SYSTEMS ENGINEERING
Research Center

A US DoD University Affiliated Research Center

Systems Security Engineering

Jennifer Bayuk
Stevens Institute of Technology
www.SERCuarc.org

SYSTEMS ENGINEERING
Research Center
A US DoD University Affiliated Research Center

Security Systems Thinking

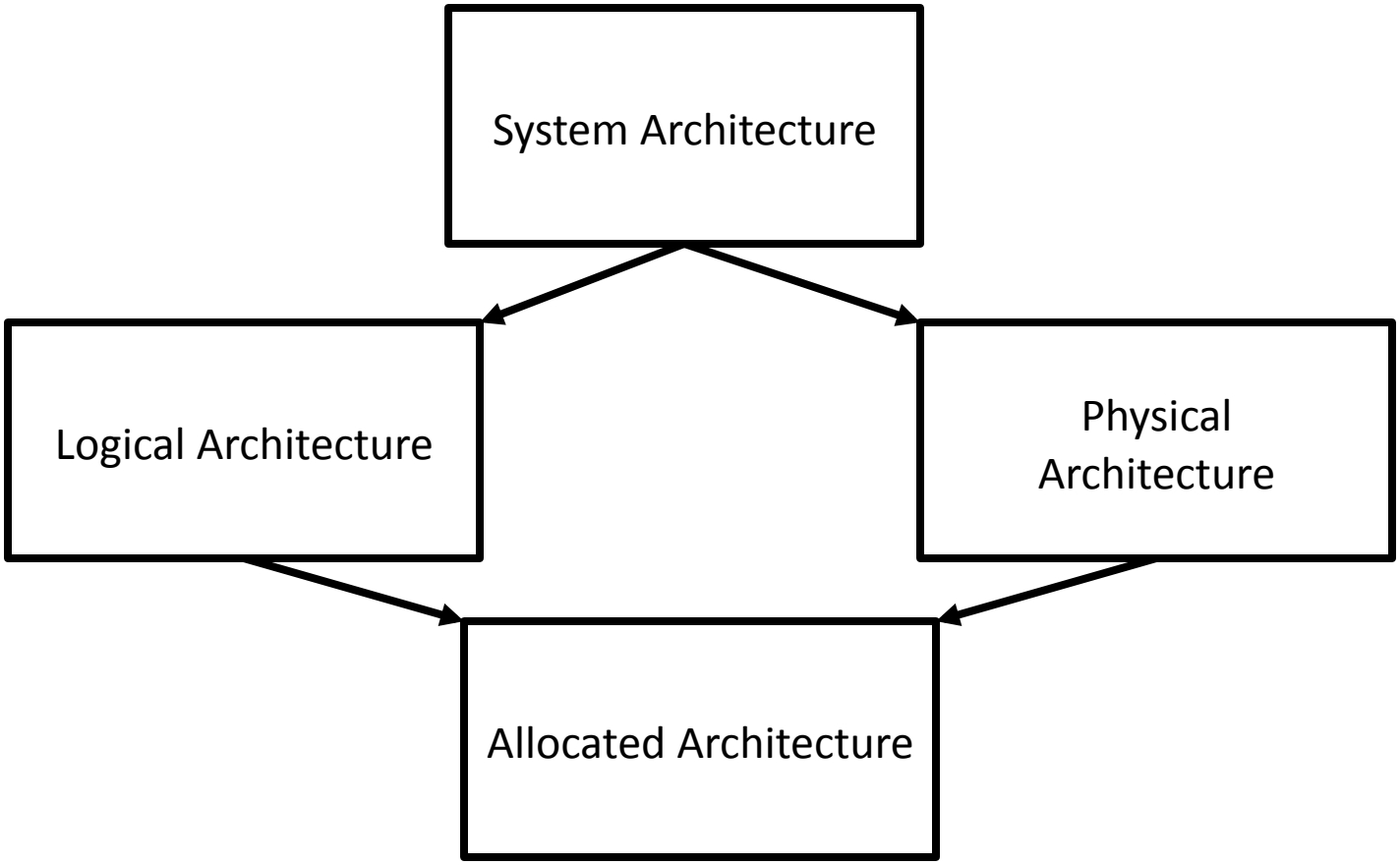
Source: J. Boardman and B. Sauser, *Systems thinking: Coping with 21st century problems, Taylor & Francis, 2008.*

Advantages of the Engineering Approach

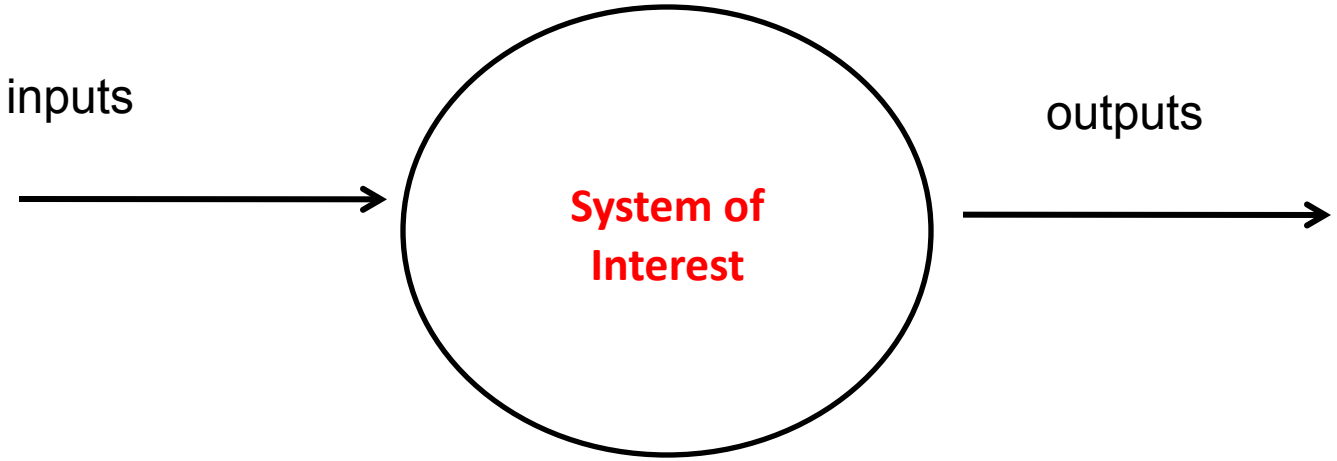
1. Manage Complexity
2. Top-down requirements tracing
3. Black box modeling
4. Logical flow analysis
5. Documentation
6. Peer Review
7. Detailed Communication

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

Systems Concepts



Systems Engineering



System Engineering Requirements Breakdown

1. **Functional**

2. **Interface**

3. **System-wide – "ilities"**

Systems security engineering required to know when it should be placed here.

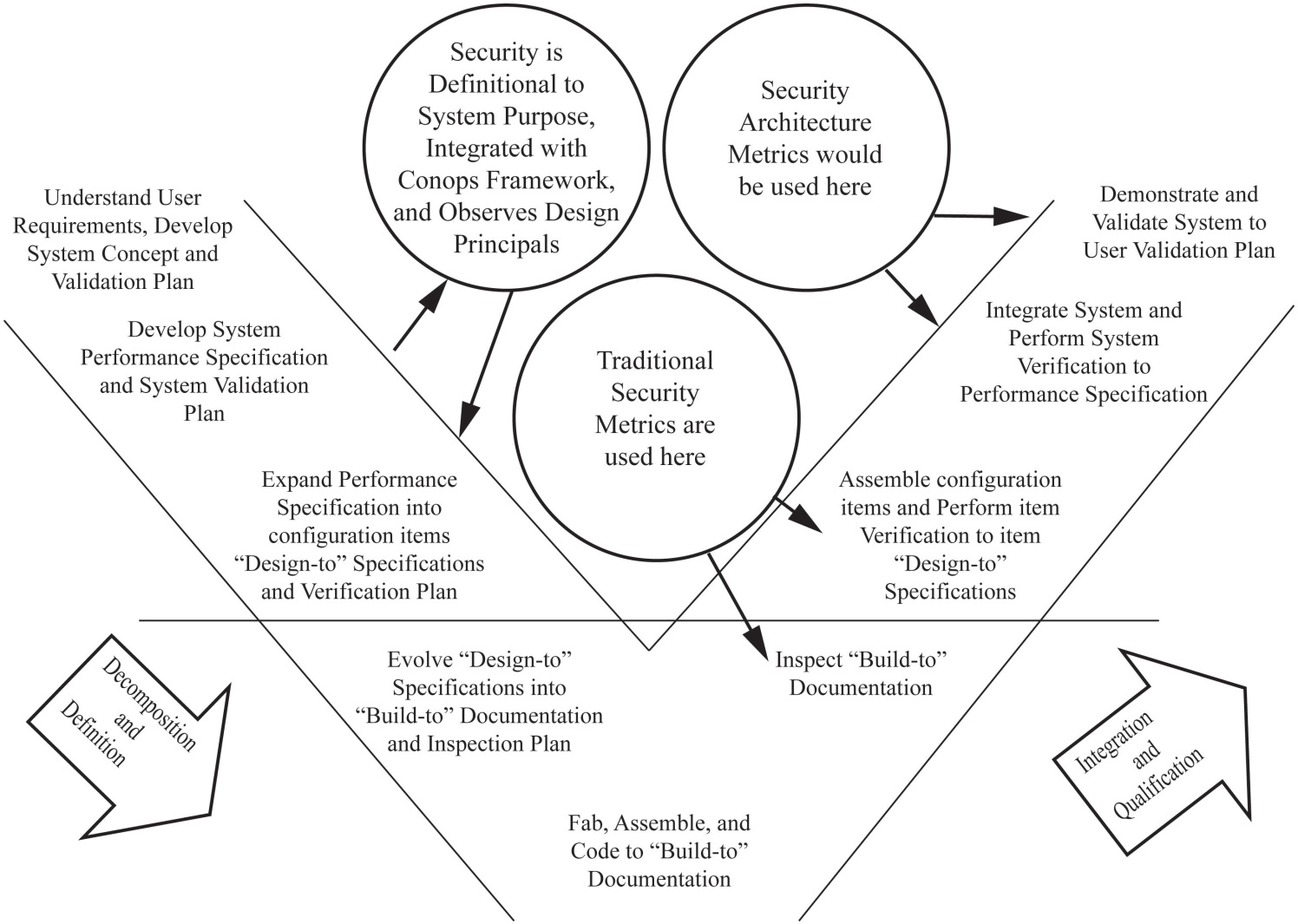
Security vulnerabilities are frequently introduced here.

Systems engineering literature traditionally places security here.

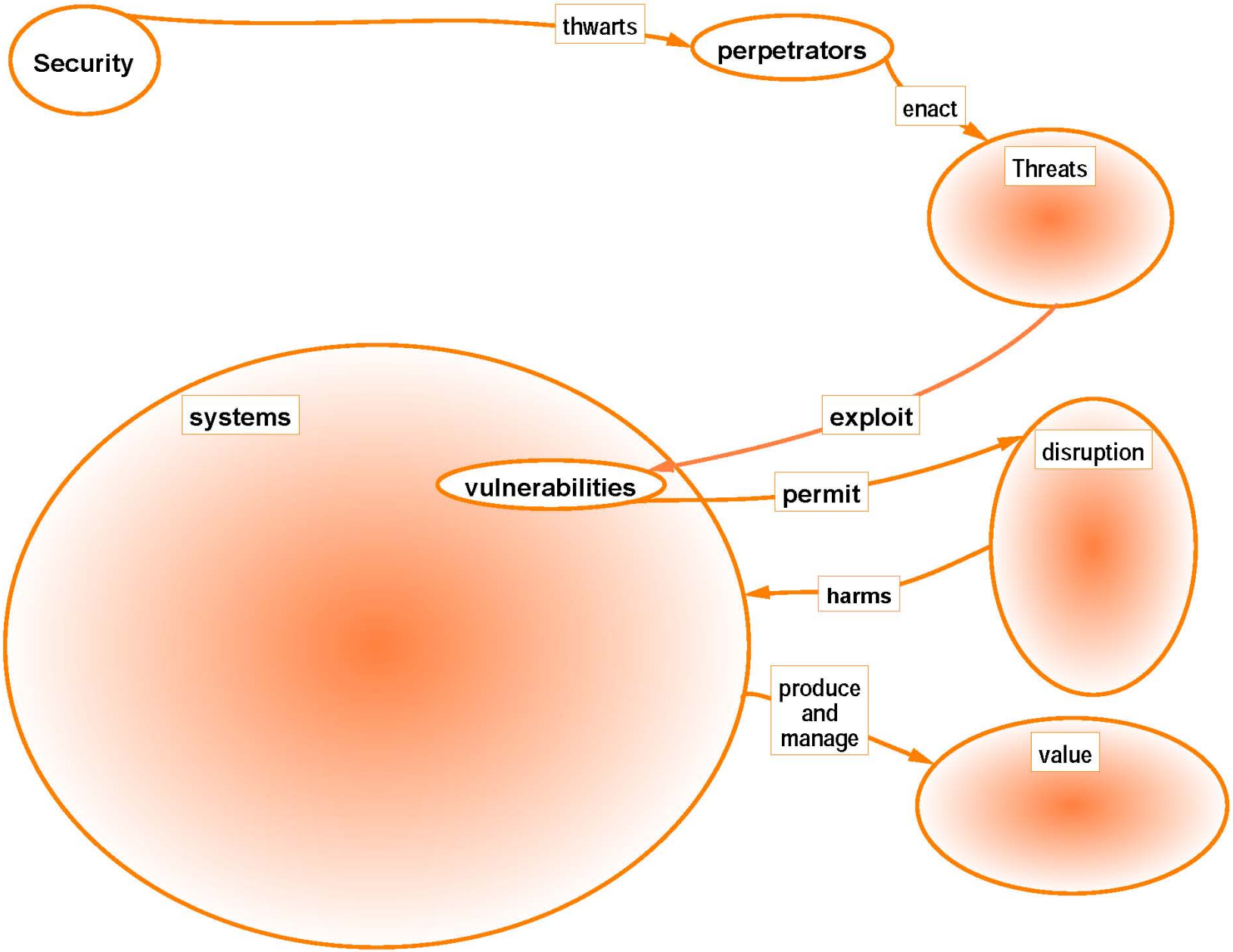
Source: Buede, *The engineering design of systems, models and methods, Wiley, 2009*

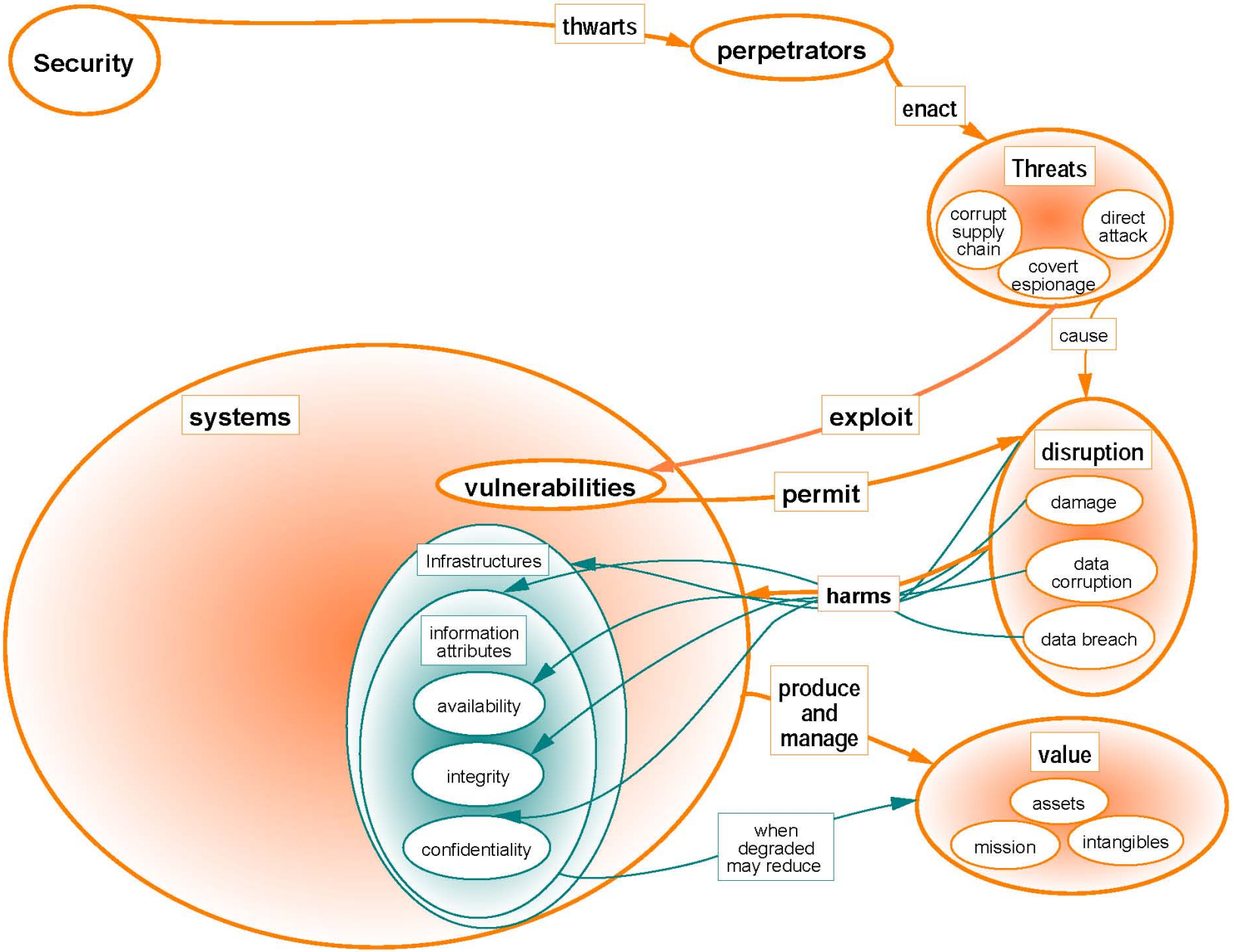
SYSTEMS ENGINEERING
Research Center
A US DoD University Affiliated Research Center

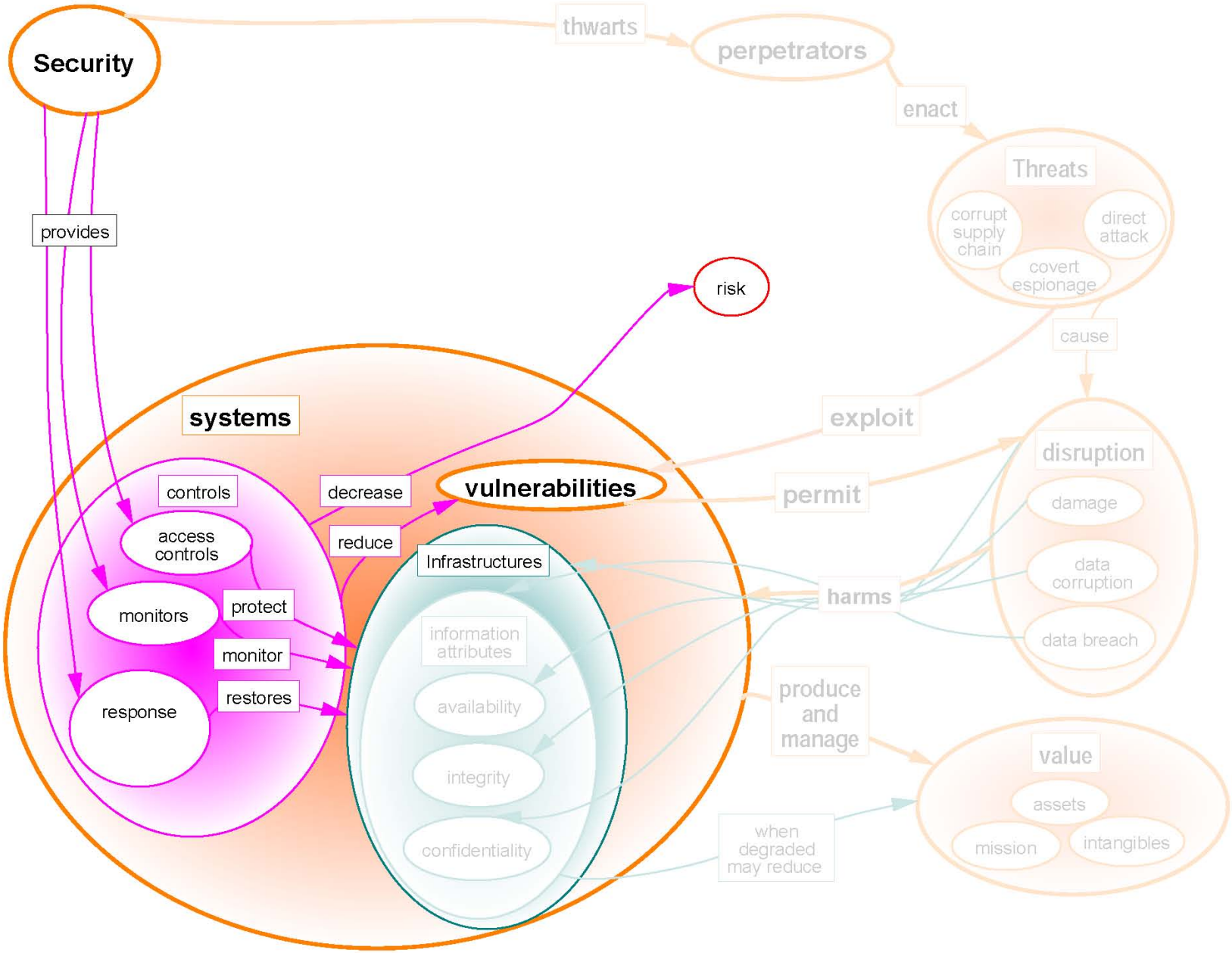
The Vee Model

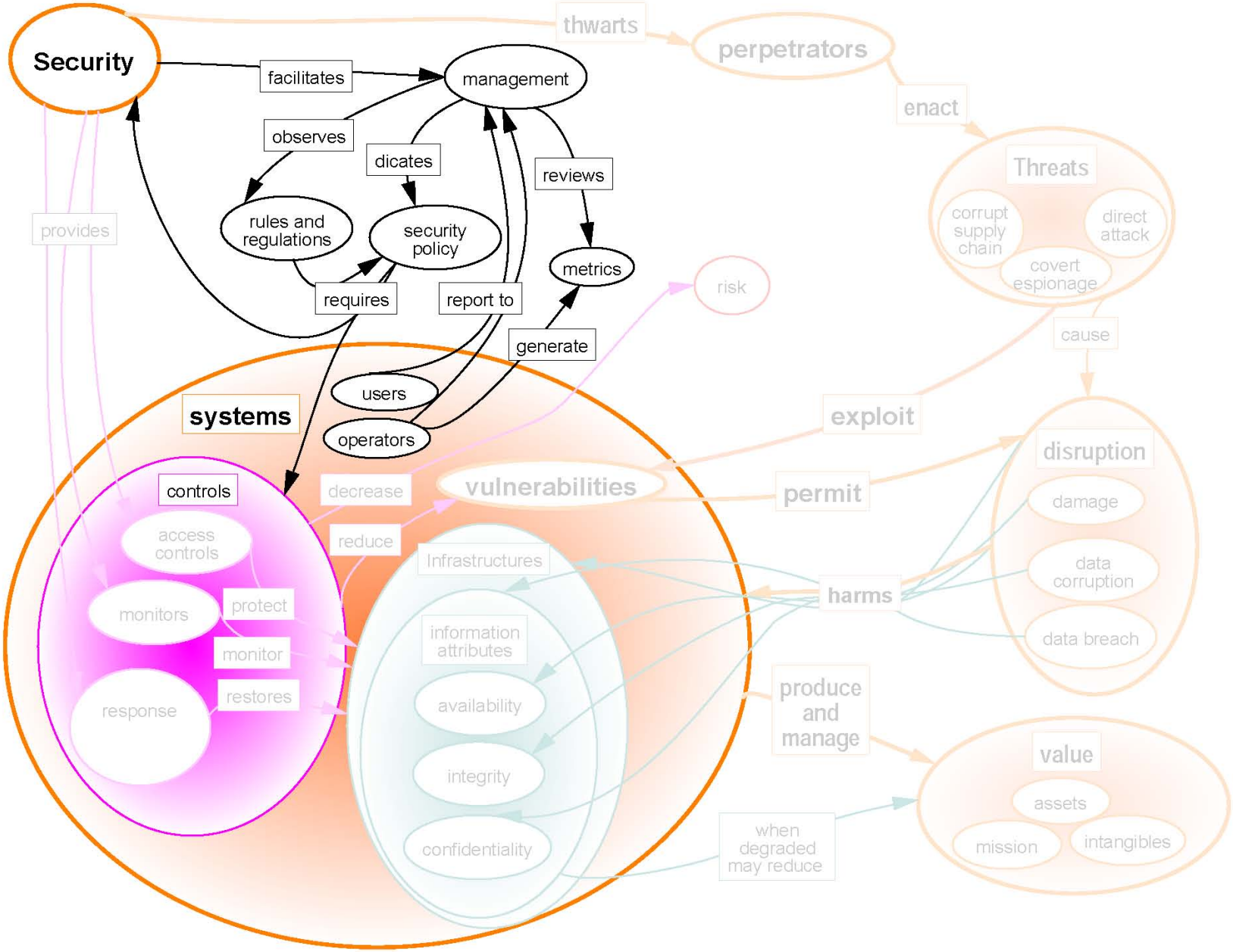


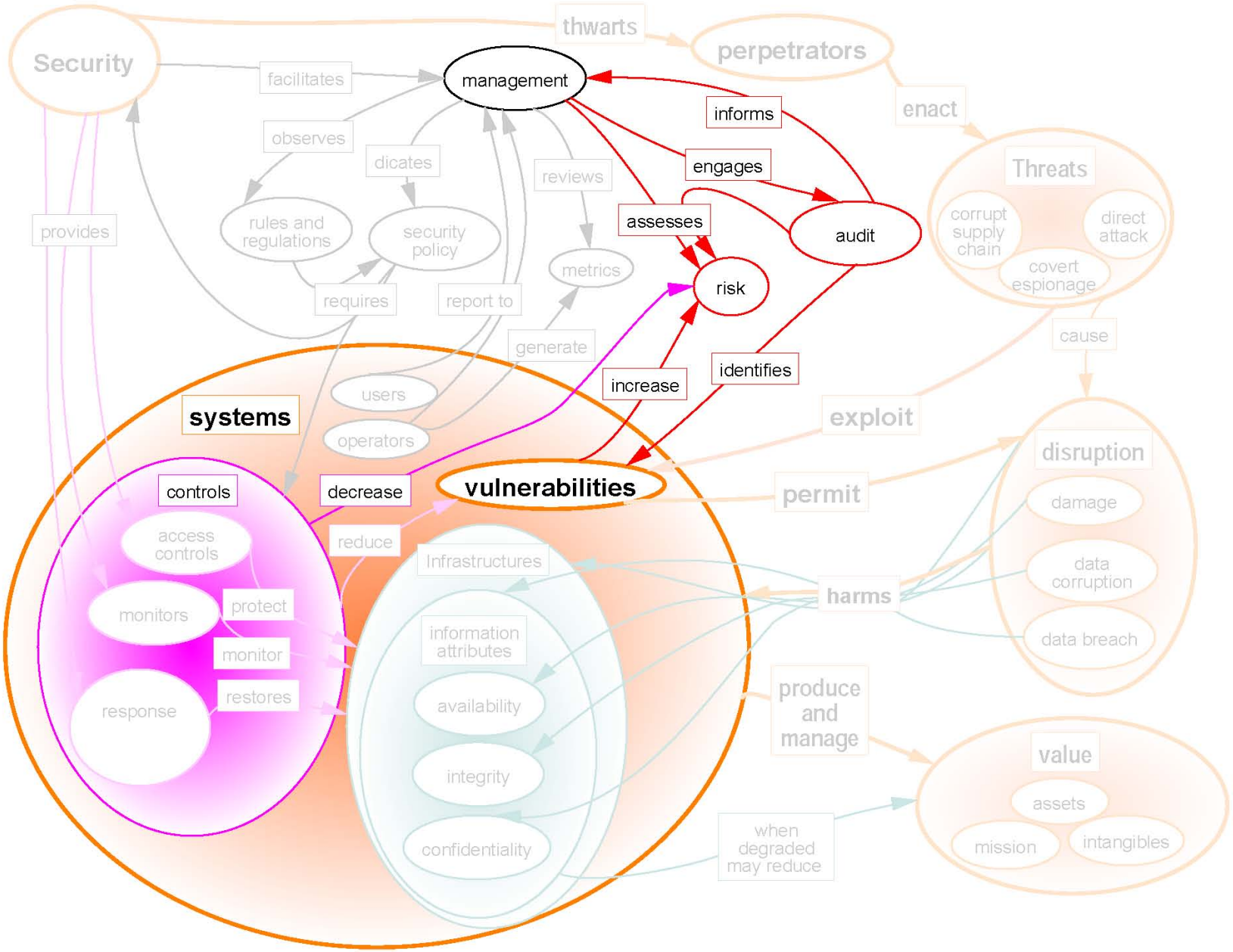
Source: Based on Buede and, Bayuk and Horowitz, An Architectural Systems Engineering Methodology for Addressing Cyber Security, Systems Engineering, 2011

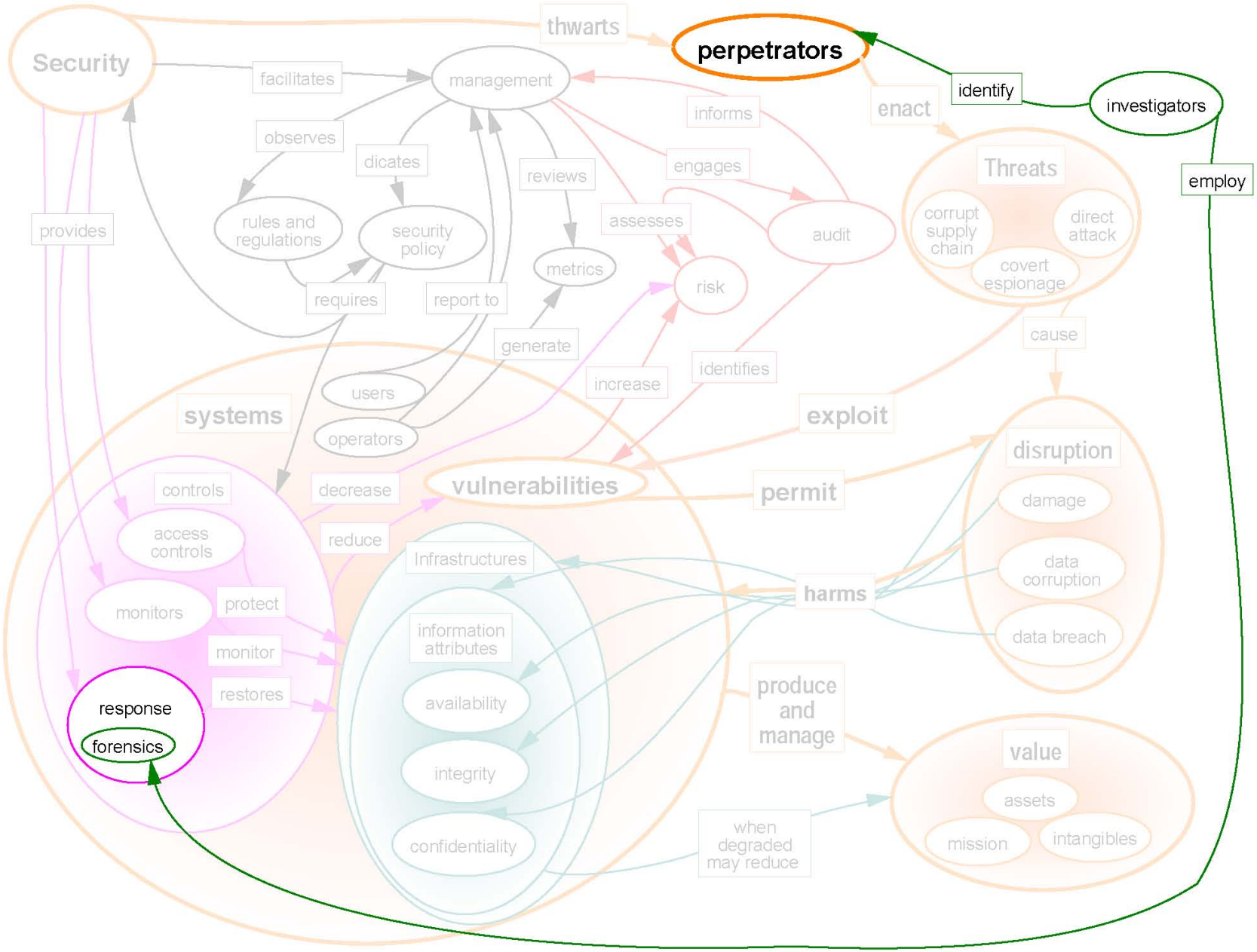

Security
thwarts
perpetrators
enact
Threats
systems
exploit
vulnerabilities
permit
disruption
harms
produce
and
manage
value

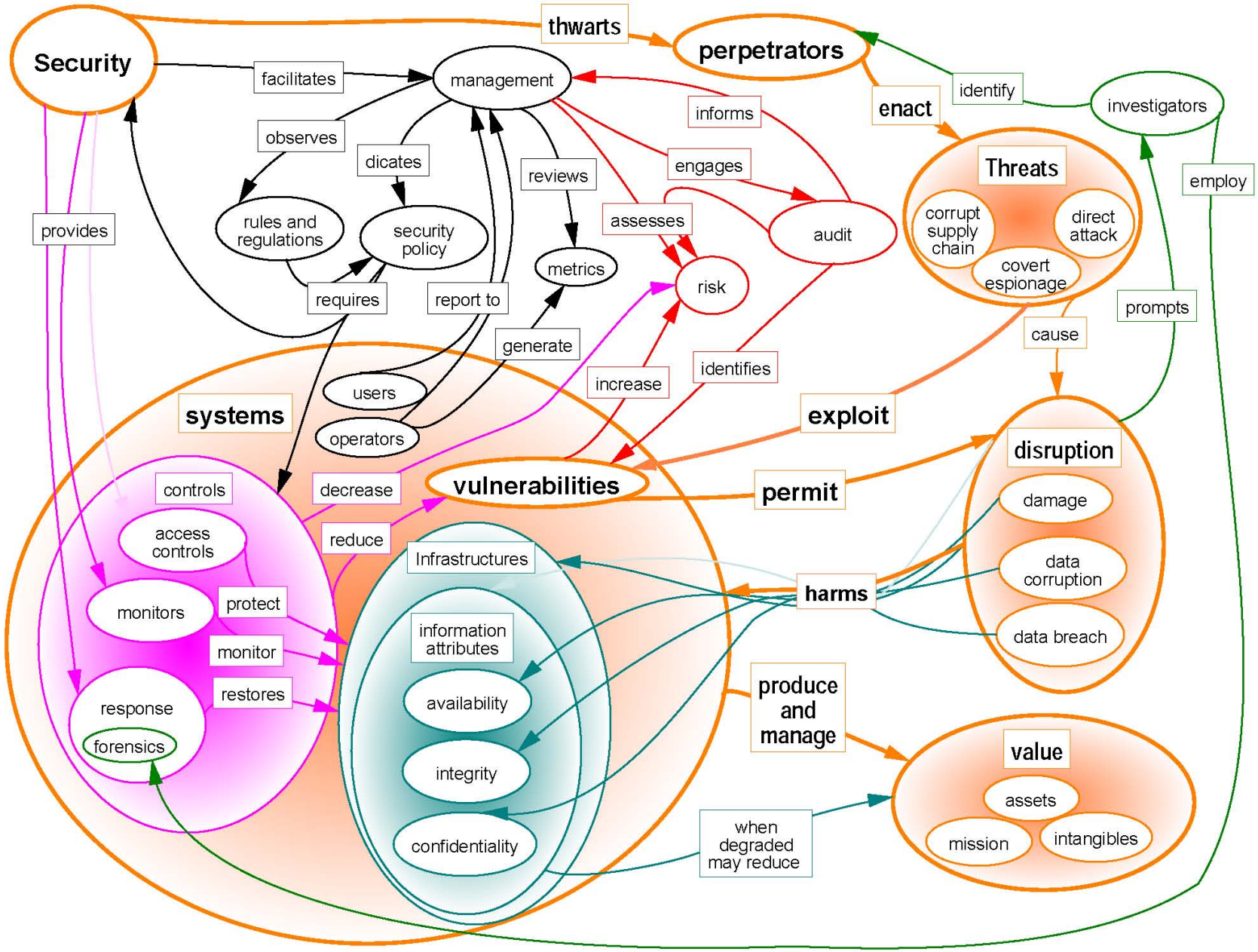

Security
thwarts
perpetrators
enact
Threats
corrupt supply chain
direct attack
covert espionage
cause
systems
exploit
vulnerabilities
permit
disruption
damage
data corruption
data breach
Infrastructures
information attributes
availability
integrity
confidentiality
harms
produce and manage
value
assets
mission
intangibles
when degraded may reduce


Security
thwarts
perpetrators
enact
Threats
corrupt supply chain
direct attack
covert espionage
provides
risk
cause
systems
exploit
disruption
controls
decrease
vulnerabilities
permit
damage
access controls
reduce
Infrastructures
data corruption
monitors
protect
harms
information attributes
monitor
data breach
restores
produce and manage
response
availability
value
integrity
assets
when degraded may reduce
confidentiality
mission
intangibles

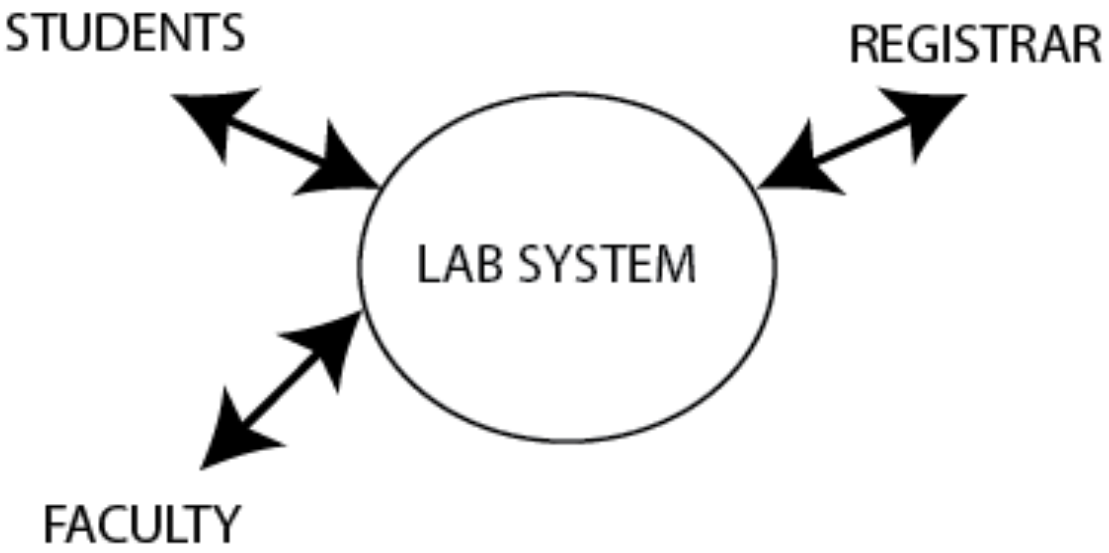

Security
facilitates
management
observes
dicates
reviews
rules and regulations
security policy
metrics
requires
report to
generate
users
operators
systems
controls
access controls
monitors
protect
monitor
restores
response
decrease
reduce
vulnerabilities
Infrastructures
information attributes
availability
integrity
confidentiality
provides
thwarts
perpetrators
enact
Threats
corrupt supply chain
direct attack
covert espionage
cause
risk
exploit
permit
harms
disruption
damage
data corruption
data breach
produce and manage
value
assets
mission
intangibles
when degraded may reduce


Security
thwarts
perpetrators
facilitates
management
enact
informs
observes
dicates
reviews
engages
Threats
corrupt supply chain
direct attack
covert espionage
provides
rules and regulations
security policy
assesses
audit
metrics
risk
requires
report to
generate
cause
identifies
increase
users
systems
operators
exploit
disruption
controls
decrease
vulnerabilities
permit
damage
access controls
reduce
Infrastructures
data corruption
monitors
protect
harms
information attributes
monitor
data breach
restores
response
availability
produce and manage
integrity
value
assets
confidentiality
when degraded may reduce
mission
intangibles

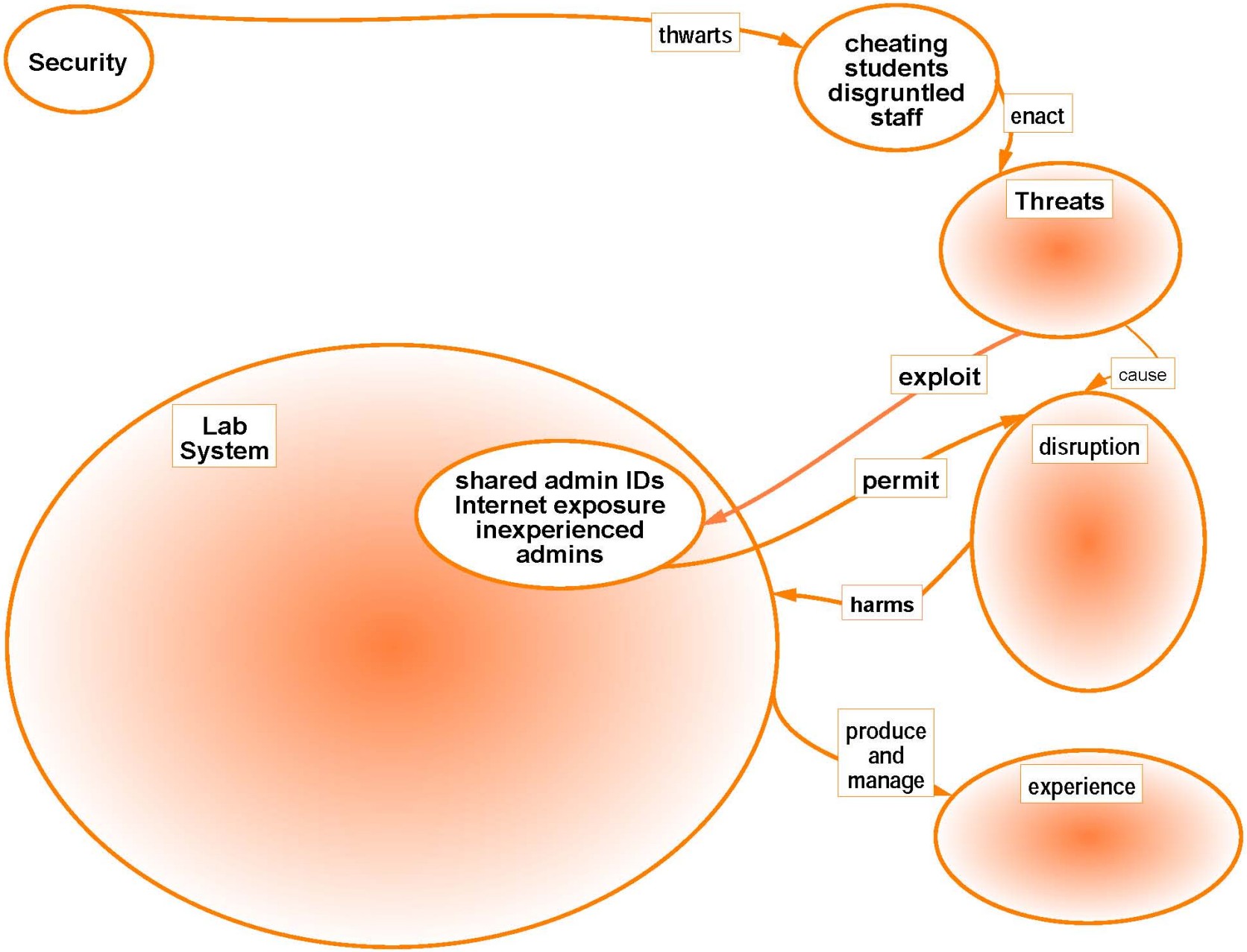

Security
thwarts
perpetrators
facilitates
management
identify
investigators
enact
informs
observes
dicates
reviews
engages
Threats
employ
provides
rules and regulations
security policy
assesses
audit
corrupt supply chain
direct attack
covert espionage
metrics
risk
requires
report to
generate
cause
identifies
increase
users
operators
systems
exploit
disruption
controls
decrease
vulnerabilities
permit
damage
access controls
reduce
Infrastructures
data corruption
monitors
protect
harms
information attributes
monitor
data breach
restores
response
forensics
availability
produce and manage
value
integrity
assets
confidentiality
when degraded may reduce
mission
intangibles

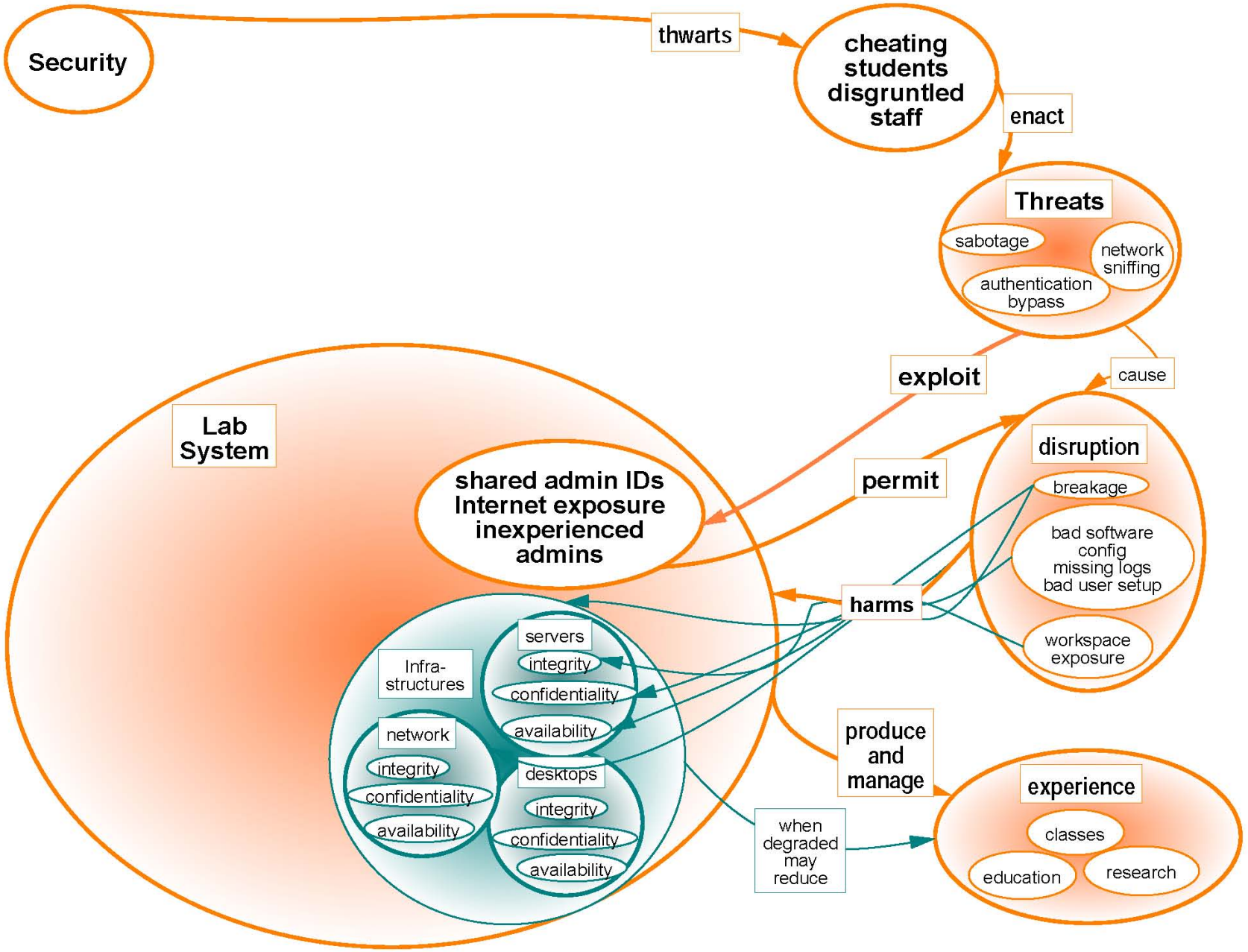

Security
thwarts
perpetrators
facilitates
management
observes
dicates
reviews
informs
engages
enact
identify
investigators
employ
provides
rules and regulations
security policy
assesses
audit
Threats
corrupt supply chain
direct attack
covert espionage
metrics
risk
requires
report to
generate
prompts
cause
users
operators
increase
identifies
systems
exploit
disruption
controls
decrease
vulnerabilities
permit
damage
access controls
reduce
Infrastructures
data corruption
monitors
protect
harms
information attributes
data breach
monitor
restores
response
forensics
availability
produce and manage
integrity
value
assets
confidentiality
when degraded may reduce
mission
intangibles

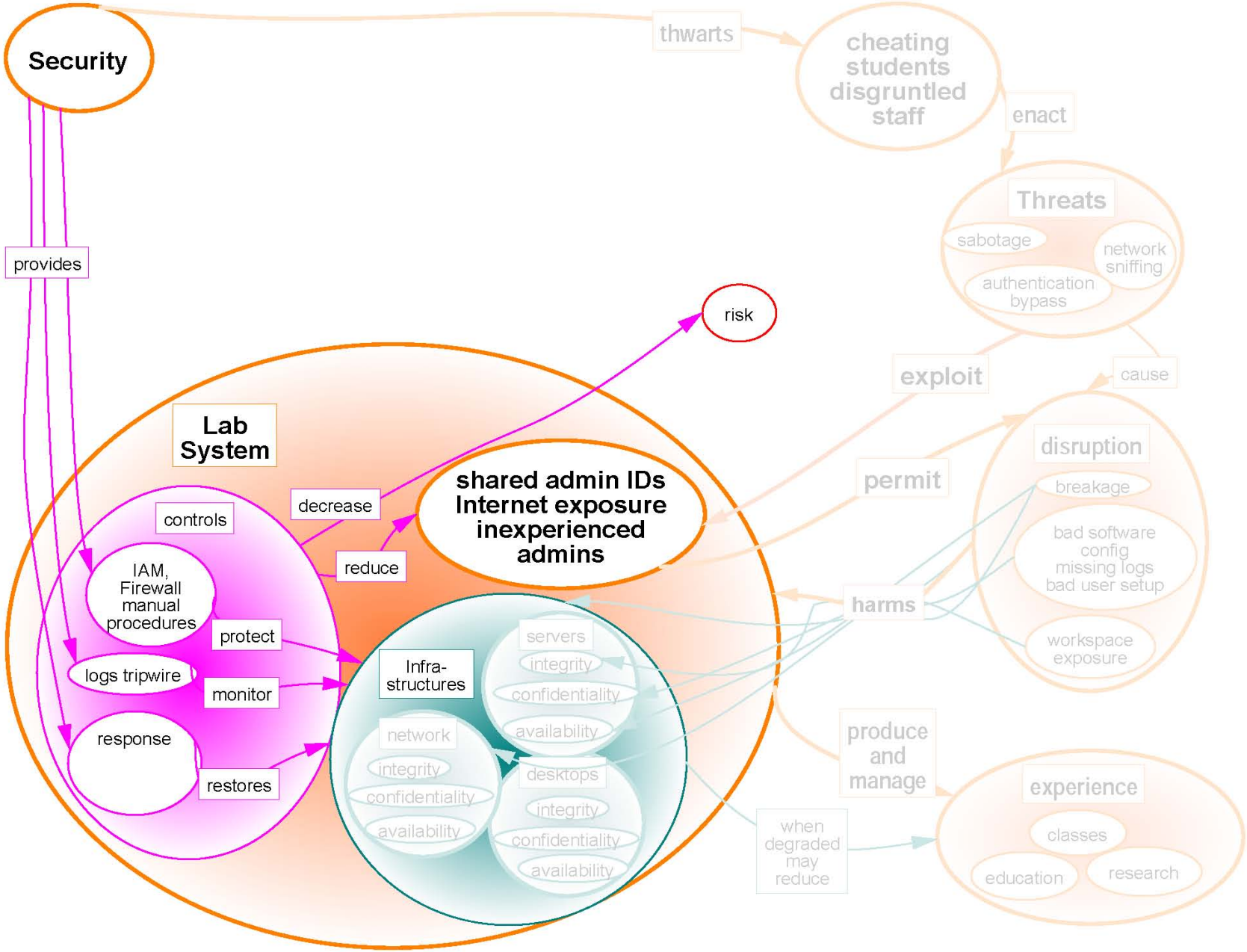
Example

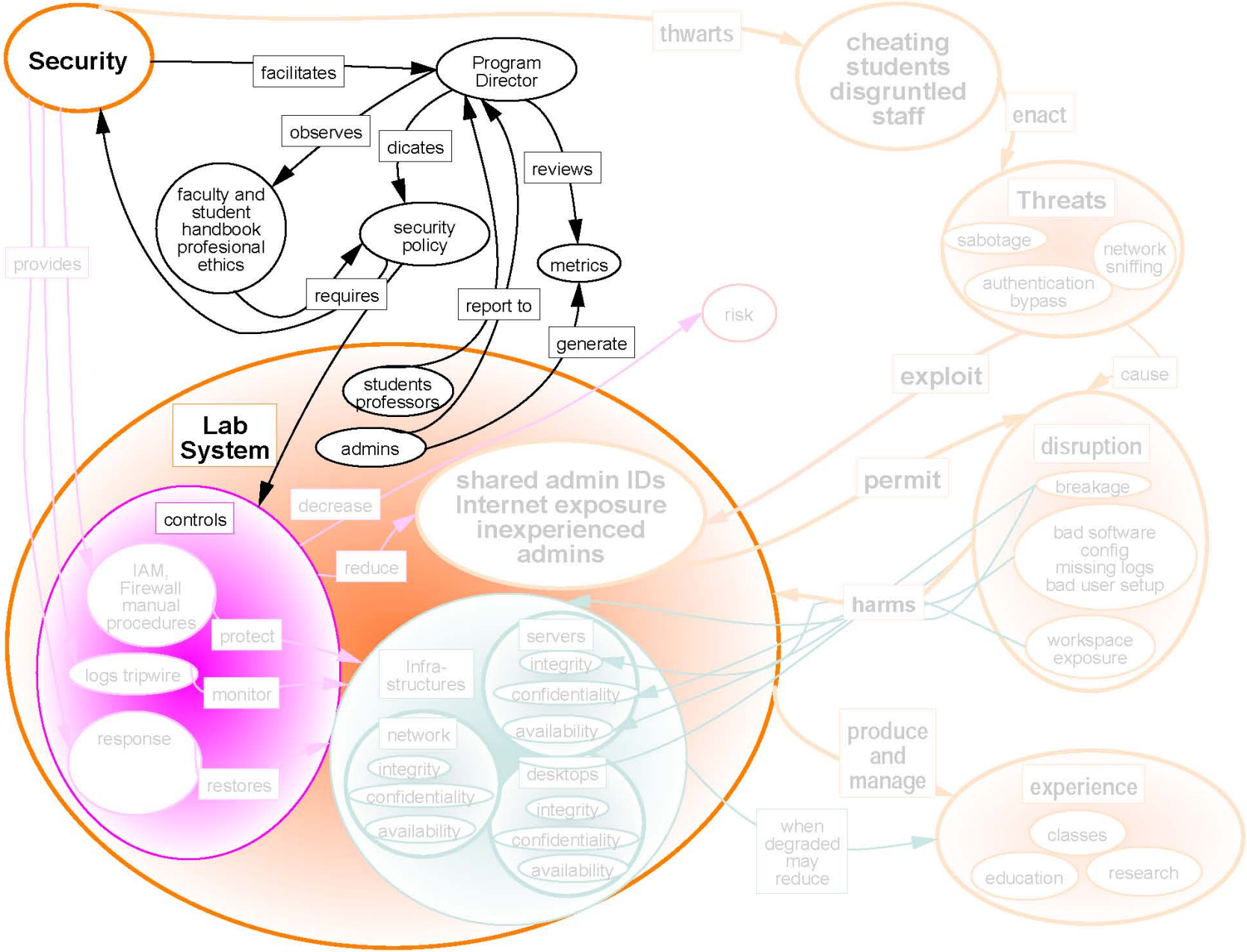


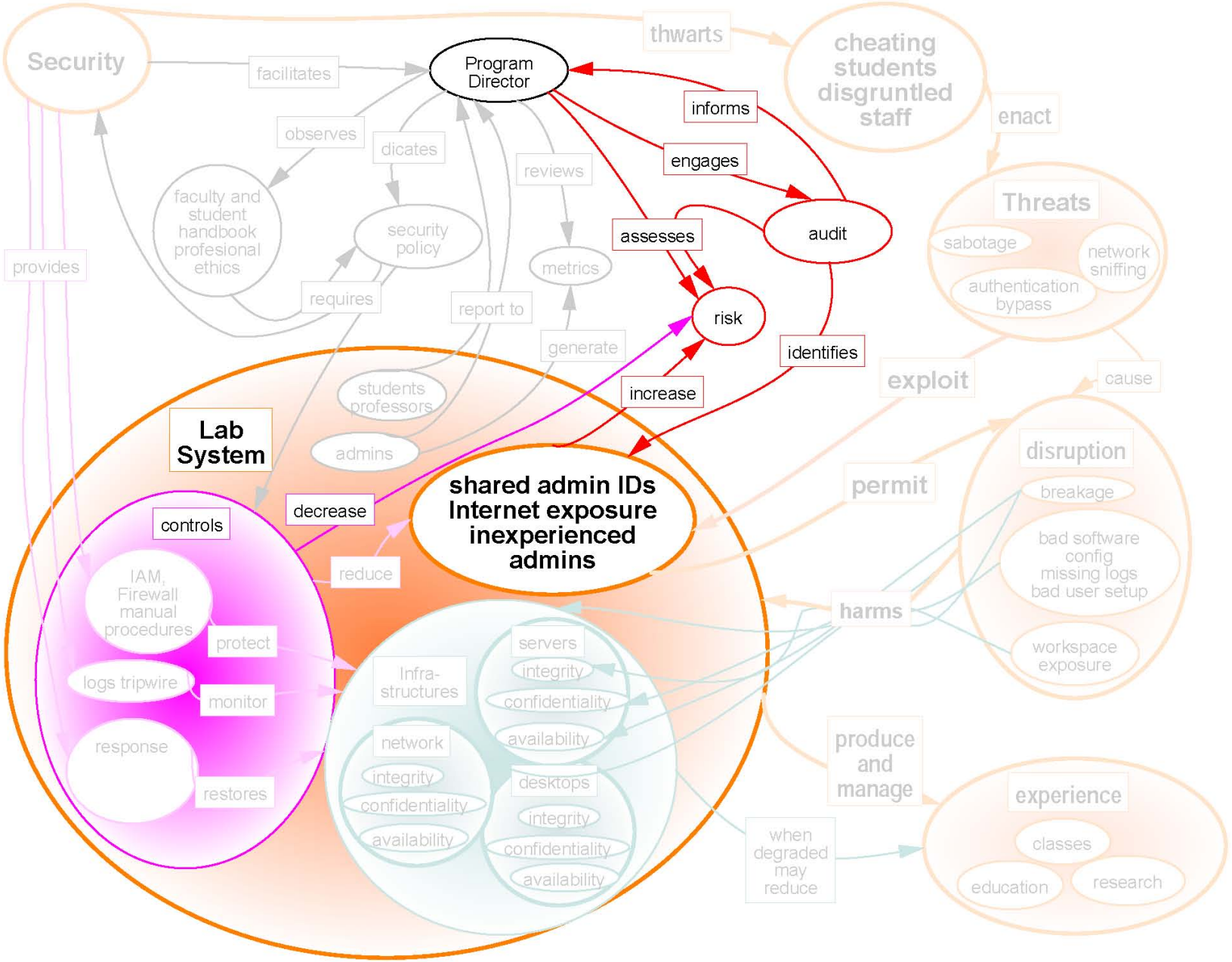
Source: Bayuk, SSE Lab Architecture Definition, 2010

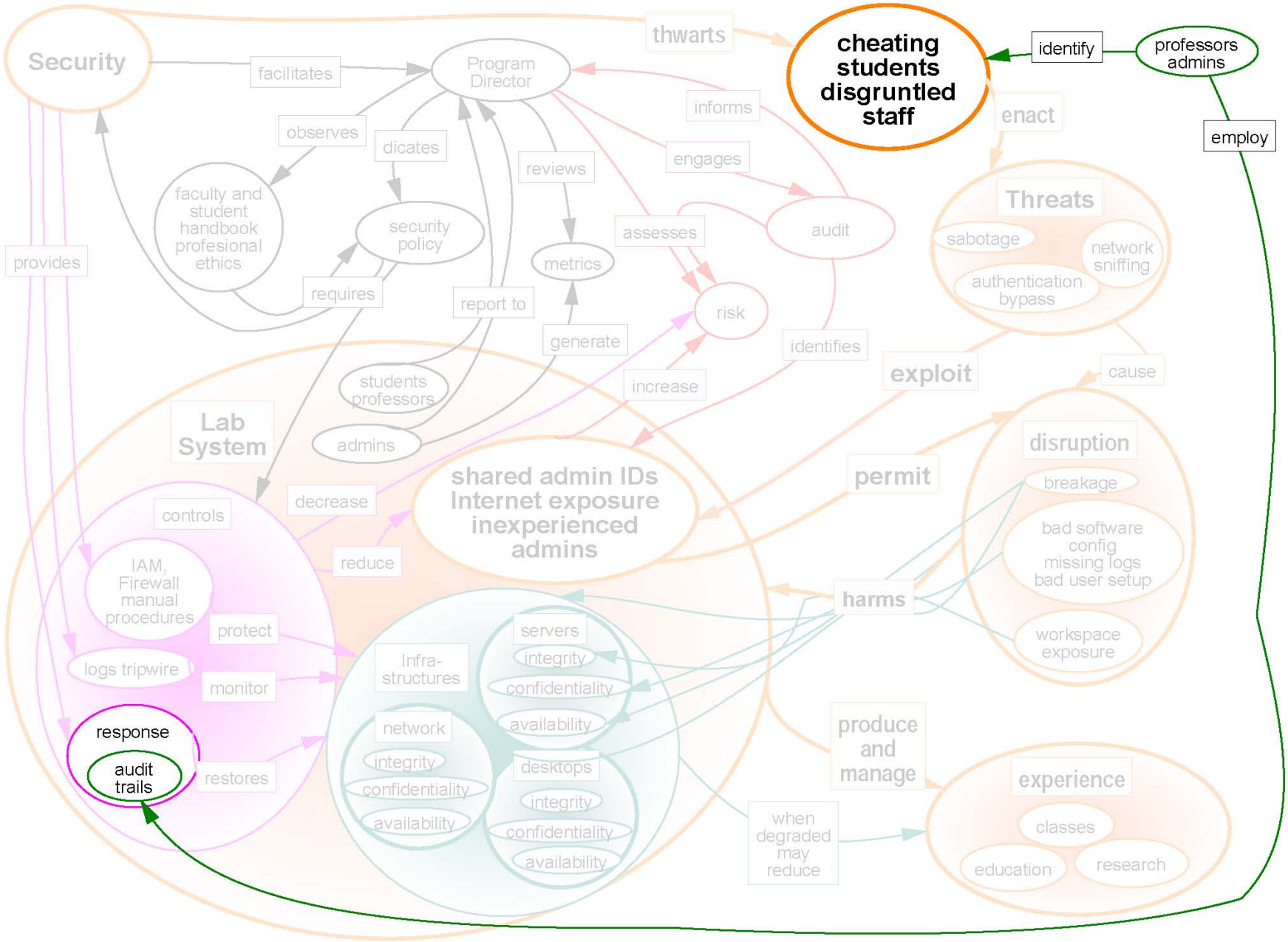

Security
thwarts
cheating
students
disgruntled
staff
enact
Threats
exploit
cause
Lab
System
shared admin IDs
Internet exposure
inexperienced
admins
permit
disruption
harms
produce
and
manage
experience

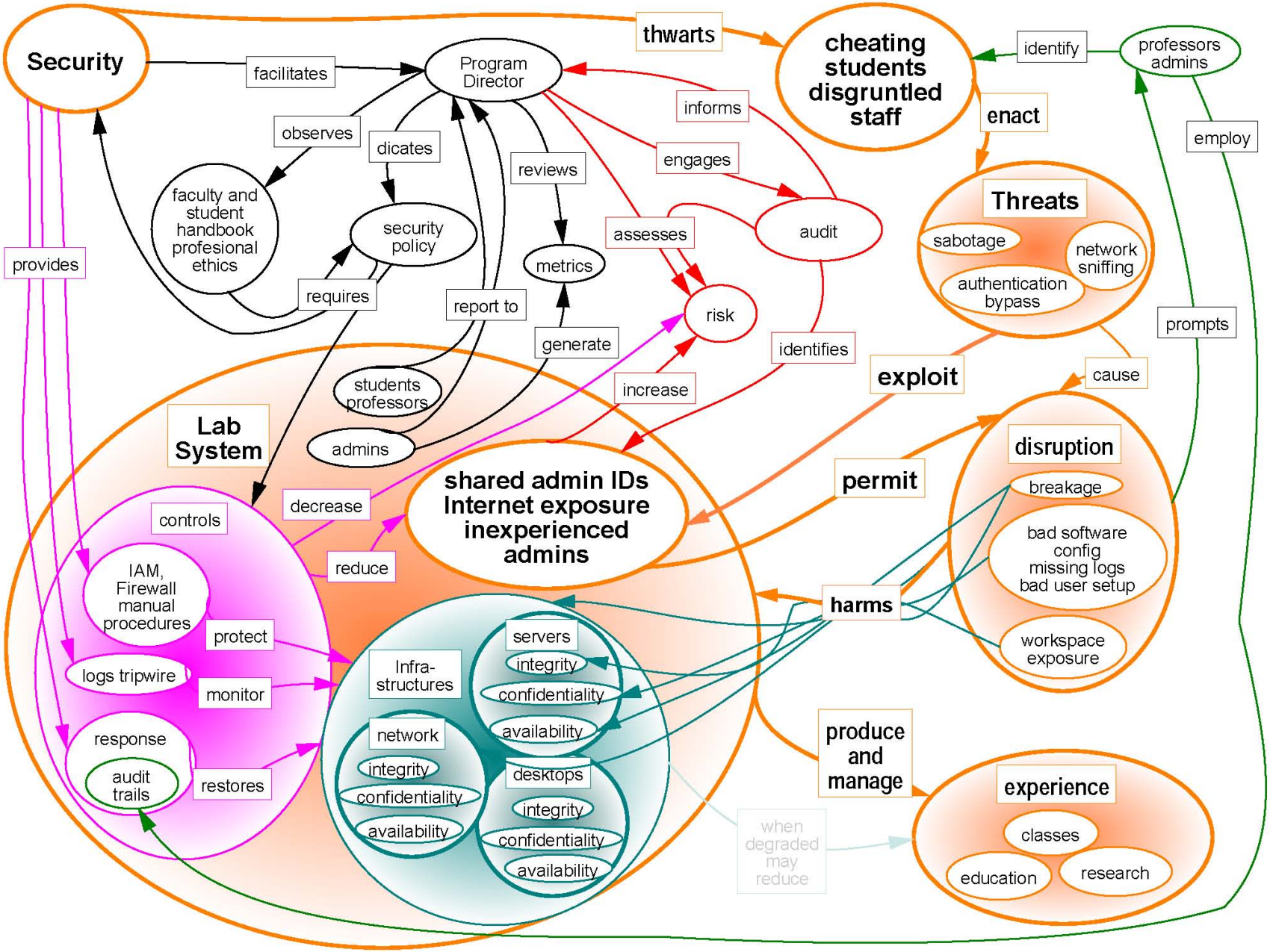

Security
thwarts
cheating
students
disgruntled
staff
enact
Threats
sabotage
network
sniffing
authentication
bypass
exploit
cause
Lab
System
shared admin IDs
Internet exposure
inexperienced
admins
permit
disruption
breakage
bad software
config
missing logs
bad user setup
workspace
exposure
harms
Infra-
structures
servers
integrity
confidentiality
availability
network
integrity
confidentiality
availability
desktops
integrity
confidentiality
availability
produce
and
manage
when
degraded
may
reduce
experience
classes
education
research


Security
thwarts
cheating
students
disgruntled
staff
enact
Threats
sabotage
network
sniffing
authentication
bypass
provides
risk
exploit
cause
Lab
System
shared admin IDs
Internet exposure
inexperienced
admins
disruption
breakage
bad software
config
missing logs
bad user setup
workspace
exposure
permit
controls
decrease
reduce
IAM,
Firewall
manual
procedures
protect
logs tripwire
monitor
response
restores
Infra-
structures
servers
integrity
confidentiality
availability
network
integrity
confidentiality
availability
desktops
integrity
confidentiality
availability
harms
produce
and
manage
when
degraded
may
reduce
experience
classes
education
research


Security
facilitates
Program Director
observes
dicates
reviews
faculty and student handbook profesional ethics
security policy
metrics
requires
report to
generate
students professors
admins
provides
Lab System
controls
IAM, Firewall manual procedures
protect
logs tripwire
monitor
response
restores
decrease
reduce
shared admin IDs Internet exposure inexperienced admins
Infra-structures
servers
integrity
confidentiality
availability
network
integrity
confidentiality
availability
desktops
integrity
confidentiality
availability
risk
thwarts
cheating students disgruntled staff
enact
Threats
sabotage
network sniffing
authentication bypass
exploit
cause
permit
disruption
breakage
bad software config missing logs bad user setup
workspace exposure
harms
produce and manage
when degraded may reduce
experience
classes
education
research

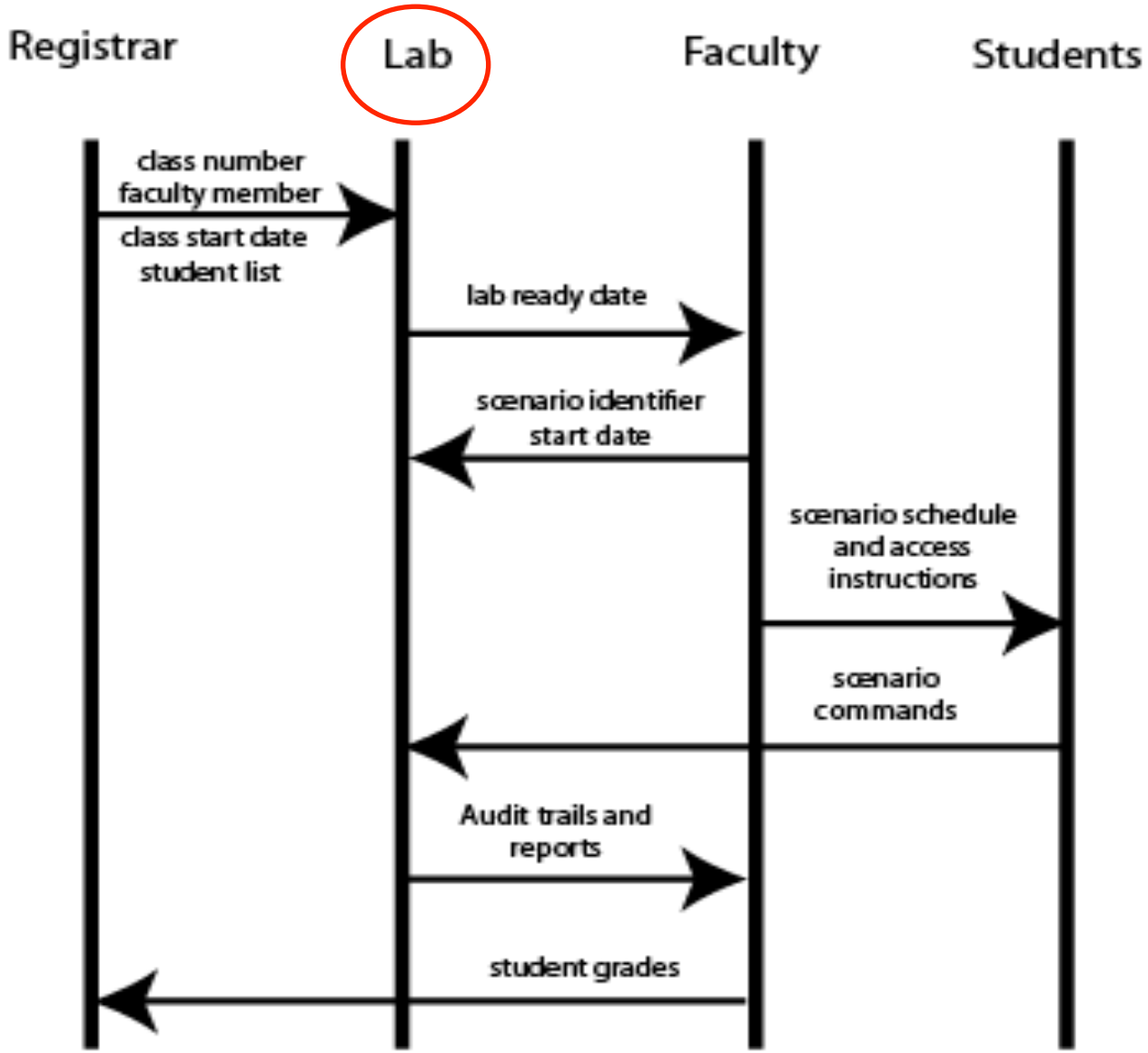

Security
facilitates
Program Director
thwarts
cheating students disgruntled staff
enact
informs
engages
observes
dicates
reviews
faculty and student handbook profesional ethics
security policy
metrics
assesses
audit
provides
requires
report to
risk
identifies
generate
increase
Threats
sabotage
network sniffing
authentication bypass
exploit
cause
students professors
admins
Lab System
shared admin IDs
Internet exposure
inexperienced admins
permit
disruption
breakage
bad software
config
missing logs
bad user setup
workspace exposure
decrease
controls
reduce
IAM, Firewall manual procedures
protect
logs tripwire
monitor
response
restores
Infra-structures
servers
integrity
confidentiality
availability
network
integrity
confidentiality
availability
desktops
integrity
confidentiality
availability
harms
produce and manage
when degraded may reduce
experience
classes
education
research


Security
thwarts
cheating students disgruntled staff
identify
professors admins
employ
facilitates
Program Director
informs
enact
observes
dicates
reviews
engages
faculty and student handbook profesional ethics
security policy
audit
Threats
sabotage
network sniffing
authentication bypass
provides
assesses
metrics
requires
report to
risk
generate
identifies
exploit
cause
students professors
admins
increase
Lab System
shared admin IDs Internet exposure inexperienced admins
permit
disruption
breakage
bad software config missing logs bad user setup
workspace exposure
decrease
controls
IAM, Firewall manual procedures
reduce
protect
logs tripwire
monitor
harms
servers
integrity
confidentiality
availability
Infra-structures
network
integrity
confidentiality
availability
desktops
integrity
confidentiality
availability
response
audit trails
restores
produce and manage
when degraded may reduce
experience
classes
education
research


Security
facilitates
Program Director
thwarts
cheating students disgruntled staff
identify
professors admins
employ
observes
dicates
reviews
informs
engages
enact
faculty and student handbook profesional ethics
security policy
metrics
audit
assesses
Threats
sabotage
network sniffing
authentication bypass
provides
requires
report to
risk
generate
identifies
prompts
exploit
cause
students professors
admins
Lab System
increase
shared admin IDs Internet exposure inexperienced admins
permit
disruption
breakage
bad software config missing logs bad user setup
workspace exposure
decrease
controls
reduce
IAM, Firewall manual procedures
protect
harms
logs tripwire
monitor
Infra-structures
servers
integrity
confidentiality
availability
response
audit trails
restores
network
integrity
confidentiality
availability
desktops
integrity
confidentiality
availability
produce and manage
when degraded may reduce
experience
classes
education
research

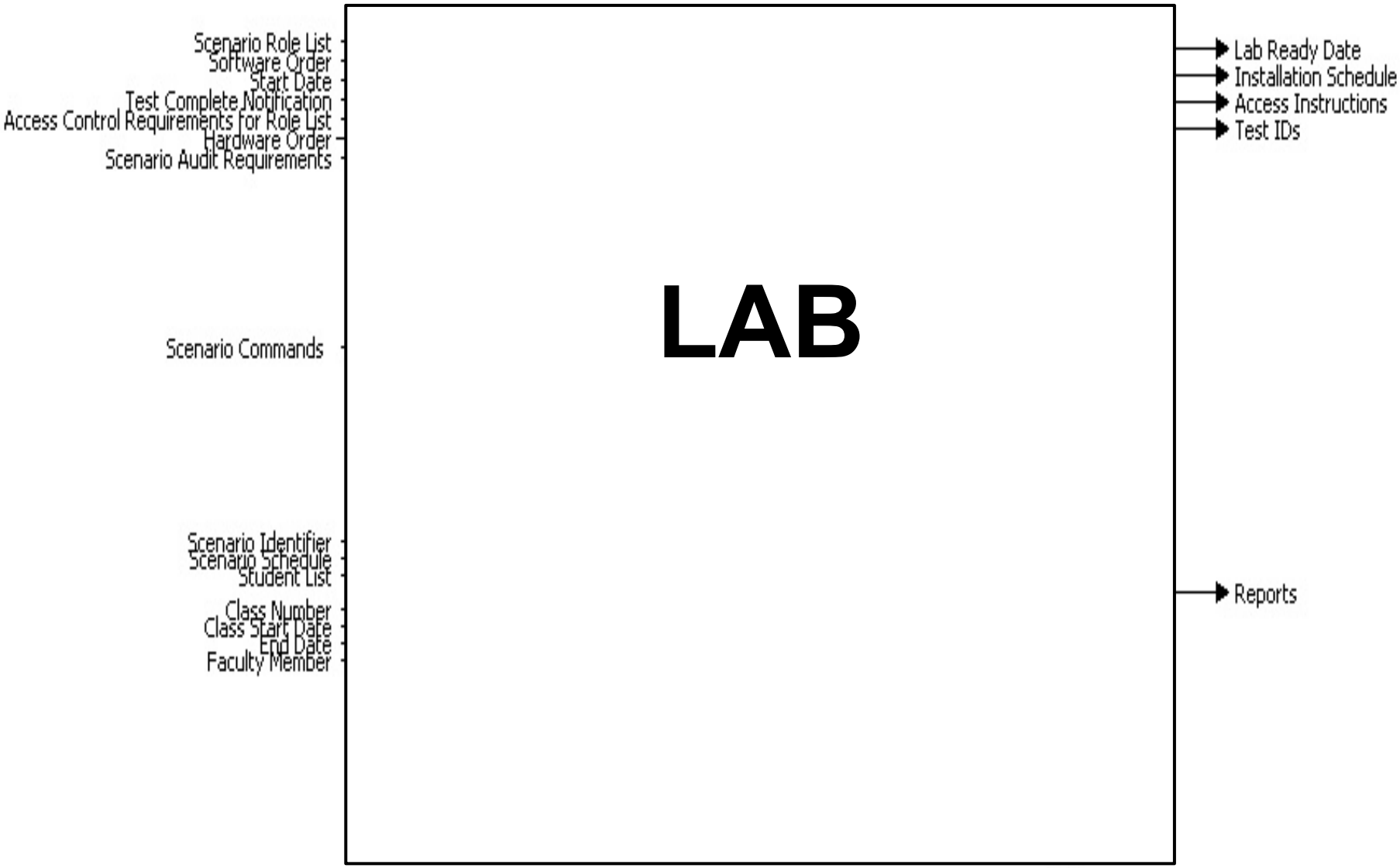
SYSTEMS ENGINEERING
Research Center

Requirements Gathering Example



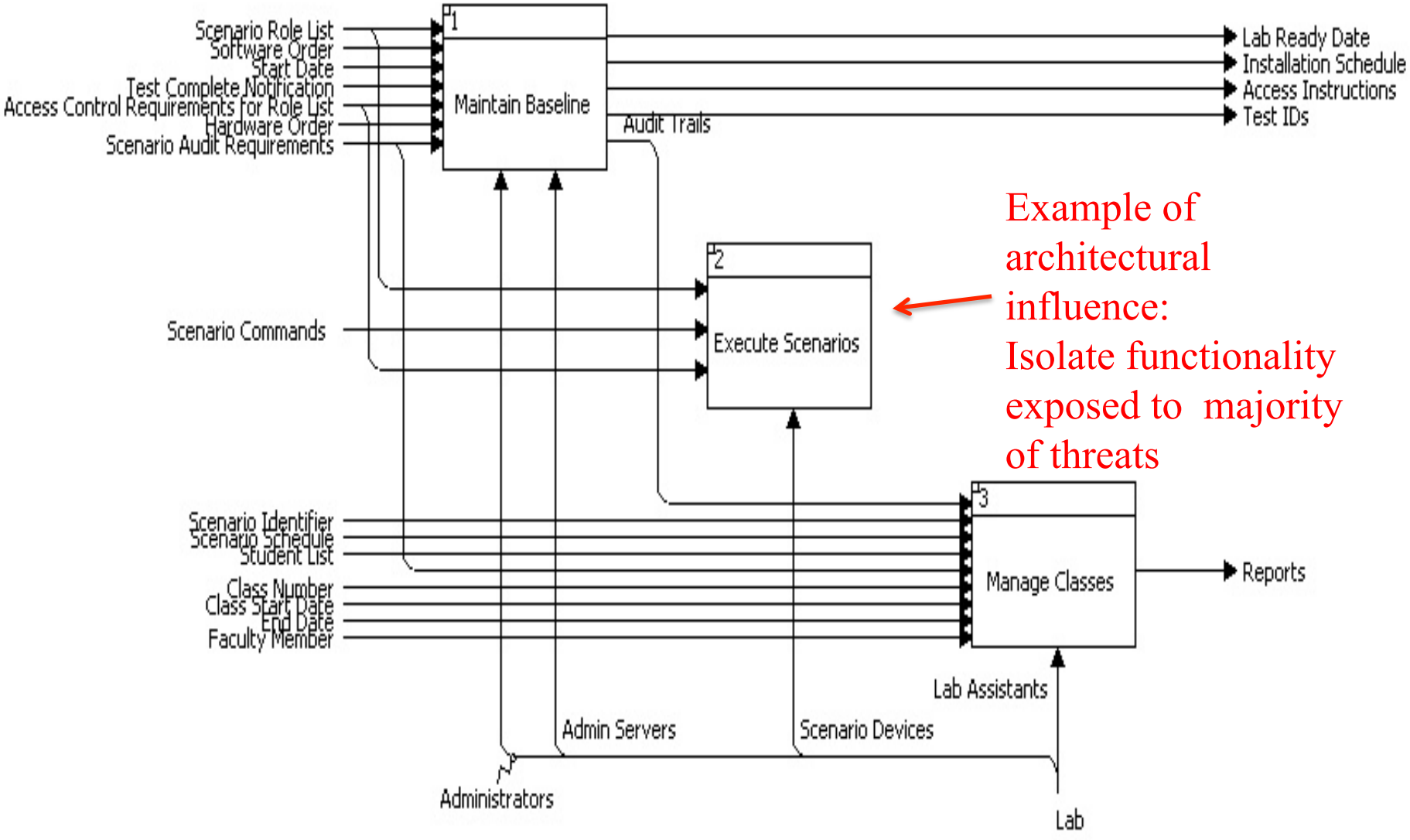
Source: Bayuk, SSE Lab Architecture Definition, 2010

Input and Output Requirements



Source: Bayuk, SSE Lab Architecture Definition, 2010

Functional Decomposition



Source: Bayuk, SSE Lab Architecture Definition, 2010

SYSTEMS ENGINEERING
Research Center
A US DoD University Affiliated Research Center

Security Metrics

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 adequately secure?

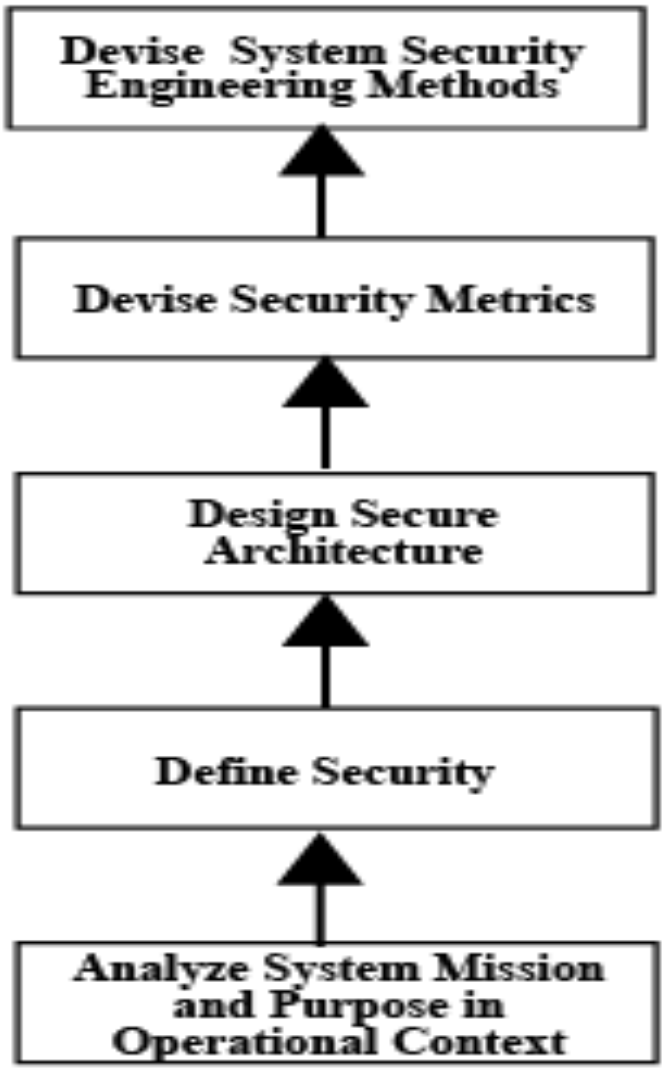
SYSTEMS ENGINEERING
Research Center
A US DoD University Affiliated Research Center

SERC Security Roadmap

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.**

SYSTEMS ENGINEERING
Research Center

SERC Security Approach



Security Systems Engineering Community

- If each SERC member concentrated on one system of interest and could prove something provided more or less security in that context, then we could, in combination, demonstrate the utility of the systems engineering methodology.
- Though such an engineering approach may seem like practical application rather than research to some in our community, they may be overlooking the fact that security is not at all well understood, and so any serious investigation of its properties constitutes a research endeavor.