# BPS Operational Resilience

**Bhesh Krishnappa**

**August 17, 2020**

# Agenda

- Why Resilience Matters
- Cyber Resilience Work at RF
- RF Cyber Resilience Assessment Tool
- Operational Resilience and Ongoing Work

# Risk Management vs. Resilience

**Limitations**

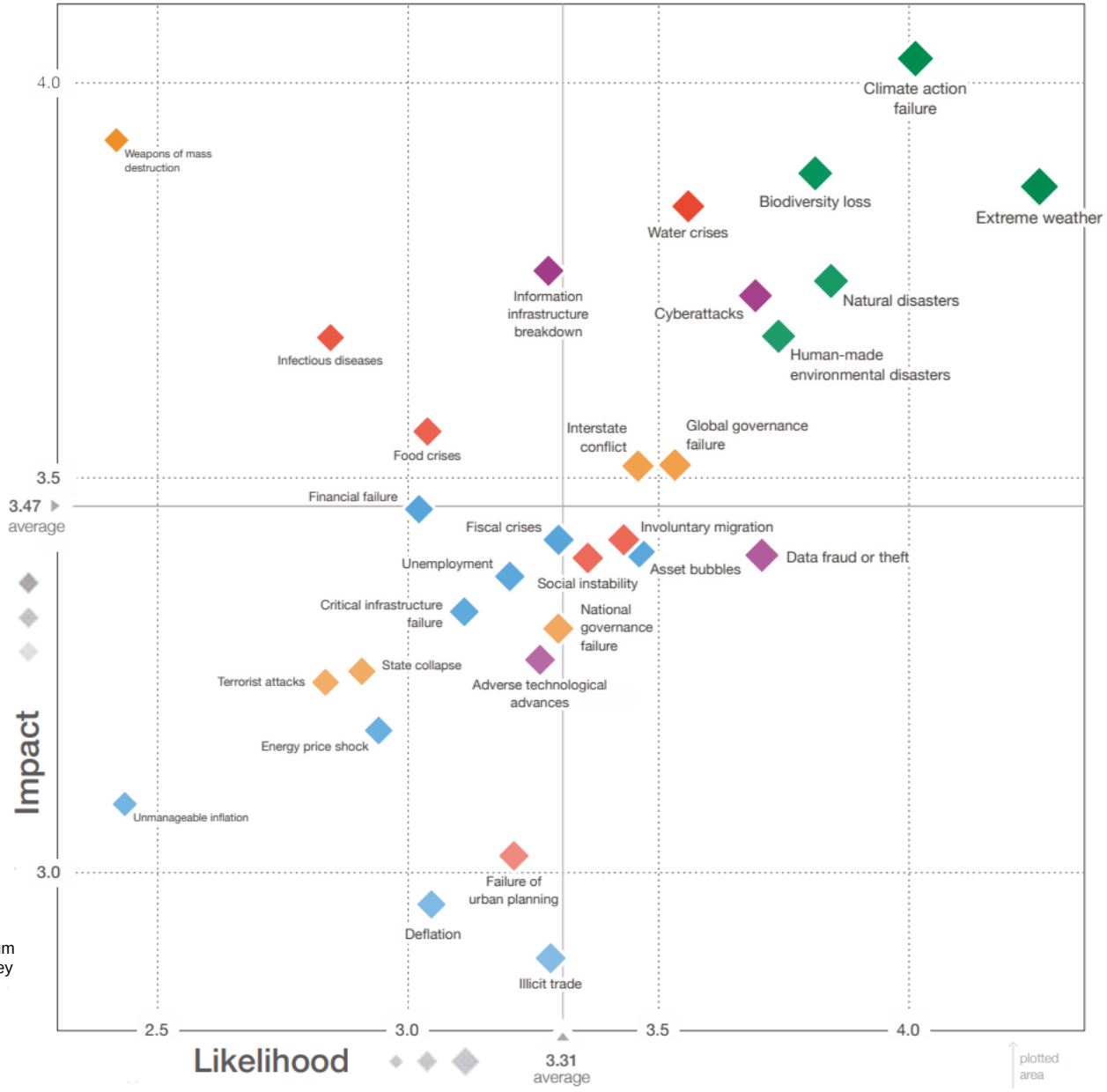
- Traditional risk management looks at risk reduction vs. enhancing the ability to deal with systemic risk
- All risks cannot be identified (anticipated) across all areas
- Risk quantification is difficult
- Black swans are increasing (i.e., weather, pandemic, physical/cyber attacks)

## Reductionist approach vs. strategic capabilities for agility and adaptation

Resilience enhances the risk management toolkit in several aspects and may lead to higher safety and security, in particular in a complex, interconnected risk landscape. We consider resilience-based strategies as an answer to systemic risk in a complex risk landscape.

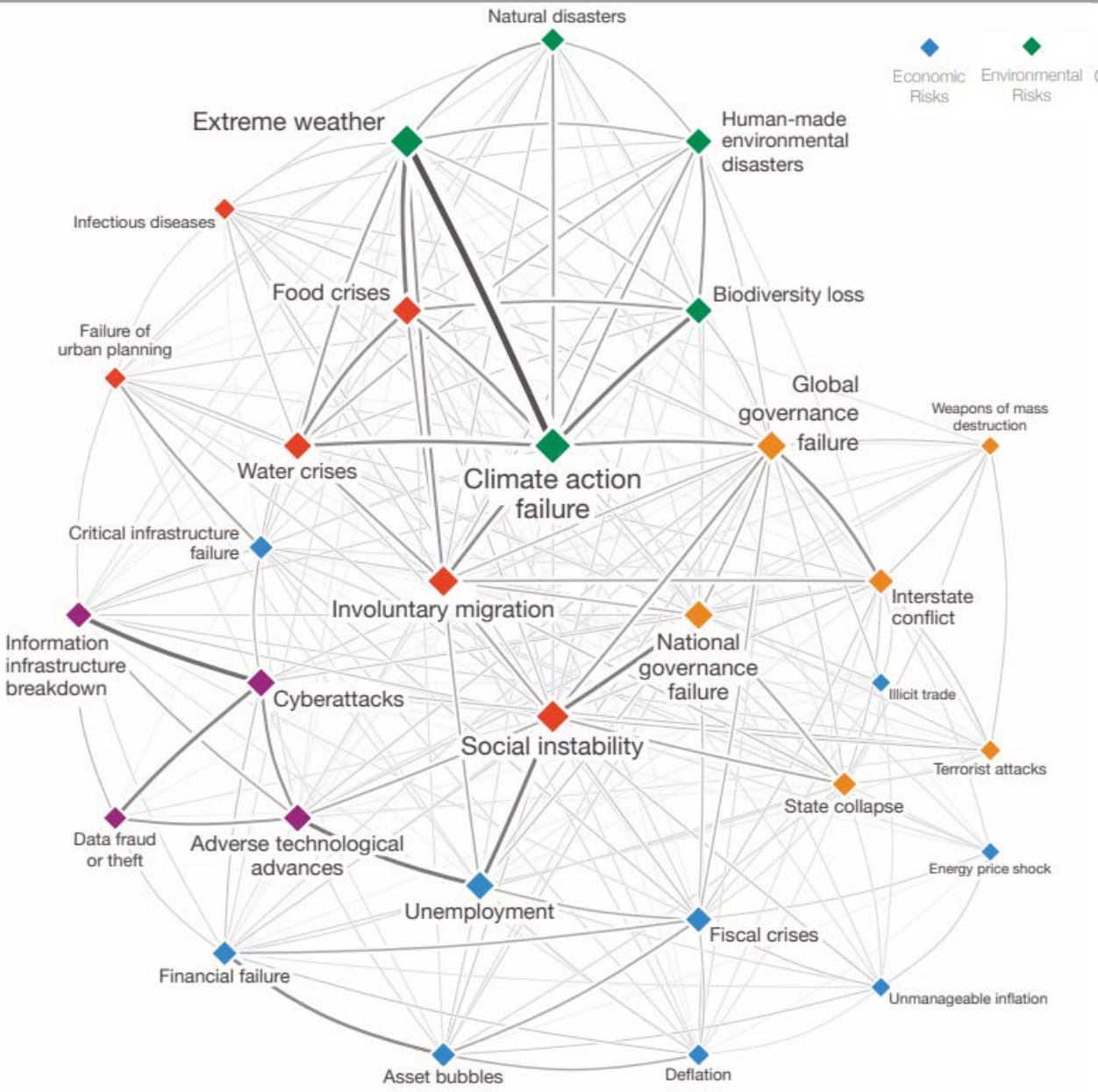
- International Risk Governance Council, 2020 Critical Infrastructure Resilience: Lessons from Insurance

# WEF The Global Risks Report 2020




Source: World Economic Forum Global Risks Perception Survey 2019–2020.

# Systems Thinking in a Connected World?

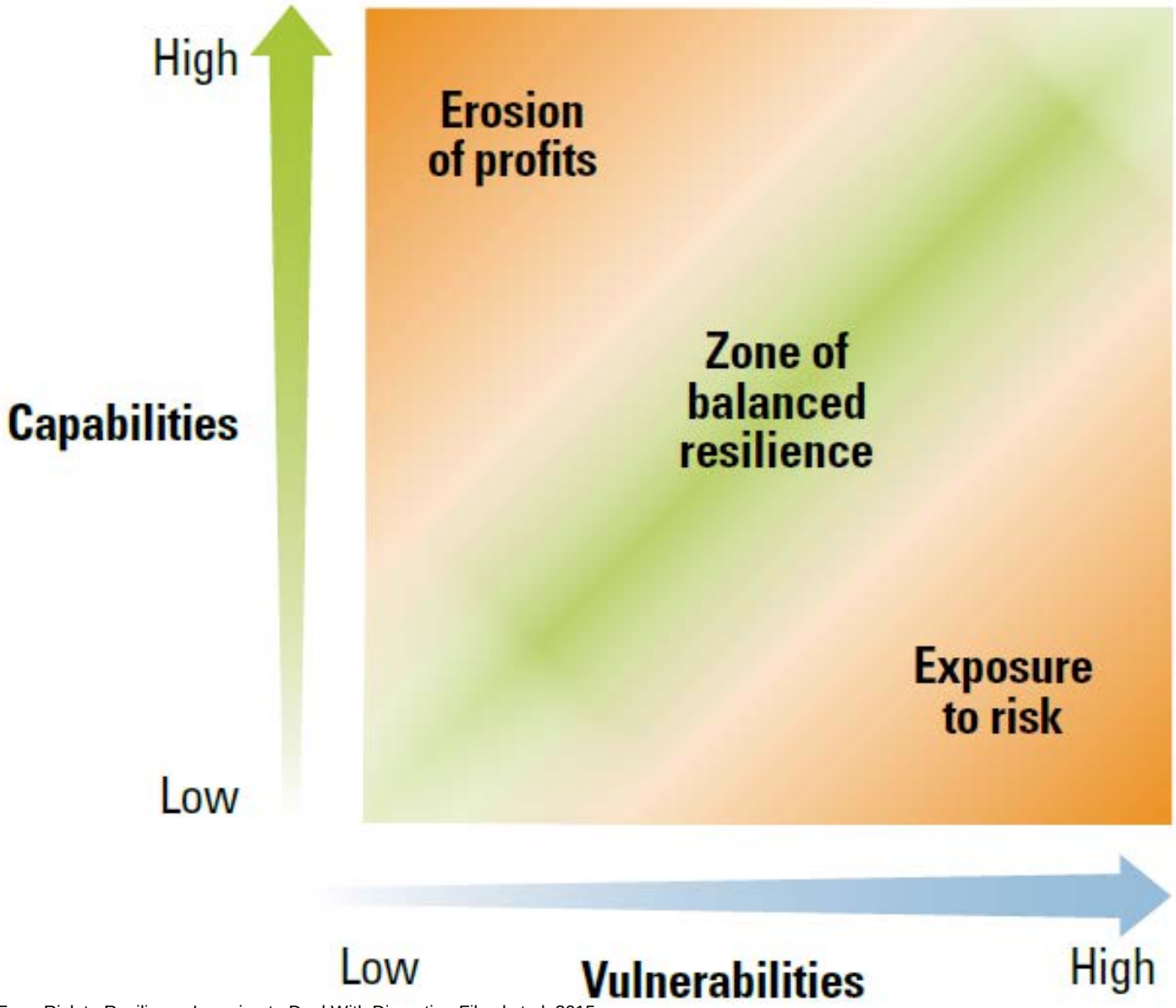




Source: The Global Risks Interconnections Map 2020

"The increasing volatility, complexity and ambiguity of the world…calls for a **resilience imperative** – an urgent necessity to find new opportunities to mitigate, adapt, and build resilience against global risks through collaboration among diverse stakeholders."
*—WEF Global Risks Report 2016*

# Zone of Balanced Resilience




Source: From Risk to Resilience:Learning to Deal With Disruption.Fiksel et al, 2015

# Advantages of Resilience Indicators

- **IDENTIFY** factors contributing to resilience
  - Investments with better ROI, or actions that enhance the resilience of the electric grid
  - Support risk management and mitigation decisions
- **MOTIVATE BPS** operators to continually assess their resilience capabilities and benchmark their performance
- Create **AWARENESS** on factors contributing to grid resiliency
- **FACILITATE** conversations inside the company on resilience indicators (healthy internal discussions that improve resilience)

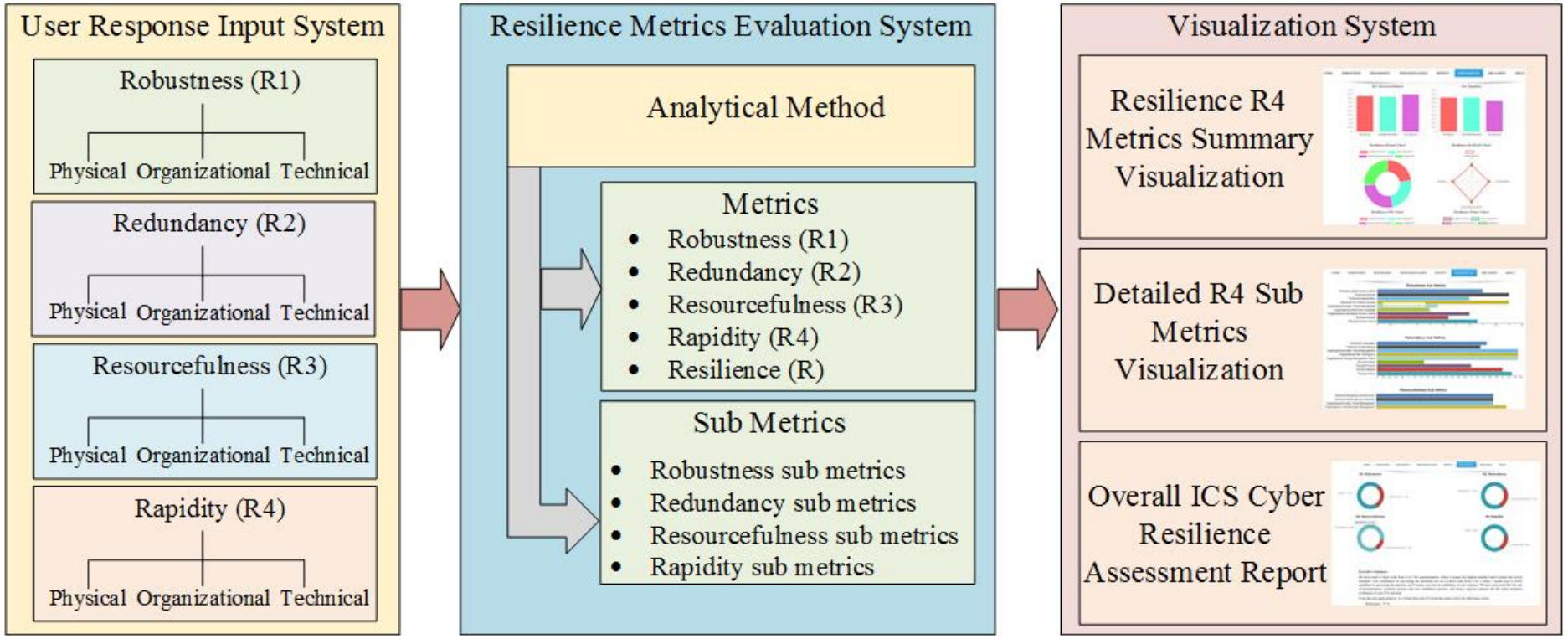
# Slido.com Poll

## What does Resilience mean to your organization?

Login to Slido.com (a virtual Q&A/polling tool) using the event code **#TechTalkRF** to share your answer. All feedback is anonymous, but we show the aggregate group feedback in realtime.

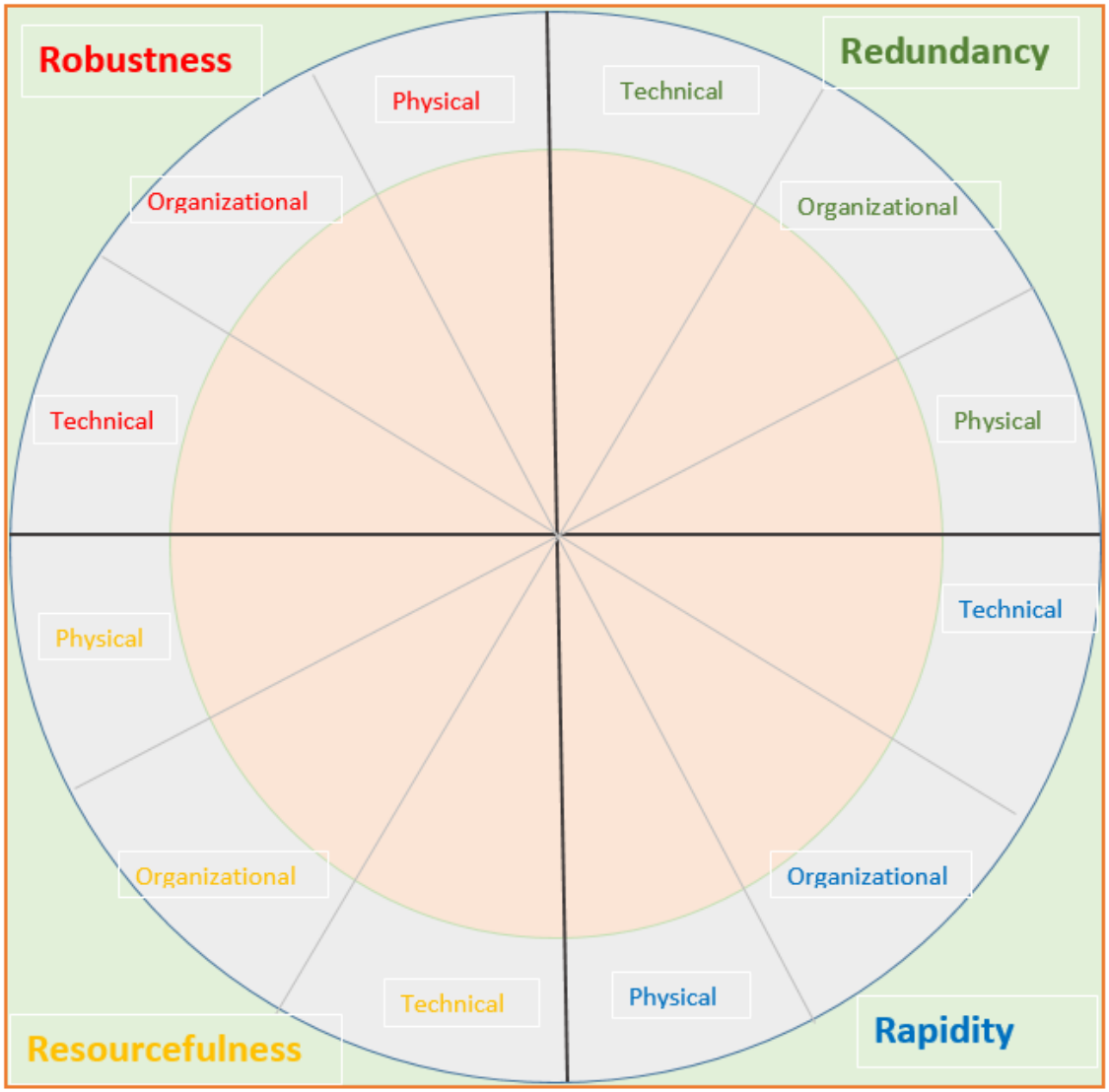
# RF Cyber Resilience Assessment Approach

## Quantitative vs. Qualitative



# R4 Framework

Ability of systems to withstand disaster forces without significant degradation or loss of performance



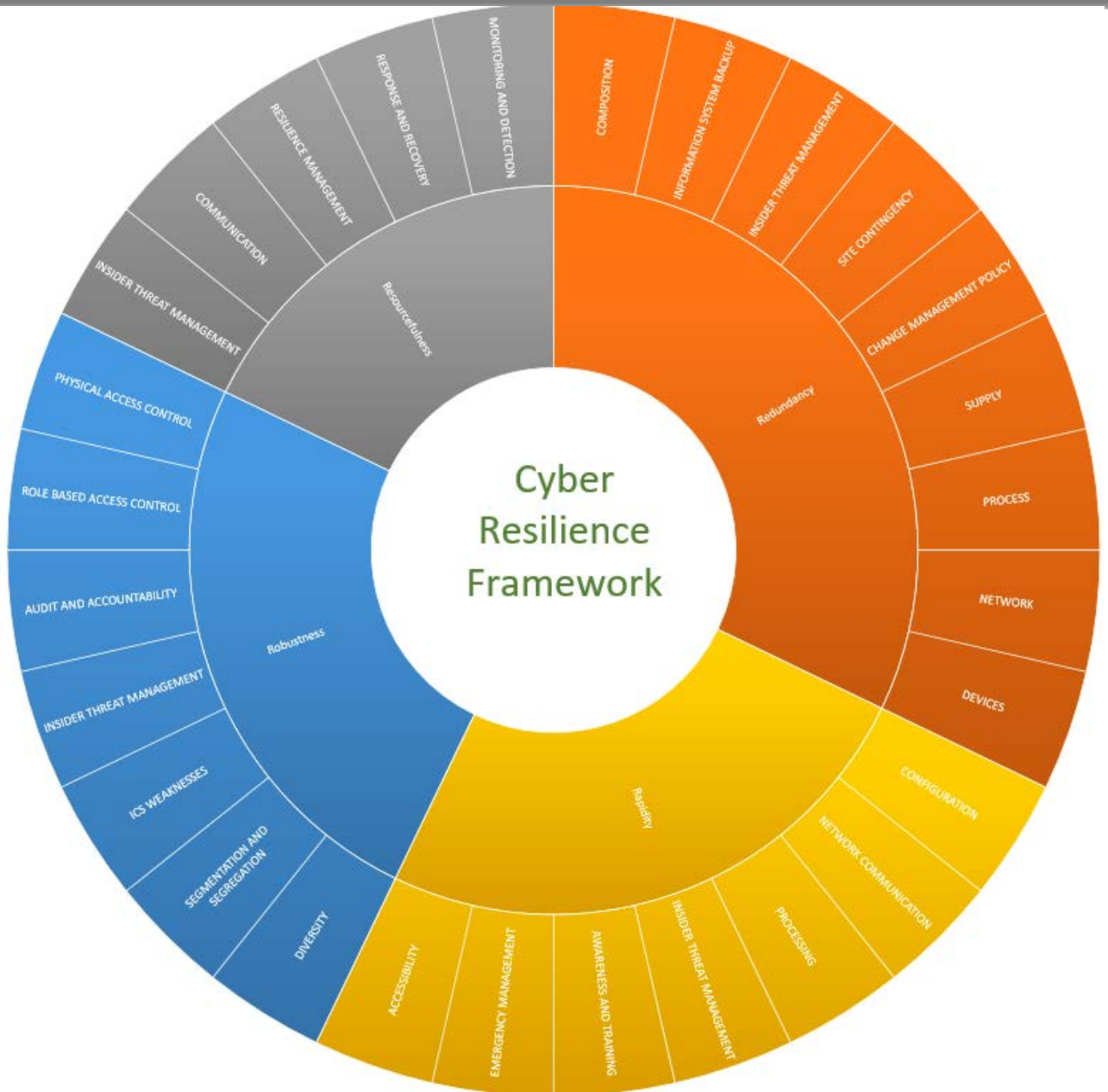

The extent to which systems are capable of satisfying functional requirements, if significant degradation or loss of functionality occurs

The ability to diagnose and prioritize problems and to initiate solutions

The capacity to restore functionality in a timely way, containing losses and avoiding disruptions

Multidisciplinary Center for Earthquake Engineering Research (MCEER) R4 Framework

# Cyber Resilience Framework




Approx. 40 categories across R4 domains

# Web-Based Self-Assessment Tool

- **The tool is a qualitative self-assessment tool based on users' understanding of resilience categories.**
- **Tool security**
  - Securely hosted in RF at https://resilience.rfirst.org
  - Data is encrypted at storage and transit
  - Multifactor authentication
  - Stringent password policy
  - State of the art network and host monitoring
- **Entity/User data is protected to maintain confidentiality and integrity.**

# R4 Indicators

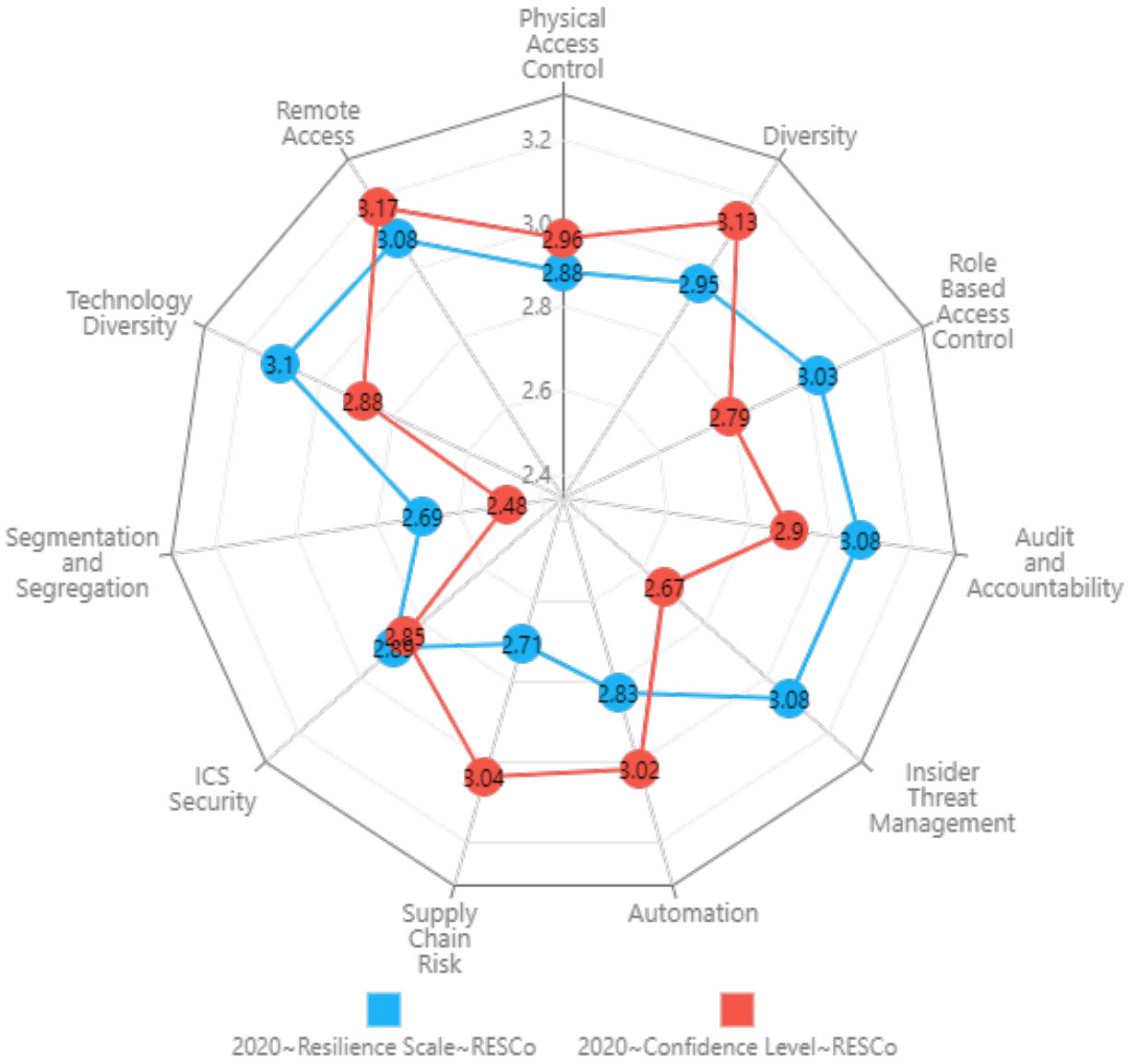
| Rapidity | | |
|---|---|---|
| Assessment | Assessment Score | |
| | 2019 | |
| | Resilience Scale | Confidence Level |
| Rapidity | 3.56 | 3.35 |
| Physical | 3.13 | 2.50 |
| Organizational | 3.88 | 4.28 |
| Technical | 3.67 | 3.28 |

Example R4 indicators (Robustness, Rapidity, Resourcefulness, Redundancy) showing areas of strength/improvement

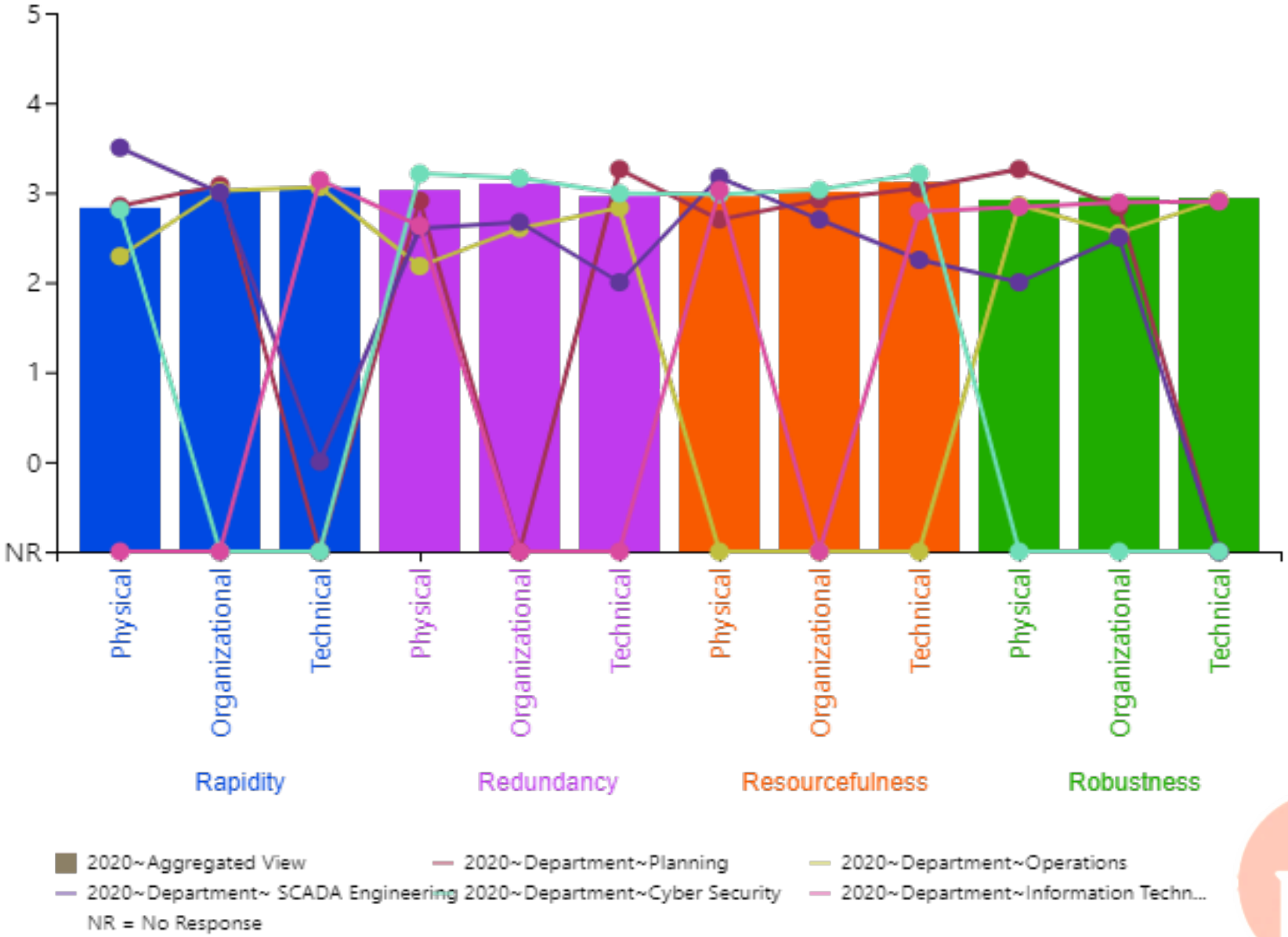
Overall company vs. department benchmarking

Leverage calibrated subject matter expertise to explore factors contributing to cyber resilience

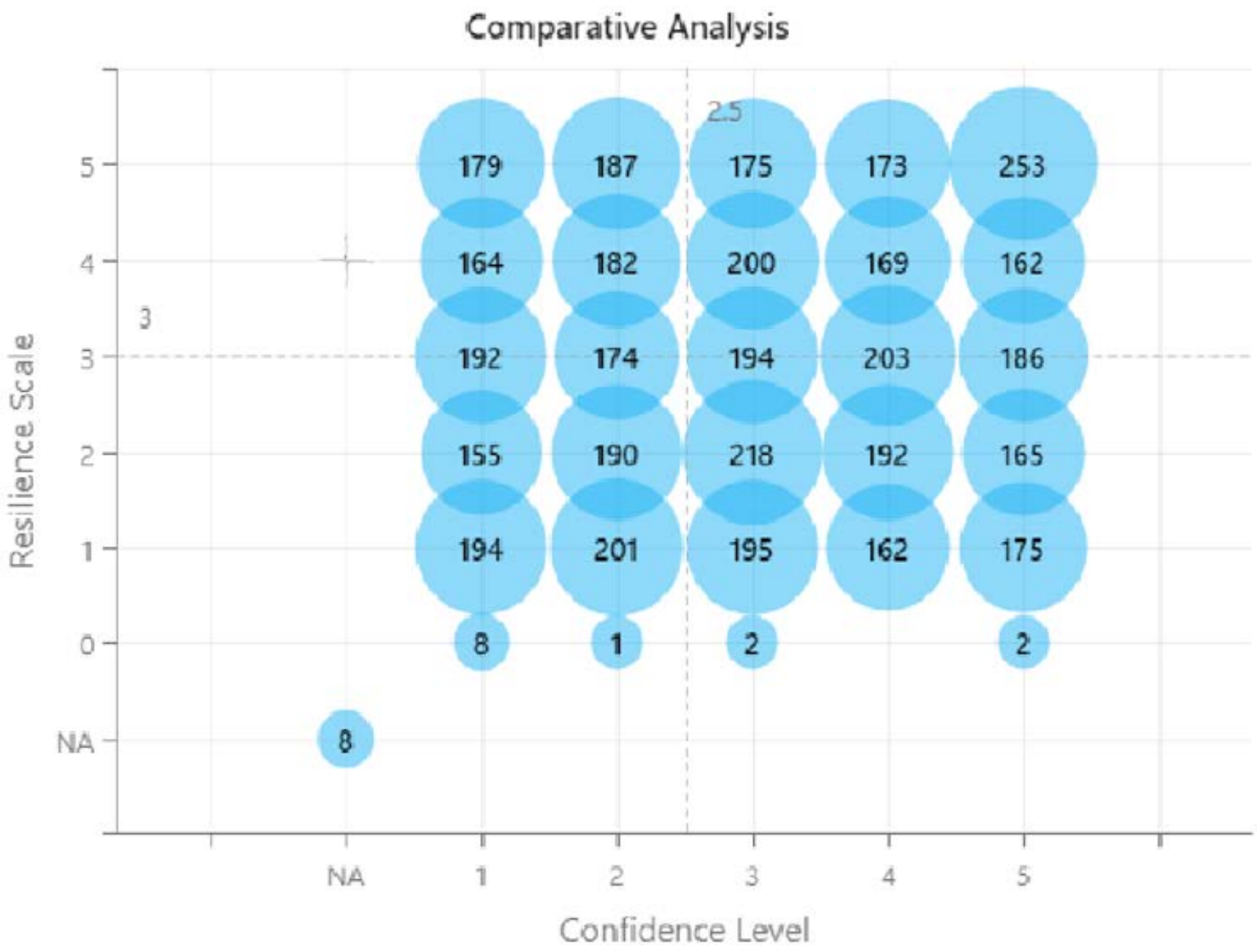
# Example Robustness Chart



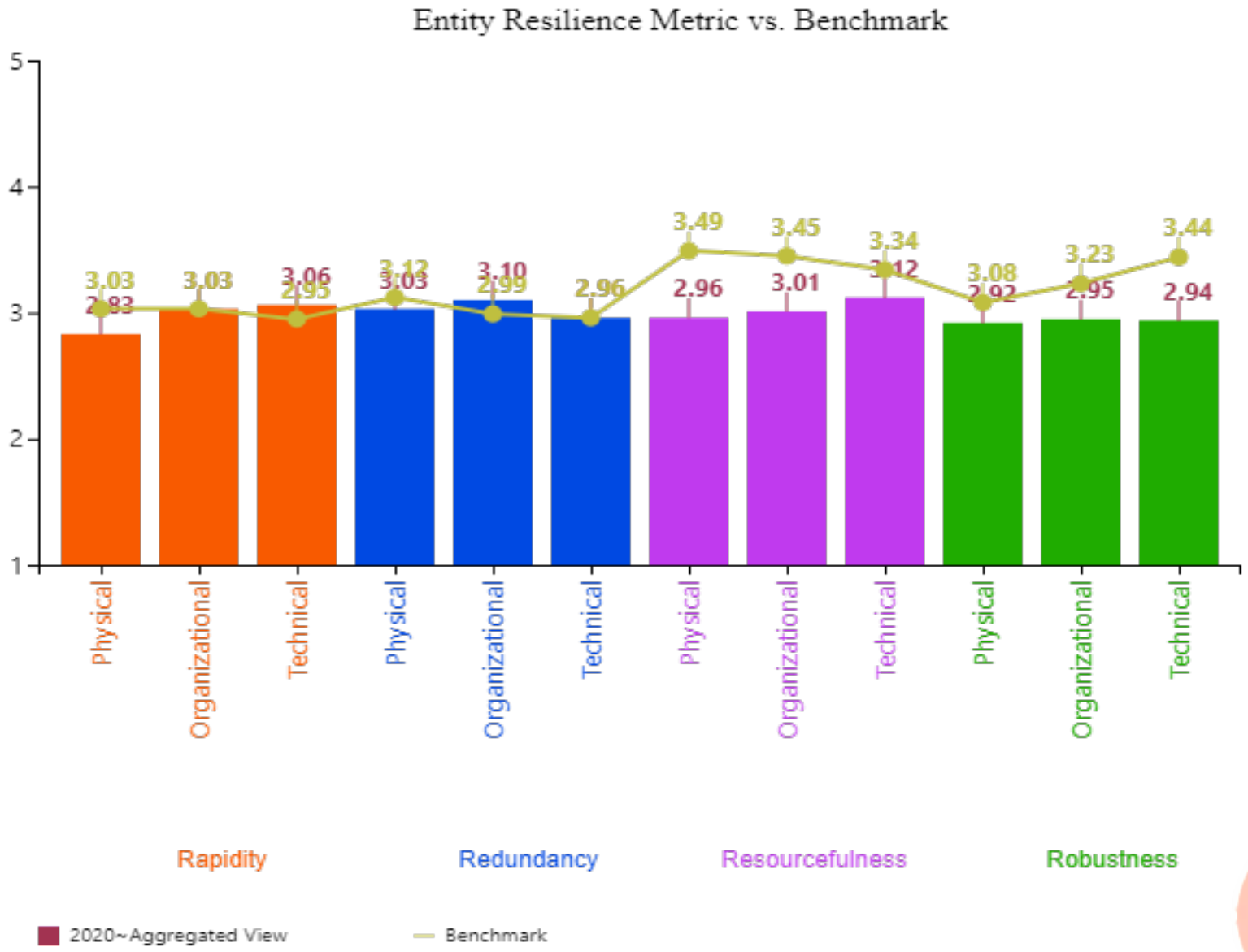
# Overall Resilience Metric



# Analysis of Resilience and Confidence
## (Across All Participants)



# Benchmark


Entity Resilience Metric vs. Benchmark
5
4
3
2
1
3.03
3.03
3.06
3.12
3.10
2.96
3.49
3.45
3.34
3.08
3.23
3.44
2.95
2.94
2.96
3.01
Physical
Organizational
Technical
Physical
Organizational
Technical
Physical
Organizational
Technical
Physical
Organizational
Technical
Rapidity
Redundancy
Resourcefulness
Robustness
2020~Aggregated View
Benchmark

# Example Recommendations

- **Technical Robustness:**
  - **ICS Weakness:**
    1. Follow the vendor recommendations and standards (NIST, NERC-CIP) for your SCADA computers, servers, ICS devices, and other critical assets.
    2. Frequently update the latest patch on the control system computers.
    3. If there is any anomaly detected in the PLC level, consult with the vendor for possible solutions or patches.

    **Reference: [11]**
  - **Segmentation and Segregation:**
    1. Apply network segmentation by segregating the sensitive OT devices from the other IT devices.
    2. Place the servers that communicate with ICS devices in a separate DMZ and restrict access of those servers from the corporate network using firewalls.
    3. Frequently check/update the firewall settings or ruleset so that it conforms to the network design and there is no traffic or message communications between the network components that are not allowed in the design or network topology.
    4. Use private VLANs to protect networks from unwanted traffic from untrustworthy devices.

    **Reference: [12]**
  - **Diversity:**
    1. Use diverse products from different vendors for the IT network.
    2. Consider using different vendors for similar type of products. For example, deploy firewalls or routers from different vendors. Choose from a list of preferred vendors whose systems are reported as less vulnerable and hard to penetrate.
    3. Use DMZ between control and corporate network and restrict message or traffic communication from DMZ towards control network unless extremely necessary.

    **Reference: [5, 12]**
  - **Logical Access Control:**
    1. Make sure the authentication process is encrypted and supported by encryption mechanisms.

# Example Recommendations (contd.)

### 3.1 Robustness

Physical


Improve from 3-Good --> 4-Very Good

Recommended Areas of Improvement

| Area | Practice | Improve | Resilience Scale |
|---|---|---|---|
| Accessibility | Accessibility - Practice 1 | My organization has adequate transportation that can be used to move assets and emergency response teams in to areas where action is needed. Transportation may include truck, crane, pickup truck and hoists. | 3.00 |
| Accessibility | Accessibility - Practice 2 | My organization is prepared to quickly deploy essential equipment such as generators, transformers and/or necessary substation equipment to restore power service when needed. | 3.02 |
| Accessibility | Accessibility - Practice 3 | All of my organization's ICS components located in business and commercial facilities are easily accessible by local transportation. | 3.32 |
| Accessibility | Accessibility - Practice 4 | My organization has the ability to physically or remotely disconnect/quarantine a malfunctioning ICS component if needed. | 2.96 |

# User Feedback

- I found this survey to be fairly enlightening and plan to share it with my leadership. This survey serves a special purpose. Often there is heavy focus on cyber, but when things go wrong, the resiliency of an organization is integral.

- In my opinion, the questions are covering a wide spectrum of industry practices, standards, devices, and platforms.

- ..discovering where there are weak areas is only important if there is some suggested ways to improve any low scores or if there is a perceived value in implementing solutions to improve an entity's cyber resilience.

# Operational Resilience

- **Study factors impacting Operational Resilience**
- **Collaborate**
  - Share practices that influence or identify operational resilience
  - RF Community of practice

# Slido.com poll

# Would you be interested in participating in a RF Operational Resilience Community of Practice?

Login to Slido.com (a virtual Q&A/polling tool) using the event code **#TechTalkRF** to further participate.

# Generation Resilience Example

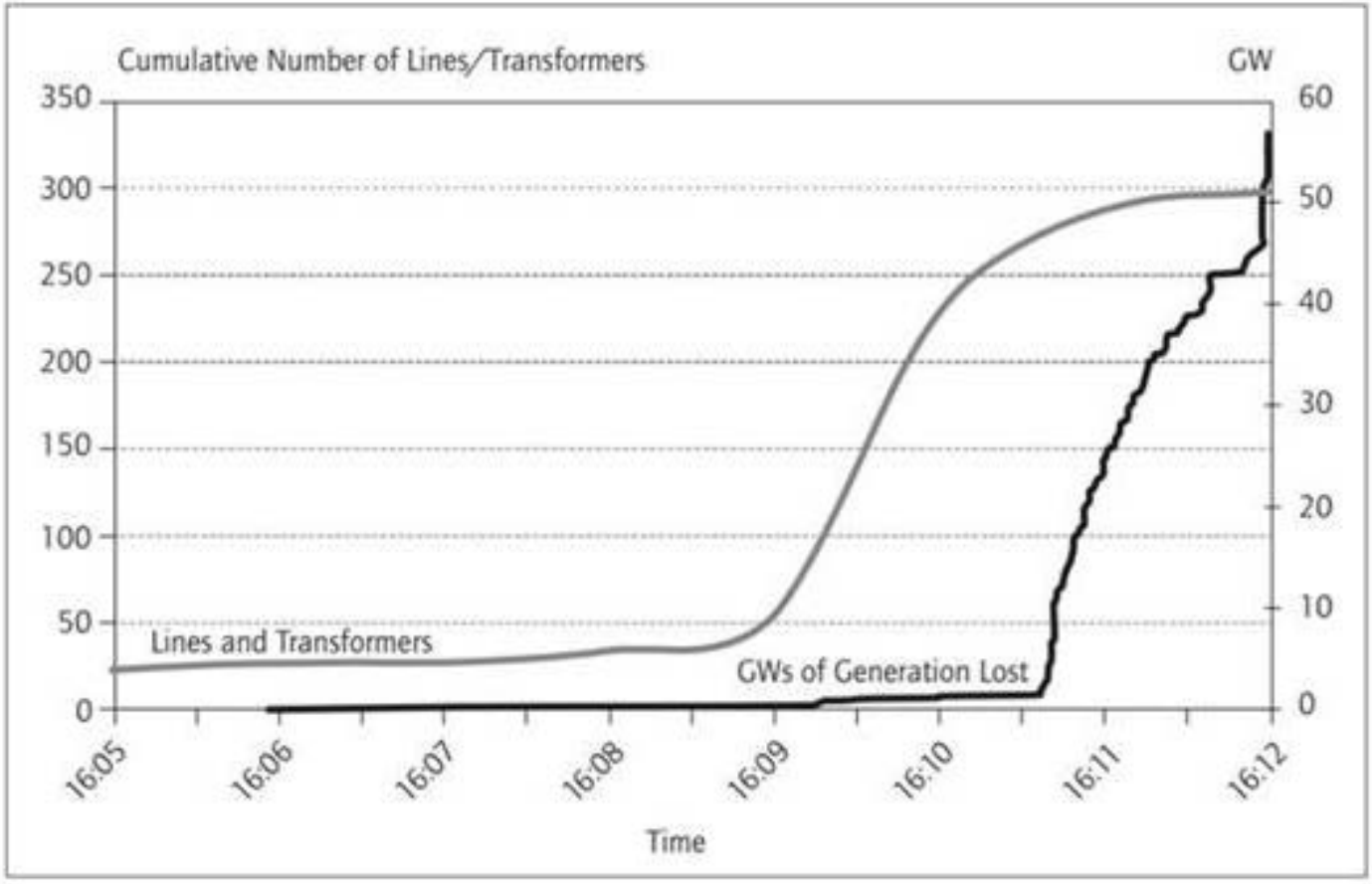


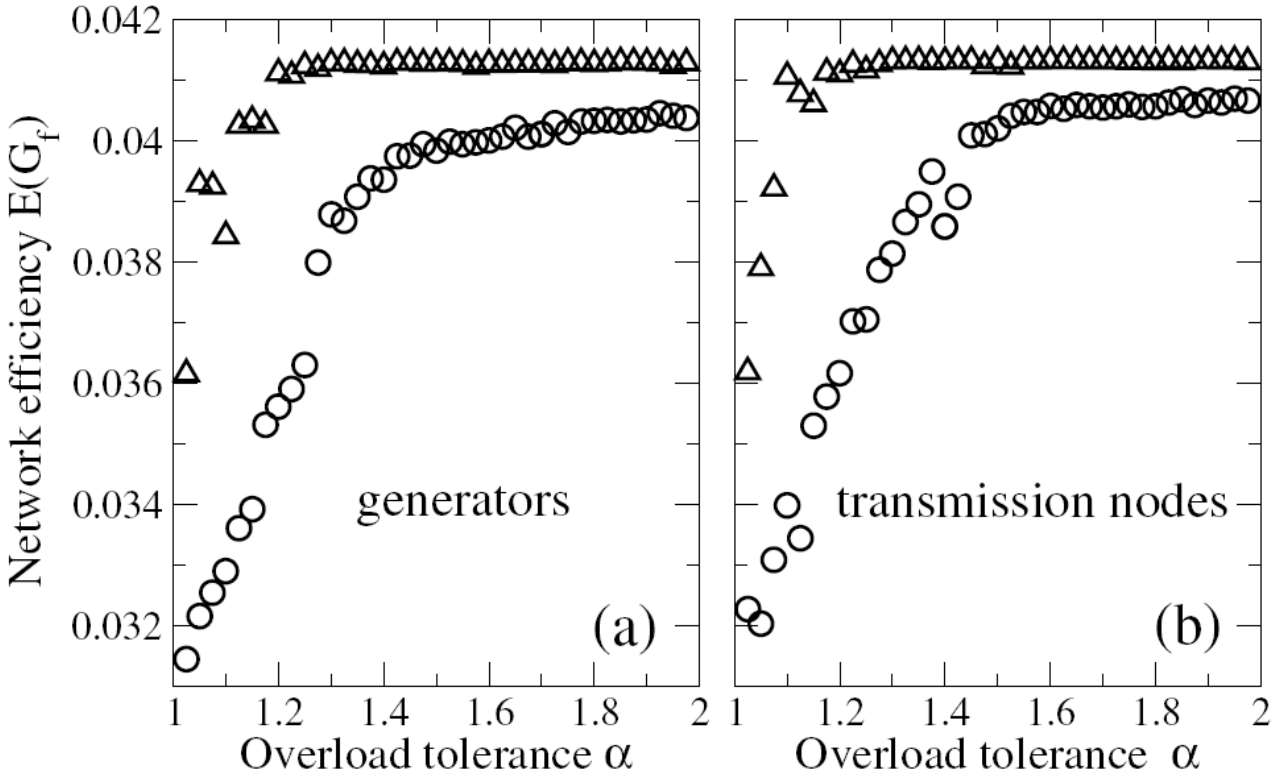

Figure 4.1: Line Trips and Lost Load During the Cascade Phase of the 2003 Blackout in North America.

Image credit: US-Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, 2004.

# BES Operational Resilience Examples

## ➢Power grid structural resilience

- *efficiency is impacted the most if the node removed is the one with the highest load*
- *highest load generator/transmission station removed*




- **Resilience depends on network topology**
- **The research studies the effects of losing nodes and its overall impact to the efficiency of network**
- **Network efficiency vs Overload tolerance – in a targeted removal or random failure scenario, increasing average capacity of each node by 30-40% above initial load can increase network resiliency.**

***Research such as this show us areas of investment or focus to increase grid resilience.***

*Source: Modeling cascading failures in the North American power grid; R. Kinney, P. Crucitti, R. Albert, V. Latora, Eur. Phys. B, 2005*

# Bridge on River Choluteca - Build to ~~Last~~ Adapt

Image source:
Economic times,
2020

# Contact Information

- **Web-based self-assessment tool – Free for all entities in RF footprint**
- **Collaborate to improve cyber or operational resilience of BPS**

Please visit the RF Contact Us page and choose Resilience from the list of Areas.