Campus-Wide Resilience Assessment

Prepared for

The 2nd National Symposium on Resilient Critical Infrastructure,
Resilience Week 2015, Philadelphia, PA

by

Frédéric Petit, Rosalie Laramore, David Dickinson, and Julia Phillips

Risk and Infrastructure Science Center, Global Security Sciences Division

Background

- Recent events reinforced the need for an all-hazards risk assessment for systems, campuses, and clusters of assets
  - September 2014: Fire in a Federal Aviation Administration air-traffic control center in Aurora, Illinois
  - April 2013: Assault on PG&E Corp's Metcalf Transmission Substation in California
  - July 2012: Trespassers gained access to a National Security Complex
  - June 2011: Los Alamos National Laboratory complex closed as an advancing wildfire threatened the installations

- Important to identify the vulnerabilities of utility systems and the enhancements that could improve their resilience

- NIST Special Publication 1190 – *Community Resilience Planning Guide* – and Interagency Security Committee Standard - *The Risk Management Process for Federal Facilities*

Challenges

- **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**

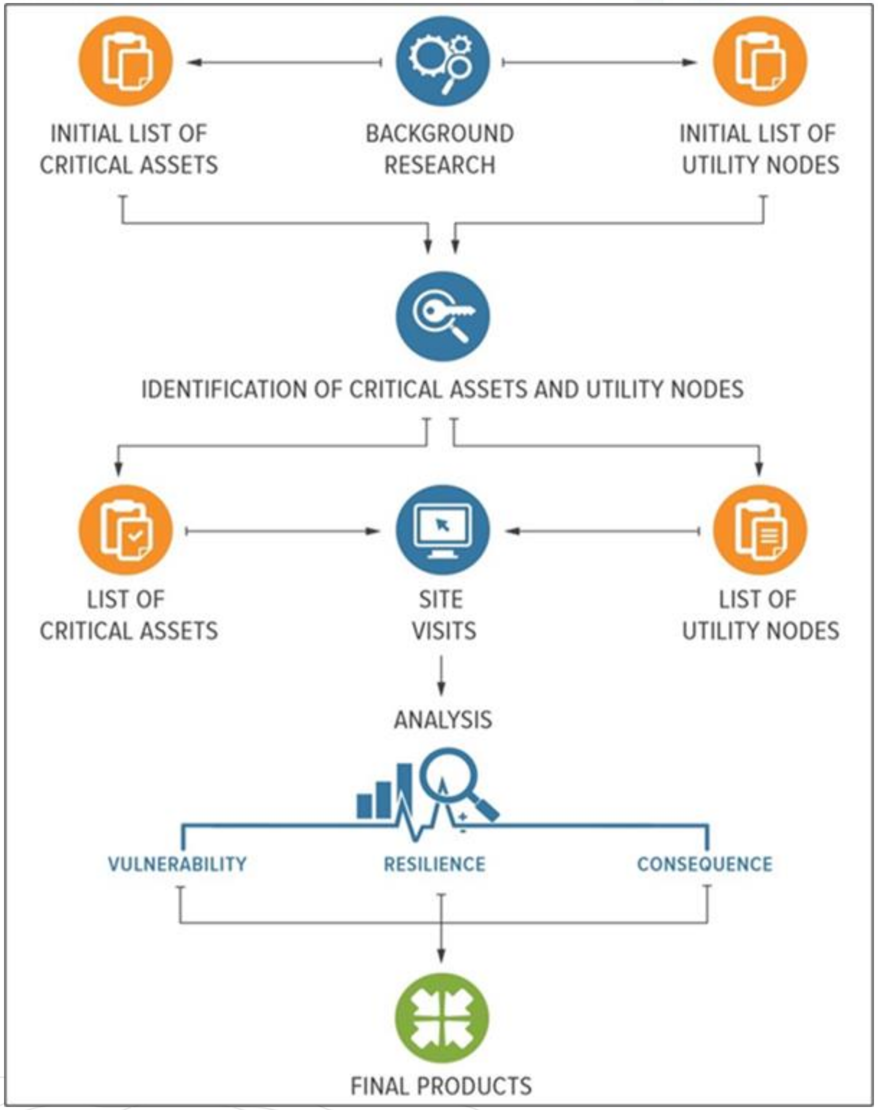
Objectives

- **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

- Verify that each critical asset can **support the enterprise wide protection and resilience posture**

- 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

Methodology



INITIAL LIST OF CRITICAL ASSETS

BACKGROUND RESEARCH

INITIAL LIST OF UTILITY NODES

IDENTIFICATION OF CRITICAL ASSETS AND UTILITY NODES

LIST OF CRITICAL ASSETS

SITE VISITS

LIST OF UTILITY NODES

ANALYSIS

VULNERABILITY

RESILIENCE

CONSEQUENCE

FINAL PRODUCTS

Background Research

- **Documents**
  - Previous reliability assessments
  - Security Operations Plan
  - Continuity of Operations Plan
  - Business Impact Analysis
  - Publicly available information

- **Initial List of critical assets and utility nodes**
  - Prioritize assets and utility nodes that are most critical for campus operations
  - **Critical assets:** buildings, equipment, or components critical for supporting essential campus functions and achieving campus missions
  - **Utility nodes:** components of utility systems that are essential for the functioning of campus' utilities and critical assets

Determining Asset Criticality

- **Function Disruption:** Percentage of the enterprise's operations that would be disrupted by the loss of the asset
  - Water system – delivery of treated water to customers
  - University or college campus – provide higher-level education to students
- **Mass Gathering:** Impact to people gathered at the asset
- **Economic:** Asset's economic contribution to the enterprise
- **Cascading Impacts:** Degree to which the loss of the asset extends beyond the enterprise's operations, for example:
  - Off-site population
  - Off-site economy
  - Other lifeline systems

Asset Criticality Index Factors

Factor	Scale				
Function Disruption	0%	1–33%	34–66%	67–99%	100%
Mass Gathering	**None** *Does not host gatherings*	**Low** *Hosts small gatherings*	**Medium** *Hosts medium-sized mass gatherings*	**High** *Hosts large mass gatherings*	**Highest** *Hosts the maximum number of people at the enterprise at any one time*
Economic	**None** *Generates no economic activity to the enterprise in a 12-month timeframe*	**Low** *Generates little economic activity to the enterprise in a 12-month timeframe*	**Medium** *Generates some economic activity to the enterprise in a 12-month timeframe*	**High** *Generates important economic activity to the enterprise in a 12-month timeframe*	**Highest** *Generates the most economic activity to the enterprise in a 12-month timeframe*
Cascading Impacts	**None** *No impacts on off-site population, off-site economy, or function of other systems*	**Low** *Minor impacts on off-site population, off-site economy, or function of other systems*	**Medium** *Some impacts on off-site population, off-site economy, or function of other systems*	**High** *Major impacts on off-site population, off-site economy, or function of other systems*	**Highest** *Greatest impacts on off-site population, off-site economy, or function of other systems*

Determining Threat Susceptibility

- **Physical Security:** Attacks intended to cause harm to a target
  - Improvised explosive devices, active shooters, and weaponization of an asset

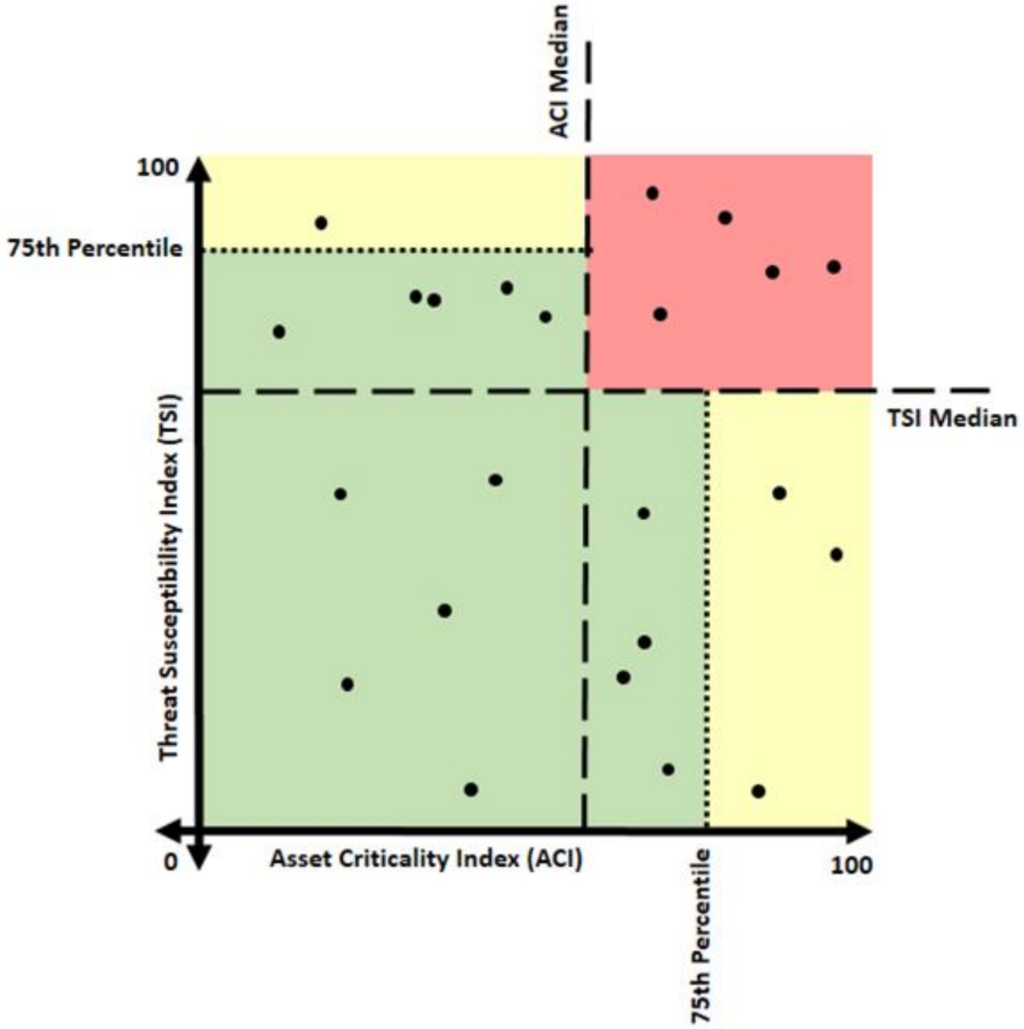
- **Natural Hazard:** Extreme meteorological, environmental, or geological events or combination of events that threaten lives, property, and other assets
  - Hurricanes, floods, and earthquakes

- **Utility Outage:** The loss of services or resources, such as electricity, gas, water, and wastewater
  - Electric power failures, natural gas outages, and water emergencies

- **Cyber:** Attacks perpetrated by an intentional threat source to alter an information system, its resources, its data, or its operations
  - Hacking and exploitation by trusted users (i.e., insider threat)

Selecting Assets to Receive Assessments

- **Red Area:** Assets with the highest asset criticality index (ACI) and threat susceptibility index (TSI) values
- **Green Area:** Assets with relatively lower ACI and/or TSI values
- **Yellow Areas:** Assets with high TSI values or high ACI values



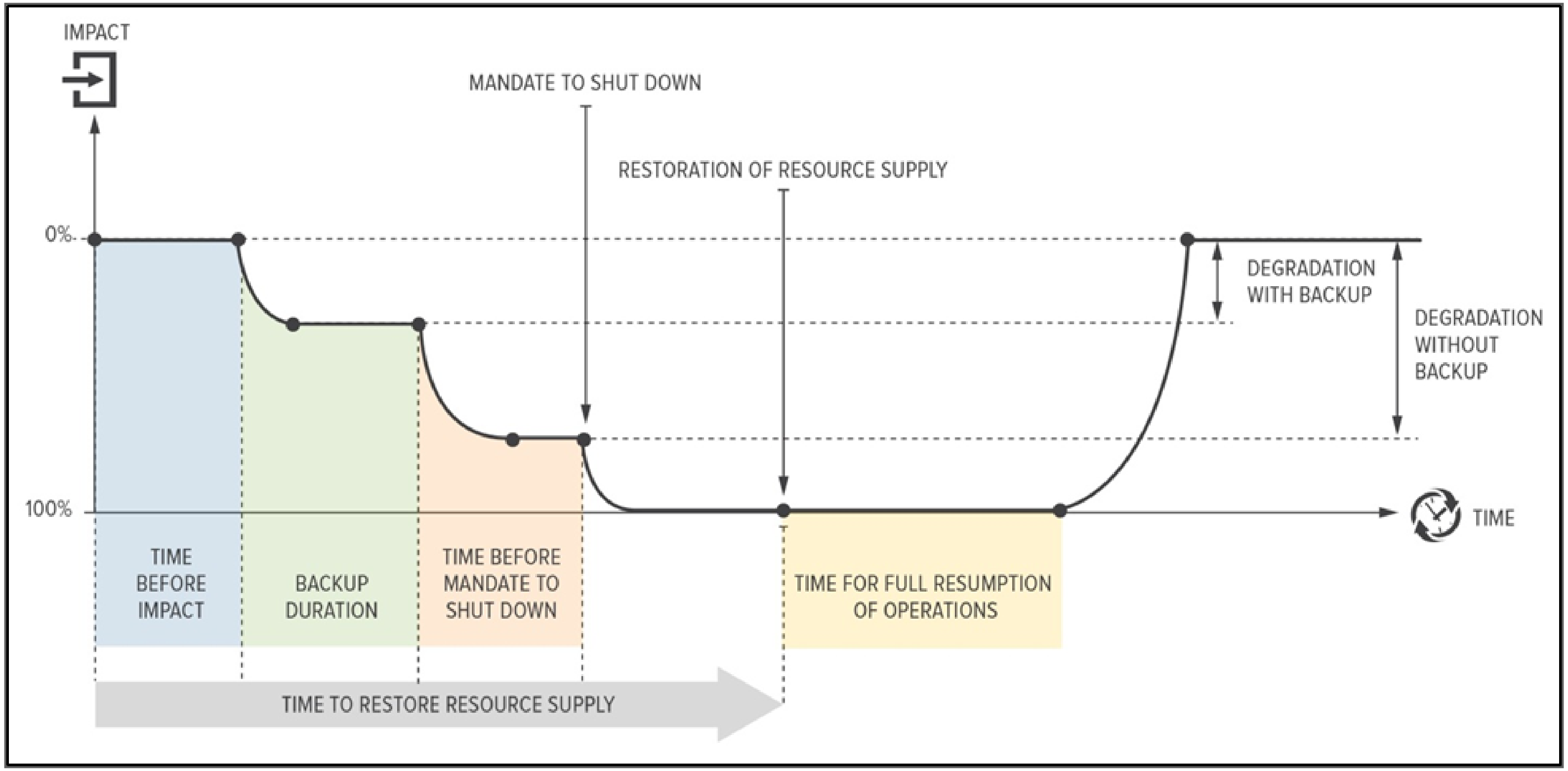
Vulnerability Analysis

Component	Definition	Influencing Factors
Physical security	Measures and features that protect a facility and its buildings, perimeter, and occupants from intrusion	The presence or absence of fences, gates, barriers, electronic surveillance (e.g., closed-circuit television and intrusion detection systems), parking controls, illumination, and entry-control procedures
Security management	Plans and procedures a facility has in place to deal with security issues	The presence or absence of a security manager, security plans and communications, procedures for handling suspicious packages and sensitive information, interactions with security working groups, and background checks
Security force	A special group of employees or contractors with security duties	The presence or absence of staffing, equipment, training, post orders, and a command-and-control system
Information sharing	The exchange of hazard and threat information with local, state, and federal agencies	The presence or absence of threat sources, employees with a national security clearance, coordination of security plans with local law enforcement, participation in security working groups, and written Memorandums of Understanding and Memorandums of Agreement with emergency services
Security activity, history, and background	Information related to previous vulnerability assessments and new protective measures that a facility may have implemented within the last year to improve its security posture	The presence or absence of prior vulnerability assessments, new and additional protective measures, different threat levels in security plans, and additional protective measures during elevated threat situations

Resilience Analysis

Component	Definition	Elements
Preparedness	Activities undertaken by an entity in anticipation of the threats/hazards, and the possible consequences, to which it is subject	Preparedness integrates awareness and planning elements. Specific actions that can be undertaken to enhance awareness related to an asset include the development of hazard-related information, including hazard assessments and information sharing, and the implementation of various measures designed to anticipate potential natural and manmade hazards. Planning-related activities include mitigation planning, response/emergency action planning, and actions undertaken to enhance continuity of operations
Mitigation measures	The facility's capabilities to resist a threat/hazard or to absorb the consequences from the threat/hazard	Mitigation measures consist of activities undertaken prior to an event to reduce the severity or consequences of a hazard. Mitigation is meant to capture information on whether the facility's owner or operator recognizes that the facility might be susceptible to certain hazards (e.g., flooding, tornadoes), has determined the possible consequences/impacts, and has undertaken efforts to mitigate the negative impacts those hazards might impose on the facility
Response capabilities	Immediate and ongoing activities, tasks, programs, and systems that have been undertaken or developed to respond and adapt to the adverse effects of an event	The on-site capabilities component groups elements of security/safety/emergency management. The off-site capabilities component groups elements characterizing the interactions with the emergency services sector to respond to an event (e.g., fire, medical emergency, or law enforcement issue) and support the facility within its boundaries. More specifically, response capabilities integrate information on emergency services and emergency operations centers
Recovery mechanisms	Activities and programs designed to be effective and efficient in returning operating conditions to a level that is acceptable to the entity	Important elements of recovery capabilities include existing restoration agreements, priority plans for restoration, and anticipated restoration time

Dependency Analysis


IMPACT
MANDATE TO SHUT DOWN
RESTORATION OF RESOURCE SUPPLY
0%
100%
DEGRADATION WITH BACKUP
DEGRADATION WITHOUT BACKUP
TIME
TIME BEFORE IMPACT
BACKUP DURATION
TIME BEFORE MANDATE TO SHUT DOWN
TIME FOR FULL RESUMPTION OF OPERATIONS
TIME TO RESTORE RESOURCE SUPPLY

Final Products

- **Interactive dashboard** of the enterprise-level assessment for security management, resilience management, and dependencies
- **Top-screen tool populated with the data inputs determining each asset's ACI and TSI** with the capability for the owner or operator to weight the threat categories differently
- **Display of enterprise and critical assets** with layers that demonstrate, for example, the following information:
  - Asset metadata (e.g., latitude/longitude, type of asset)
  - Dependency connections
  - Criticality and threat susceptibility indices
  - Final asset-level rankings
- Table of **common dependencies** within the enterprise
- Table of all **Vulnerabilities and Options for Consideration**
  - Can be manipulated to assist in their prioritization (e.g., those applicable to the most assets or those applicable to enterprise-level security and resilience management)

Conclusion

- A **tailored security and resilience assessment approach is required** for multi-asset enterprises with linked assets—possibly with diverse capabilities—where the loss of an asset impacts the whole

- Need to:
  - **Prioritize assets for assessment**, given time and effort constraints
  - **Address the interconnectedness** of the campus in order to provide a comprehensive perspective of overall risk
  - **Support decision-making** to implement mitigation measures designed to resist disruptive events on an enterprise level through an understanding of the vulnerabilities, capabilities, and impacts of loss of critical assets that make up the campus

Contact Information

Frédéric Petit	Phone: 630-252-8718 Email: fpetit@anl.gov
Rosalie Laramore	Phone: 630-252-1779 Email: rlaramore@anl.gov
David Dickinson	Phone: 630-252-5524 Email: ddickinson@anl.gov
Julia Phillips	Phone: 630-252-2505 Email: phillipsj@anl.gov

The work presented in this article was partially supported by Argonne National Laboratory under U.S. Department of Energy contract number DE-AC02-06CH11357. The submitted manuscript has been created by UChicago Argonne, LLC, Operator of 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.