SAND2007-5401P

Security Risk Assessment

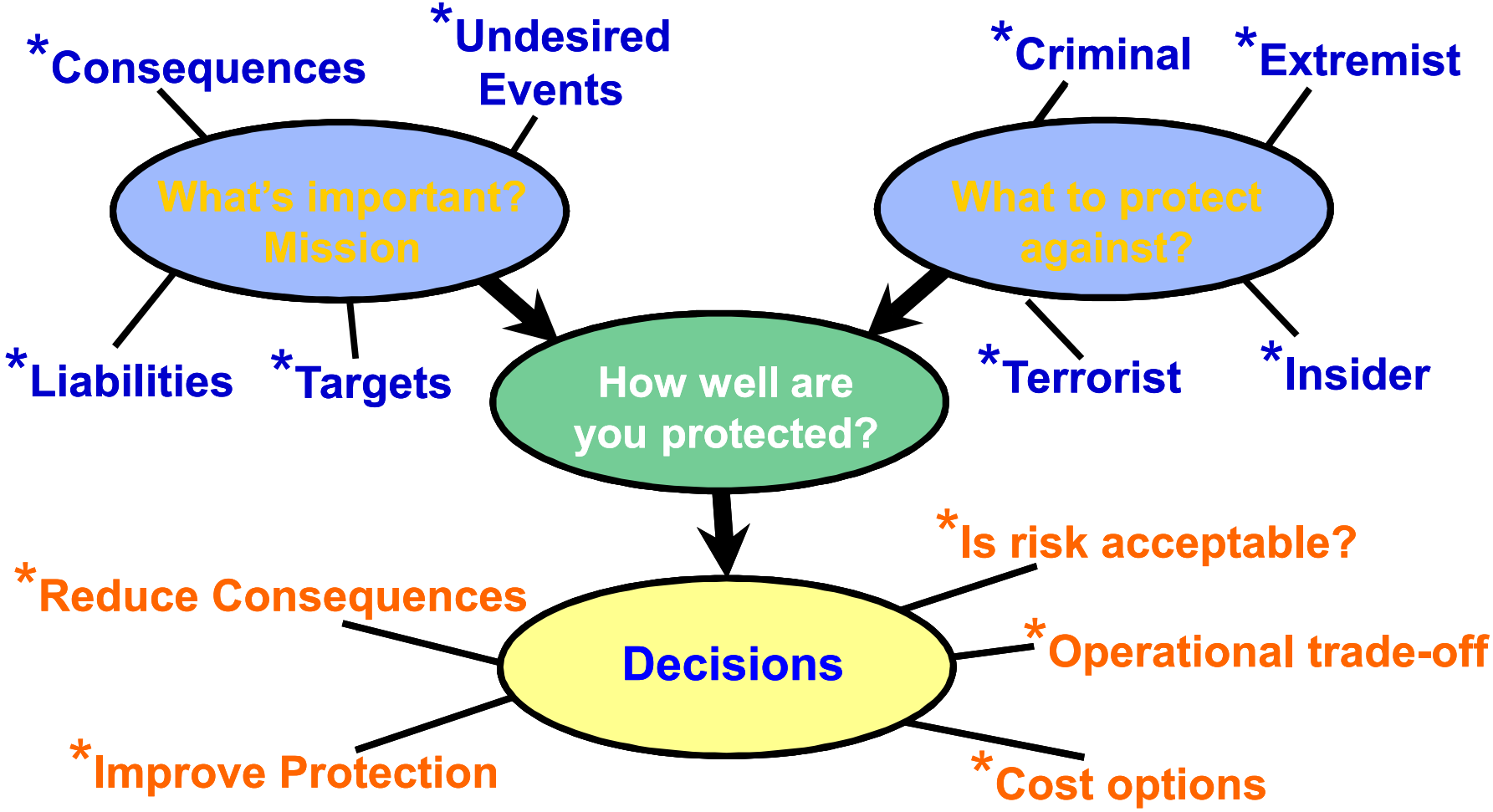
ENG300-Session 5B

Betty Biringer
Manager, Security Risk Assessment Department
Sandia National Laboratories
(505) 844-3985
bebirin@sandia.gov

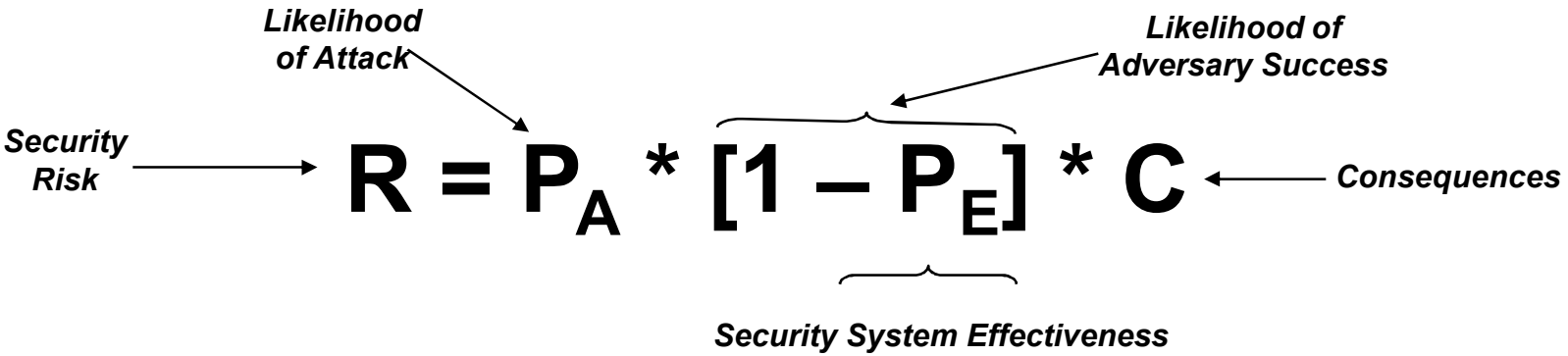
Session Objectives

- Review decisions required for a security risk assessment
- Define the three parameters used for security risk assessment
- Provide an overview of an assessment method for estimating relative security risk

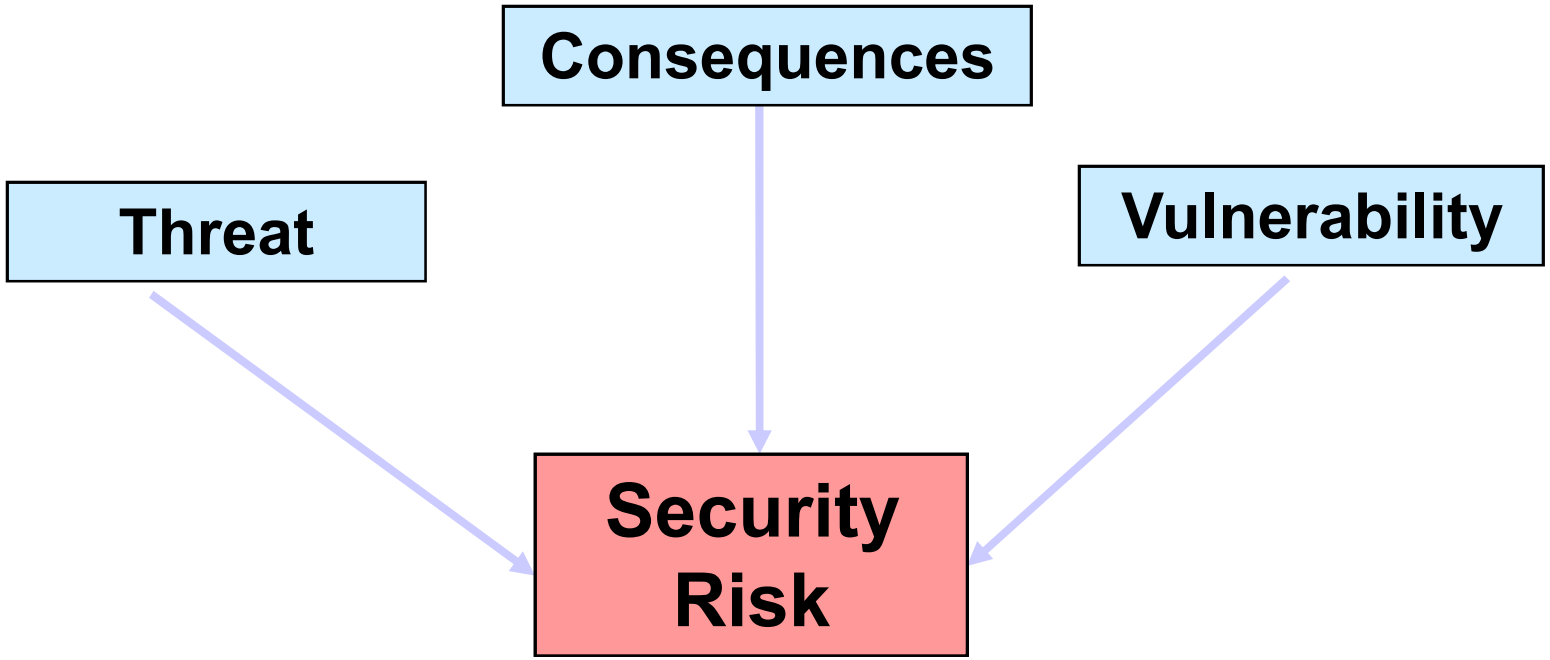
How Much Security Is Enough?



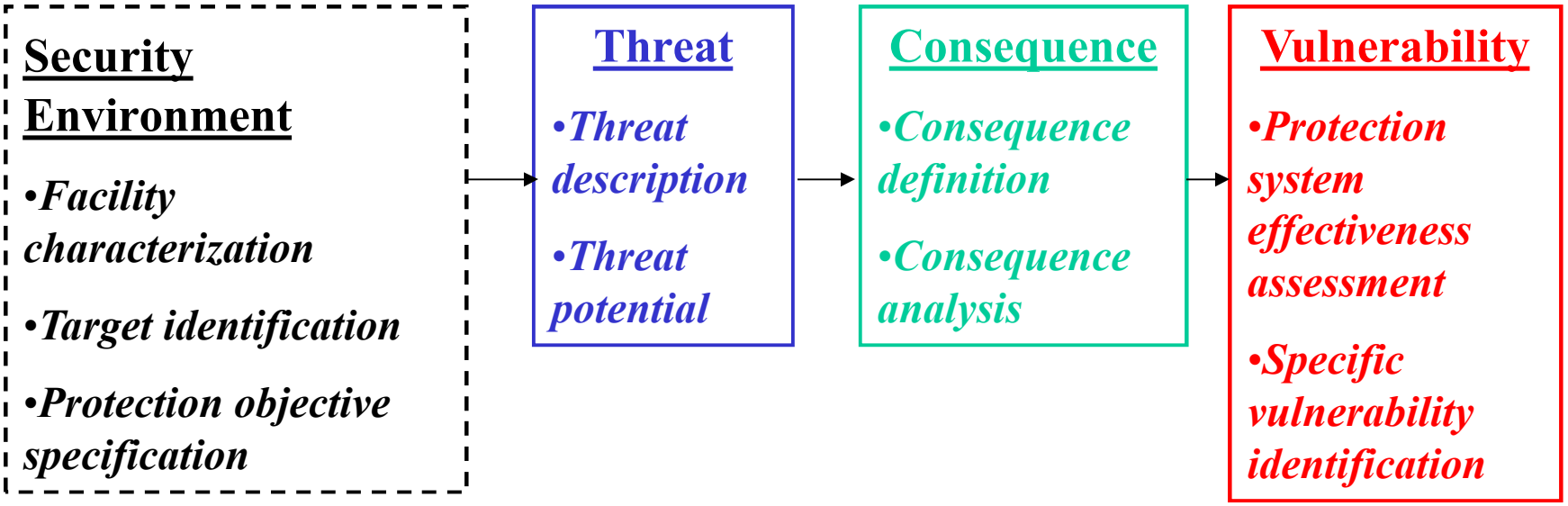
Security Risk Equation



Security Risk is a Function of:



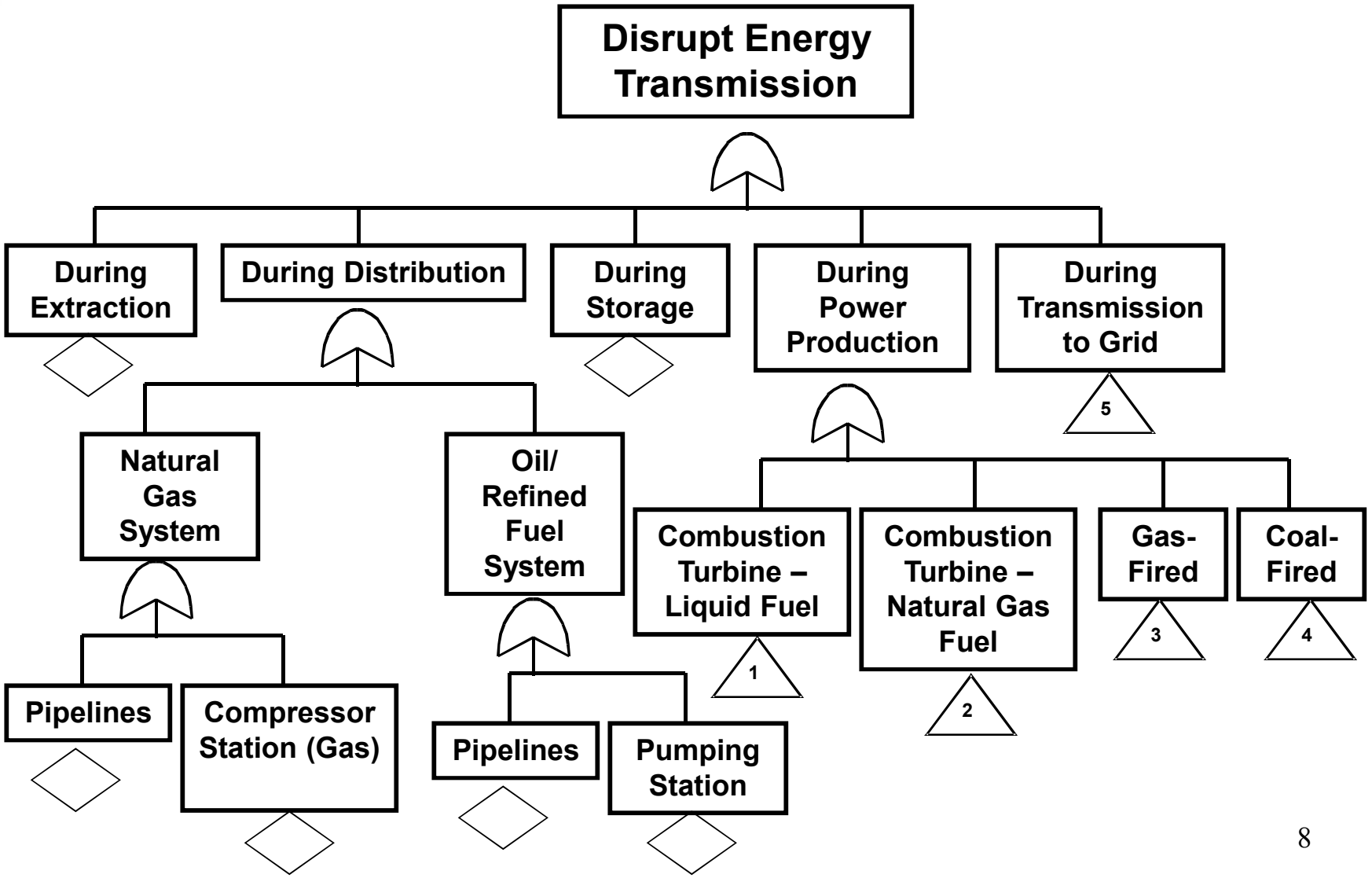
Security Risk Assessment



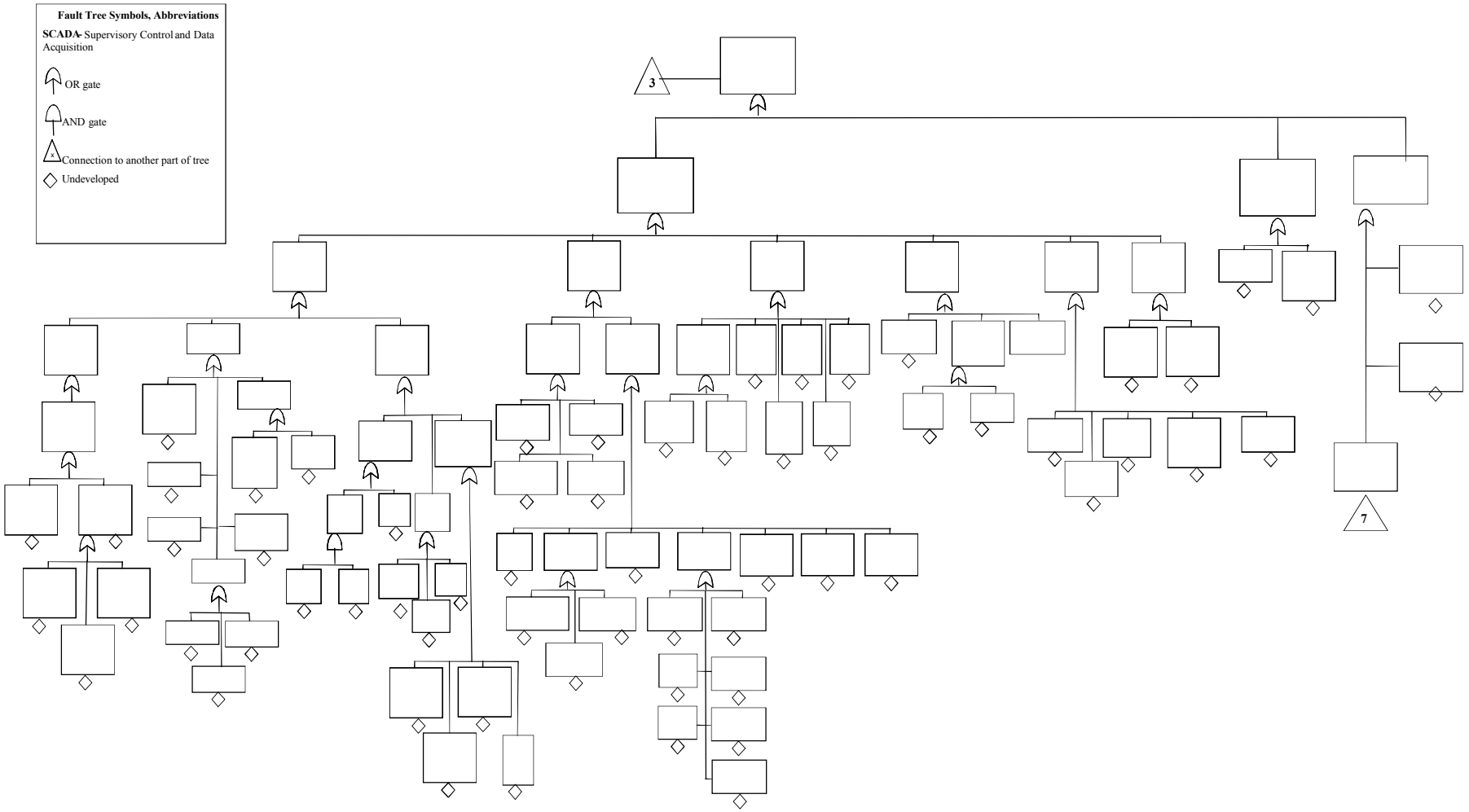
Facility Characterization

- Facility description
  - Physical layout and description
  - Information system architecture (process control/SCADA)
  - Operations
  - Physical and cyber protection system features
  - Work force
- Undesired events - what events to prevent
- Targets – what items to protect
- Protection objectives – prevent events or mitigate consequences

Top Level Fault Tree



Fault Tree for Natural Gas-Fired Electric Power.Generation Plant



Threat Definition

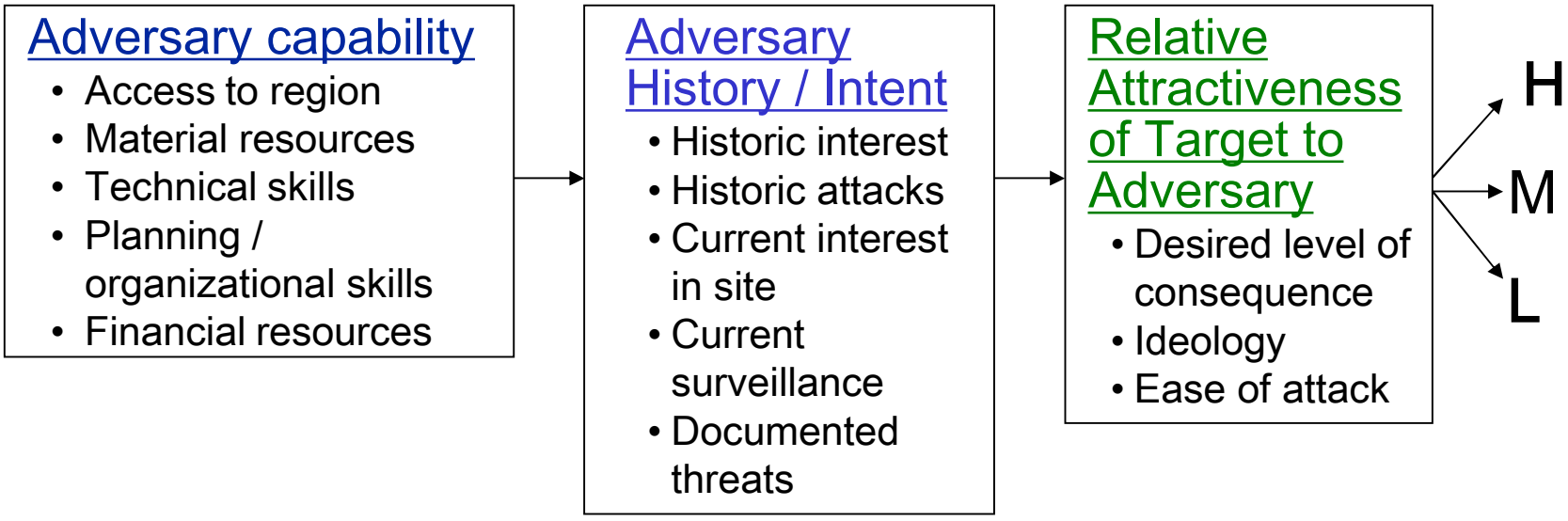
- Type of adversary
  - *Terrorists, criminals, extremists, militia, insider*
- Potential actions
  - *Theft, bombing, sabotage, damage*
- Motivations
  - *Ideological, economic, personal*
- Capabilities
  - *Numbers, weapons, equipment, transportation, technical experience*

Example Threat Spectrum

Type of Adversary	Number of Adversaries	Equipment	Vehicles	Weapons	Motivation	Tactics	Targets of Interest
International Terrorist (May include an insider colluding)	3-20	Unlimited hand/power tools, body armor, chem/bio, wireless comm	Car, pickup, 4x4, truck, semi-trailer truck, boat, barge aircraft	Handguns, automatics,[2] explosives,[3,4] chem/bio	Mass casualties, widespread fear, psychological impact, economic crisis	Catastrophic event, sniper, hostage, cyber	People. High visibility national events. Critical infrastructure. Soft largets. National icons.
Domestic Terrorist: Eco & Militia (May include an insider colluding)	3-5	Hand and power tools, body armor, chem/bio	All terrain vehicle, car, pickup, 4x4, truck, boat, aircraft	Handguns, automatics,[2] explosives,[3,4] chem/bio, incendiary devices	Retaliate against the government. Make a political statement. Change business practice.	Catastrophic event, hostage, sniper, arson, cyber	Specific government facilities. Facilities with environmental issues. People.
Extremists	5–10	Signs, chains, locks, hand tools	Car, pickup, 4x4, truck, boat, bus	Incendiary devices, clubs	Make a political statement. Protest.	Protest, civil disobedience, assault, damage, destruction, cyber	Facilities with political or environmental significance.
Criminal	2–3	Hand tools	Car, pickup, 4x4, truck	Handguns, automatics,[2] knives	Financial gain. Steal property.	Property theft, cyber	Banks, electronic equipment suppliers, high-monetary assets.
Gangs	5-100	Hand and improvised tools	Car, pickup, 4x4	Handguns, automatics,[2] knife	Gang superiority (turf), harassment	Assault, drug manufacturing	
Vandals / Hackers	2–5	Spray paint, rocks, knifes	Car, pickup	Handguns, automatics[2]	Vandalism.	Damage, destruction, hacking (cyber)	Conveniently located facilities.
Insider[1]	1	On-site equipment	Car, pickup, 4x4, boat	Handguns, automatics,[2] explosives[3,4]	Disgruntled.	Destruction, violence, theft, cyber	Facility asset(s) and equipment. Fellow employee(s)

Threat Potential

- Relative score – not a probability
- Scored per undesired event and per adversary group



Consequence Assessment

- Consequence of loss of the target should be developed.
- Establish units of consequence
  - Loss of human life
  - Loss of dollars
  - Loss of asset
  - Loss of operations/activity

- Rank in order of importance/value
- Assign relative value to each consequence

Sample Consequence Table

Measure of Consequence	High	Medium	Low
Economic loss (property loss + revenue)	> $5M	$1 – 5M	< $1M
Economic loss (users)	> $5M	$1 – 5M	< $1M
Deaths	>3	1 - 3	0
Geographic Impact	National	Regional	Local

Prioritization

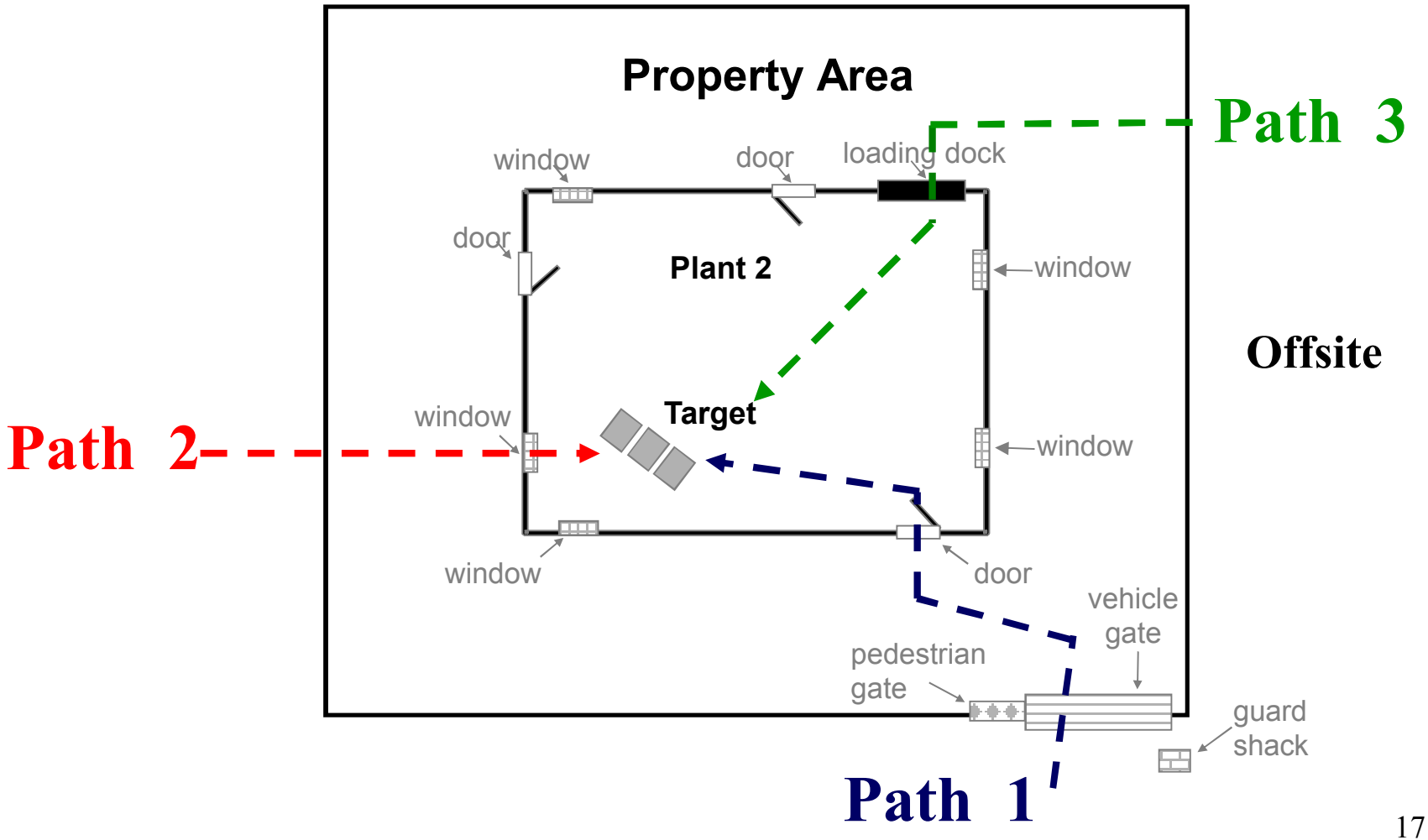
Consequence				
High	Terrorist (sabotage)		Insider (theft)	
Med		Insider (sabotage)		
Low	Vandal (graffiti)		Hacker (web deface)	
	Low	Med	High	

Threat

System Effectiveness

- A measure of how effectively security system meets protection objective(s):
  - Physical attack: Prevent undesired event(s) with functions of detection, delay, response
  - Cyber attack: Preserve confidentiality, integrity, and availability of critical data with functions of authentication, authorization, audit

Physical Paths



Physical Protection Functions

Detection

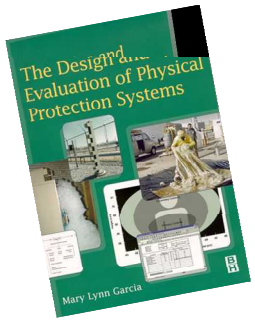
- Intrusion Sensing
- Alarm Communication
- Alarm Assessment
- Access Control
- Contraband Detection

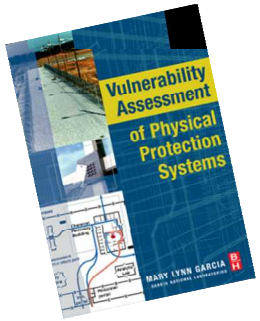
Delay

- Barriers
- Dispensable Barriers

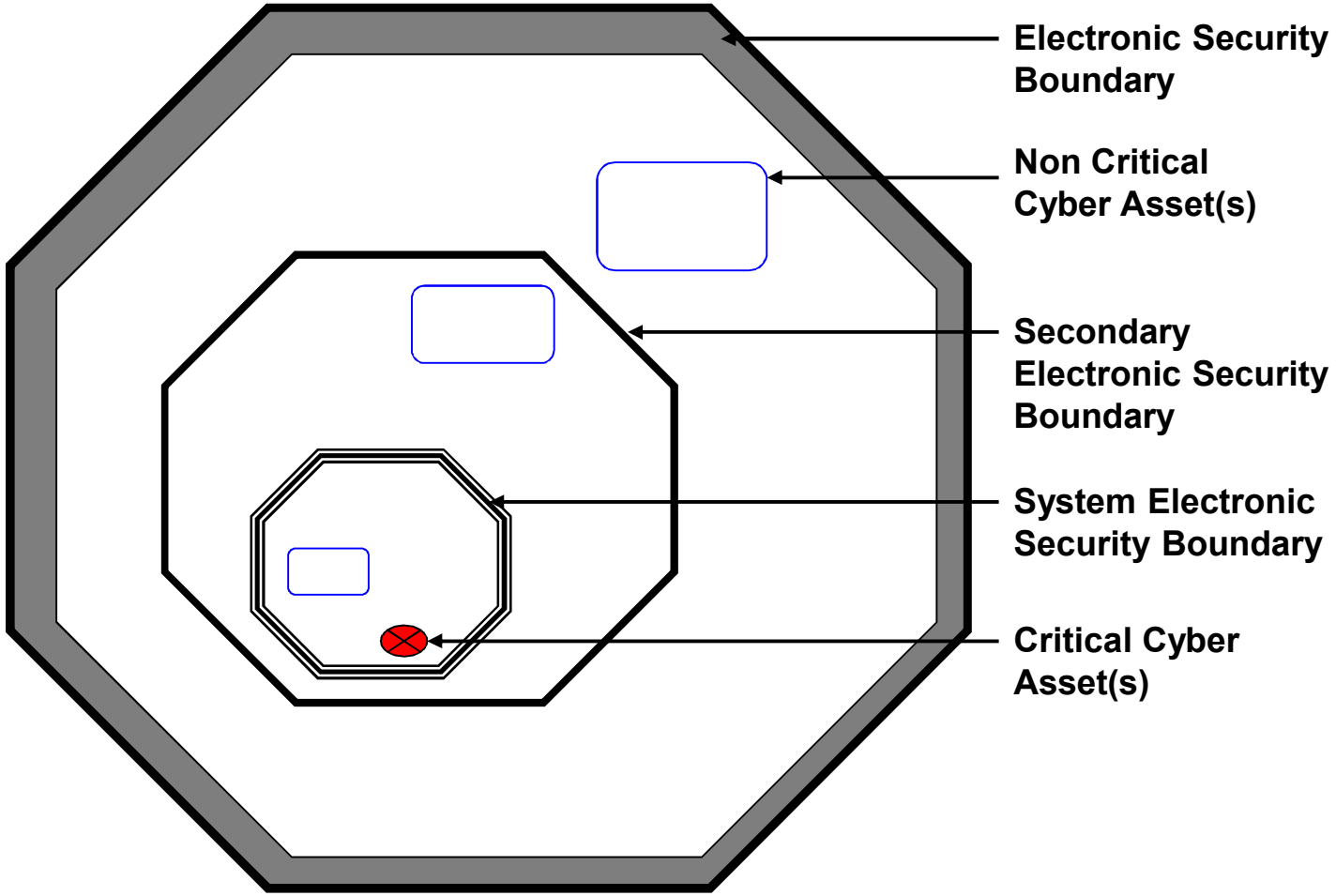
Response

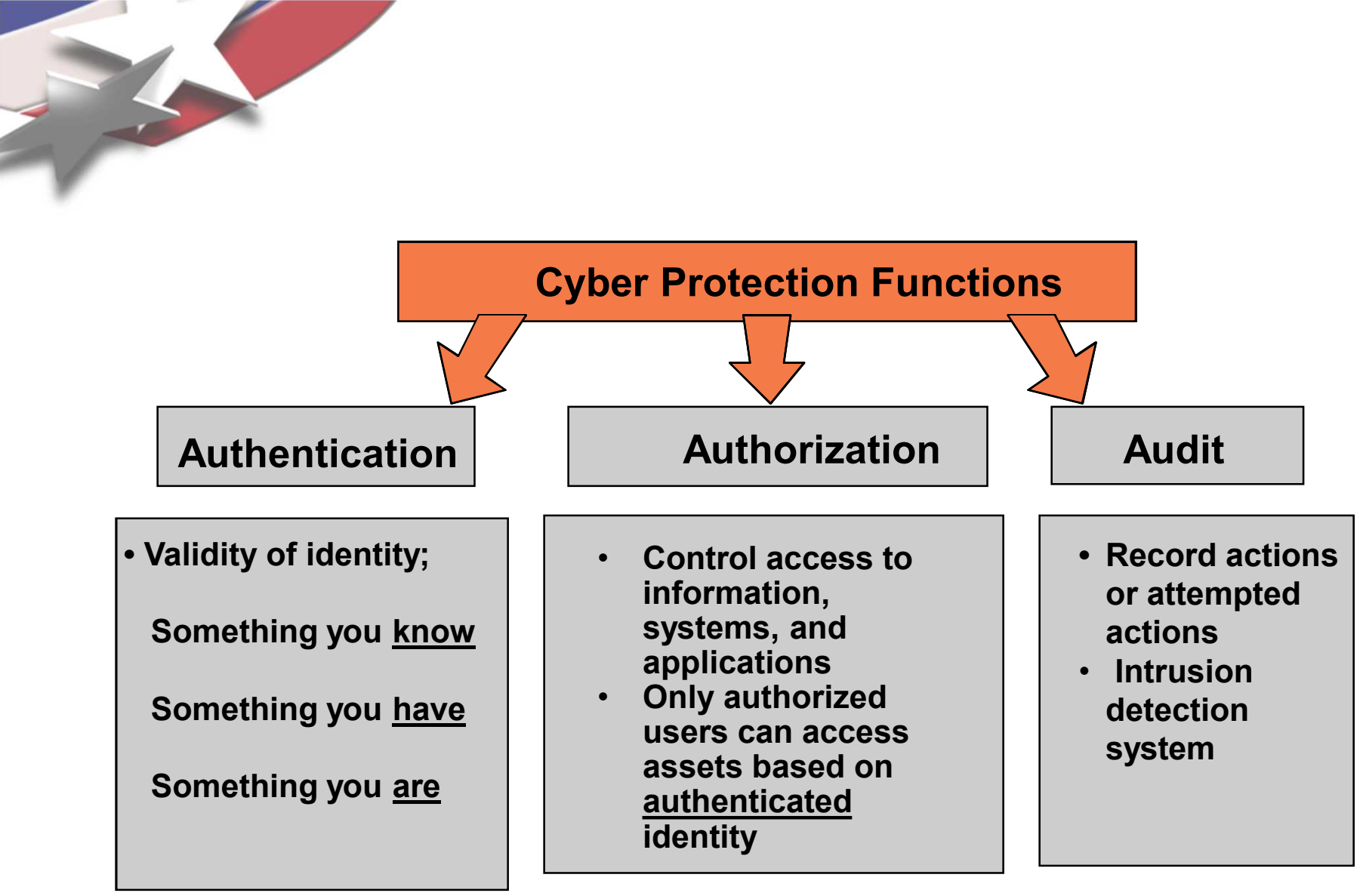
- Interruption:
  - Communication to Response Force
  - Deployment of Response Force
- Neutralization



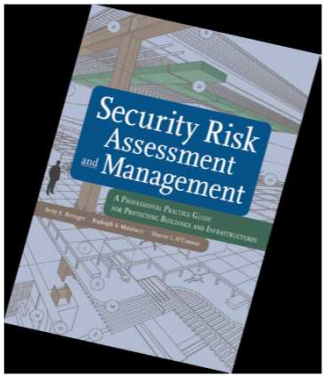


Cyber Paths


Electronic Security Boundary
Non Critical Cyber Asset(s)
Secondary Electronic Security Boundary
System Electronic Security Boundary
Critical Cyber Asset(s)


Cyber Protection Functions
Authentication
Authorization
Audit
• Validity of identity;
Something you know
Something you have
Something you are
• Control access to information, systems, and applications
• Only authorized users can access assets based on authenticated identity
• Record actions or attempted actions
• Intrusion detection system

Security Risk Assessment



Security Environment Description

Threat Assessment

Consequence Assessment

Vulnerability Assessment

Risk Estimation

Risk Acceptable?

Y

N

End (Periodic Review)

Propose Upgrades and Recommendations

Reducing Security Risk

- Reduce Threat level
  - Deterrence
  - Difficult to measure
- Reduce Vulnerability
  - Detection, Delay, Response
  - Authentication, Authorization, Audit
- Reduce Consequence level
  - Mitigation features
    - Redundant equipment
    - Function transfer
    - Structural hardening
  - Improve emergency response

SNL Security Risk Assessment Methodologies

- RAM-D (Dams)
  - Interagency Forum for Infrastructure Protection
- RAM-T (Electrical Utility Transmission Systems)
  - Interagency Forum for Infrastructure Protection
- RAM-W (Municipal water systems)
  - American Waterworks Research Foundation, EPA
- RAM-C (Communities)
  - Partnerships w/communities and law enforcement agencies
- RAM-CF (Chemical facilities)
  - DOJ, EPA, many chemical industry stakeholders
- RAM-P (Prisons)
  - DOJ, State Department of Corrections
- RAM-E (Pipelines, Electric Power Generation, in development)
  - DOE, Gas Associations, Oil/Gas Industry
- RAM-FAA (airspace management facilities)
- RC RAM-W (RAMCAP/NIPP compliant version)
  - Under direction of ASME with support from DHS. EPA

See www.sandia.gov/ram

Summary

- Decisions required for a security risk assessment
- Security risk is a function of threat, vulnerability, and consequence
- Security risk assessment provides valuable information for risk managers