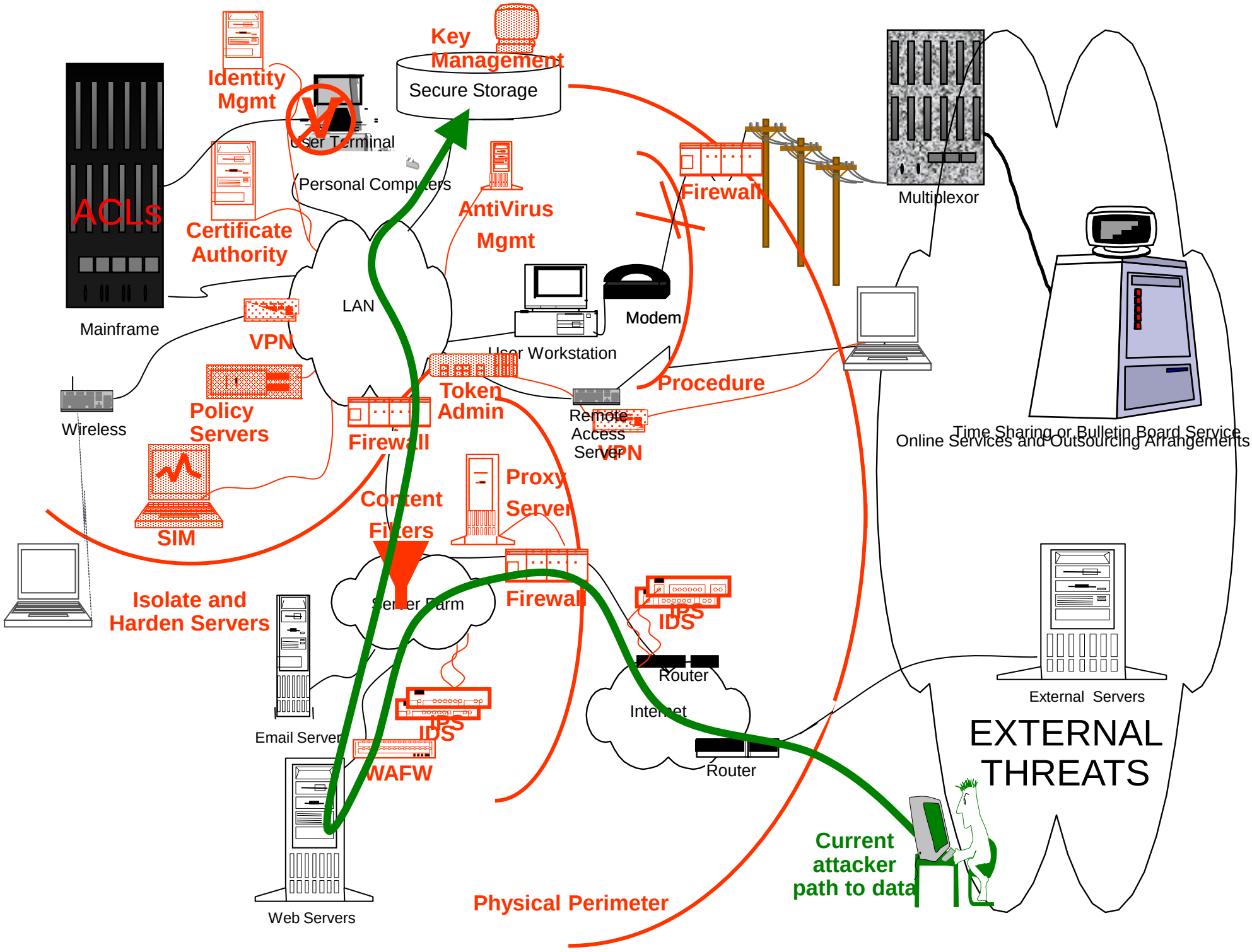
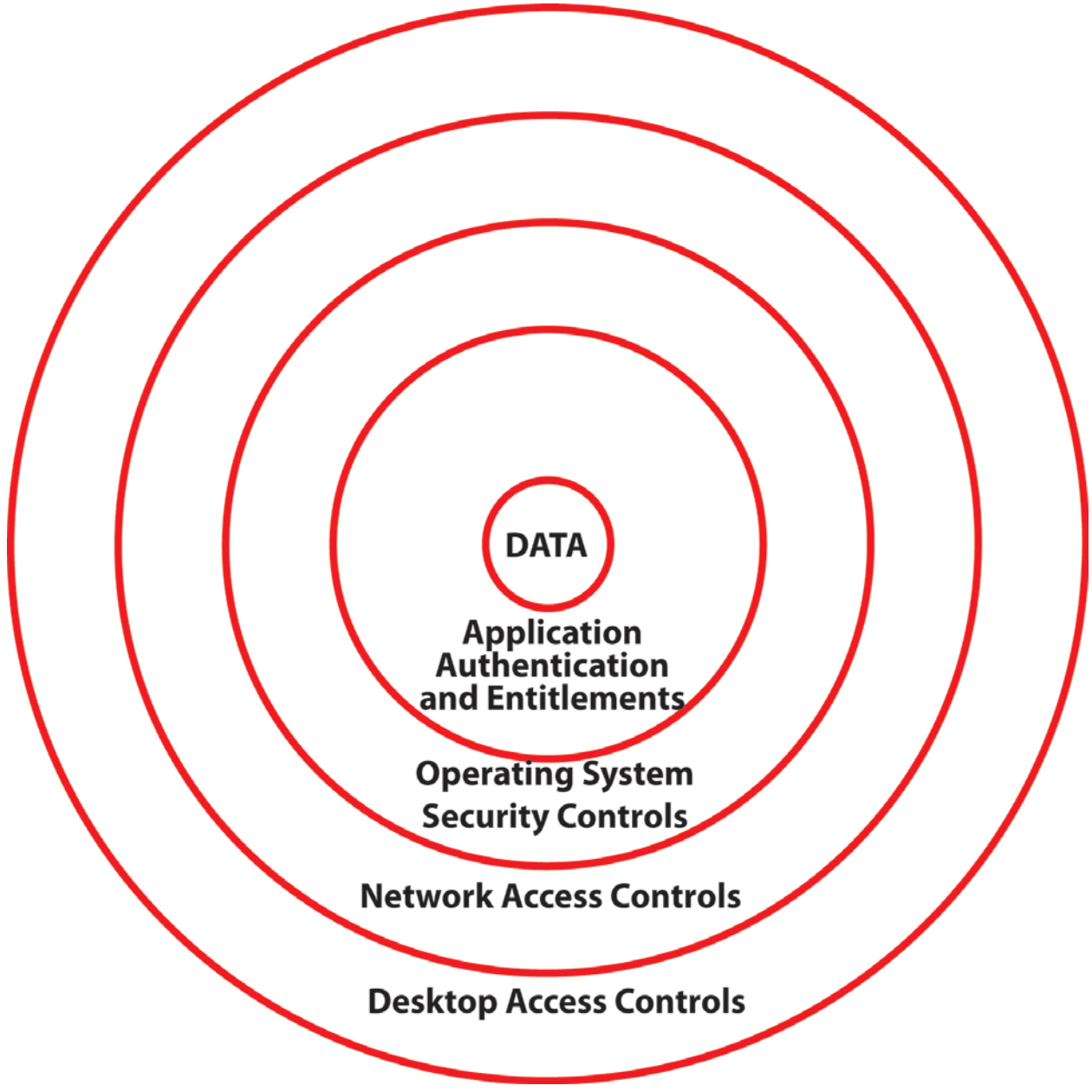
# High Confidence Systems and Software
# May, 2010
# Security Systems Engineering


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

# *Defense in Depth*

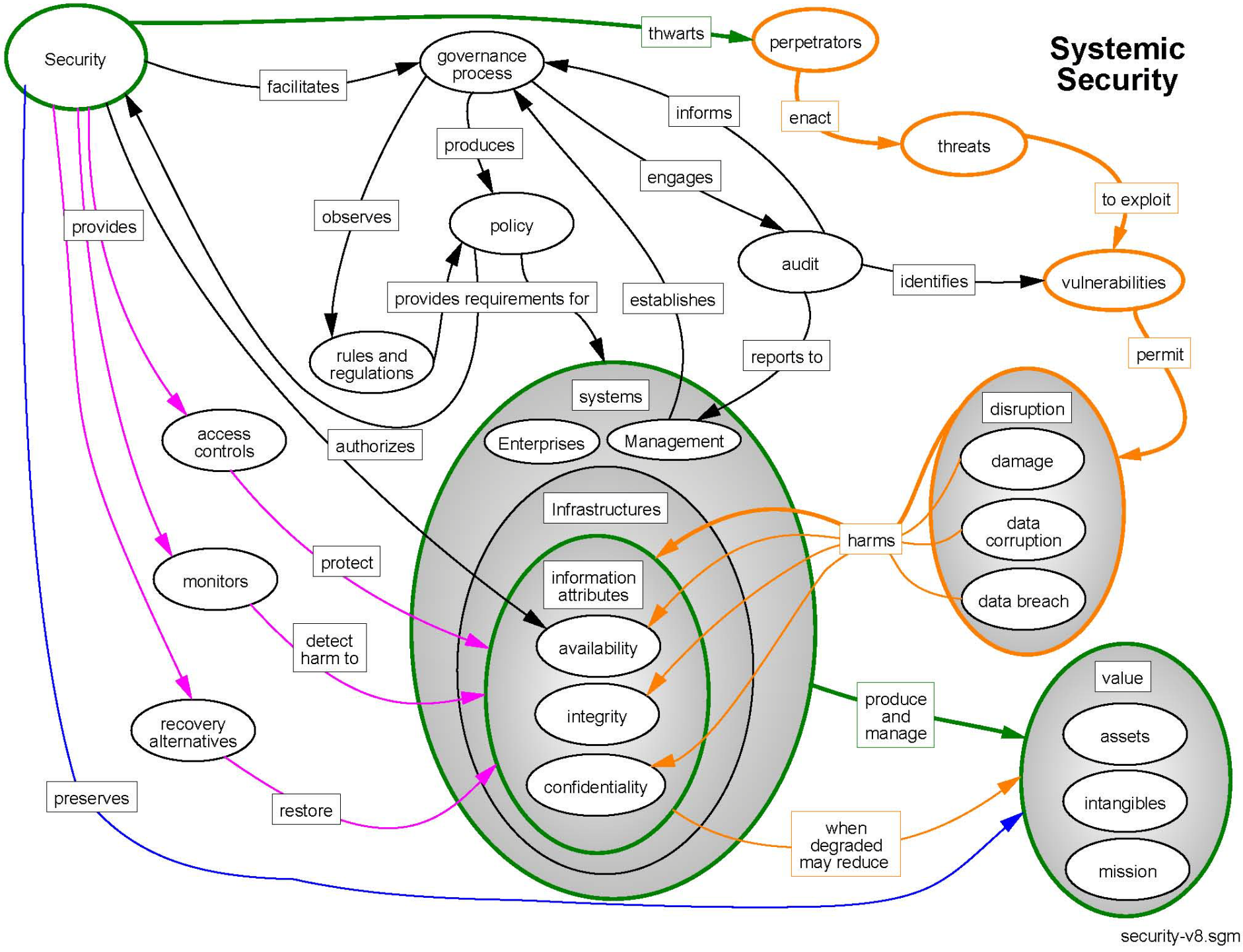
STEVENS Institute of Technology



# *Perimeter Security Pros and Cons*

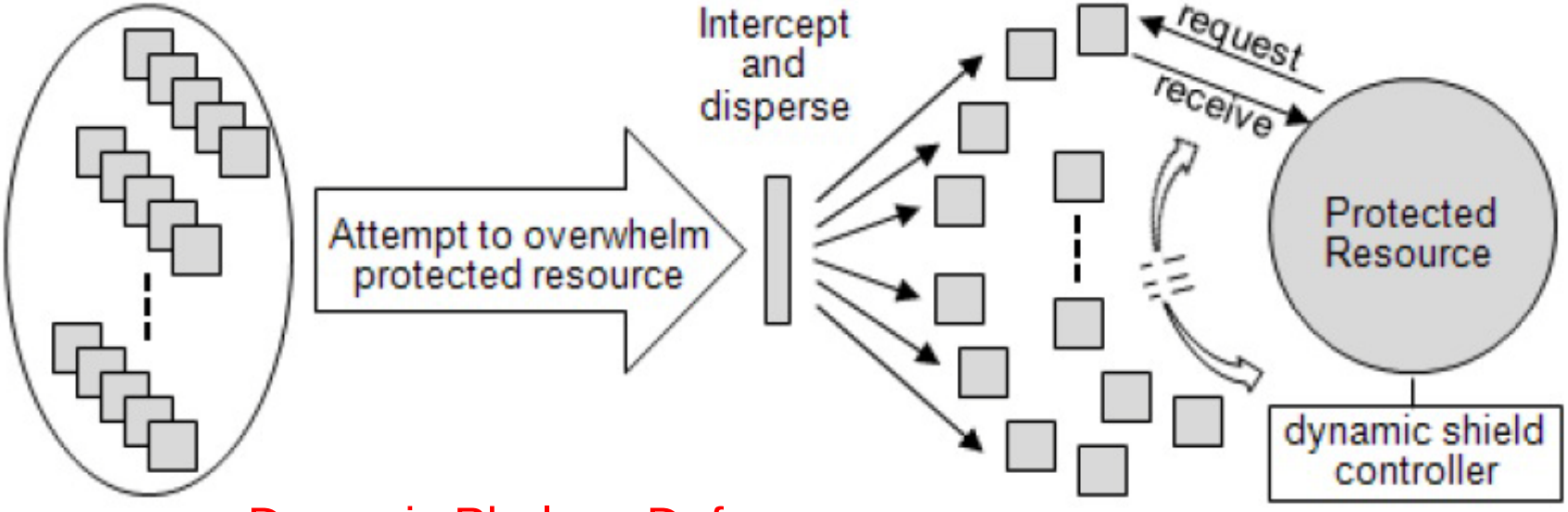
STEVENS Institute of Technology

| Defense in Depth | |
|---|---|
| **Pros** | **Cons** |
| Separates security development from time to market pressures | System-specific cyber risks are not considered in design |
| Can be added responsively | Lack of tools available for customized security solutions |
| Costs and support structures have economy of scale | Security workforce misappropriates risk reduction |
| Administrative methods and training are readily available | Attack and supply chain exploits are easily transferable |
| Supported by standardized sets of best practices | Solutions ignore integration issues |

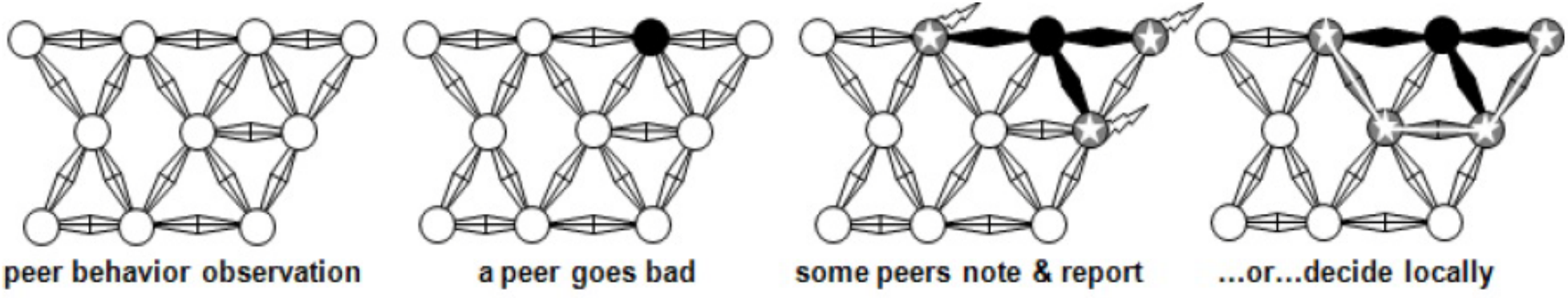



**Systemigram software from: Boardman and Sauser, Systems Thinking: Coping with 21st century problems, Taylor & Francis, 2008.**

# Situational Pattern Examples



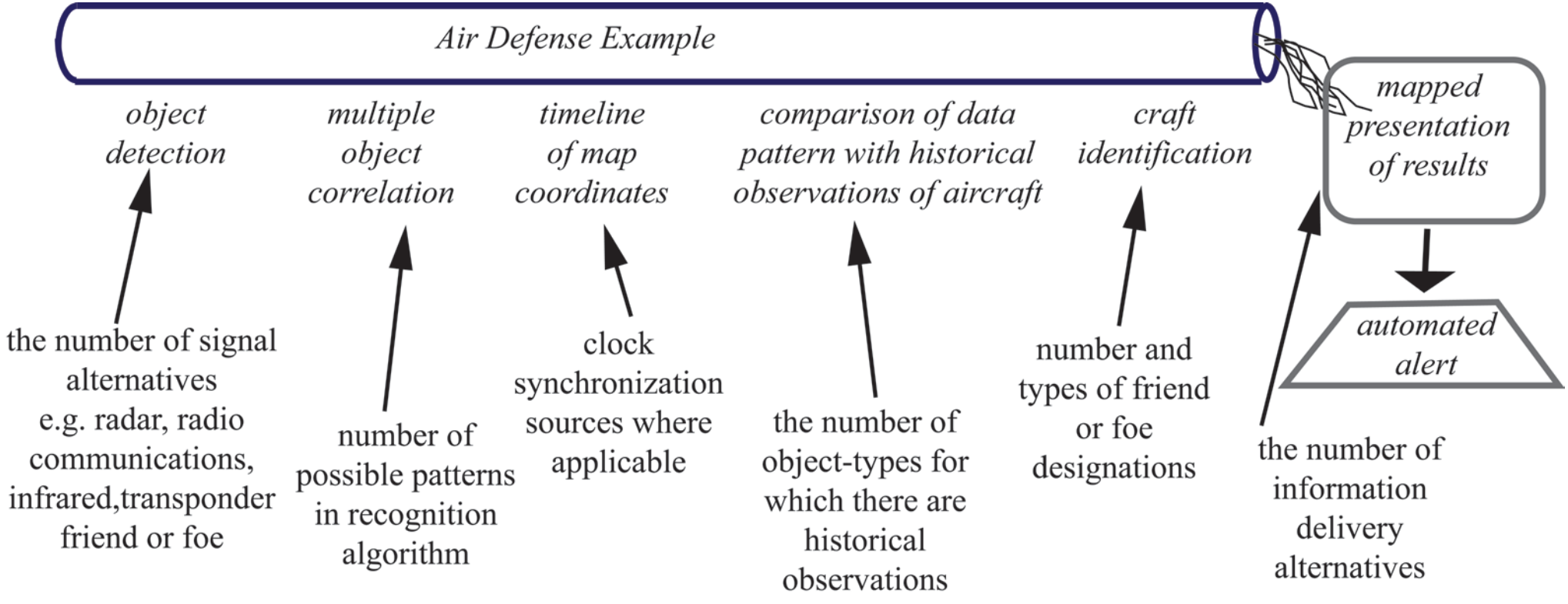

»Dynamic Phalanx Defense




»Peer Behavior Monitoring

*Source: Dove and Shirey, On Discovery and Display of Agile Security Patterns, CSER, 2010,*

# Architectural Patterns




*Source: Bayuk and Horowitz, SERC 2010*


Create a ***definition of systems security*** that allows researchers to identify problems whose solution would significantly improve enterprise security posture. This definition would evolve and be the thread that links all other research areas to a common goal.

Utilize the evolving security definition and framework to define ways to ***measure security effectiveness***. The area will help define measurable attributes that reflect properties of a secure system. It should provide taxonomy by which to distinguish between measureable attributes that are inherent in system design versus externally measured attributes such as success in achieving goals for attack resistance.

Define ways to map enterprise asset landscapes to threat landscapes in order to identity system security requirements. Identify holistic approaches to defending and recovering from disruptions. ***Devise frameworks*** with which to weigh decision factors related to security such as risk, costs, and time.

Develop innovative ways to ***improve the proficiency of the security engineering workforce*** ranging from systems architects who “design in” security based on security policy, to the operators whose decisions in the field reinforce or undermine security policy.

SYSTEMS ENGINEERING
Research Center

STEVENS
Institute of Technology

*www.sercuarc.org*

***Questions? Discussion?***

***Follow-up:***
***jennifer.bayuk@stevens.edu***