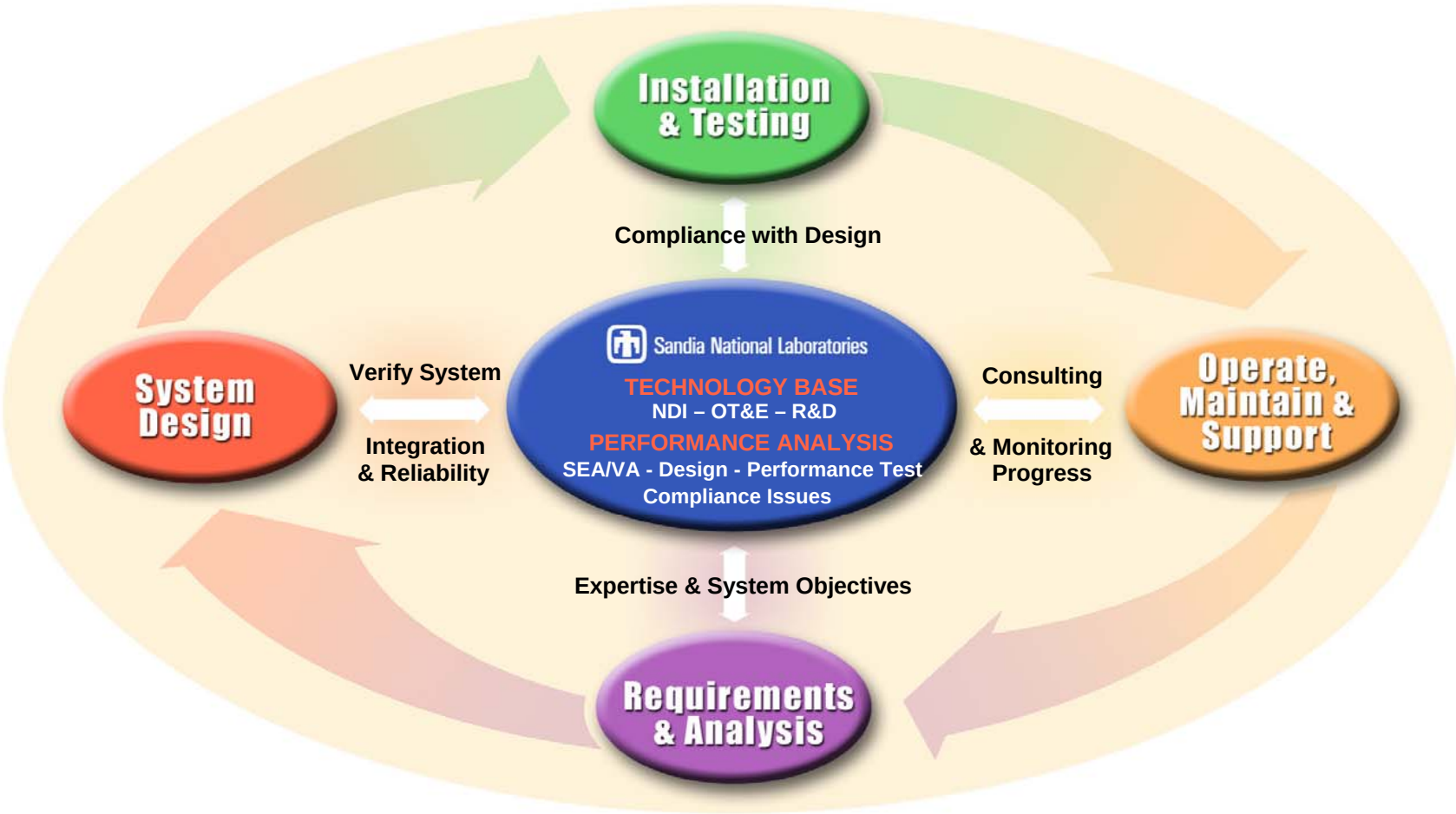
Sandia National Labs' Security Risk Assessment Methodologies

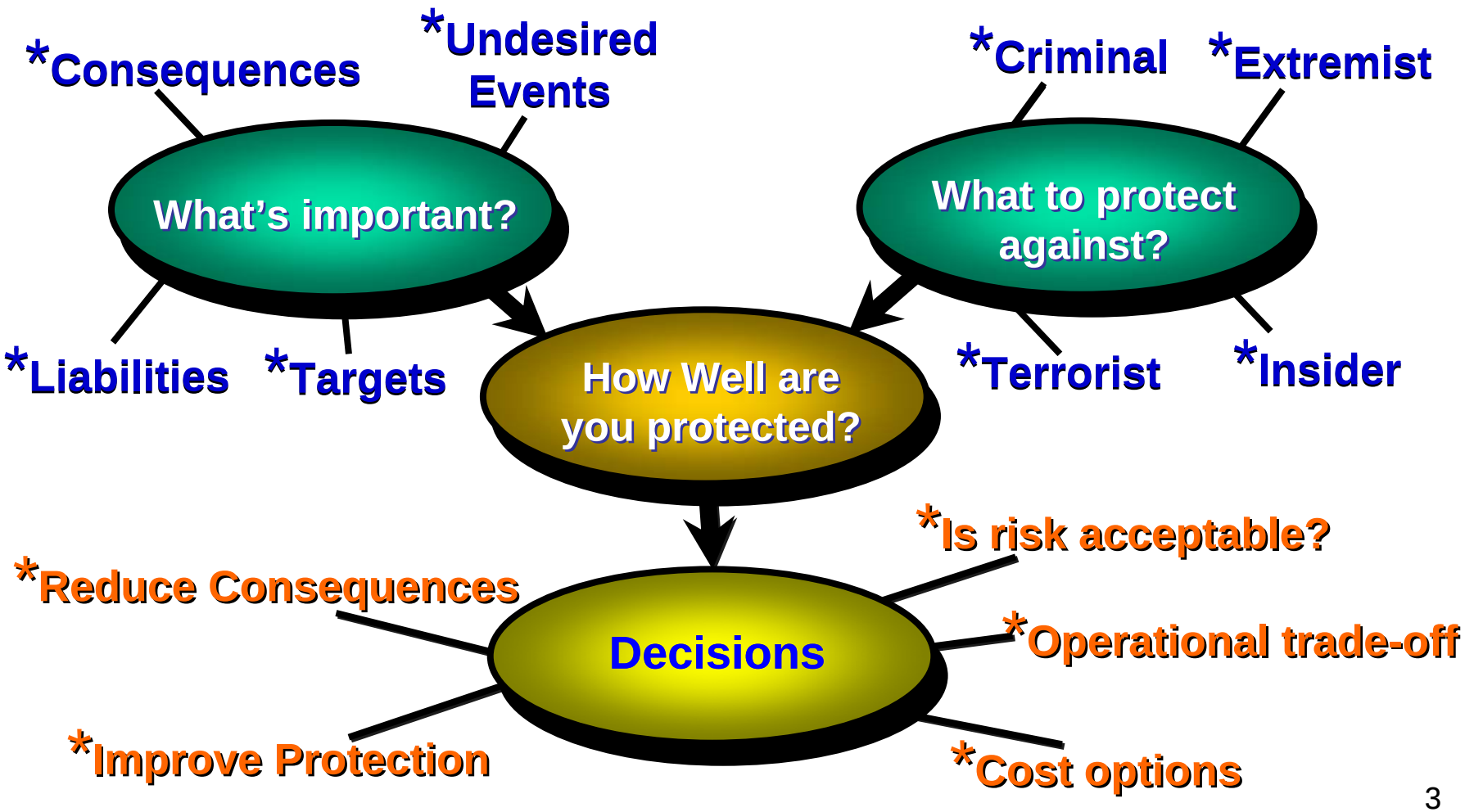
www.sandia.gov/ram

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

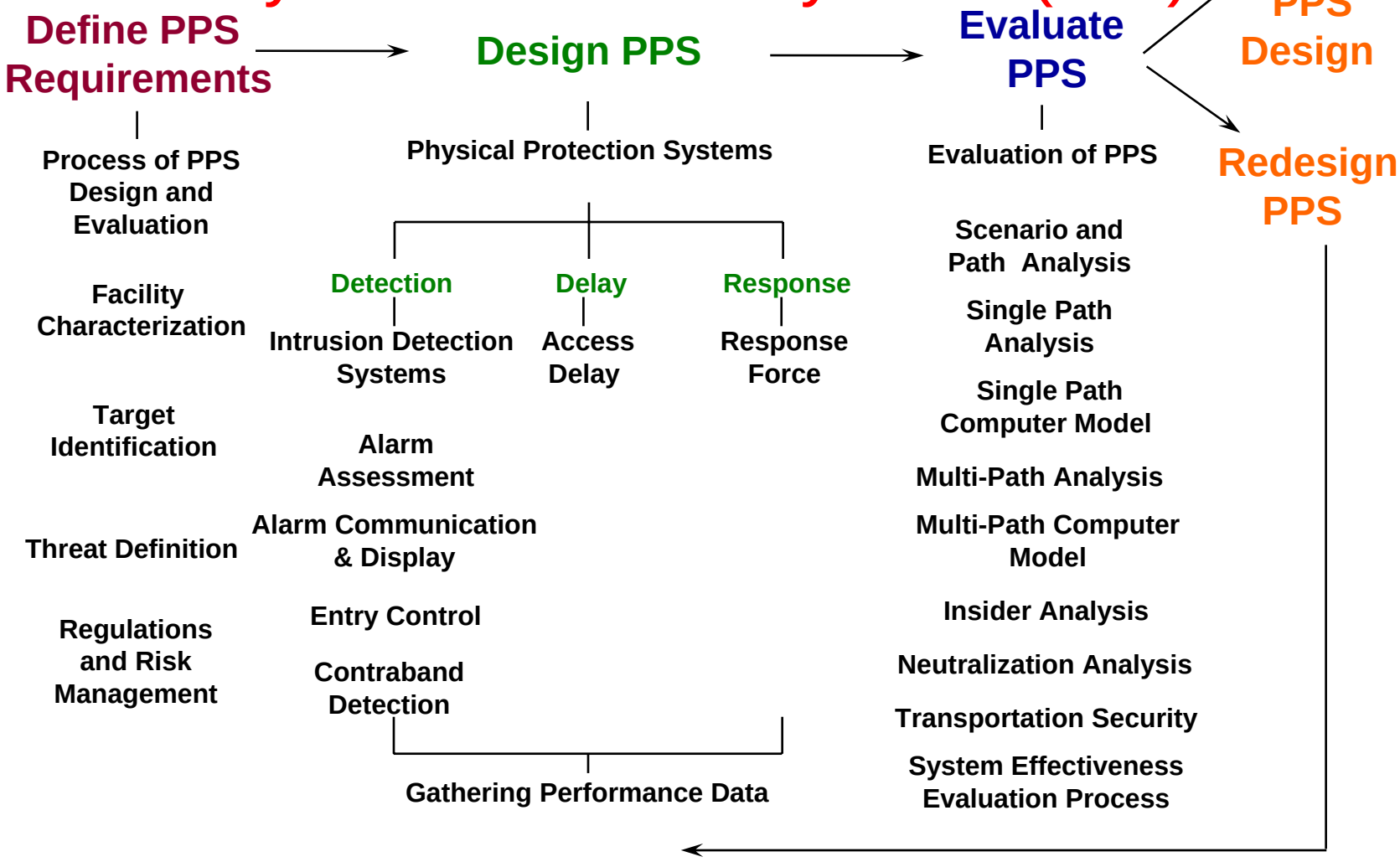
Systems Engineering Approach to Security



How Much Is Enough?



Design and Evaluation Process Outline (DEPO) for Physical Protection Systems (PPS)



Sandia National Laboratories Vulnerability & Risk Assessment Methodologies

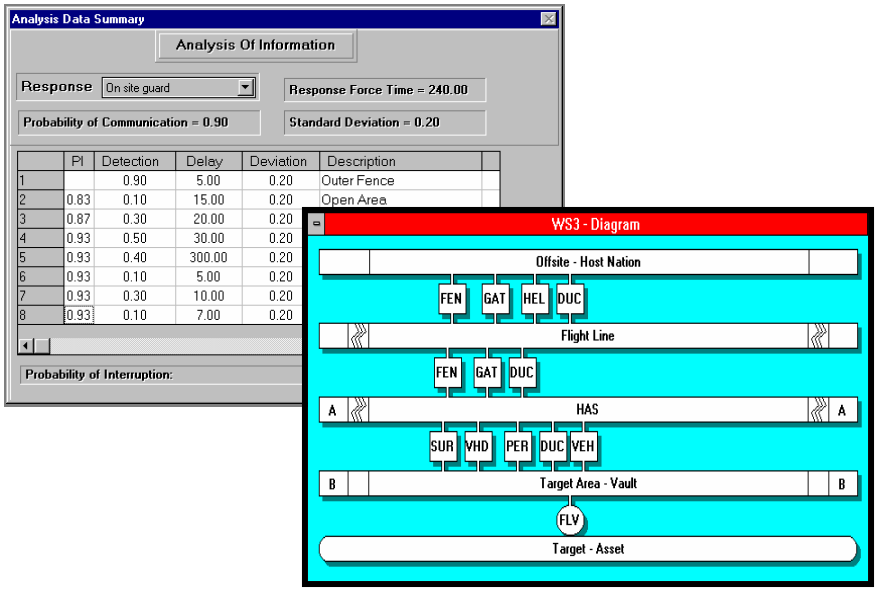
- **RAM-D (Dams)**
  - **Interagency Forum for Infrastructure Protection**
- **RAM-T (Electrical Utility Transmission Systems)**
  - **Interagency Forum for Infrastructure Protection**
- **RAM-W (Municipal water systems)**
  - **AwwaRF, EPA**
- **RAM-C (Communities)**
  - **Partnerships w/communities 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)**
  - **DOE, Gas Associations, Oil/Gas Industry, Power Utilities**
- **Other critical infrastructures**
  - **Interdependencies (energy, transportation, comm...)**
- **DOE, DoD and Other applications**

  Facility/installation vulnerability assessments, SEAs

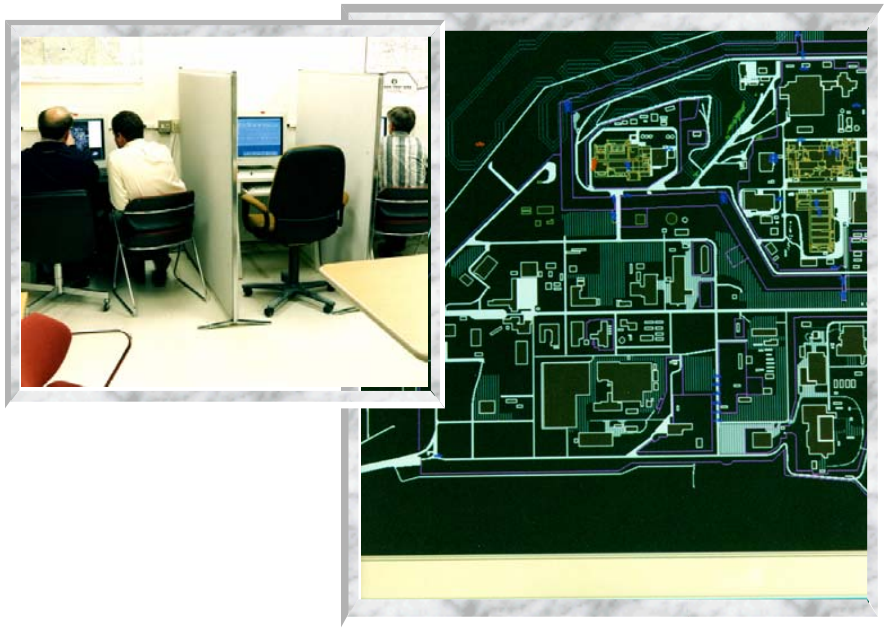
Vulnerability Analysis Tools

- A vulnerability analysis is a systematic analysis involving expertise in all parts of a physical protection system (analogous to a probabilistic risk analysis in reactor safety)
- Analysis tools tend to fall in two groups

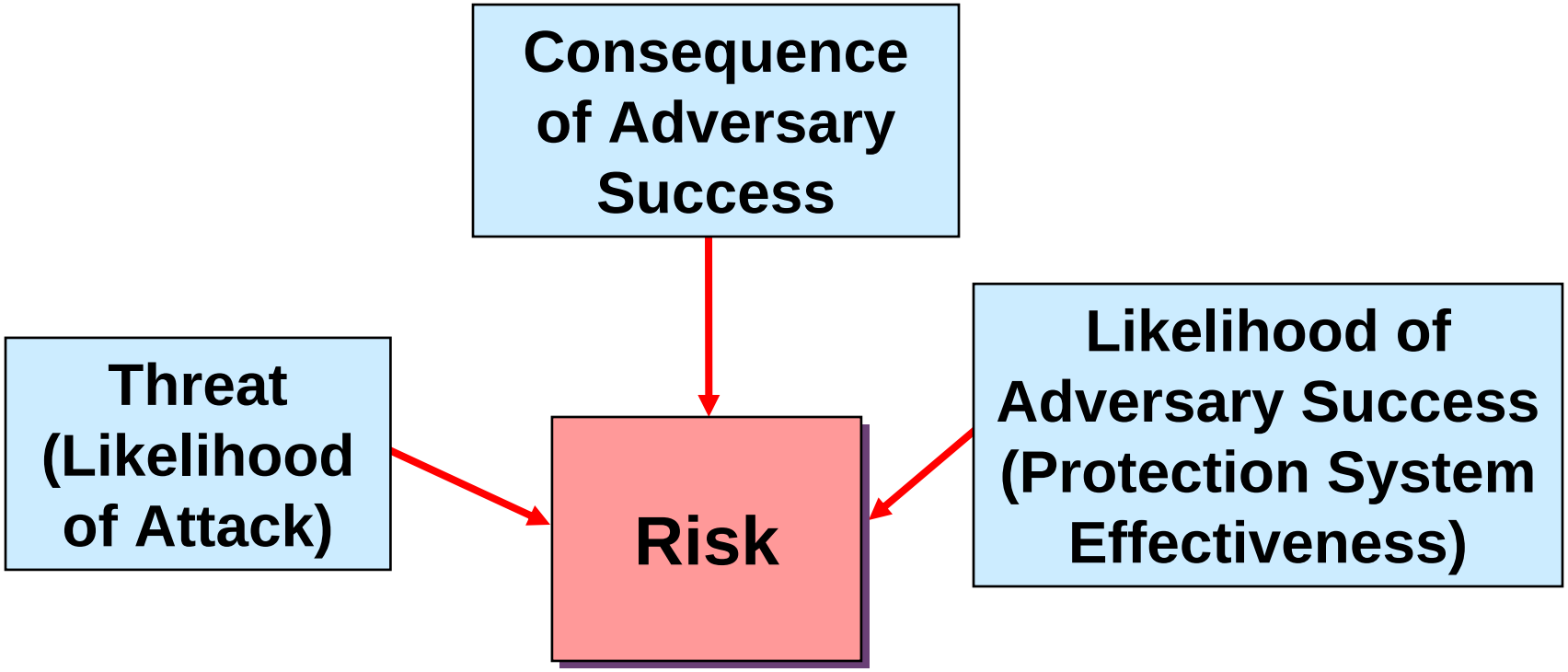
Adversary Path analysis



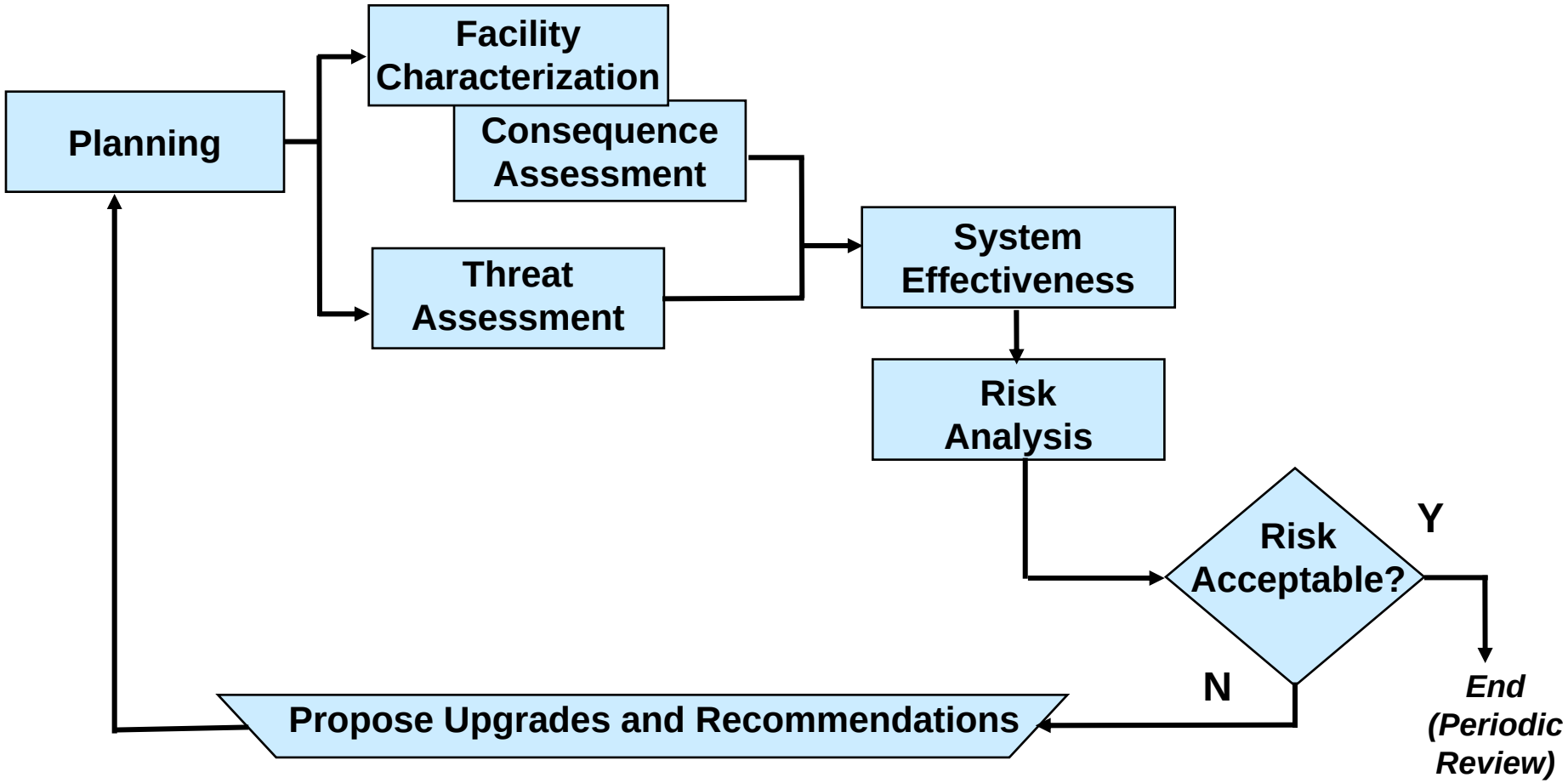
Force-on-Force analysis



Components of Risk

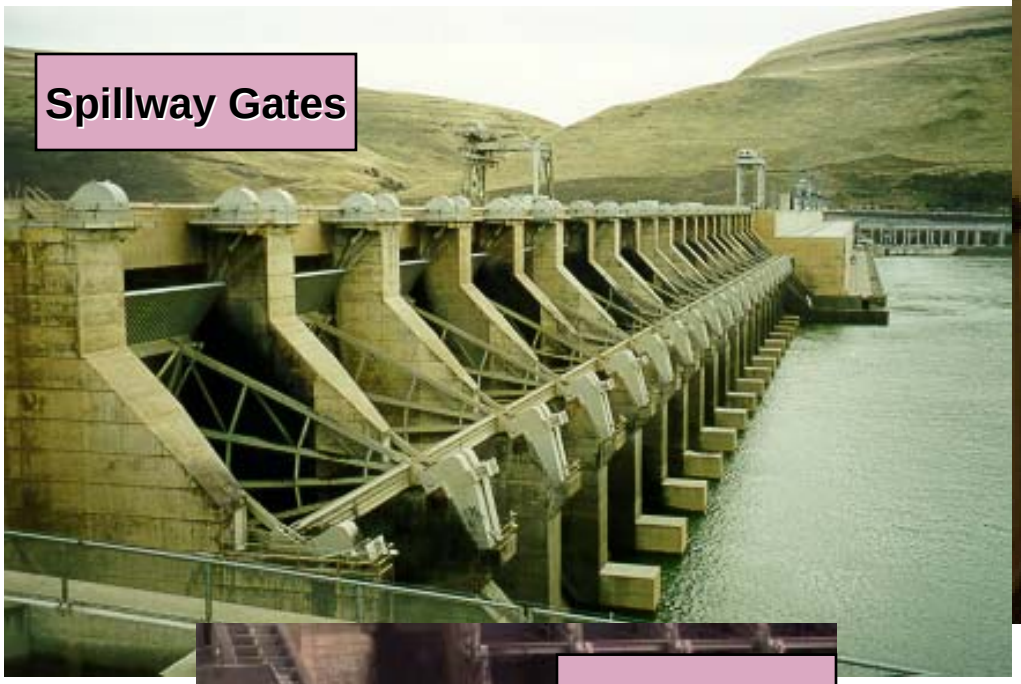


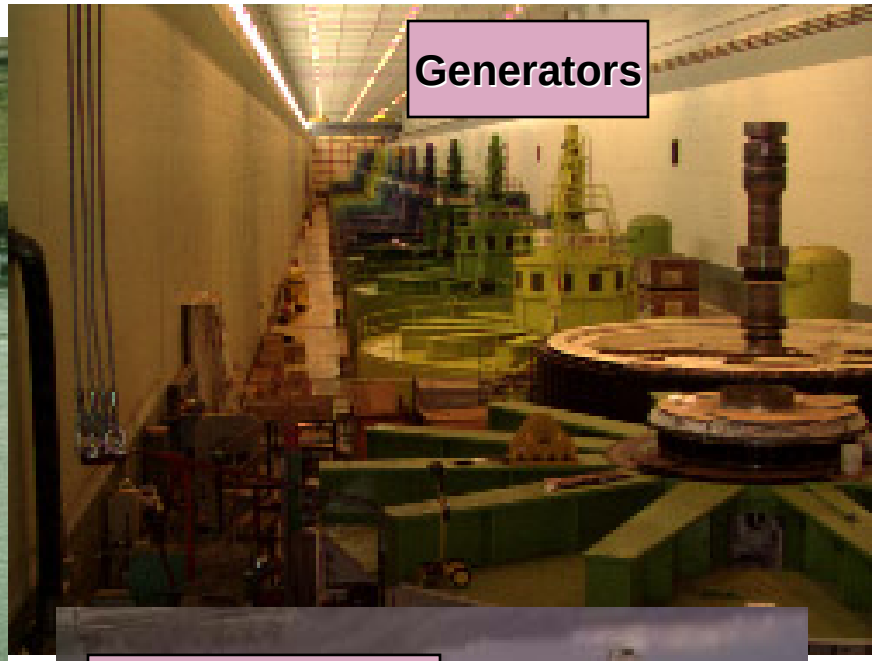
Generic Risk Assessment Methodology Process

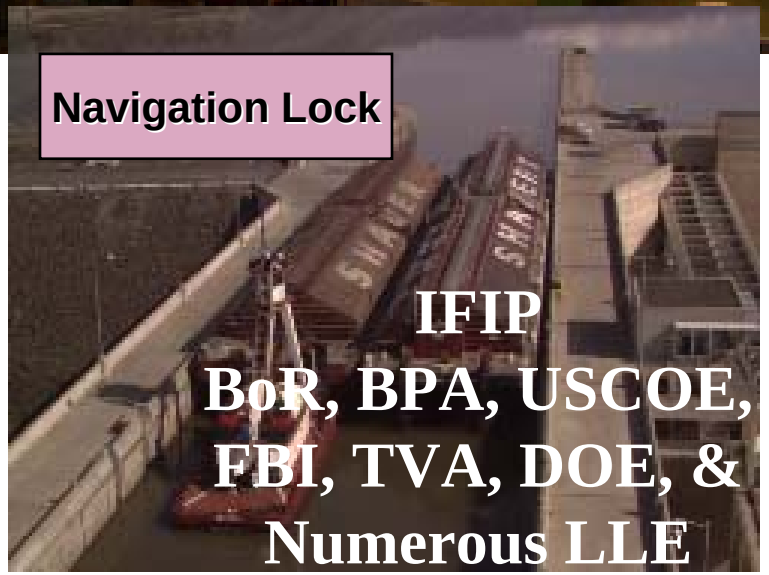


Note: Each critical infrastructure (CI) follows a RAM process developed specifically for that CI.

Risk Assessment Methodology for Dams (RAM-D)







Risk Assessment Methodology for Transmission (RAM-T)









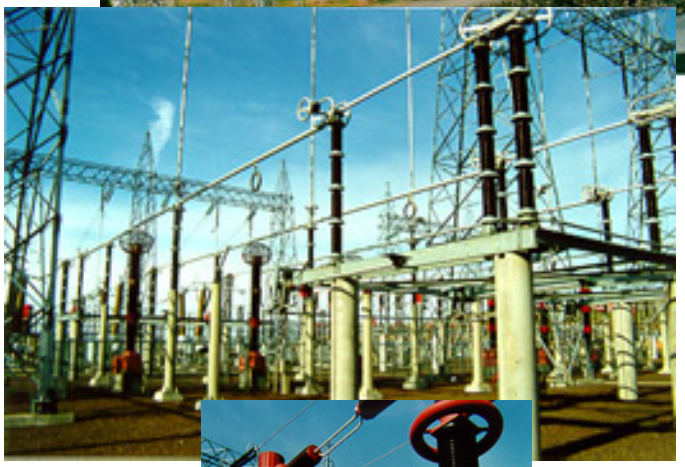

Application of
IFIP Security Methodology for
High Voltage
Electrical Power Transmission
to BPA Facilities

(RAM - T^{SM})

Conducted by the
Interagency Forum for Infrastructure Protection
(IFIP)

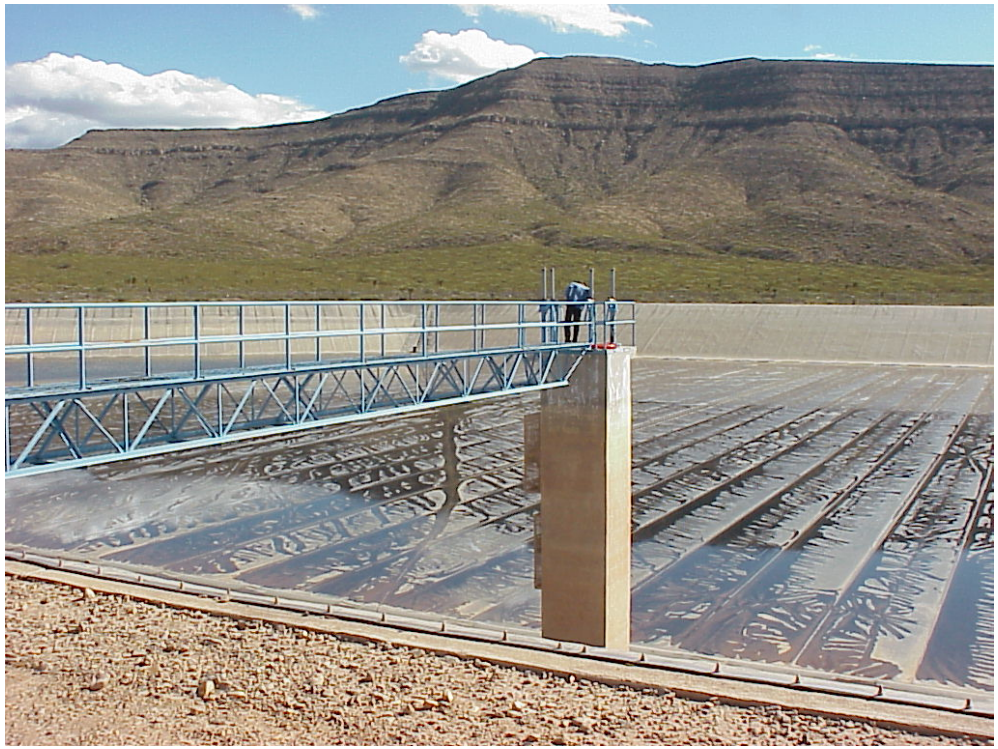
Prepared and Delivered by
Sandia National Laboratories
Rudy Matalucci, Project Manager
505-844-8804

October 2000

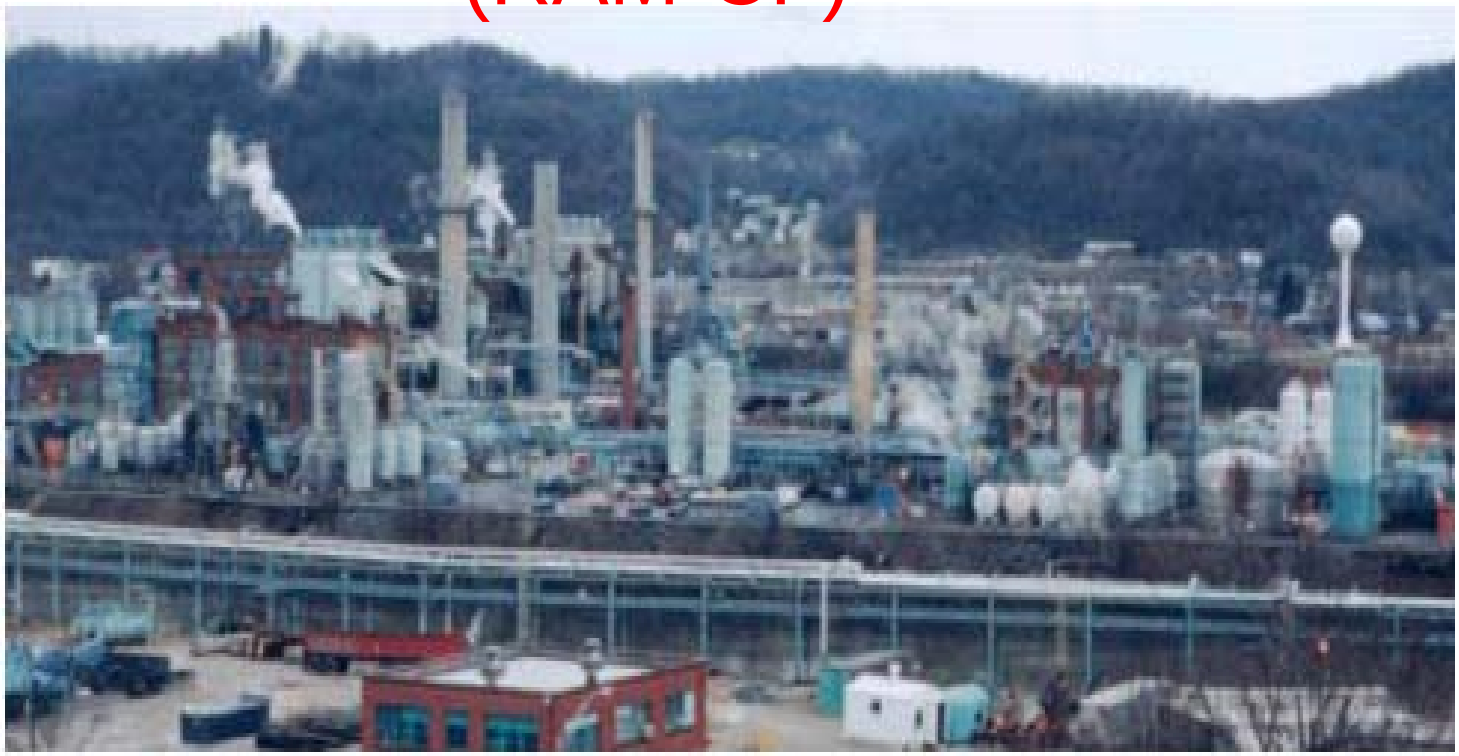




Risk Assessment Methodology for Water Utilities (RAM-W)

- EPA
- AwwaRF
- American Water Works Association
- Local Water Utilities



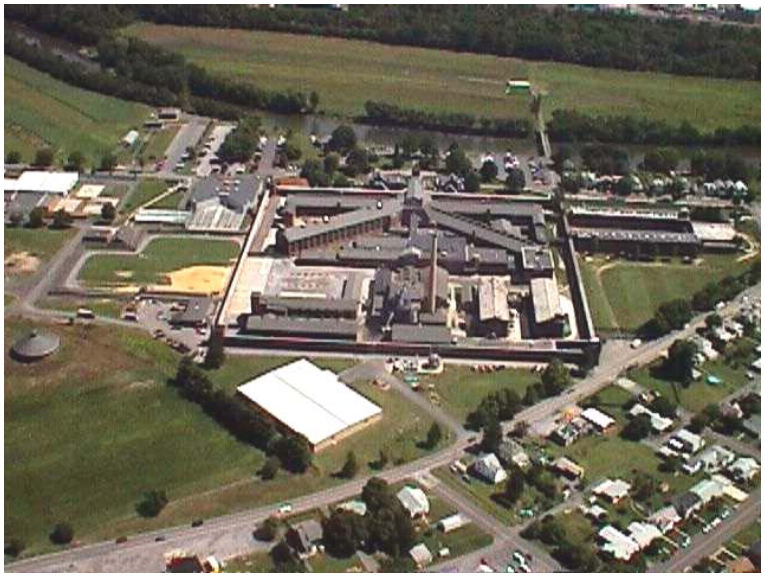
Risk Assessment Methodology for Chemical/Petrochemical Facilities (RAM-CF)



- Funded by NIJ/USDOJ and EPA.
- Risk assessment methodology for assessing the security of chemical facilities.
- Developed in cooperation with chemical industry and other stakeholders

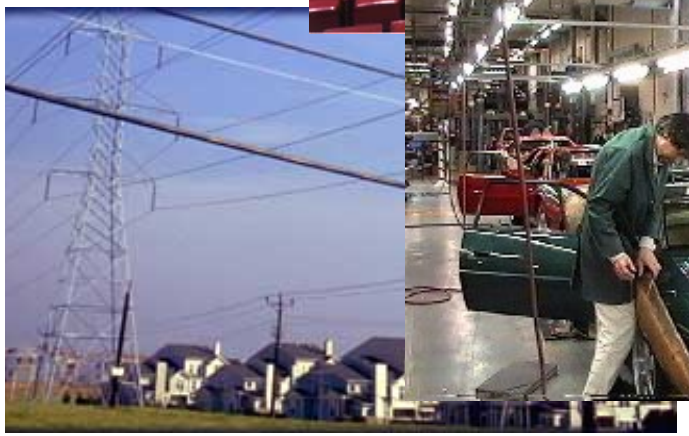
Security Risk Assessments and Security Design Reviews for Correctional Facilities (RAM-P)

Vulnerability Analysis and Video Assessment Upgrades for the Correctional Facilities



- Funding provided by DOJ/NIJ
- Developed in cooperation of the ACA and several State Dept of Corrections

Risk Assessment Methodology for Communities (RAM-C)

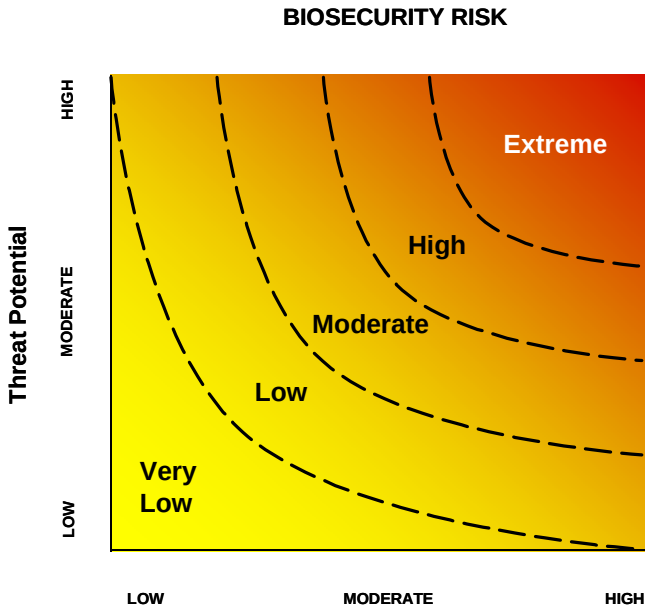


- Funding provided by DOJ/NIJ
- Developed in cooperation with State/Local government agencies numerous communities across the country

Risk Assessment Methodology for Energy Infrastructures (RAM-E)

- Funding provided by DOE Office of Energy Assurance and NETL
- Developed in cooperation with GTI, INGAA, AGA, TVA, PNM, NERC

Biological Risk Assessment Methodology (BioRAM)

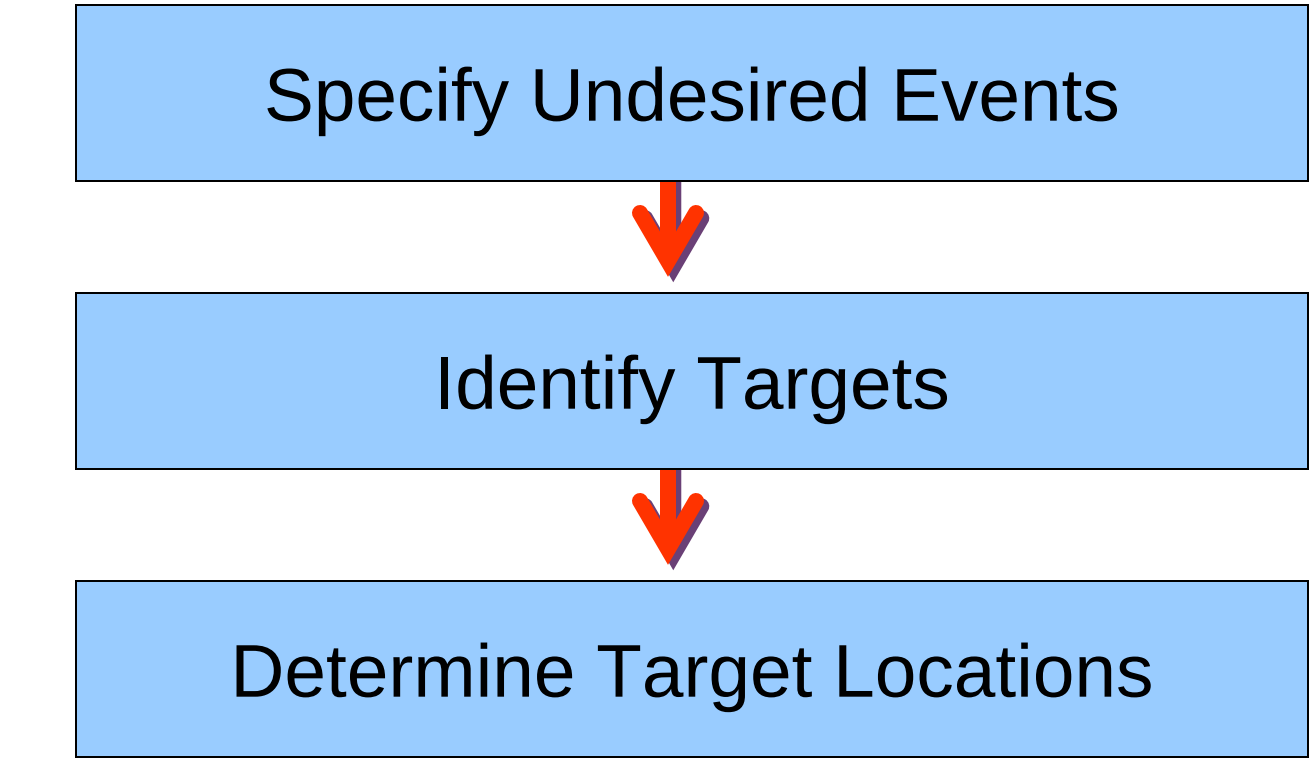


- Funding provided by internal Sandia Laboratory Directed Research and Development

Planning

- Define Security Goals
  - Considering what is important
    - Protect lives
    - Protect property
    - Prevent loss of services
  - The financial resources available
  - The acceptability of the potential consequences of an adversary action

Facility Characterization and Target Identification



Consequences Assessment

- Determine consequence parameters
  - e.g., loss of life, economic impact, loss of mission
  - Develop measurement criteria values
- Determine severity for loss of asset/target
  - Prioritize targets

Threat Assessment

- Adversary types and capabilities
- Consider adversary scenarios
- Identify information sources
- Develop defined threat(s)
- Likelihood of attack process

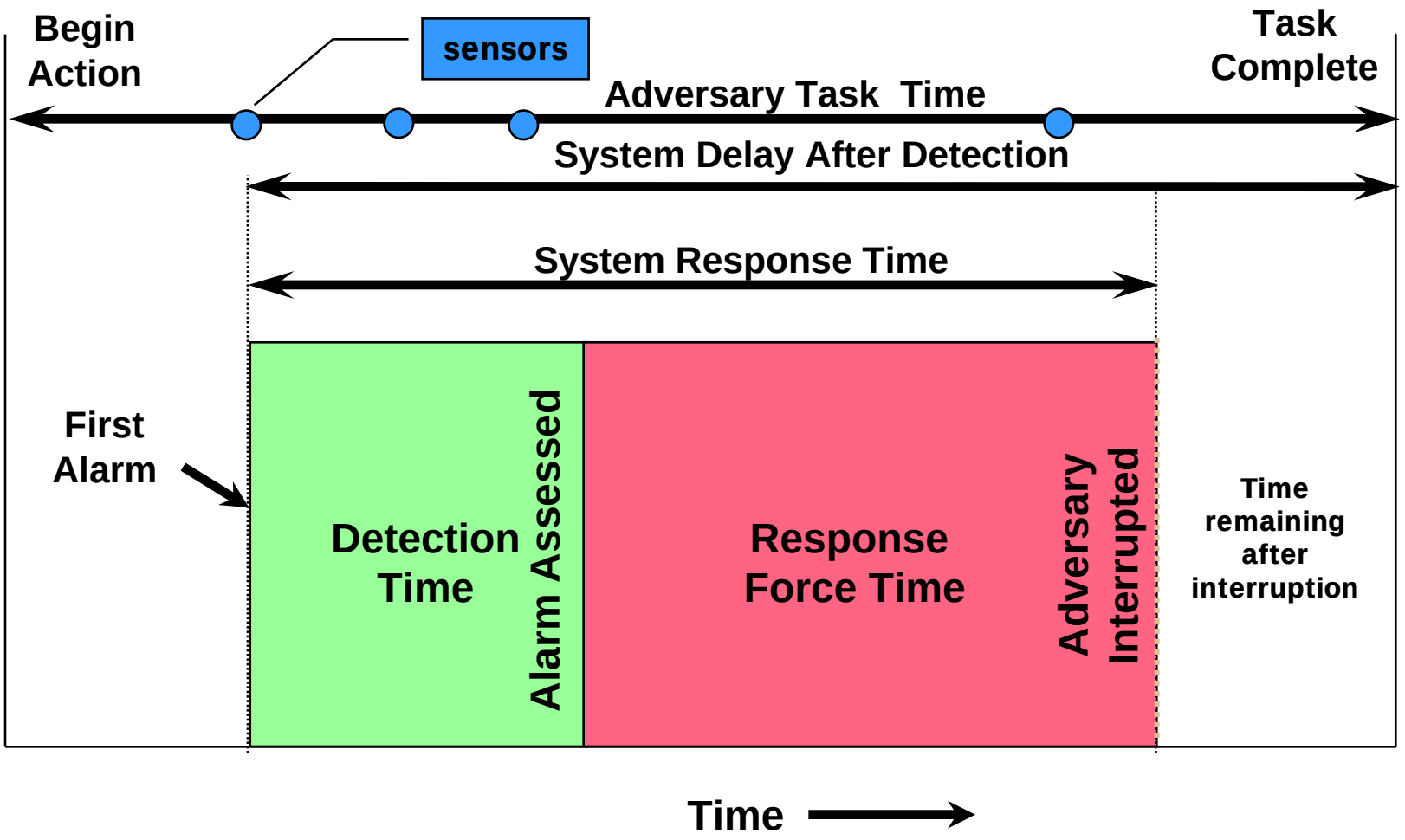
Non-State Actors

Local extremist

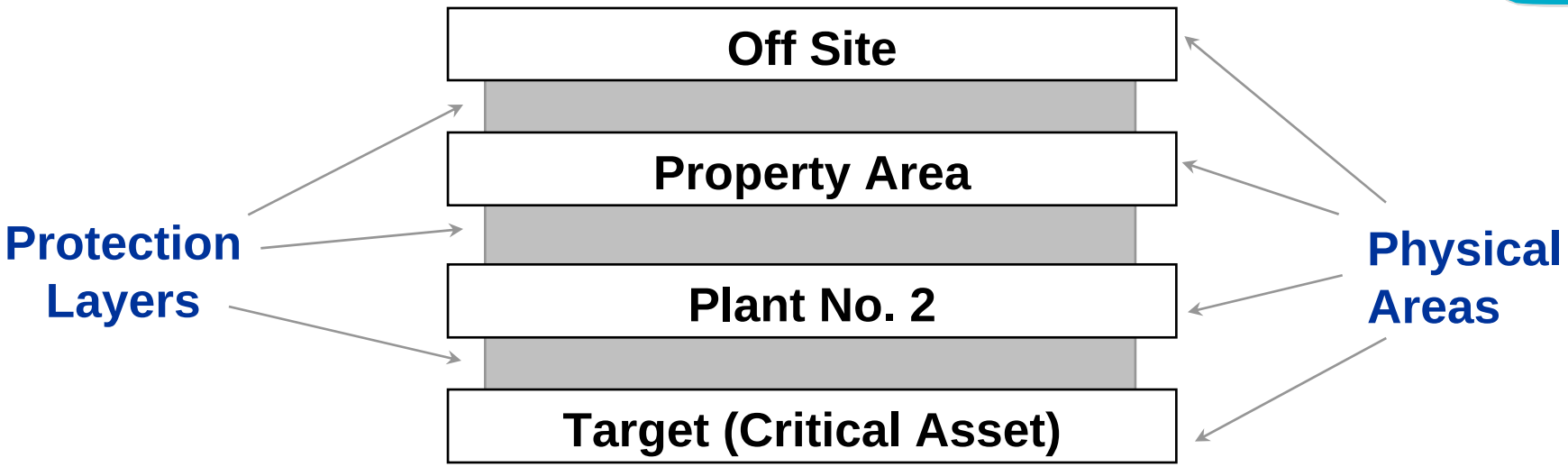
System Effectiveness

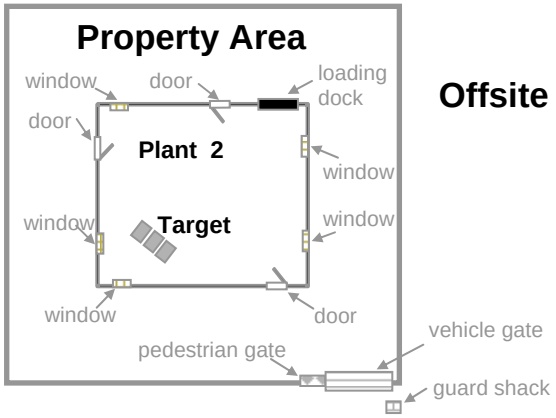
- A measure of how effectively the Physical Protection System (detection, delay, response) prevents an adversary from successfully causing an undesired event
- Also considers how operational, safety and emergency response measures prevent an undesired event
- Considers capabilities of the defined threat
- Review polices and procedures

Adversary Task Time vs. Physical Protection System



Adversary Sequence Diagram (ASD)





- Graphical model used to help evaluate effectiveness of a facility PPS
- Represents:
  - Paths that adversaries can follow to accomplish sabotage or theft
  - PPS elements along paths
- Used to determine most vulnerable path for specific PPS and threat

Risk Analysis and Reduction

- Determine relative risk
- Consider constraints
  - Legal, operational, budget, resources, etc.
- Accept risk or change:
  - Likelihood of attack, system effectiveness, and/or consequences
- Leaders and Facility Owners' Decisions
  - Acceptable risk?
  - What to budget?
  - How to balance risk?

Summary

- Long heritage of security analysis, design, implementation and testing
- Applications from hardened targets to critical infrastructure
- Systematic approach begins with requirements and ends with design that achieves these requirements
- SNL helps agencies understand their security issues and their solution options.