

# MULTI-ASSET PROTECTION AND RESILIENCE ASSESSMENT



**FRÉDÉRIC PETIT, JESSICA TRAIL, DAVID DICKINSON, AND JULIA PHILLIPS**

**Risk and Infrastructure Science Center  
Argonne National Laboratory**

Session D – Resilience Perspectives  
3<sup>rd</sup> National Symposium on Resilient Critical Infrastructure, Lisle, IL

August 18, 2016

# BACKGROUND

- Important to **identify the vulnerabilities** of multi-asset enterprises **and the enhancements** that could improve their resilience
- **Several guides and Standards**
  - NIST Special Publication 1190 – *Community Resilience Planning Guide*
  - Interagency Security Committee Standard - *The Risk Management Process for Federal Facilities*
  - *PS-Prep<sup>TM</sup> standards*
- **Require intermediate assessment** between the Infrastructure Survey Tool (IST) and the Regional Resiliency Assessment Program (RRAP)

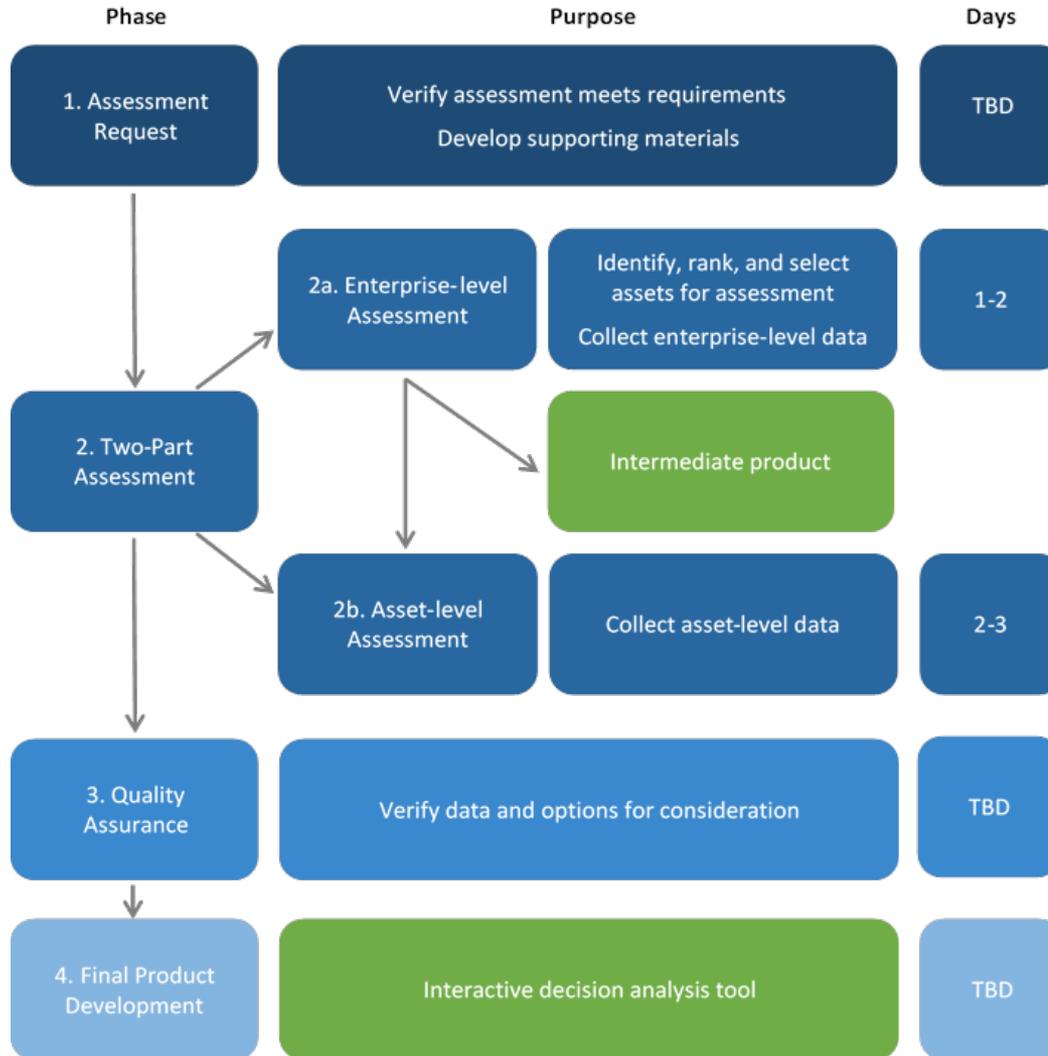
# CHALLENGES

- Apply to systems, campuses, and building clusters
  - Many buildings or facilities with diverse missions
  - Group of buildings or facilities belonging to a single organization that are in close proximity within a minimal or undefined perimeter area
  - University or college campus, a multi-facility entertainment venue, or geographically separated but connected systems
- Time and effort constraints for conducting the assessment
- Information sharing and data protection

# OBJECTIVES

- Allow comparison of the multi-asset enterprise's security, resilience, and dependency characteristics to other similar enterprises (e.g., water system to water system) across the Nation by way of enterprise-level indices
- Provide owners and operators with an interactive decision analysis tool to compare assets within the enterprise based on criticality and threat susceptibility
  - Identify vulnerabilities and prioritize corresponding options for consideration to better detect, deter, delay, mitigate, and recover from an adverse event at the asset- and enterprise-level
- Leverage the multi-criteria decision analysis methodology utilized within the Infrastructure Survey Tool

# PROPOSED PROCESS

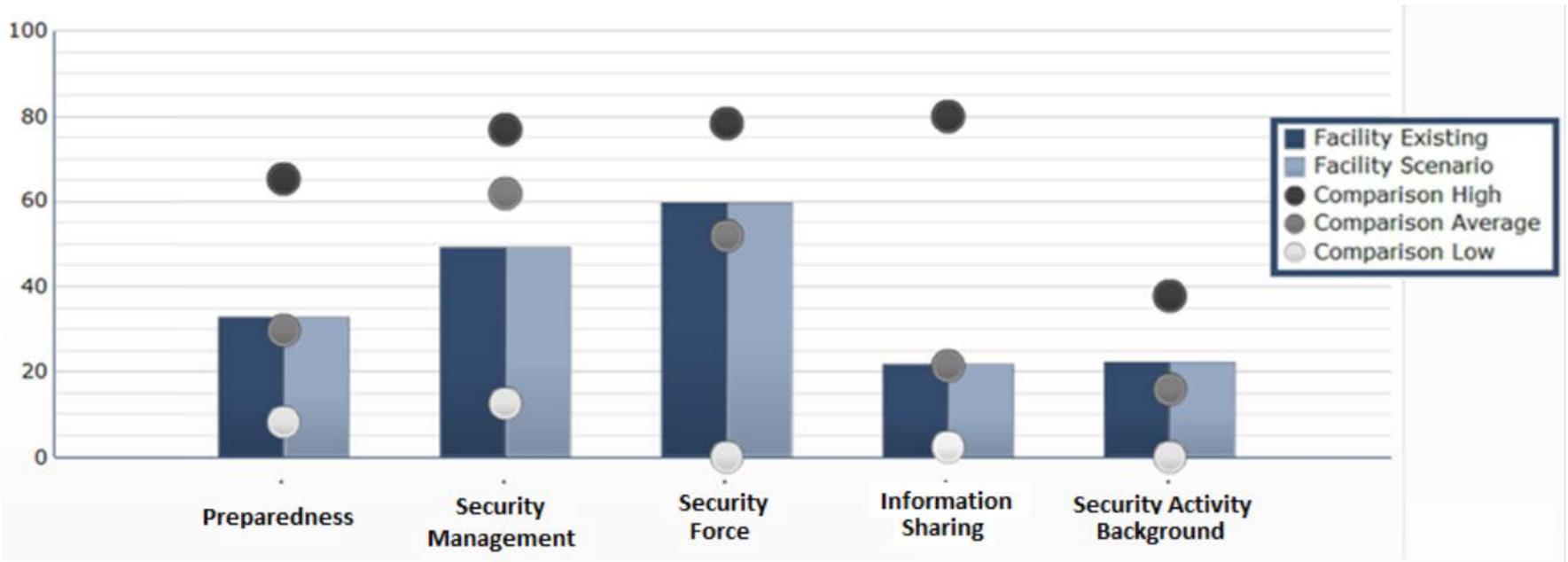


# PROCESS – ENTERPRISE-LEVEL ASSESSMENT

- Gather enterprise-level security management, resilience management, and dependency information
- Use of decision analysis and Multi-Attribute Utility Theory for defining enterprise-level indices:
  - Security Management
  - Security Force
  - Information Sharing
  - Security Activity Background
  - Preparedness (Resilience Management)

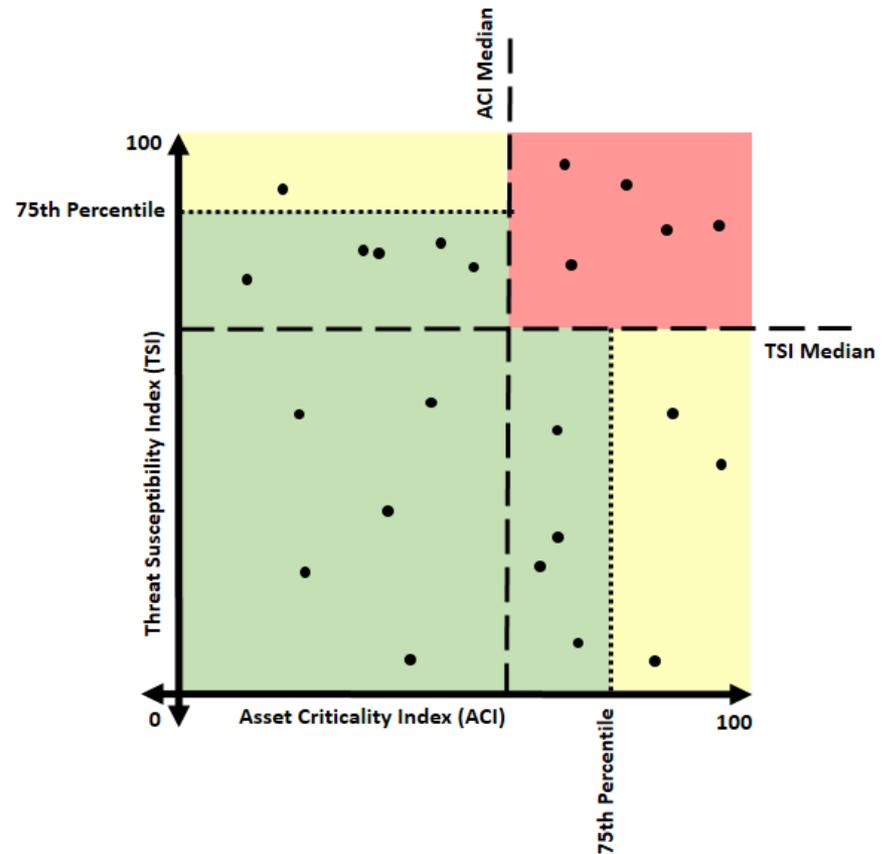
# PROCESS – ENTERPRISE-LEVEL ASSESSMENT

- Use questions from the [Infrastructure Survey Tool \(IST\)](#)
- Indices vary from 0 to 100



# PROCESS – ENTERPRISE-LEVEL ASSESSMENT

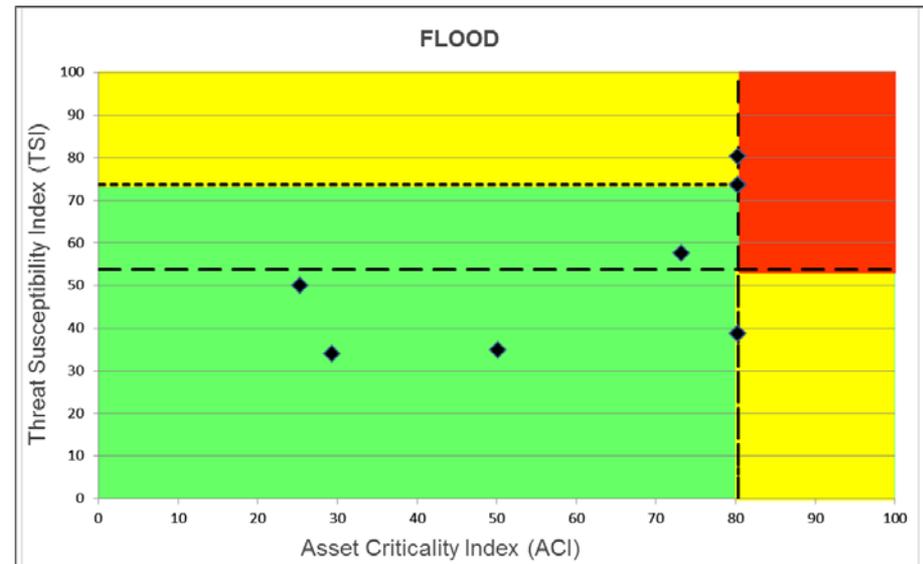
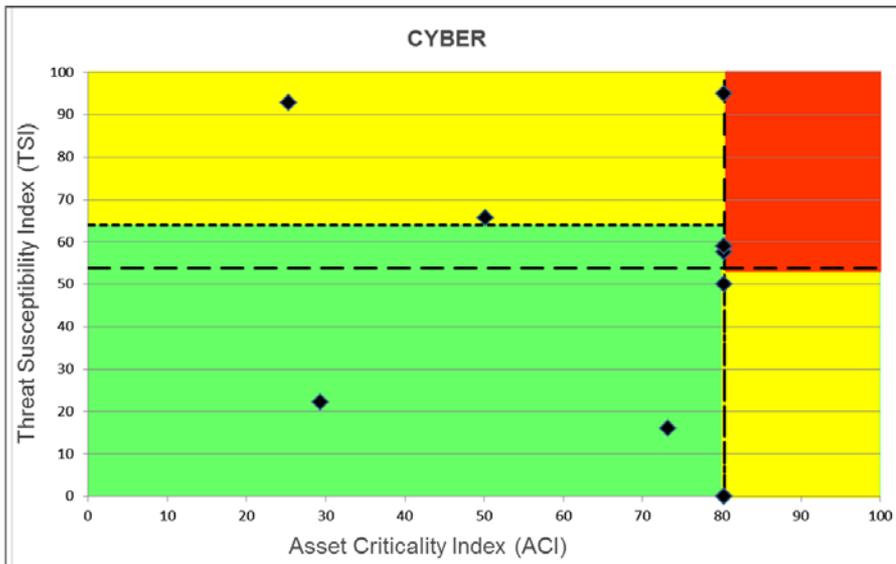
- Complete an **inventory of enterprise significant assets**
- Use **decision analysis principles**
  - **Asset Criticality Index (ACI):** Impacts (operational, loss of service, safety, and economic) and criticality modifiers (access and symbolic importance)
  - **Threat Susceptibility Index (TSI):** manmade threats (cyber and physical attack types) and natural hazards



# PROCESS – ENTERPRISE-LEVEL ASSESSMENT

Cyber		
Assets	Asset Criticality Index (ACI)	Threat Susceptibility Index (TSI)
Asset 1	25	93
Asset 2	29	22
Asset 3	50	66
Asset 4	73	16
Asset 5	80	0
Asset 6	80	0
Asset 7	80	58
Asset 8	80	59
Asset 9	80	50
Asset 10	80	95

Flood		
Assets	Asset Criticality Index (ACI)	Threat Susceptibility Index (TSI)
Asset 1	25	50
Asset 2	29	34
Asset 3	50	35
Asset 4	73	58
Asset 5	80	39
Asset 6	80	39
Asset 7	80	74
Asset 8	80	74
Asset 9	80	74
Asset 10	80	80



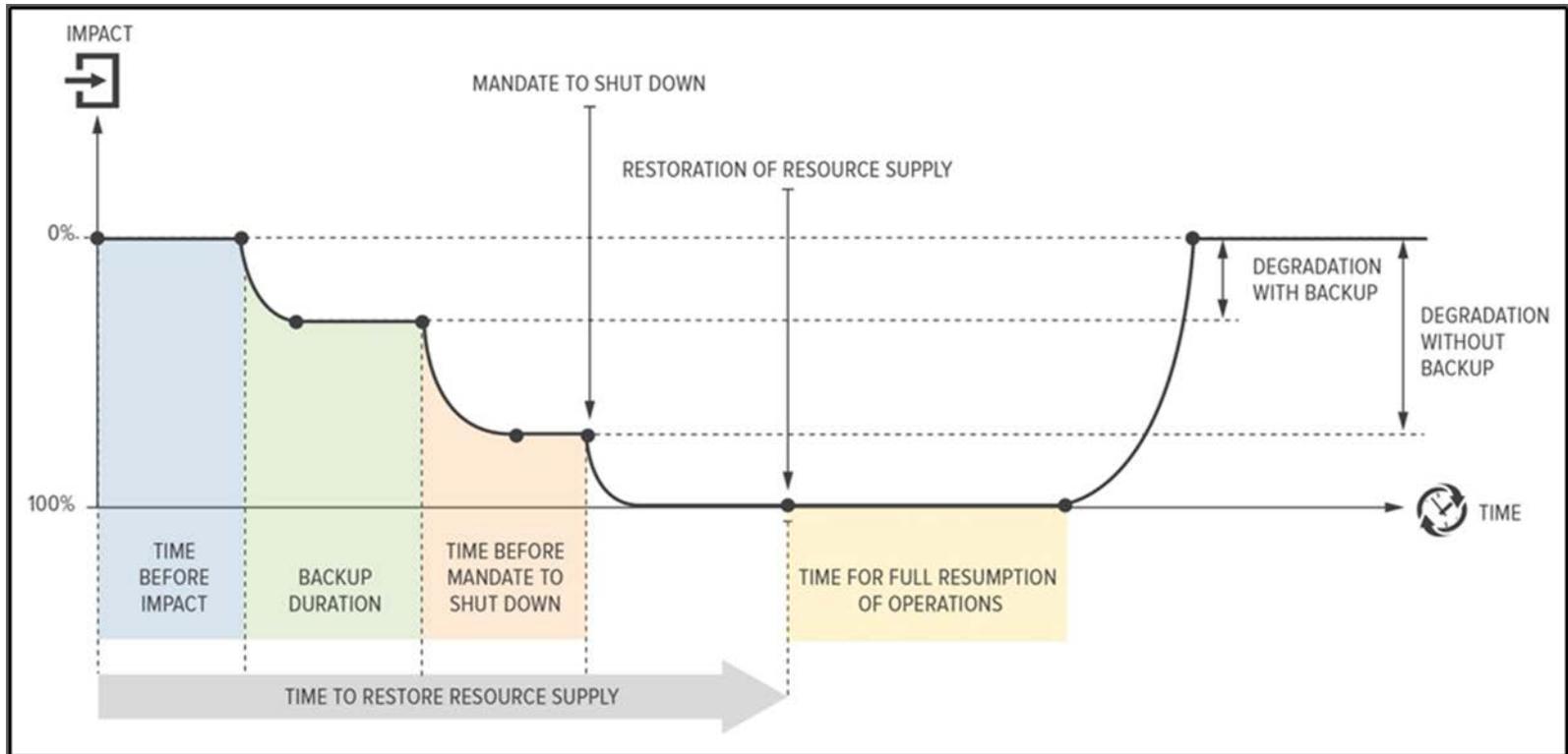
# PROCESS – ASSET-LEVEL ASSESSMENT

- Use the ranked list of assets with the highest asset criticality index and threat susceptibility index values to select assets to receive assessments
- Gather asset-specific security, resilience, and dependency information
  - Definition of vulnerabilities and options for consideration (VOFCs)
  - Characterization and visualization of upstream dependencies

# PROCESS – ASSET-LEVEL ASSESSMENT

- Identify asset vulnerabilities
  - The facility does not have a perimeter fence. The lack of perimeter fencing may allow unrestricted access to the facility and critical areas within the facility.
- Define options for considerations based on security and resilience standards
  - Install fencing appropriate for the facility type
  - Provide access control by channeling individuals through authorized access points
  - Explore the option of providing enhanced intrusion detection
  - Design the fence line to maximize natural surveillance

# PROCESS – ASSET-LEVEL ASSESSMENT



# POTENTIAL OUTPUTS

- **Interactive dashboard** of the enterprise-level assessment for security management, security force, resilience management, and dependencies
- **Assets ranking** populated with the data inputs determining each asset's asset criticality index and threat susceptibility index
- **GIS Display** of enterprise and critical assets:
  - asset metadata (e.g., latitude/longitude, type of asset)
  - dependency connections
  - criticality and threat susceptibility indices
  - asset-level rankings
- **Dependency Curves**
- **Table of all VOFCs**

# IMPLEMENTATION

- Amended the Infrastructure Survey Tool question set for the proposed assessment approach to include high-level security management and resilience management questions for enterprise-level data collection
- Conducted elicitations to weight asset criticality index factors, threat susceptibility index values, and threat susceptibility index threat categories
- Developed a data collection toolset
- Refine final products
- Apply methodology in pilot projects

# CONCLUSION

- A tailored security and resilience assessment approach is required for multi-asset enterprises with linked assets
- Need to prioritize assets for assessment, given time and effort constraints
- Address enterprise's interdependencies in order to provide a comprehensive perspective of overall risk
- Support decisionmaking to implement mitigation measures through an understanding of the vulnerabilities, capabilities, and impacts of loss of critical assets that make up the enterprise.

# THANK YOU!

# QUESTIONS?

**Frédéric Petit**

**Phone:** 630-252-8718

**Email:** [fpetit@anl.gov](mailto:fpetit@anl.gov)

The submitted presentation has been created by UChicago Argonne, LLC, Operator of Argonne National Laboratory ("Argonne"). Argonne, a U.S. Department of Energy Office of Science laboratory, is operated under Contract No. DE-AC02-06CH11357. The U.S. Government retains for itself, and others acting on its behalf, a paid-up nonexclusive, irrevocable worldwide license in said article to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government.