Security Layer Failures and Integrated Dependency

IAEA International Conference on
Physical Protection of Nuclear Material and Nuclear Facilities
13-17 November 2017

Brian Maxwell and Dyrk Greenhalgh
United States Department of Energy
Office of Enterprise Assessments

U.S. DEPARTMENT OF ENERGY

EA Enterprise Assessments

Presentation Outline

- Enterprise Assessments introduction
- Layers in security design
- Single points of failure
- Security component dependencies
- Security system dependencies
- Testing for integrated dependencies
- Case study
- Conclusion

Office of Enterprise Assessments

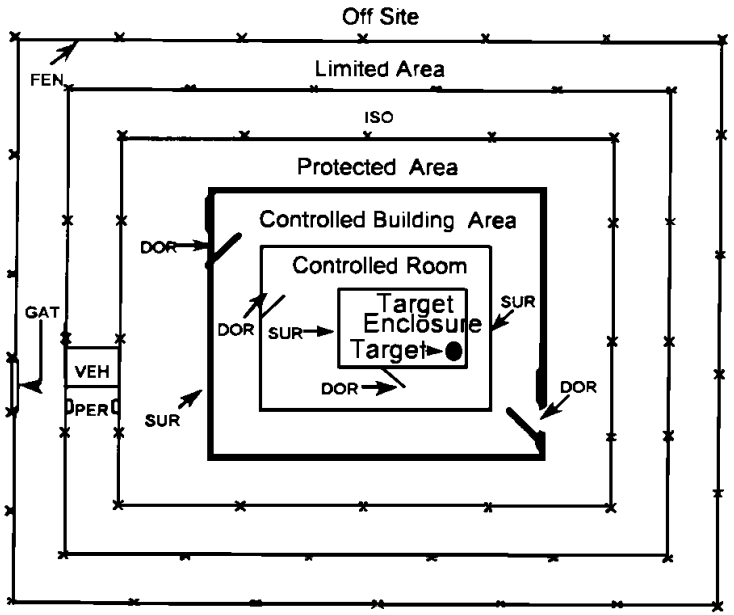
The Mission of the U.S. Department of Energy's (DOE) Office of Enterprise Assessments is to:

- Report on the status of protection measures of DOE sites
- Implement regulatory enforcement programs
- Operate the DOE National Training Center

Layers in Security Design

INFCIRC/225/Revision defines defense in depth as:

"the combination of multiple layers of systems and measures that have to be overcome or circumvented before physical protection is compromised."



Layers in Security Design

- Layers integrate various detection and delay components, and response strategies
- For example, an unauthorized attempt to penetrate a security layer would result in detection of adversary actions, delay of forward progress, and a response to interrupt the adversary
- A failure of a component in one layer should not affect other layers or components

Single Points of Failure

- Power systems
- Communications infrastructure
- Alarm management systems
- Non-complementary sensors
- Supply-chain management
- Personnel

Component Dependencies

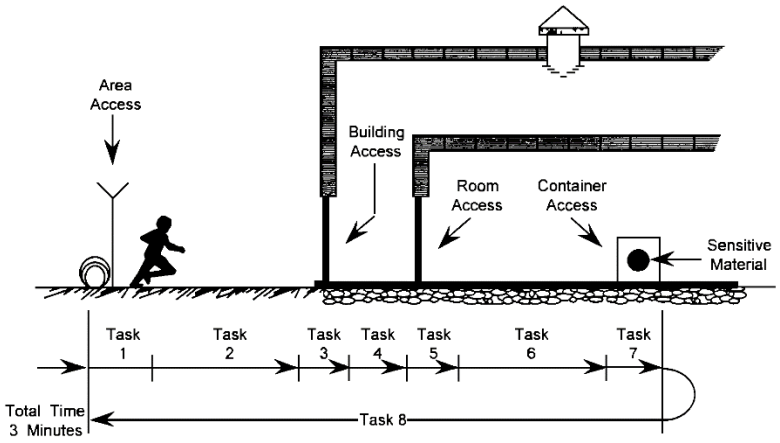
- Identical component use throughout the system
- Compensatory measures
- Life-safety override of security components

System Dependencies

- Detection, delay, and response order within a layer
- Programmatic elements
- Rules of engagement
- Performance assurance

Measuring Layer Interdependency

- Testing across system boundaries
- Scenario determination using adverse condition
- Difficulty in creating proactive policies



Time Estimate

Task	Mean Time (minutes)	Cumulative Time (minutes)	Task Description
1	0.1		Climb over fence
2	0.3	0.4	Run 76 m
3	0.8	1.2	Force door
4	0.4	1.6	Walk 45 m
5	0.2	1.8	Cut lock
6	0.1	1.9	Walk to container
7	0.2	2.1	Open container and gather material
8	0.9	3.0	Escape
	3.0		Total (approx. 3 minutes)

Case Study

Security Breach at Special Nuclear Materials Storage Facility

- Failures in testing and maintenance program
- High false alarm rates led to delay in alarm response
- Complacency of protective force officers
- Over reliance on inadequate compensatory measures
- Misinterpretation of and adherence to existing security policy
- Communications breakdown regarding ongoing facility repairs
- Inadequate funding and resource allocation
- Fractured management structure led to confusion of accountability and responsibility

Conclusion

- Common failure modes contribute to adverse affects throughout the entire system
- Broadening the evaluation of layer interaction is important
- Integrating this information with future design and enhancements provides additional layers of resilience

Thank You

Questions?

Brian Maxwell

Brian.Maxwell@hq.doe.gov

United States Department of Energy

Office of Enterprise Assessments