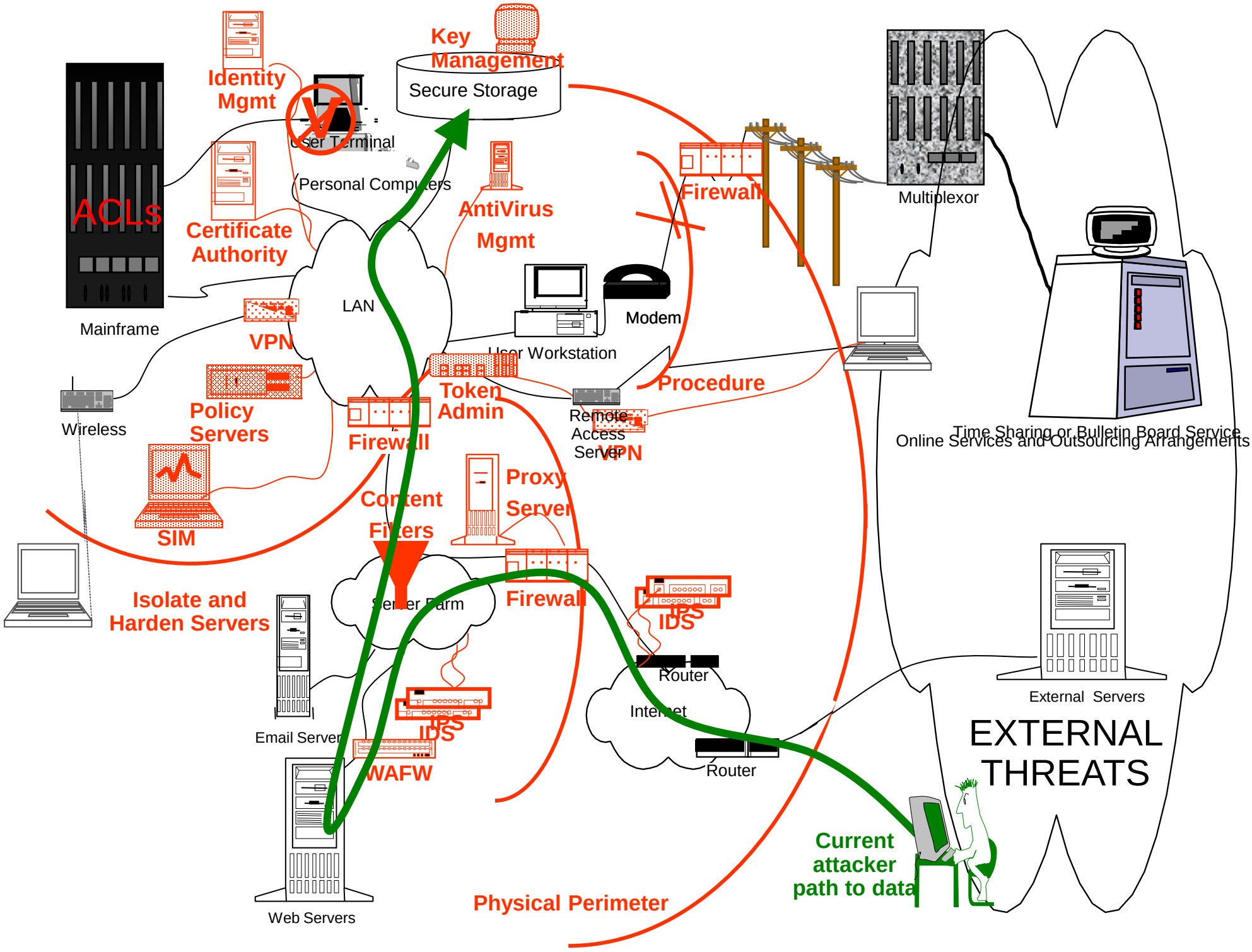
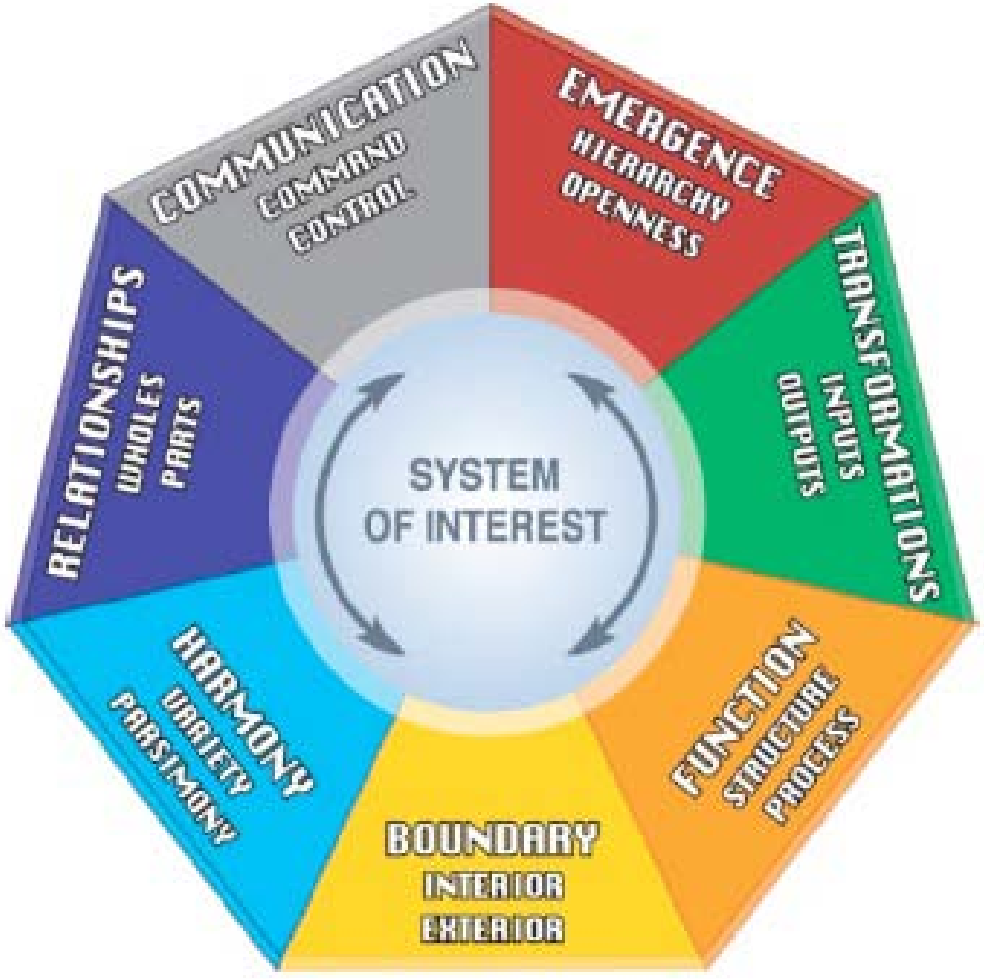
Metricon 5.5
Verification versus Validation

Jennifer Bayuk
Cybersecurity Program Director
School of Systems and Enterprises
jennifer.bayuk@stevens.edu


Key Management
Secure Storage
Identity Mgmt
User Terminal
Personal Computers
ACLs
Certificate Authority
AntiVirus Mgmt
Firewall
Multiplexor
LAN
Mainframe
VPN
Modem
User Workstation
Wireless
Policy Servers
Token Admin
Firewall
Remote Access Server
VPN
Procedure
Time Sharing or Bulletin Board Service
Online Services and Outsourcing Arrangements
SIM
Content Filters
Proxy Server
Server Farm
Firewall
IPS
IDS
Isolate and Harden Servers
Router
Internet
External Servers
Email Server
IPS
IDS
WAFW
Router
EXTERNAL THREATS
Current attacker path to data
Web Servers
Physical Perimeter

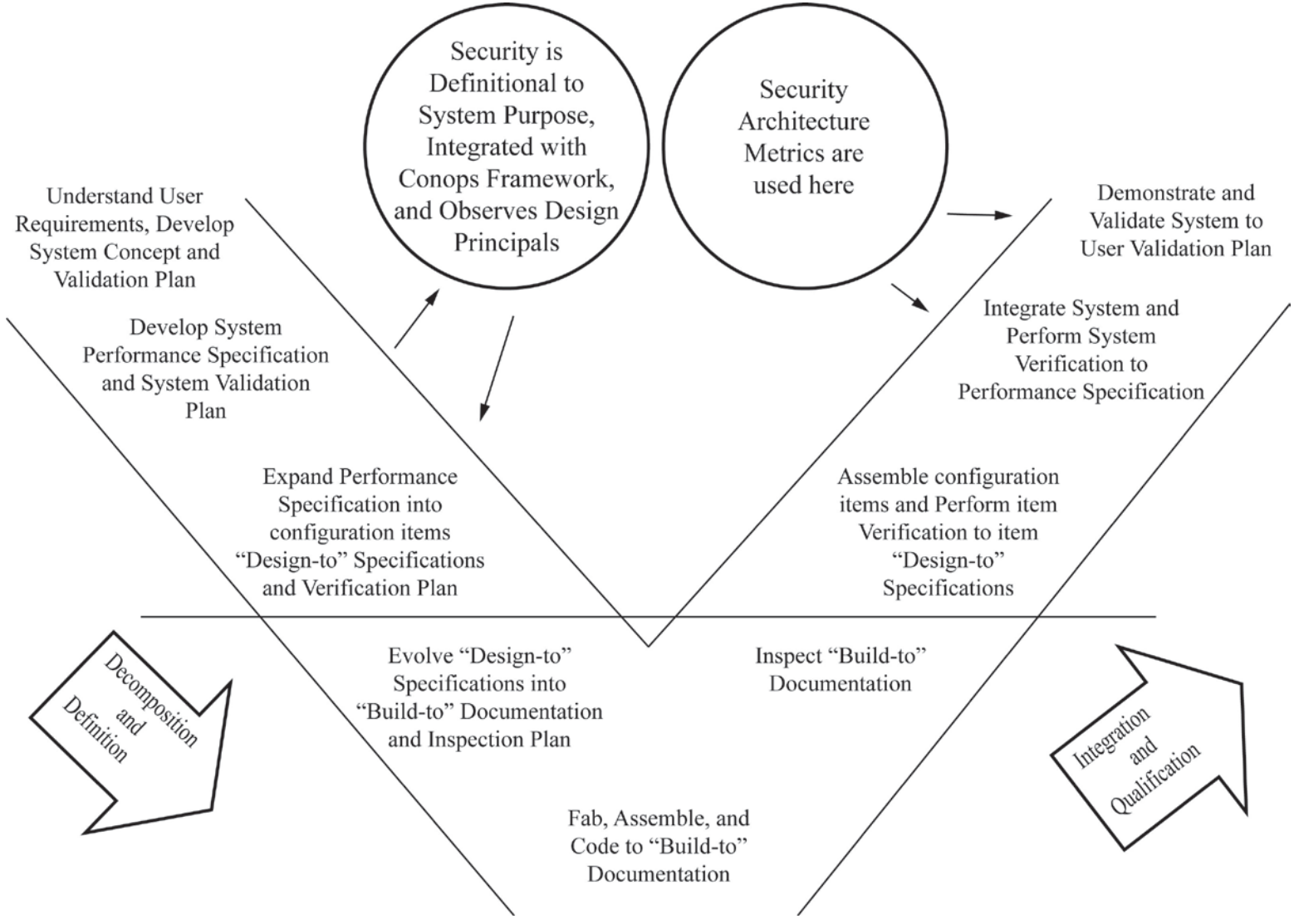
Systems Thinking

STEVENS INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY



Source: J. Boardman and B. Sauser, *Systems thinking: Coping with 21st century problems, Taylor & Francis, 2008.*

The Vee Model



Source: Based on Buede and, Bayuk and Horowitz, An Architectural Systems Engineering Methodology for Addressing Cyber Security, Systems Engineering, 2011

Advantages of the Engineering Approach

1. Manage Complexity
2. Top-down requirements tracing
3. Black box modeling
4. Logical flow analysis
5. Documentation
6. Peer Review
7. Detailed Communication

Adapted from: J. Sherwood, A. Clark and D. Lynas, Enterprise security architecture, CMP Books, 2005.

Traditional Requirements Process

1. Functional

2. Interface

2. System-wide – “ilities”

3. System-wide – “ilities”

Focus on systems security engineering is required to know when it should be placed here.

Security vulnerabilities are frequently introduced here.

Systems engineering literature traditionally places security here.

Source: Buede, *The engineering design of systems, models and methods, Wiley, 2009*

Today's Security Requirements
…*a charitable interpretation*…

STEVENS
INSTITUTE *of* TECHNOLOGY
THE INNOVATION UNIVERSITY

Functional – What is necessary for mission assurance?

Nonfunctional – What is necessary for system survival? What is necessary to anticipate changing threat environments?

V and V - What is necessary to ensure requirements are met?

Must include security requirements to support:

- System Mission and Purpose
- System Lifecycle Maintenance

Should address:

- Adaptability, flexibility, agility, redundancy, robustness, scalability….

V and V

Verification : Did we build the system right?

Validation: Was the right system built?

Also known as:

Correctness – *Do the security features work?*

Effectiveness – *Is the system secure?*

Systems Engineering Verification Activity

- Identify Verification and Validation Targets
- Define Verification and Validation Approach
- Perform Verification
- Perform Validation
- Provide Verification and Validation Results

Source: ISO 28127

SYSTEMS ENGINEERING
Research Center

A New Security Approach

- Clear problem statements
- Thorough problem background description including a full literature review
- Clearly defined solution criteria
- Proposed hypothesis formulated to shed light on a solution and how it may be proven or disproven
- Summary of contributions to field and a statement of next steps

A Systematic Look at Security

Security:	**Something that thwarts perpetrators who enact threats that exploit system vulnerabilities to cause damage that adversely impacts system value.**
Security Feature:	**A system capability that contributes to its security.**
Security Metric:	**Measurement that characterizes an attribute of the system of interest that is proposed to have both face and construct validity in the context of a hypothesis that the system is secure.**
Security Framework:	**The concept of operations, mission, and environment under which a system operates.**

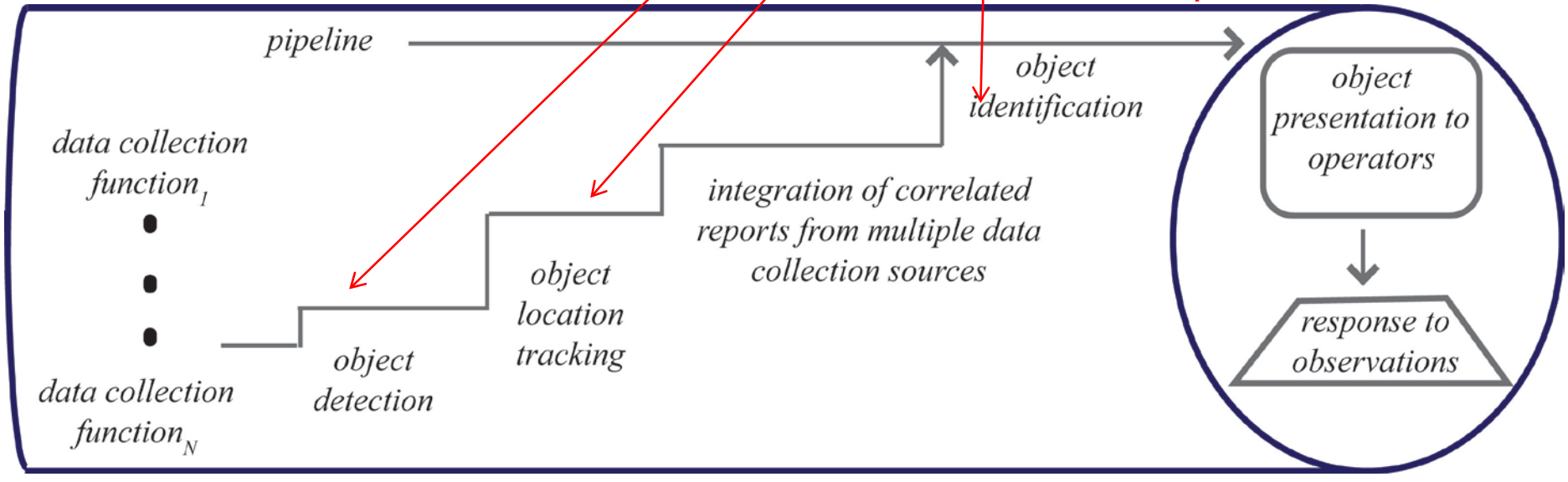
Frameworks

- Patterns at system level
- Security is identified with resiliency of mission
- Systemic security features are functional requirements
- Architecture security metrics verify and validate functional requirements

Possible Functional Security Metrics:

- sensor signal-to-noise ratios
- data integrity cross-platform checks
- the type and number of information delivery alternatives available to the end user/operator

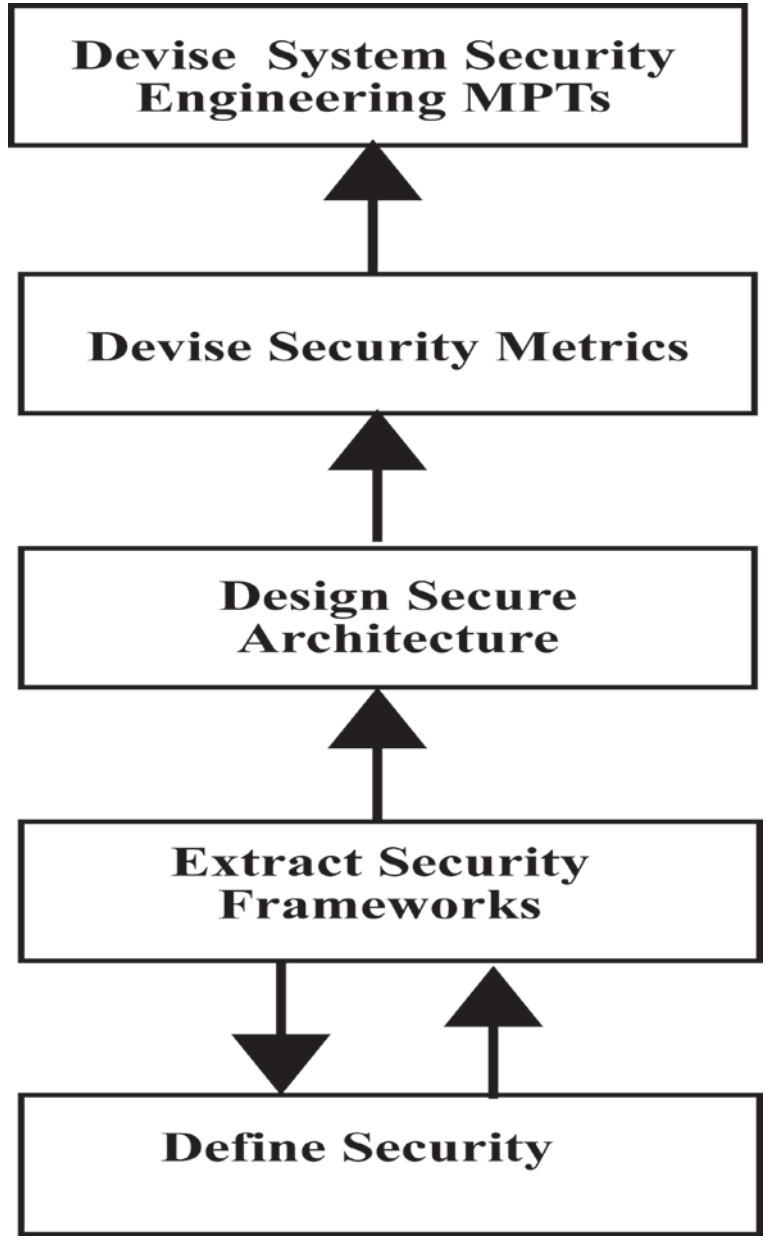
Example: Pipelined monitors



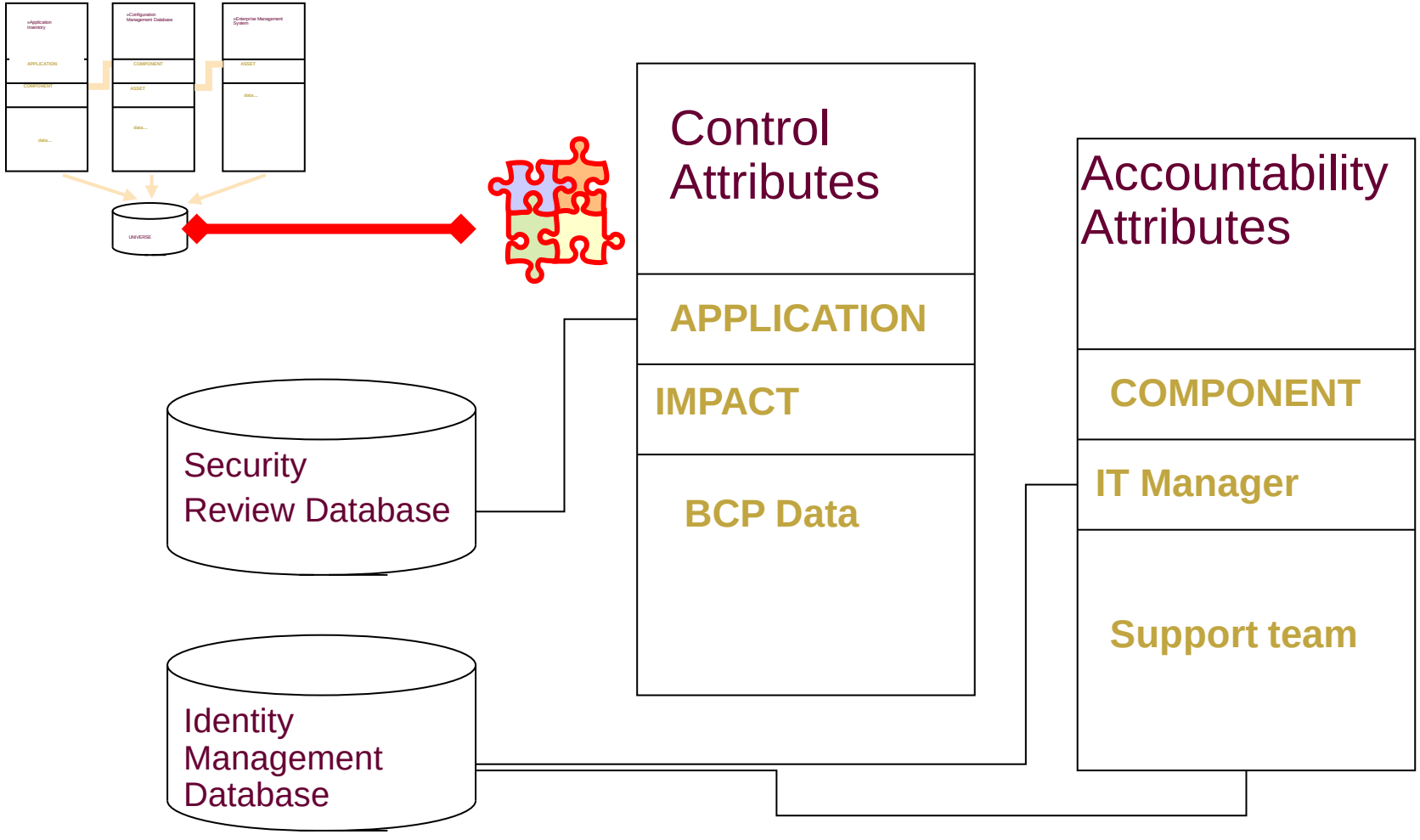
Source: Bayuk and Horowitz, An Architectural Systems Engineering Methodology for Addressing Cyber Security, Systems Engineering, 2011

New Security Methodology

SYSTEMS ENGINEERING
Research Center



Link Indexes to Security Data



Common Indexes cannot be expected to exist in different realms and different management domains.

Expectations for linkage must be articulated.

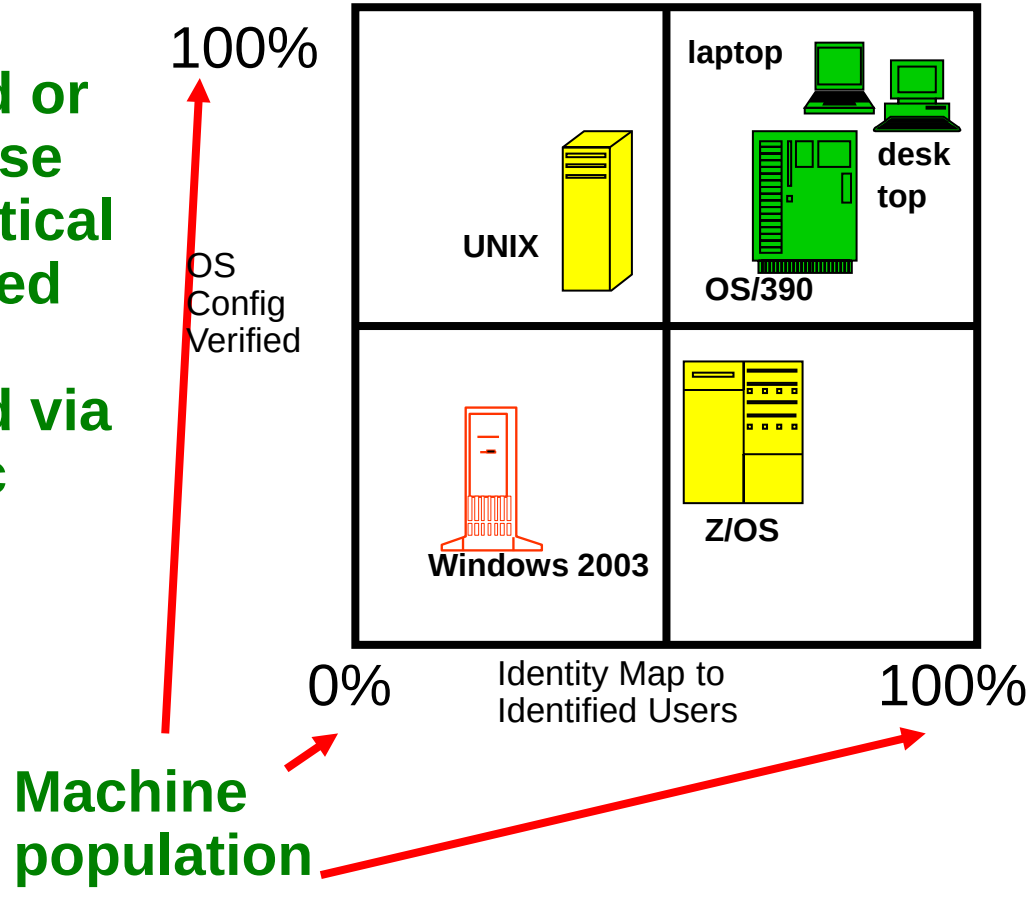
Source: *Bayuk, ISACA Training 2009*

Example System Security Verification Processes

	Input/ Output	**Configuration Compliance**	**Peer Review**	**Completion Criteria**
Testing	Continuous monitoring	Change control verification		
Analysis		Automated configuration checking	Segregation of oversight duties	Process metrics
Inspection	Quality Control	Audit and Assessment	Red/Blue Teams	

Presentation Techniques

Total patched or otherwise automatically verified to be secured via specific tools



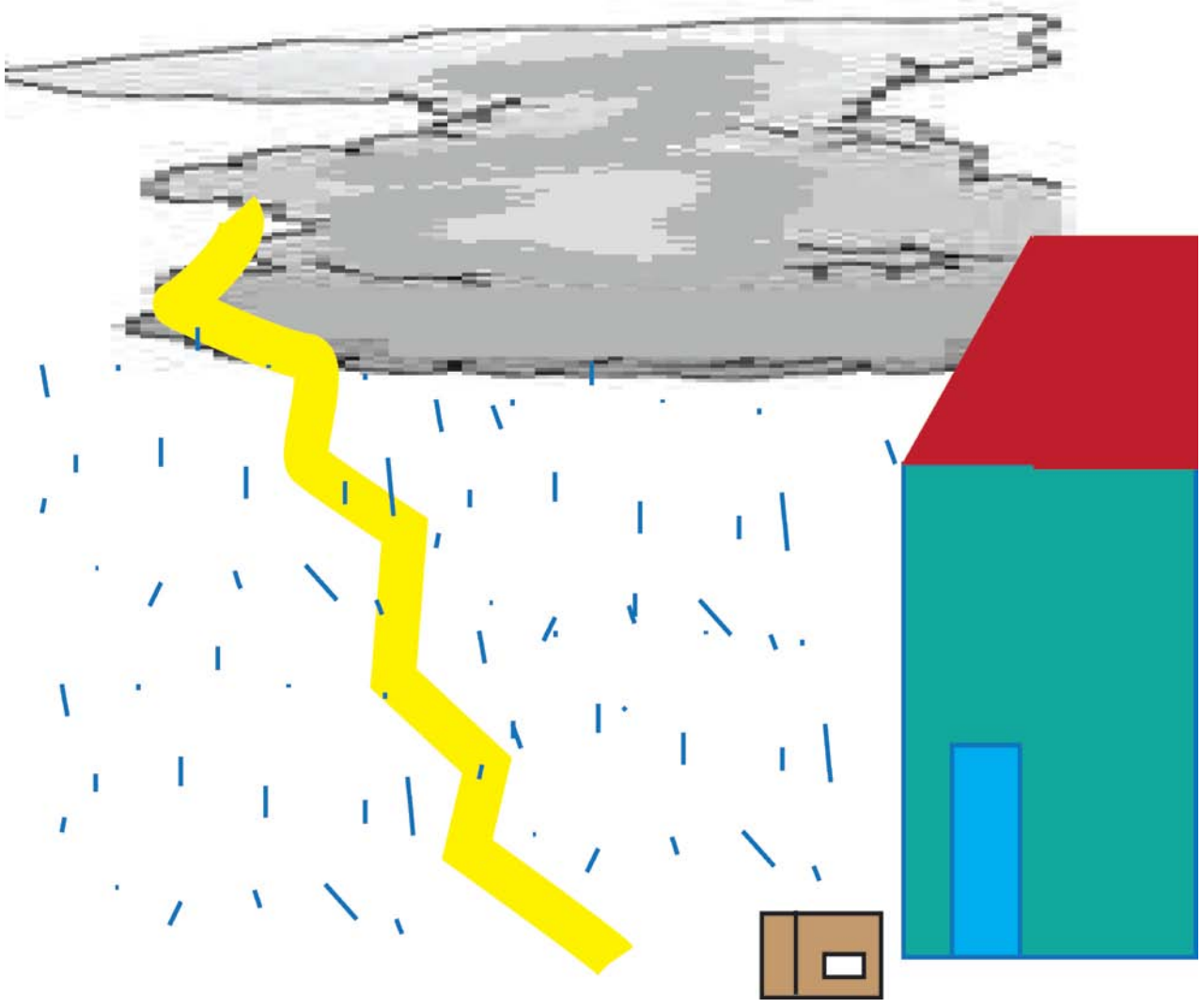
Facilitates comparison between different types of technology, business units, etc, often used for audit remediation.

Source: *Bayuk, Metricon 3.5, 2008*

Validation Criteria

- content validity
- face validity
- criterion validity
- construct validity

Validation



Source: Bayuk, Enterprise Security for the Executive, 2010

STEVENS
INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY

Questions? Discussion?

Follow-up:

jennifer@bayuk.com