What's the Difference between Reliability and Resilience?

By Aaron Clark-Ginsberg, Stanford University

The ability to keep the lights on in the event of a cyber-incident is a major concern for the electric sector. Power grid resilience and power grid reliability are both frequently, and often interchangeably, referenced in conversations about keeping the lights on. This begs the question: what is the difference between reliability and resilience? This brief describes the difference between reliability and resilience in relation to cyber-incidents and the power grid.

Understanding reliability

For the electric sector, reliability can be defined as the ability of the power system to deliver electricity in the quantity and with the quality demanded by users. Reliability is generally measured by interruption indices defined by the Institute of Electrical and Electronics Engineers Standard 1366.

Reliability means that lights are always on in a consistent manner. This is a binary view of system performance where systems are either functional or failed.

Cyber-incidents can result in power failures, compromising the reliability of the electric grid. For example, the Northeast blackout of 2003 left an estimated 55 million people across Canada and the United States without power and was caused by a software bug in the alarm system at a control room.

Understanding resilience

Resilience, stemming from the root, *resilio*, meaning to leap or spring back, is concerned with the ability of a system to recover and, in some cases, transform from adversity (Alexander, 2013). The National Infrastructure Advisory Council (2009, 8) defines critical infrastructure resilience as:

> *"…the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event."*

Resilience approaches emphasise the idea that disruptive events occur regularly and that systems should be designed to bounce back quicker and stronger because the impact was less. Figure one provides an illustration of this idea:

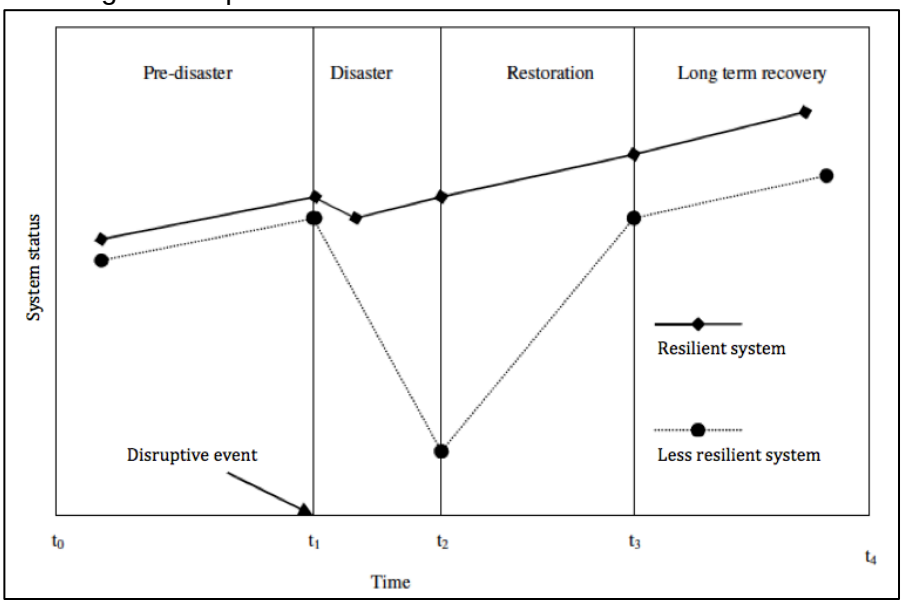

Figure 1: A resilient versus less resilient system (modified from Mayunga, 2007)

The figure shows the more resilient system is better able to withstand the disruptive event compared to the less resilient system. In the power grid, when a shock hits, the *impact* is smaller (maybe part of the grid is knocked out, or there are brown outs) and the *recovery* is faster (full service is restored). This suggests the idea that there is a flexible continuum between functional and failed, so moves beyond the rigid duality promoted by reliability.

Resilience operates from a systems perspective, understanding incidents as a complex imbedded process occurring at the intersection of natural and human forces across multiple scales, evolving and changing over time. Complexity and change stresses the idea that disruptive events cannot always be anticipated, but that when they occur they should result in learning and adaptation. Adaptation is critical when trying to build resilience against cyber-incidents, given the quickly evolving nature of the cyber landscape.

Reliability and resilience

From the above, it is clear that reliability and resilience are both relevant concepts in relation to the power grid. Reliability, with its focus on keeping the lights on, can be described as the end goal of the power grid. In order to meet this goal in the case of evolving cyber-threats the power grid needs to be resilient, as cyber incidents might occur in manners that compromise reliability. Recovering faster and learning and adapting from previous mistakes are important.

While interlinked, a resilient grid is not necessarily one that is reliable and a reliable one is not necessarily resilient. As long as a grid comes back quickly it can be considered resilient. Rolling brownouts might be more acceptable under a resilient framework, as resilience allows for intermediary positions between on and off. This suggests that while reliability may be the goal of a power grid, resilience may be a realistic compromise that reflects the changing nature of cyber-incidents. However, reliability is still a critical measure as it is important to provide power in a consistent manner with as few disruptions as possible. Indeed, this suggests that resilience can be a compromise and necessary component of reliability but that reliability should remain the ultimate end goal of a power system.

References

ALEXANDER, D. 2013. Resilience and disaster risk reduction: an etymological journey. *Natural Hazards and Earth System Sciences Discussion,* 1**,** 1257-1284.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE) 2012. IEEE Guide for Electric Power Distribution Reliability Indices. *IEEE Std 1366-2012 (Revision of IEEE Std 1366-2003)***,** 1-43.

NATIONAL INFRASTRUCTURE ADVISORY COUNCIL (NIAC) 2009. Critical Infrastructure Resilience Final Report and Recommendations. National Infrastructure Advisory Council.

MAYUNGA, J. S. 2007. Understanding and applying the concept of community disaster resilience: a capital-based approach. *Summer academy for social vulnerability and resilience building,* 1**,** 16.

Aaron Clark-Ginsberg is a postdoctoral scholar at Stanford's Center for International Security and Cooperation. He is currently researching the impact of CIP standards on the resilience of the United States Power grid. If you would like to learn more about power grid resilience or you are an industry stakeholder willing to provide information for the research on current critical infrastructure risks, resilience, and regulatory practices please contact Aaron at aaroncg@stanford.edu.

This article was produced as part of a project funded by the US Department of Homeland Security, but the views and conclusions in this article are the author's.