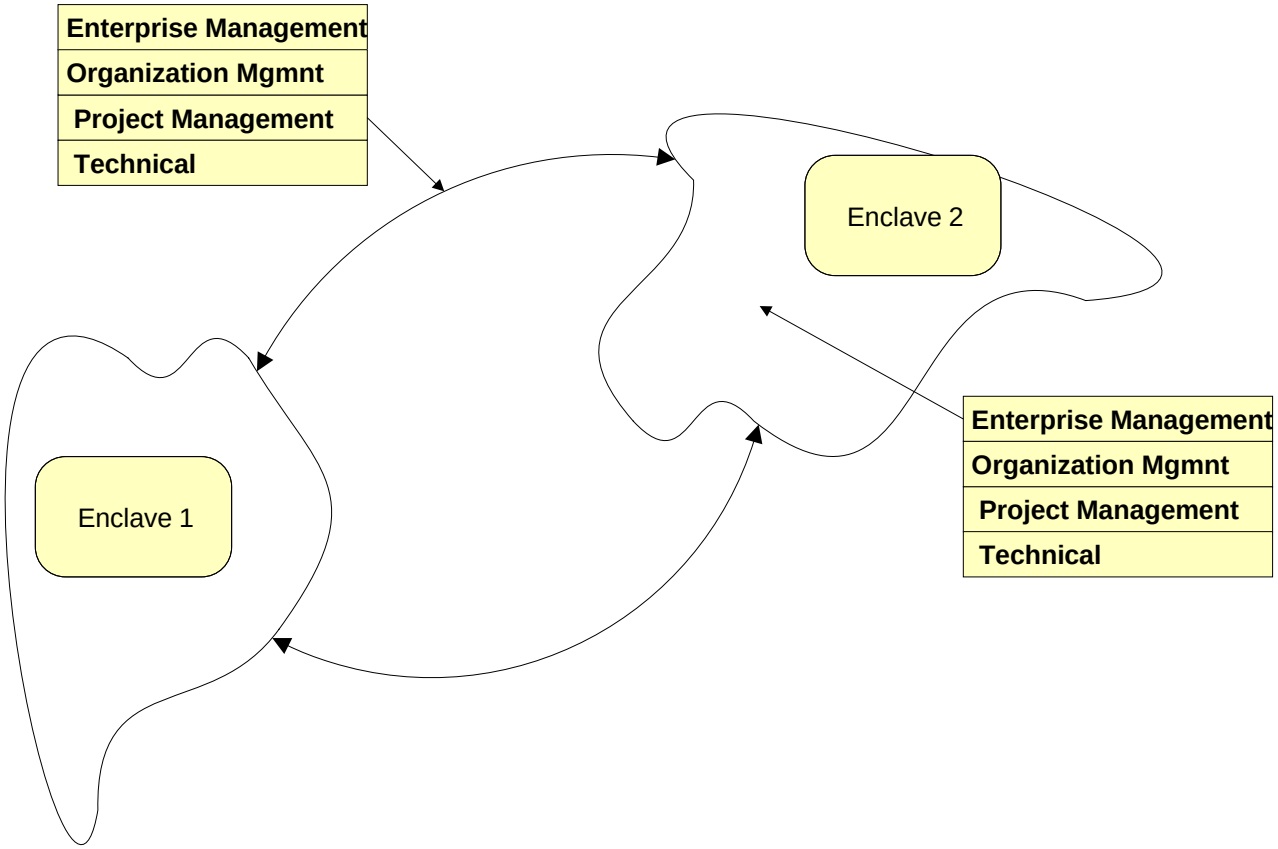
Practical Software and Systems Measurement

	Typical Concerns (in development)	Example Measurement frameworks
Enterprise Management	Productivity, cost, strategy, litigation, commercial viability and growth. Effectiveness of safety or security management systems; exploitation versus regeneration Enterprise risk	Financial accounting systems ERP Balanced Scorecard Strategy Maps
Organisation Management	Process improvement, maturity, people, learning, effectiveness, efficiency, integration of standardised activity, portability, institutionalisation, benchmarking	CMMI +SAFE SafeGauge Human Resources
Project Management	Delivery to plan, schedule, cost, meeting requirements, product performance, product maturity (or design stability); scope of safety work; safety risk trades; project risk monitoring, team volatility	Project Management tools PSM SPEL
Technical/ Speciality	Professional practice (e.g. safety engineering), safety risk assessment, risk mitigation, ALARP decision-making, effectiveness and efficiency of techniques, learning, regulatory compliance, certification	Domain-specific measurement concepts System Safety engineering concepts Hazard Tracking System

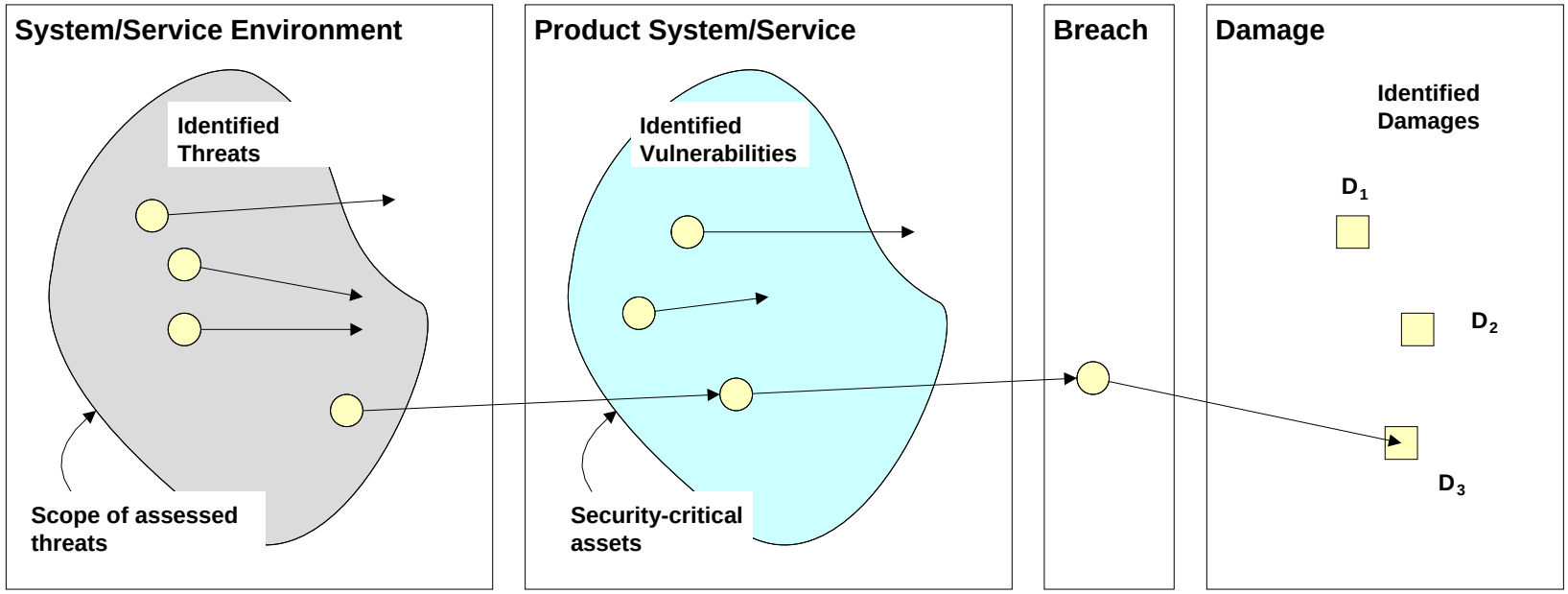
Information Needs Model



Information Needs in Networked Systems



Security Concept Model



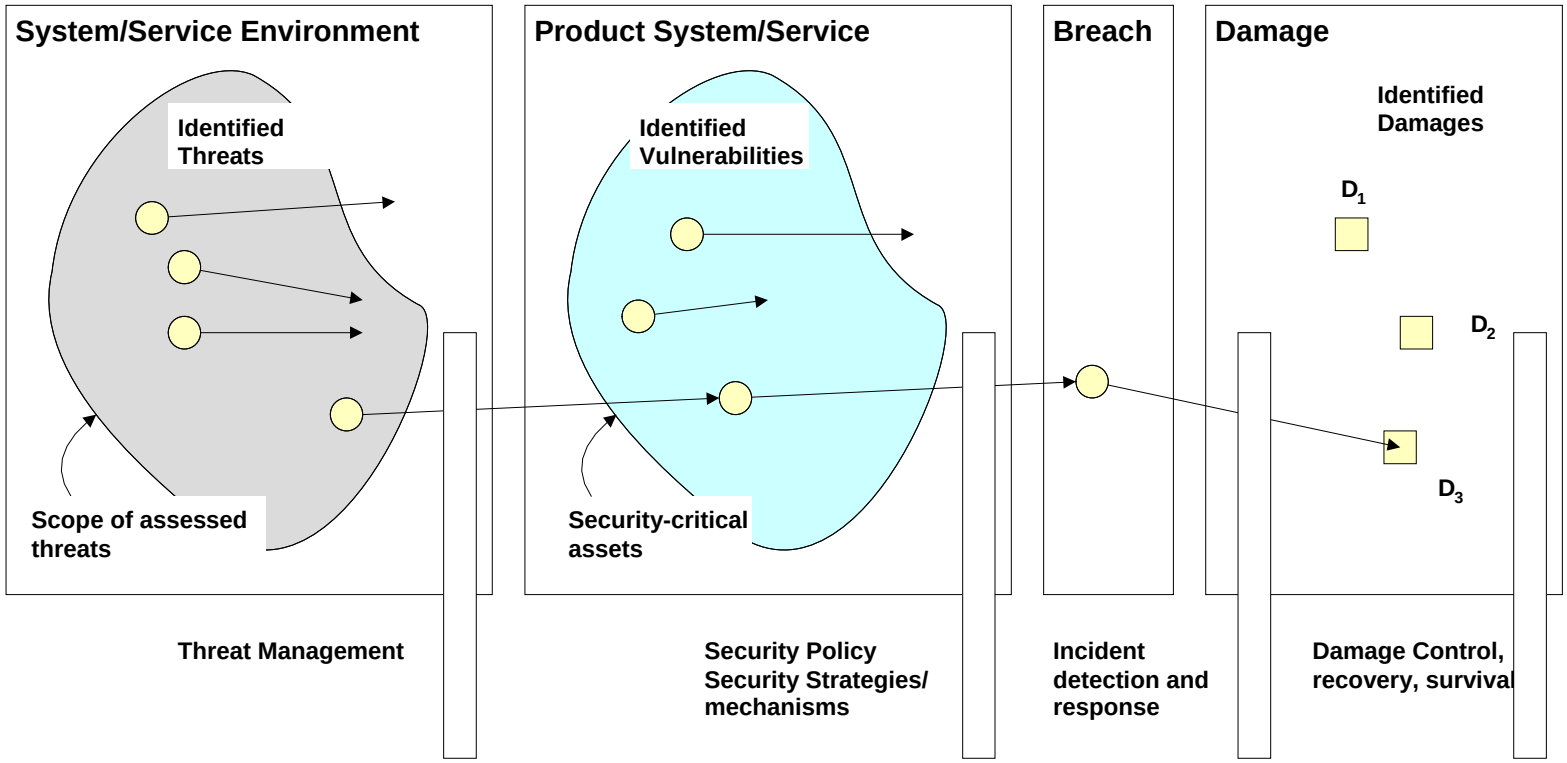
Threat: capability, intent
Threat type

Vulnerability
Vulnerability type
Vulnerability attack likelihood and severity

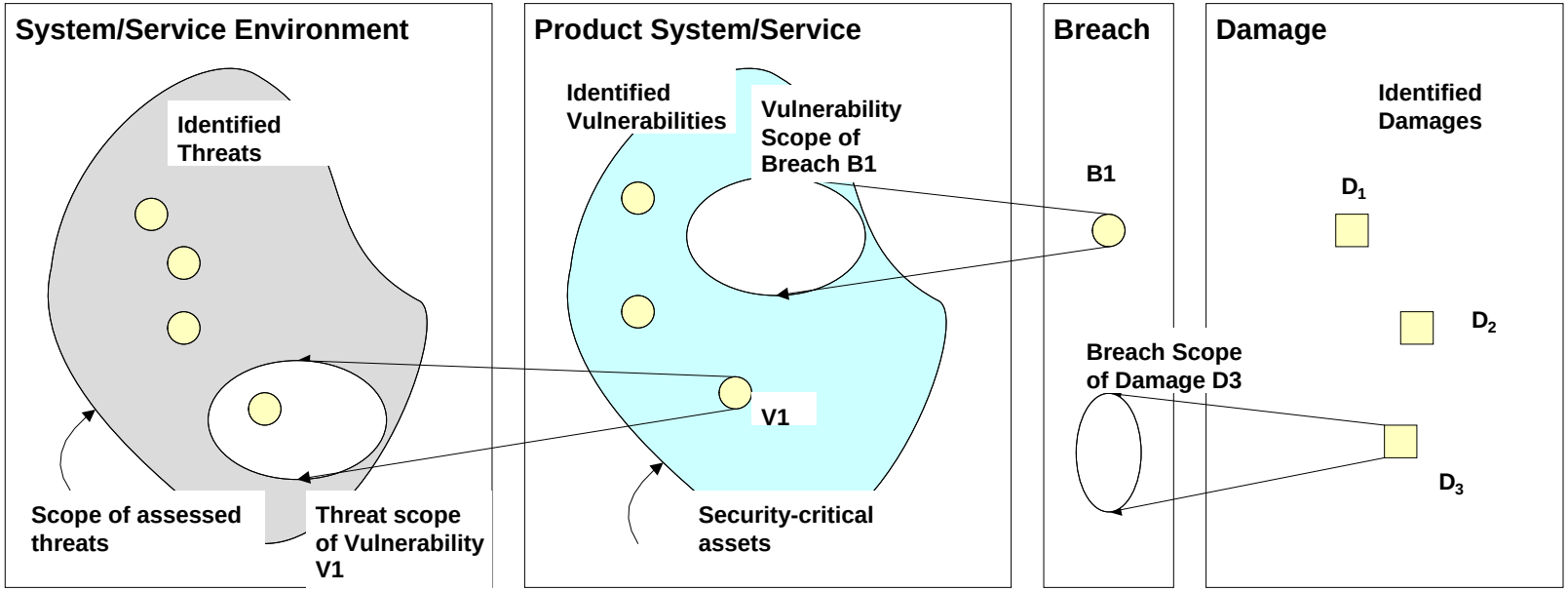
Security incident
Incident type
Incident likelihood

Damage scope
Damage severity
Damage likelihood

Security: risk management



Security: scope and estimation



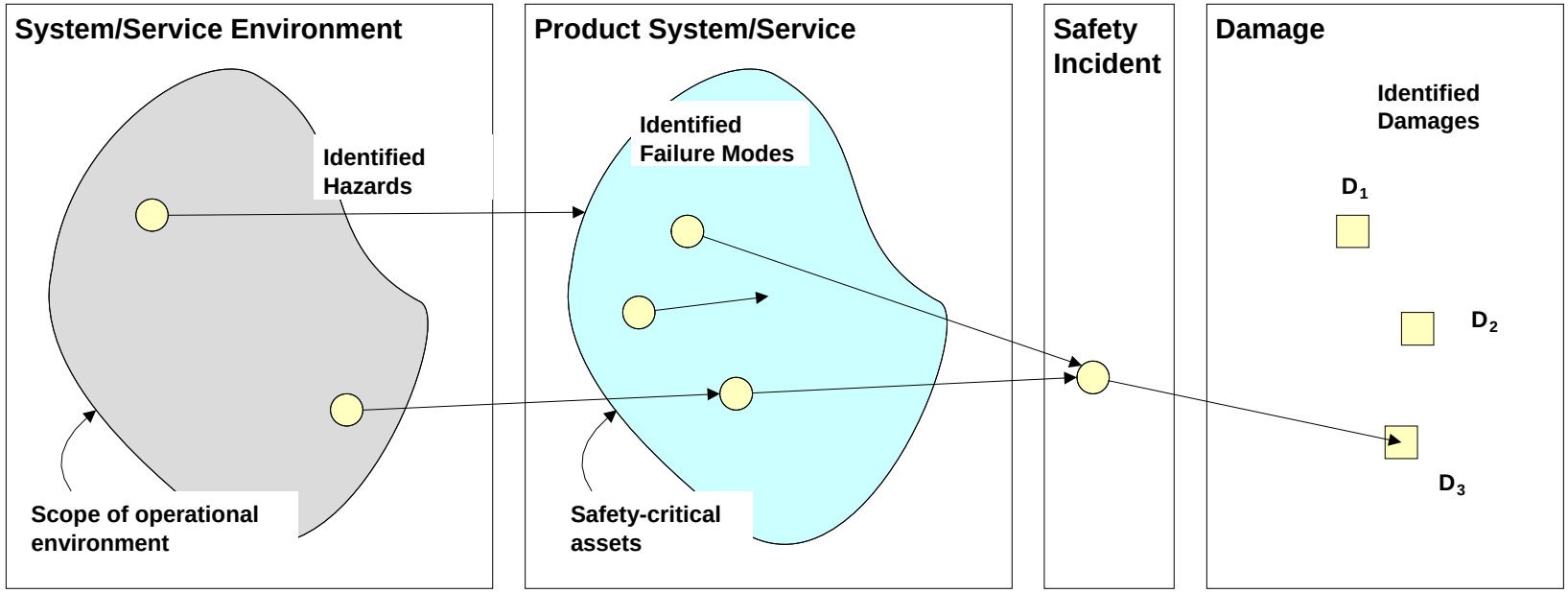
Threat: capability, intent
Threat type

Vulnerability
Vulnerability type
Vulnerability attack likelihood and severity

Security incident
Incident type
Incident likelihood

Damage scope
Damage severity
Damage likelihood

Safety Concept Model



Hazard: likelihood of accident, severity
Hazard type
Exposure time

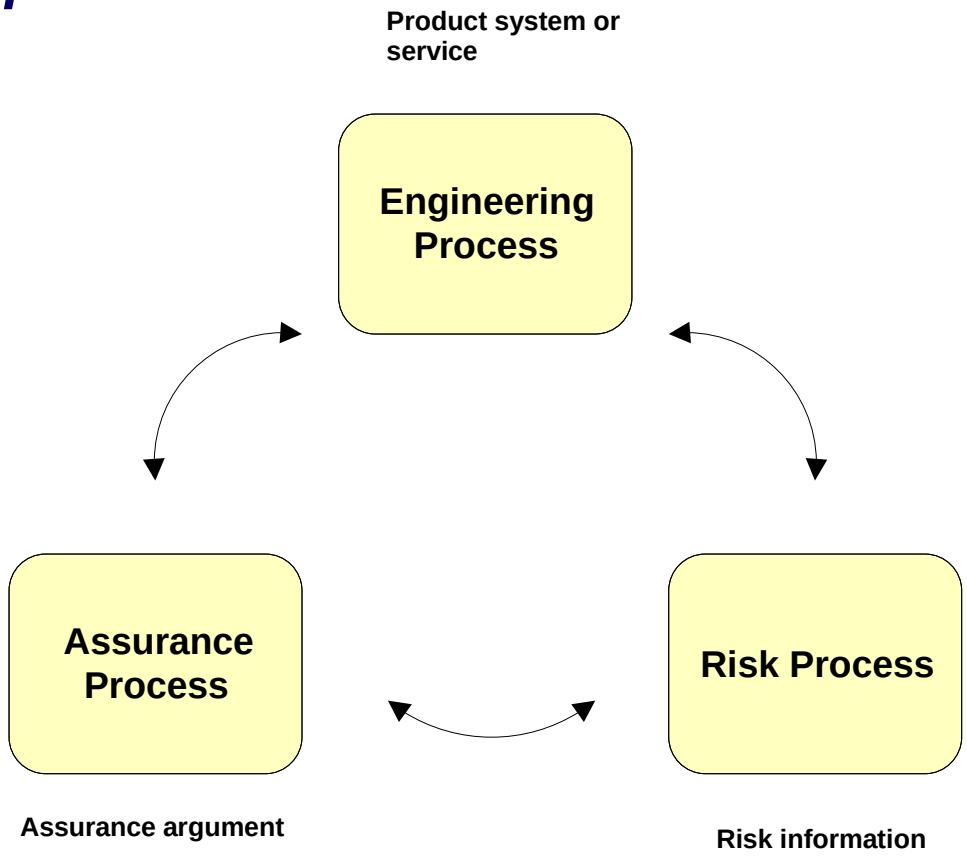
Failure Mode: type
accident likelihood
severity

Safety incident
Incident type
Incident likelihood
Accident Scenario

Damage scope
Damage severity
Damage likelihood

Engineering, risk, assurance

- *SSE-CMM*



Three Types of Risk Management

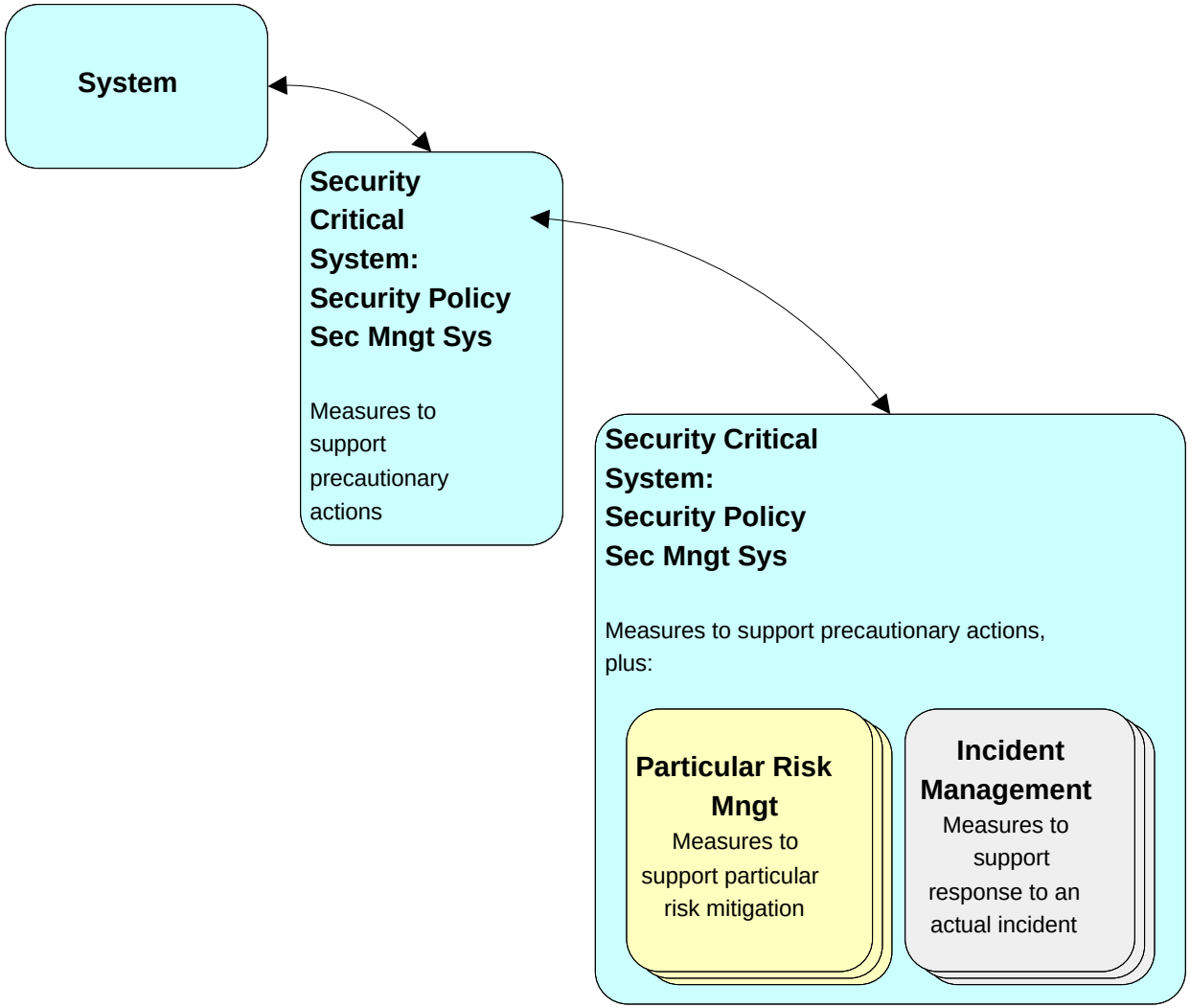
1. ***General precautions: systematic responses to generally recognised risks; e.g. Security Policy, ISMS, best practice audit***
2. ***Specific responses to potential future incidents; implies particular risk mitigation – ALARP***
3. ***Specific responses to actual incidents; damage limitation***

Measurement Applications

Measured Organization/ System/ technology

Risk Management Category	Security Threat Management			
	Threat Management	Vulnerability Management	Incident Management	Damage Management
Precautionary				
Particular Risks				
Actuals				

State-Dependent Measurement



Measurement Against Plan BS 7799-2:2002

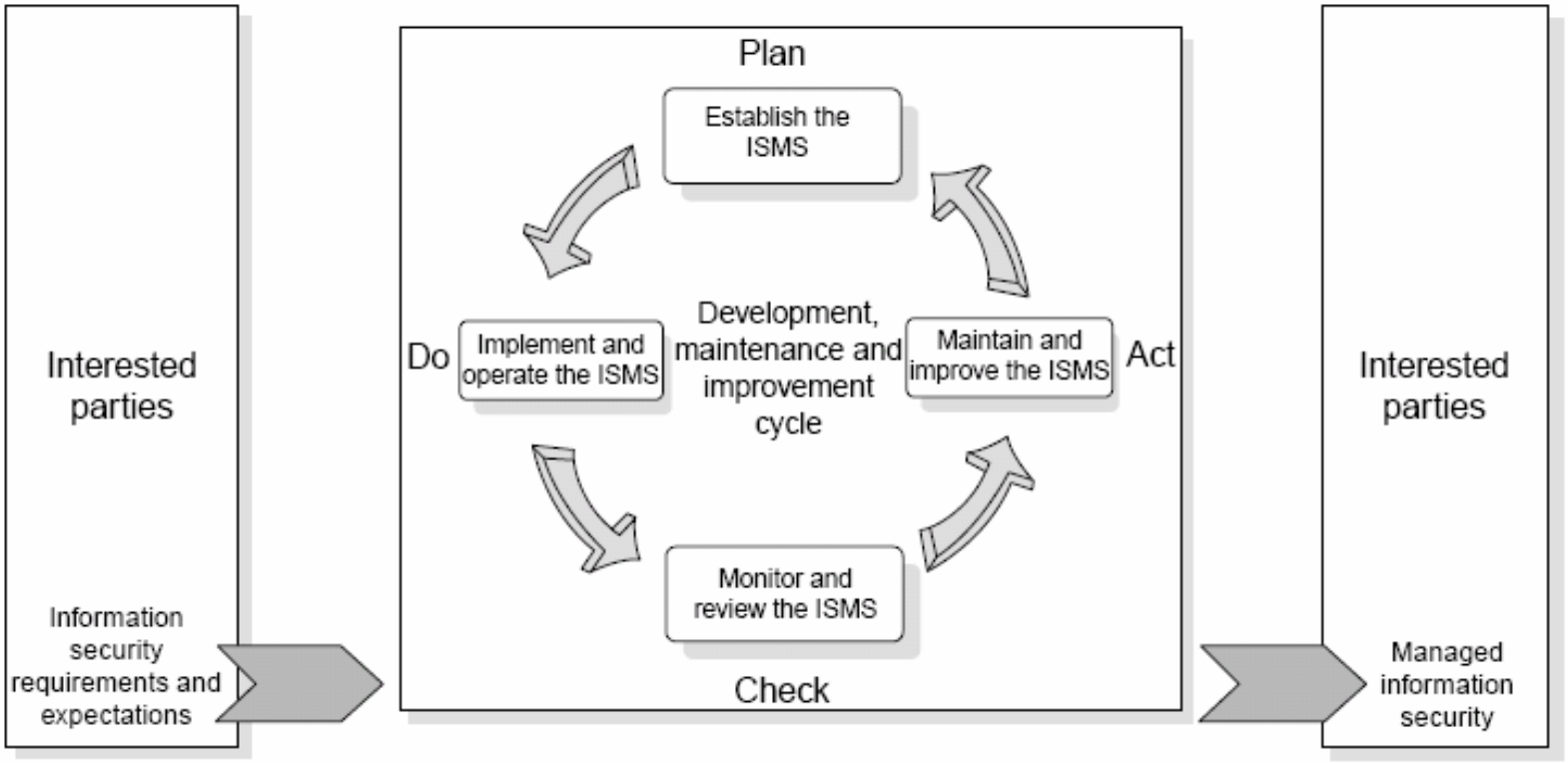
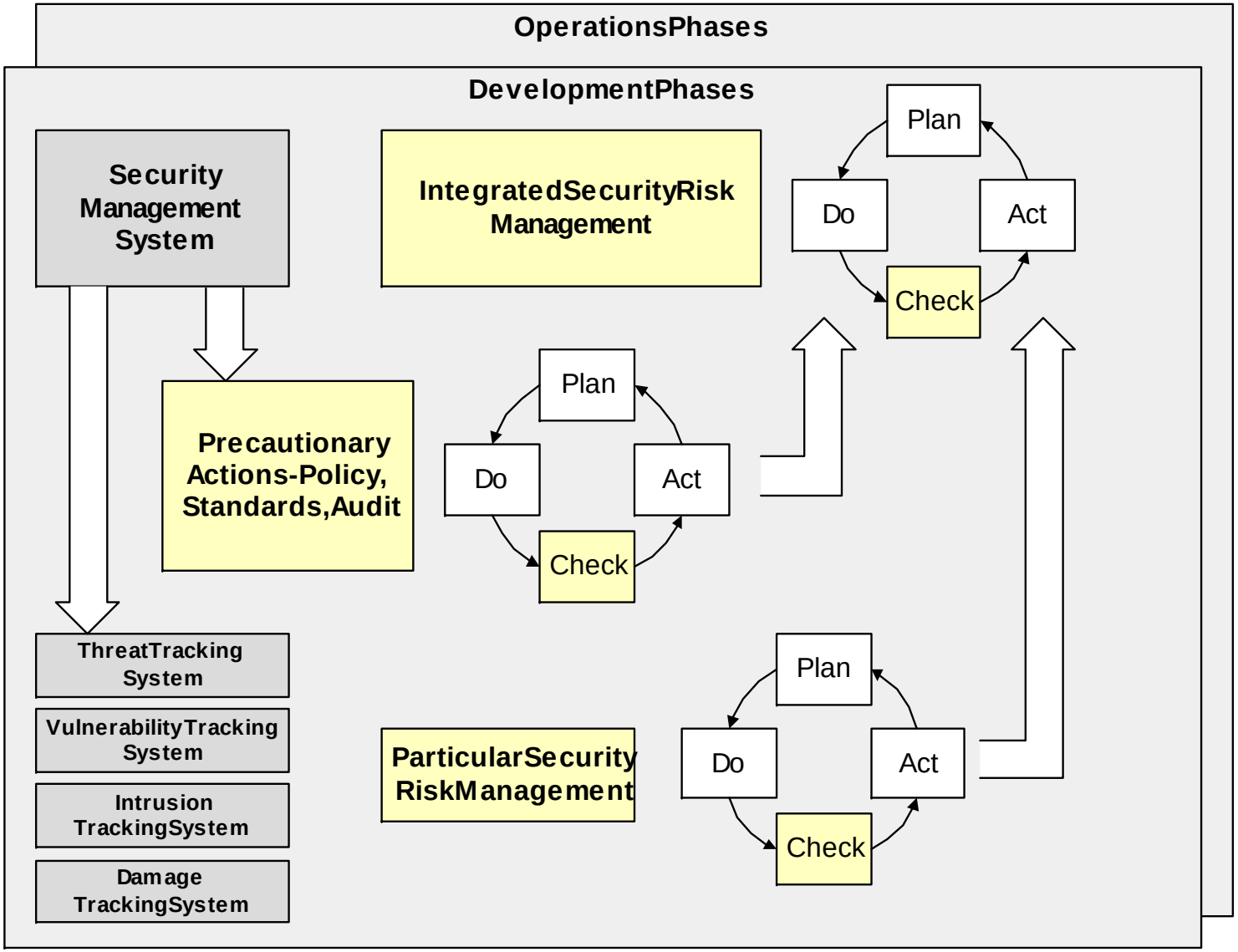
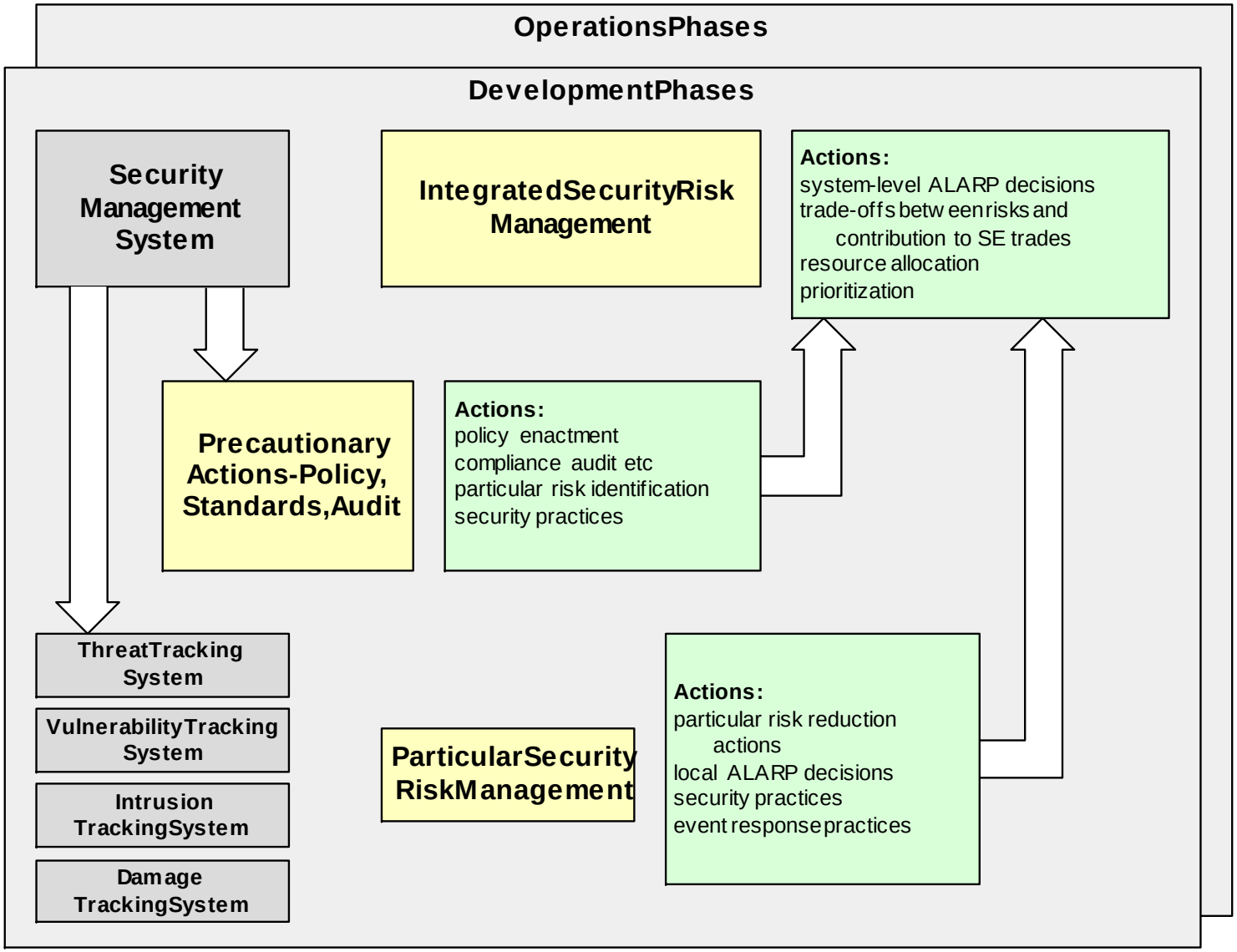


Figure 1 — PDCA model applied to ISMS processes

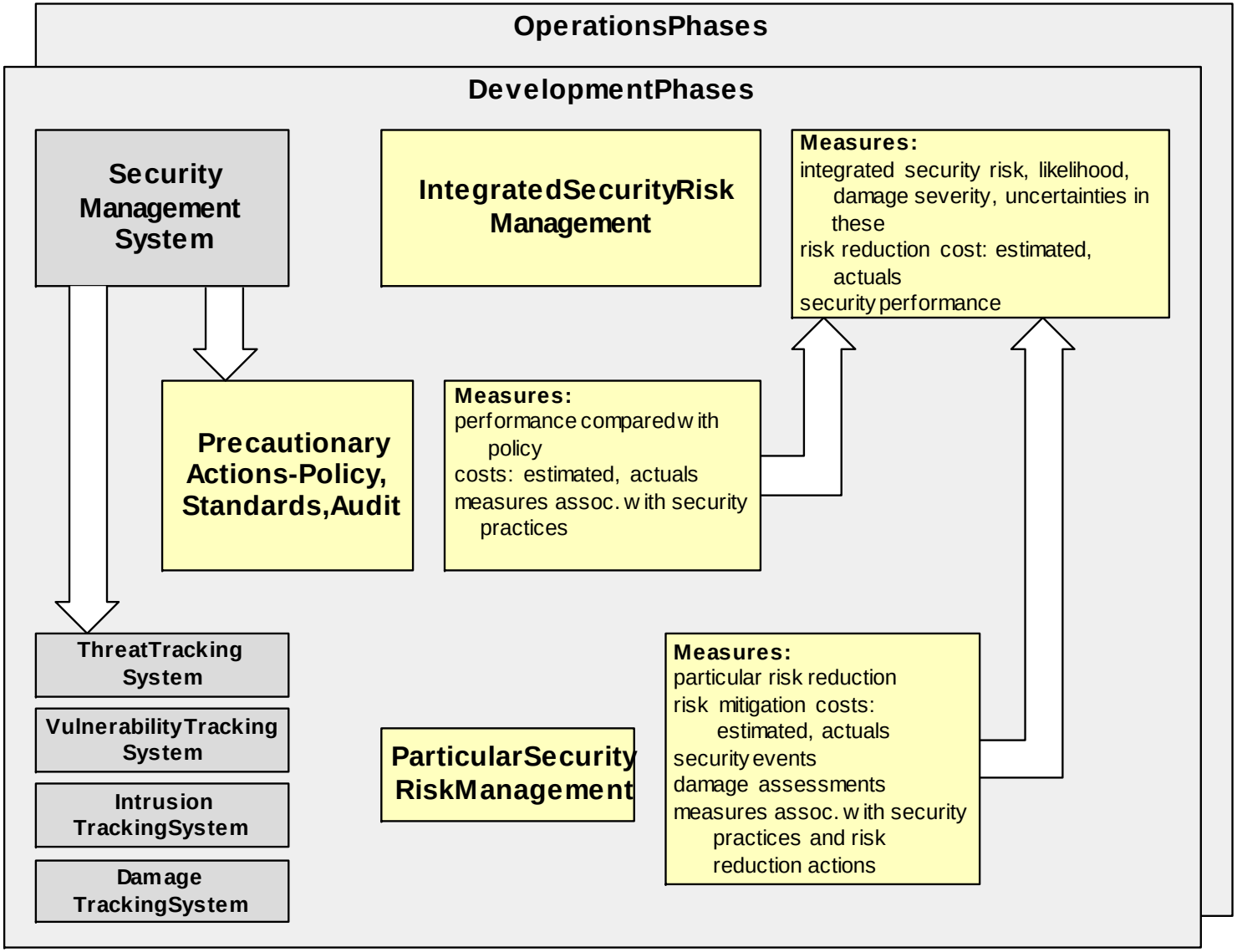
Practical Software and Systems Measurement



Practical Software and Systems Measurement



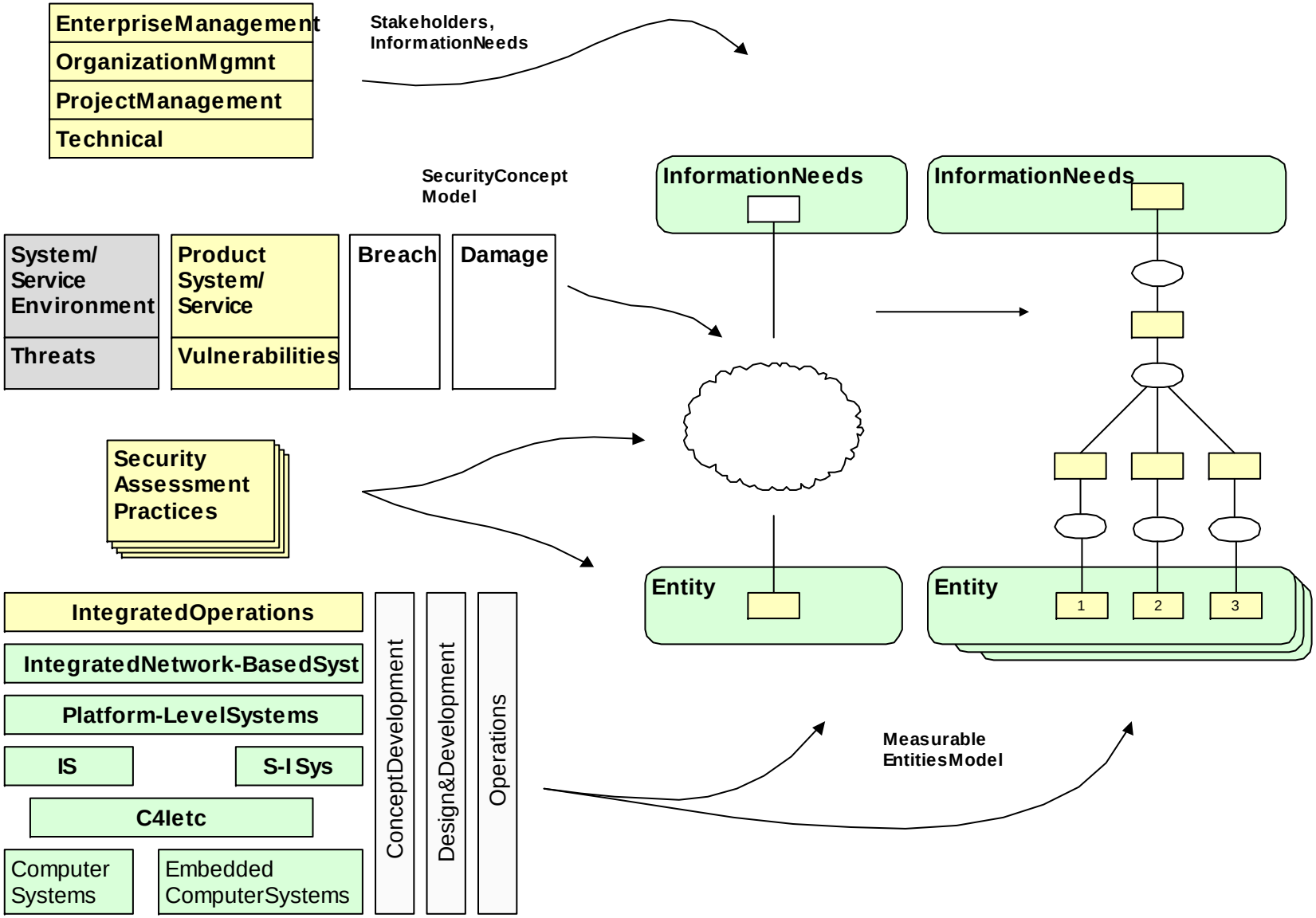
Practical Software and Systems Measurement



Safety and Security Integration

- ***Specialty domains that contribute to Sys Eng***
- ***Both benefit from a risk management approach***
- ***Trade offs with other attributes, mission performance, cost, schedule***
- ***Trade- space embraces Sys Eng, Project Mngt, Operations Mngt***

Practical Software and Systems Measurement



Review Questions

- ***Is this a useful framework? What are the main things that are missing?***
- ***How can/ could we tell if the framework is useful?***
- ***What about the process maturity view?***
- ***What about the enterprise level? Cost of security?***
- ***What about assurance?***
- ***Is the model too abstract? Do we need more direct mapping to practical measures?***

3. Brainstorm Security Measures

- ***Threat Agents and Threats***
  - ***Threat management***
- ***Vulnerabilities***
  - ***Security strategies, policy, mitigations***
- ***Security Incidents/ events/ intrusions***
  - ***Incident detection and response***
- ***Damage***
  - ***Control, recovery, survival***

Threat Agents and Threats

Threat Agent count

Threat Agent capability, compared with System Vulnerabilities

Threat Agent intent

Threat Risk (likelihood, potential damage severity, confidence in these assessments), linked with System Vulnerabilities

Threat Trees

Threat Management

Threat risk mitigations; tracking cost, schedule, status

Residual Threat Risk

Vulnerabilities

Identified Vulnerabilities (count)

Vulnerability Risk (likelihood of breach, severity of potential damage)

Strength of Function

Vulnerability Risk Mitigations

Non-compliances with Security Policy and Plan

Vulnerability risk mitigations; tracking cost, schedule, status

Residual vulnerability risk

Compliance Status with Common Criteria, or checklist compliance

Security Evidence for assurance purposes

Various mitigation actions at levels of System security

Specialty security (IS, IT, network, sw, physical)

Engineering support during development; trade-offs

Security Incidents/ Events/ Intrusions

Potential Incident Counts, Attacks

Threat/vulnerability/damage mapping

Incident Risk (likelihood and severity of damage)

Actual Incident Counts, Attacks

Status of incidents

Timing of Incidents

Incident detection and response

Potential

Incident risk mitigation actions: tracking cost, schedule, status

Actual

Incident response: tracking scope, cost, schedule, time, status

Damage

Potential

Damage Risk (likelihood, scope, severity)

Damage cost and other effects

Actual

Damage scope

Damage Control, Recovery, Survival

Potential

Damage risk mitigation actions: tracking cost, schedule, status

Actual

Response, recovery action: tracking cost, schedule, status

Operationalize Measures

- ***Identification of measurable entities and attributes***
- ***However, generic so can be mapped to different security specialties and target systems***
- ***Threat, Vulnerability, Breach and Damage Tracking Systems***
- ***Policy/ ISMS frameworks***
- ***Reference out to existing frameworks***

Review Questions

- ***How can we continue to develop security measurable concepts?***
- ***What are we missing?***
- ***How can we transition to measurement constructs?***
- ***How can we test measurement proposals?***

4. PSM Security Additions

Product Size, Stability and Scope	Scope - Security (internal response)	Security Requirements
		Security-Critical Functions
		Security-Critical Components
		Security-Critical Interfaces
		Security-Critical Modes
		Security Enclaves
		Security Change Workload
	Scope - Security (external threat)	Threats
		Threat capability
		Threat Intent

Product Quality	Dependability - Security	Vulnerabilities
		Vulnerability Risk
		Breach Scenario Risk
		Check List Items
		Common Criteria Status
		Security Assessments & Assumptions
		Mitigation Status
		Security Incidents & Accidents
	Assurance - Security	Security Argument

Questions

- ***Do we need an information need pertaining to the environment?***
- ***Can we reference out to existing standards, where appropriate*** ***e.g. SP 800-55?***
- ***Should we explicitly distinguish between measurement against (a) policy, (b) plan, (c) particular risk?***

5. Plan Next Steps

- ***Update White Paper to v3.0, issued October for feedback, December***
- ***Review and 'final' update at February 2005 TWG, to v4.0.***
- ***Trials***
- ***Engaging with security engineering communities***
- ***iCMM/CMMI etc***