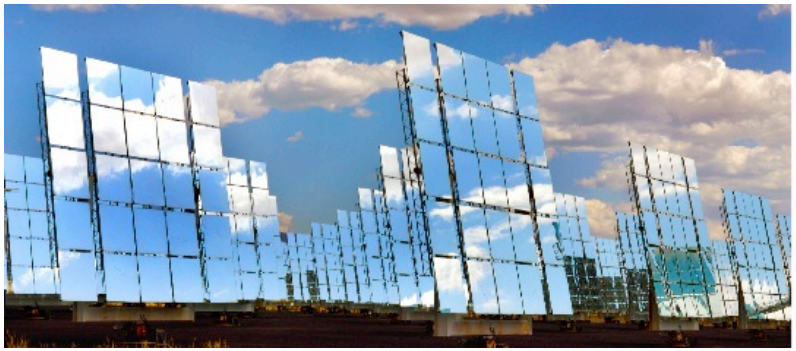
Exceptional service in the national interest

Sandia National Laboratories



Resilience Efforts for Micro and Macro Grids

Cesar A. Silva-Monroy

Oct. 8, 2015

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000

Defining Resilience

Presidential Policy Directive (PPD) 21

"the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."

-PPD-21: Critical Infrastructure Security and Resilience

"without some numerical basis for assessing resilience, it would be impossible to monitor changes or show that community resilience has improved. At present, no consistent basis for such measurement exists…"

-Disaster Resilience: A National Imperative, National Academy of Sciences

Reliability and Resilience

- Significant historical focus on power systems *reliability*
  - N-1 reliability – ensures delivery subject to the loss of exactly one system component (e.g., transmission line or generator)
  - Conceptually, these are binary boundary conditions…
  - … and say nothing about what happens when you cross the boundary!
- SNL proposed new, risk-based metrics for grid resiliency
  - Extend reliability definitions to include threat and consequence
- Metrics will be leveraged in two primary contexts
  - During operations
    - To facilitate operate-through and system recovery
    - To differentiate between equivalent "reliable" states
  - Planning
    - To adapt the system by justifying infrastructure investments
    - To recover rapidly when applied to sparing models

Grid Resiliency Metric Development

- Leveraging prior work at SNL for Department of Homeland Security
  - Not previously specialized to electric power systems

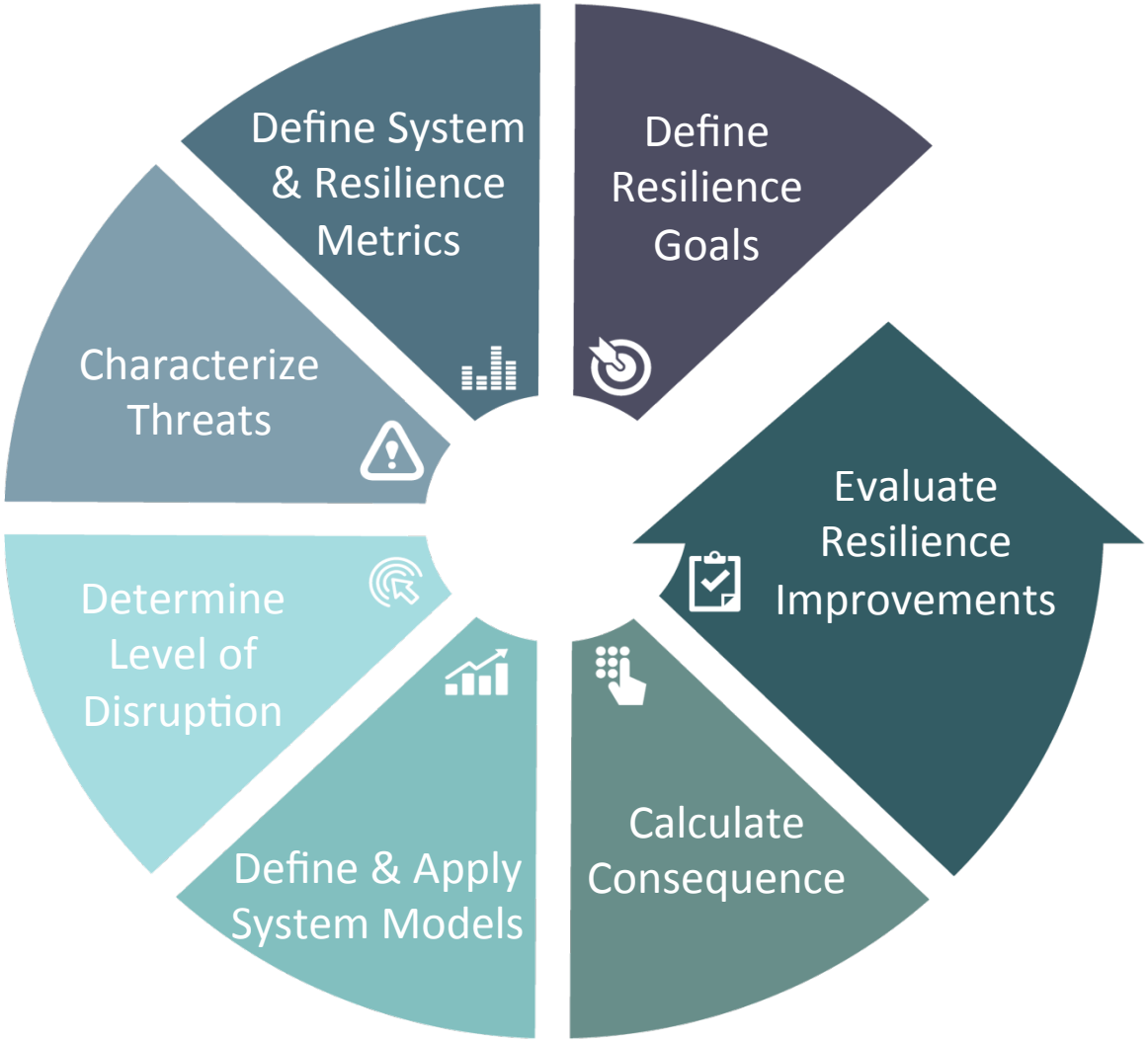
- Grid resiliency is a function of the threats under consideration

- Grid resiliency metrics are parameterized by:
  - Financial statistics ($/MW hour lost, fines, non-utility economic impact)
  - Safety statistics (deaths due to loss of load, emergency response failures)
  - Security statistics (impact on military and DHS concerns)

- Grid resiliency metrics are vector-valued functions
  - Vector components include relevant performance statistics (e.g., financial loss, safety measures, security measures)

- *Key challenge is utility and regulator acceptance and adoption*

Resilience Analysis Process



Define Resilience Goals

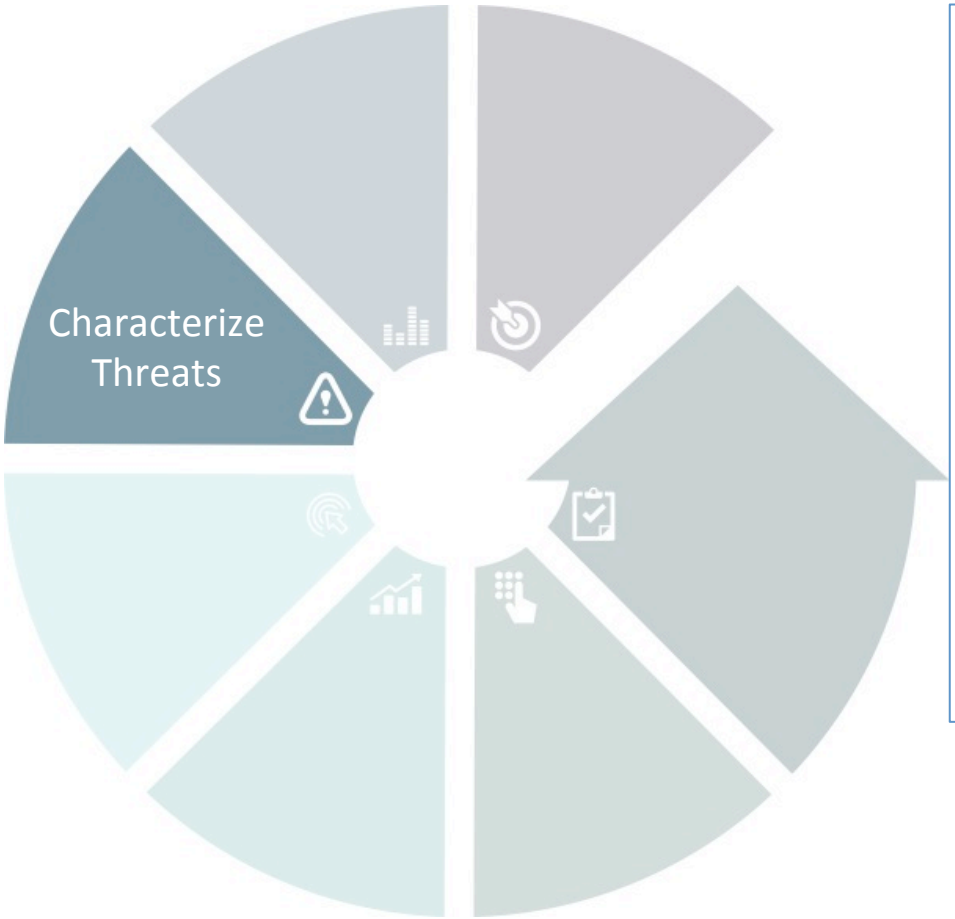
Determine:

- The decisions to by made
    - Assess vs. improve
- For improvements, the scope of potential changes
- The questions to address
- How resilience aligns with current processes
- The stakeholders and their concerns
- Where goals are in competition and where they align

Define System & Resilience Metrics

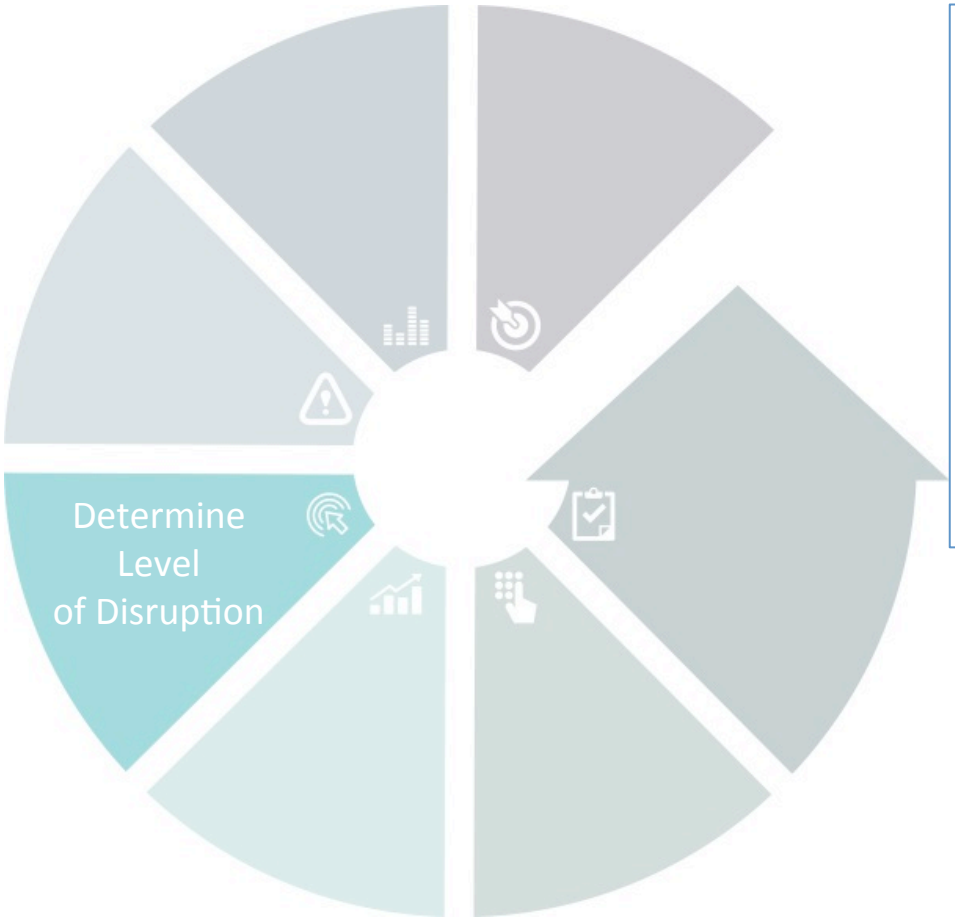
- Determine system boundaries
  - As broad or narrow as necessary to address goals
  - Dependent on stakeholders
- System will usually include multiple interdependencies
  - Infrastructure
  - Repair
  - Economics
  - ...
- Determine metrics necessary to measure progress

Characterize Threats



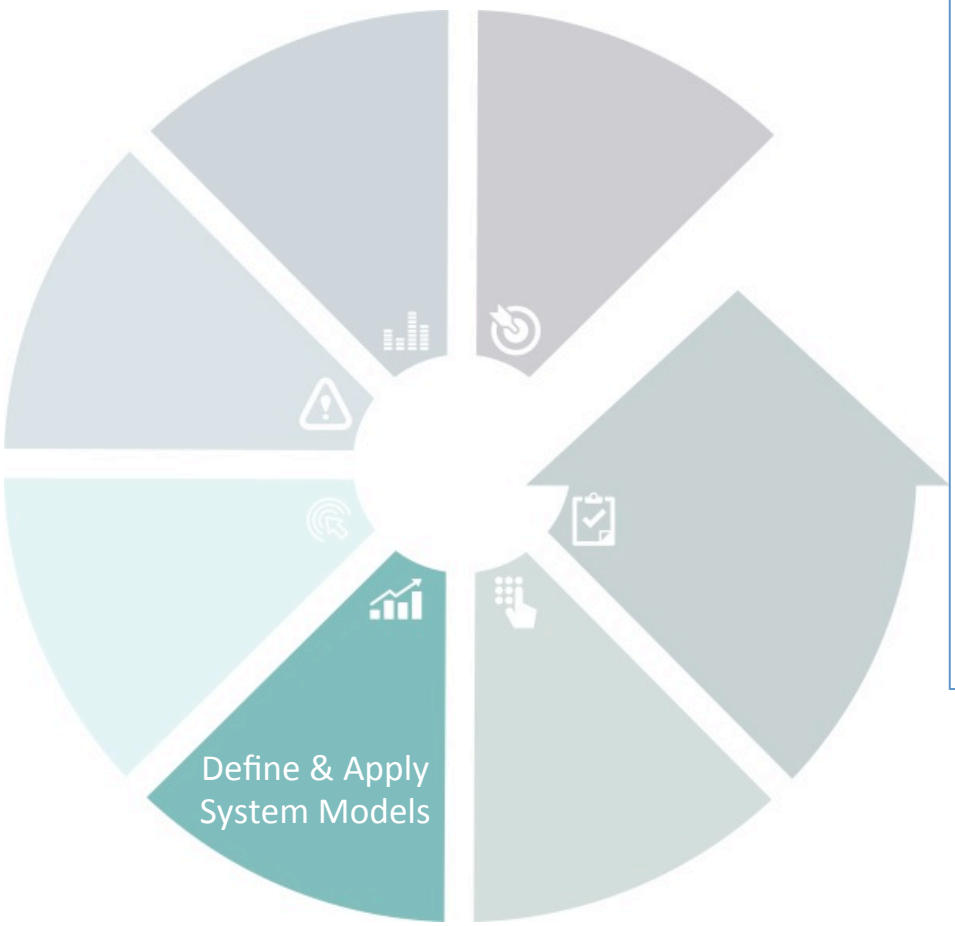
- Identify threats to the system
  - Natural disasters
  - Terrorism
  - Accidents
  - Aging
  - Global issues (i.e. climate)
- Characterize the threats and associated uncertainties
  - Subject Matter Experts (SMEs)
  - Historic data
  - Analytics
- Single-event vs. multi-event analysis

Determine Level of Disruption



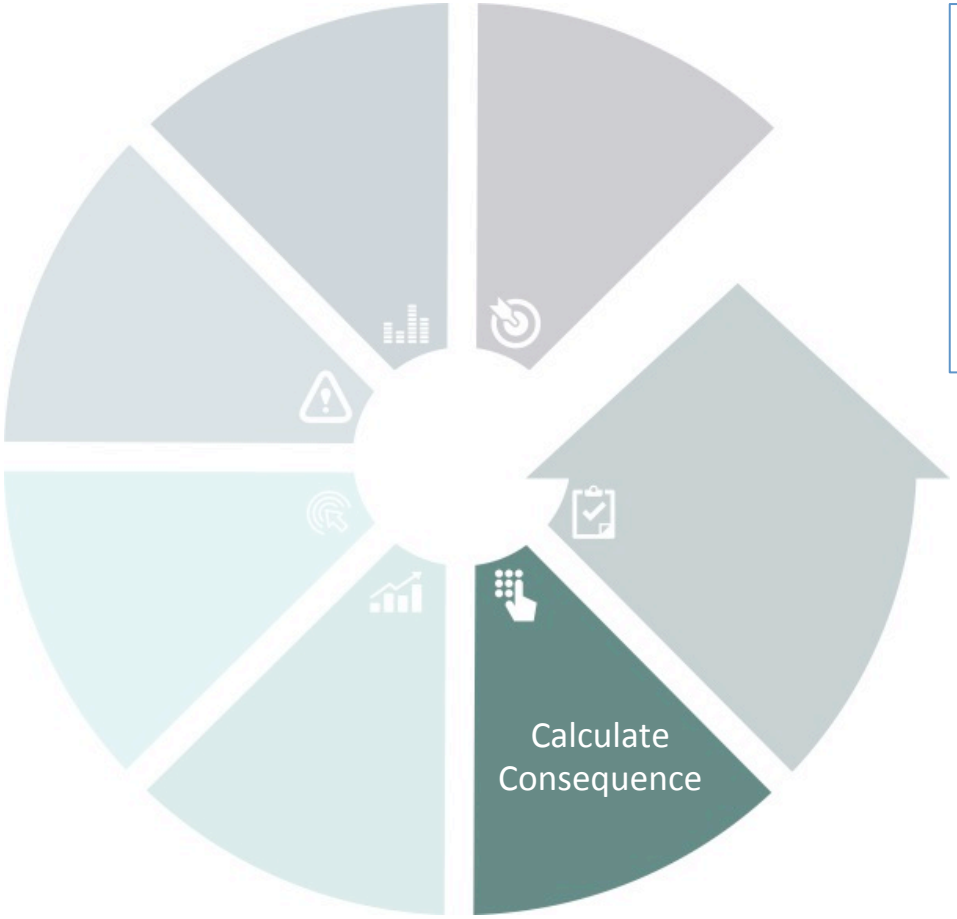
- Determine how the system is impacted by the identified threat
  - What elements are impacted?
  - What is the level of disruption?
- Determine in a similar manner to threats
  - SMEs
  - Historic data
  - Analytics (i.e. FEMA's HAZUS model)
- Characterize damage uncertainty

Define & Apply System Models



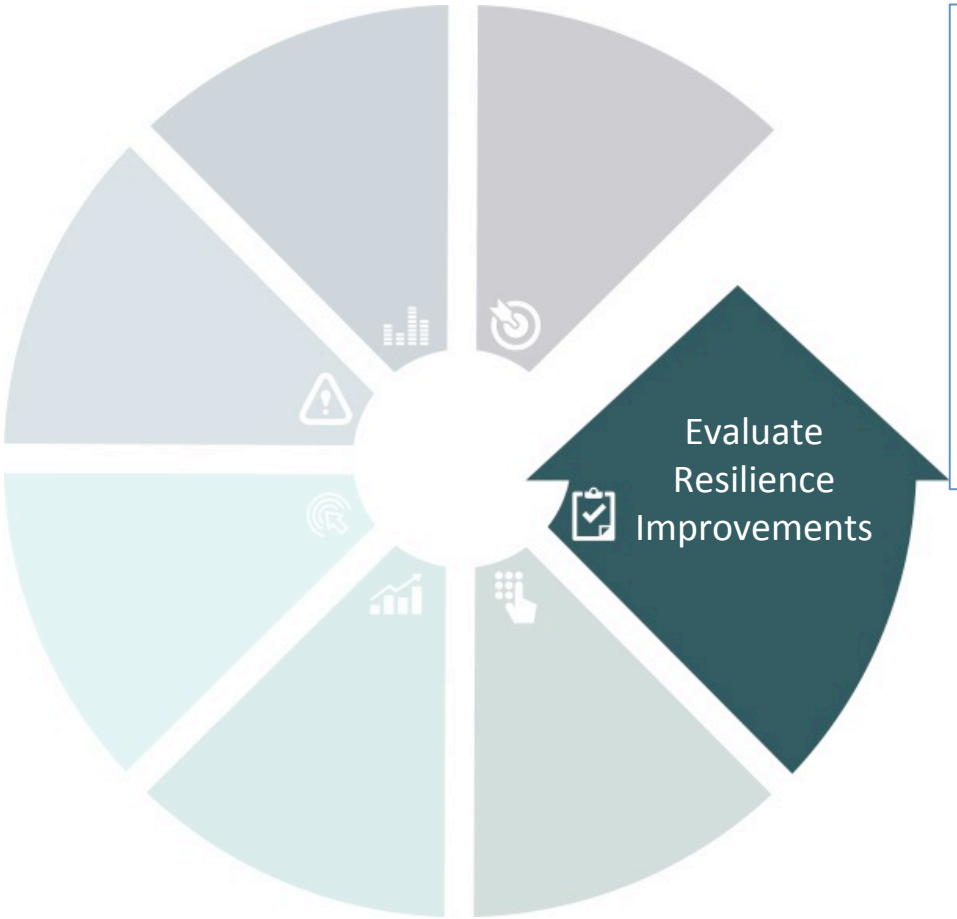
- Identify needs to assess system performance given disruption scenario
- Capture relevant aspects of sub-systems
- Many types of information may be required
    - Direct infrastructure models
    - Data, subject matter expertise
    - Economic, safety, and other analyses
- Interdependencies between different infrastructures will likely exist
- Additional uncertainty will arise
    - i.e., repair time uncertainty

Calculate Consequence



- Convert system performance indicators to defined resilience metrics
- Provides numerical basis for assessing system resilience
- Metrics characterized by probability distributions

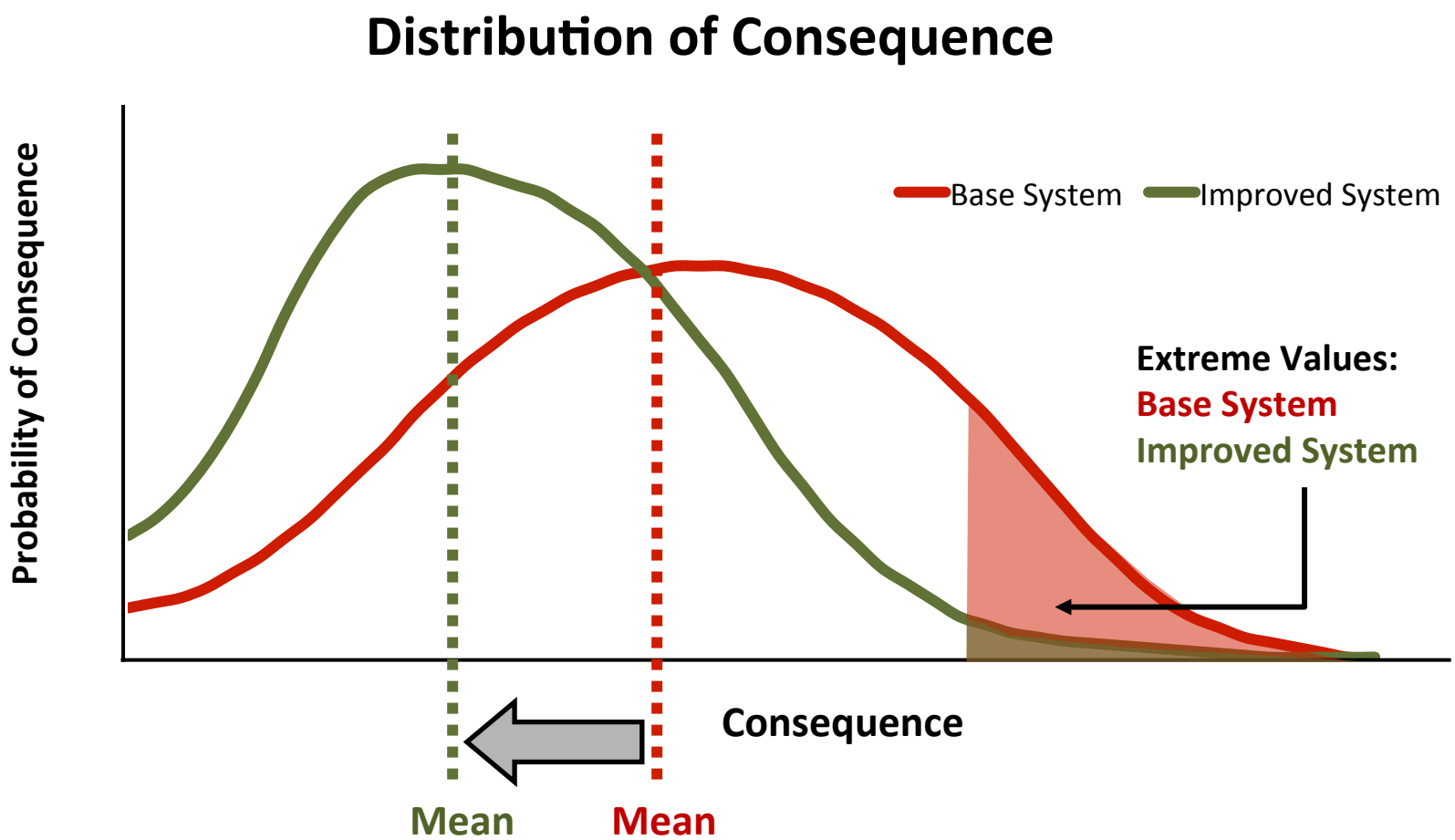
Evaluate Resilience Improvements



- Assess alternatives to improve resilience
  - Infrastructure improvements
  - Policy or operational changes
  - Additional resources for recovery
- Identify constraints (i.e. budget)
- Analyze alternatives and identify best strategies
- Track progress over time

Decisions are enabled by comparison of the energy system resilience metrics

Evaluate Resilience Improvements



Translating From Delivery Failure to Consequences

Moving from reliability to resiliency requires augmentation of the core reliability operations model with delivery failure consequence models and data

Consequence is quantified along a number of dimensions

Safety

Security

Economic

Distinct decision-makers focus on different aspects of consequence

a) Consequences are likely to be weakly or at most moderately correlated
b) Ultimately, resiliency analysis is multi-objective in nature

Cumulative MWh Not Served is NOT a Direct Measure of Consequence

Resiliency analysis shifts focus to what a delivery infrastructure enables

Examples of consequence due to MW hours not served include:

- Number of lives at risk
- Economic loss
- Impacts on interdependent infrastructures

Models that translate MW hours not served to consequence can vary dramatically in fidelity and computational requirements

- Simple scaling factors
- Spreadsheet models
- System dynamics models
- Simulation and agent-based models
- …

We acknowledge that MWh-to-consequence transformations involve both art and science – but they are critical to resiliency analysis

Current Projects at Sandia

- Resilience to Geomagnetic Disturbances (GMDs) in collaboration with PJM
- Resilience to weather, physical and cyber threats in collaboration with AEP

GMD Resilience Operations

- Main failure mechanism is voltage collapse due to reactive power loss in power transformers that provide a path to ground for Geomagnetically Induced Currents (GICs)
- Operations:
  - Change generator dispatch set points
  - Trade-off between increased operating costs and increase resilience
  - Threat is characterize using NERC's definition of GMD events
  - Alternative operating plan or guidelines to maximize resilience (minimize GMD consequences)
- Inputs:
  - Power flow case
  - GIS substation information
  - Transformer configuration and resistance
  - Substation grounding information

GMD Resilience Planning

- Planning:
  - Voltage support devices
  - GIC blocking devices
  - Where should I place these devices given a budget?
- Inputs
  - Same as for operations
  - Capital costs of hardening alternatives
- Non-linear stochastic optimization problem
- Leverage SNL's HPC resources

Multi-threat Resilience

- Considering a much broader set of threats
  - Weather
  - Physical
  - Cyber
- Operations
  - What are my most vulnerable assets?
- Planning
  - Which hardening options give me “best bang for buck”?
  - Sparing strategy
- SMEs at AEP to create a MWh lost to consequence translation and better understand/describe the threats

QUESTIONS

casilv@sandia.gov