

# Measuring and Enabling Resiliency\_\_\_ in Microgrids

### A. Srivastava, Washington State University

Associate Professor, Washington State University Director, Smart Grid Demonstration and Research Investigation Lab Co-Director, UI-ASSIST Center Contact: asrivast@eecs.wsu.edu September 3, 2018



Microgrid Symposiums Bucharest 2018



# What is resiliency?

Can we measure resiliency?

# How do we enable resiliency?

Learning based on projects: DOE CREDC, NSF Microgrid, DOE ARPA-E, GMLC 1.3.9 Idaho Falls, GMLC: City of Cordova (DOE RADIANCE Project), DOE AGGREGATE

# What is Resiliency?

#### definition

	[the ability] to recover and resume operations within acceptable levels of service.
	a cyber system's ability to function properly and securely despite disruptions to that system
	a holistic view of cyber risk, which looks at culture, people and processes, as well as technology
	A system's ability to withstand cyber attacks or failures and then quickly reestablish itself
	ability of systems and organizations to withstand cyber events
	ability to withstand and recover quickly from unknown and known threats
	an organization's ability to recover and return to normal operations after a cyber attack
	an organization's ability to respond to and recover from a cybersecurity incident
	the ability to provide and maintain an acceptable level of service when facing attacks and challenges to normal operation
0	Cyber resilience = cyber security + business resilience
1	the ability to operate the business processes in normal and adverse scenarios without adverse outcomes
2	identifying and responding to security breaches
3	the persistence of service delivery that can be justifiably be trusted, when facing changes and mainly regarded as fault tolerance
4	maintaining the system's critical functionality by preparing for adverse events, absorbing stress, recovering the critical functionality, and adapting to future threats
5	withstand a major disruption because of unknown event
6	organizations capability to cope with cyber attacks
7	'robustness' and 'survivability' measured in terms of performance and sustained availability. It also implies elements of both confidentiality and integrity
8	
_	The ability of a nation, organization, or mission or business process to anticipate, withstand, recover from, and evolve to improve capabilities conditions, stresses, or attacks on the supporting cyber resources it needs to function
9	the ability of a substance or object to spring back into shape
0	the ability of a system that is dependent on cyberspace in some manner to return to its original [or desired] state after being disturbed
1	the ability of an organisation to understand the cyber threats it's facing, to inform the known risks, to put in place proportionate protection, and to recover quickly from attack
2	the ability of an organization to continue to function, even though it is in a degraded manner, in the face of impediments that affect the proper operation of some of its components
3	the ability of cyber systems and cyberdependent missions to anticipate, continue to operate correctly in the face of, recover from, and evolve to better adapt to advanced cyber threats
4	the ability of systems and organizations to develop and execute long-term strategy to withstand cyber events
5	the ability of systems and organizations to withstand cyber events
6	the ability of systems to anticipate/withstand/ recover from attacks and failures
7	the ability to adapt and respond rapidly to disruptions and maintain continuity of operations
8	the ability to continuously deliver the intended outcome despite adverse cyber events
9	the ability to operate in the face of persistent attacks
0	the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions
1	the ability to prepare for and adapt to changing threat conditions while withstanding and rapidly recovering from attacks to infrastructure availability
2	the ability to prepare for and recover quickly from both known and unknown threats
3	the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation
4	the ability to recover from or easily adjust to misfortune or change
5	the ability to recover, returning to an original state, after some event that disrupts this state
6	the ability to withstand attacks and failures, as well as to mitigate harm more than in other domain
7	the capability of a supply chain to maintain its operational performance when faced with cyber-risk
8	the capacity to recover quickly from difficulties; toughness
9	

the ability Could resign processing of Clark-Ginsberg" (Stanford, DHS) a What Provide the redshiftence?"

the alignment of prevention, detection, and response capabilities to manage, mitigate, and move on from cyberattacks. It is the capacity of an enterprise to maintain its core purpose and integrity in the face of cyberattacks



It is not a question of "if" but a question of "who face significant physical and cyber threats, res priority for our electricity system.

 L. Smith, Chairman of the US House Science Technology Committee

https://science.house.gov/legislation/hearings/full-committee-hearing-resiliency-electric-grid-s-only-

Enhancing the **RESILIENCE** of the Nation's Electricity System

### **Resilience Motivation**



Stop/Prevent

extreme event

impact of



Minimize power outage downtime Supply critical loads during contingency



Microgrid, Renewable DER Integration

# Increasing Weather Events and Resiliency

400% increase in number of weather related power outages over the last 20 years, in US.







In 2012, Superstorm Sandy left more than 8.5 million customers without power.

Report on economic Benefits of Increasing Electric Grid Resilience to Weather Outages estimates the average annual cost of weather-related power outages to be between \$18 and \$33 billion over the past decade.

To reduce these losses and avert discontinuity of power supply during unfavorable weather events, we must re-engineer our existing systems to be *resilient* to weather changes.



Region-wise most financial losses as a result of power integruption due to weather-related events. Source: NCDC





## Resilience

 the power or ability to return to the original form, position, etc., after being bent, compressed, or stretched; elasticity.



 ability to recover readily from illness, depression, adversity, or the like; buoyancy.



Used since 1620 originated from Latin



**Withstand** any sudden inclement weather or human attack on the infrastructure.



**Respond** quickly, to restore balance in the community as quickly as possible, after an inevitable attack.



**Adapt** to abrupt and new operating conditions, while maintaining smooth functionality, both locally and globally.

Ρ

**Predict** or **Prevent** future attacks based on patterns of past experiences, or reliable forecasts.



## **Taxonomy of Resiliency**





## **Approaches towards studying Resiliency**

Consequence

J.

Probability



System A and System B show different resiliency based on what reconfiguration algorithms are there in the DMS [RAND]

Sandia National Lab Conceptual Framework for deriving Resiliency Metrics as a PDF. Higher Resiliency is shifting the peak to the left.

Consequence

Base System

Improved System

Extreme Values: Base System Improved System

Distribution of Consequence

Mean

Mean



## Multi-criteria Decision for Physical Resiliency



## **Overview of resiliency quantification process**



# Summary of steps to compute composite resiliency metrics



## **Test System: Multiple CERTS Microgrids**





#### CERTS Multiple Microgrids Topological Resiliency Analysis Results

Scenario	Nodes	$l_G$	< k >	$< k^2 >$	$p_c$	$f_c$	$\lambda_2$	$\Re_{\tau}$
Normal	29	3.248	2.029	5.63	0.44	0.64	2.317	0.83
$\mu G^1$ Island	29	2.444	2.294	5.36	0.62	0.62	3.213	0.87
$\mu G^2$ Island	29	2.667	1.931	7.84	0.48	0.66	3.563	0.91
$\mu G^1, \mu G^2$ Island	27	2.704	7.96	0.48	0.66	0.83	1.11	0.89

#### CERTS Multiple Microgrids Composite Resiliency Analysis Results

Scenario	p	$p_c$	$\lambda_{eqp}$	PFF	LNLF	$\Re_{\tau}$	R
Without DG	0.333	0.64	0.005	0.62	0.33	0.83	0.47
With DG, $\mu G^1$ Island	0.333	0.62	0.86	0.84	0.93	0.49	0.91
With DG, $\mu G^2$ Island	0.333	0.66	0.88	0.94	0.85	0.61	0.87
With DG, $\mu G^1$ , $\mu G^2$ Island	0.333	0.66	0.005	0.86	0.91	0.55	0.85

17



### **Measuring Resiliency in Alaska**



**Operational Resilience Metric** 

## What is CANVASS?

- Canvass stands for Cyber-Attacks and Network Vulnerability Analytics Software for Smart Grids
- Free, open-source, platform-independent resiliency-computation toolkit
- It can model extreme evnts and restoration and resiliency computation algorithms – with ability for user to define own metrics and scenarios.
- It enables easy power system modeling and interdisciplinary resiliency engineering research by abstracting lower level (hard-to-learn) open-source:
  - power simulation software [GridLAB-D],
  - network analysis library [NetworkX],
  - OS-based socket libraries [TCP/IP]
  - Packet Manipulation library [ScaPy]

into a single, easy-to-use Python package.

- Multiple interdependent infrastructure modeling, such as cyber-physical power grid, along with crew transport network.
- It can interface with Real-Time Simulation software through socket programming.

#### High-Level Multi-domain Application Layer



#### Low-level domain-specific APIs

https://sgdril.eecs.wsu.edu/research-interests-and-grants/industrial-grade-products/pycanvass/

## **Enabling Resilient Grid**



#### By System Design:

- · Redundancy and system approach
- Embedding resiliency concepts in operational and planning practice
- Automation, flexibility, adaptability, and physical network switching and hardening
- Resilient Communication Networking
- Providing incentive for resiliency

#### By Cyber Security and Weather Resistance Measure:

- Cyber-Physical Threat Detection
- Integrated Defense Plan

#### By Robust Computing and Data Analytics:

- Distributed coordination
- · Centralized, decentralized, distributed

#### By Robust Mathematical Algorithm and Robust Control:

- Distributed optimization
- Robust convergence and time guarantee
- Distributed coordination for RAS

#### By Physical System Measure:

- Reconfiguration and resource allocation
- Controlled islanding

## Interconnected Microgrid Networking Strategy to leverage available resources during contingencies



Utility Substation Bus Bar

## Resilience Analysis of Puerto Rico\* using CANVASS



## Takeaway: Resiliency metric is MCDM problem

The definition of resilience – depends upon our vantage point, or what we are investigating.

**Resilience is different from Reliability.** High Reliability does not ensure high resilience, but high resilience ensures high reliability.

Usually resilience depends on multiple factors.

Multi-criteria Decision Making (MCDM) approaches work well to define and quantify resiliency.

### Most important threat

- The most important threat to the power grid is a force of nature - <u>http://cybersquirrel1.com/</u>
- Humans have to catch up...



TOTAL SUCCESSFUL CYBER WAR OPS AS OF 2017.08.07 - 2111

Agent	Success
Squirrel	1049
Bird	556
Snake	101
Raccoon	90
Rat	49
Cat	24
Marten	23
Jellyfish	13
Human	3*

### **Further Reading**

- S. Chanda, A. Srivastava, M. Mohanpurkar, R. Hovsapian, "Quantifying Power Distribution System Resiliency Using Code Based Metric", IEEE Transaction on Industry Applications, 2017
- S. Chanda and A. K. Srivastava, "Defining and enabling resiliency of electric distribution systems with multiple microgrids," IEEE Trans. Smart Grid, 2016
- S. Chanda, and A. K. Srivastava, "Quantifying Resiliency of Smart Power Distribution Systems with Distributed Energy Resources", IEEE International Symposium on Industrial Electronics (ISIE), Buzios, Brazil, June 2015
- P. Bajpai, S. Chanda, A. Srivastava, "A Novel Metric to Quantify and Enable Resilient Distribution System using Graph Theory and Choquet Integral", IEEE Transactions on Smart Grid, 2016
- V. Venkataramanan, "A Real Time Cyber Physical Testbed for Microgrid Resiliency Analysis", M.S., August 2015
- A. Srivastava, G. Hemingway, A. Bose, J. Sztipanovits, S. Roy and C.-C. Liu, "Model-based Integration Technology to Enable Resilient Next-Generation Electric Grid", NSF Energy Cyber Physical System Workshop, Washington DC, December, 2013

# **Thank You**

# Acknowledgement: DOE including CREDC, NSF, INL

Our Disaster Recovery Plan Goes Something Like This...

Anurag K. Srivastava asrivast@eecs.wsu.edu

