INL/MIS-22-67165-Revision-0

# Enhancing Resilience of our Nations Critical Infrastructure

November 2023

Changing the World's Energy Future

Ronald Earl Fisher, Celia Helene Porod

Idaho National Laboratory

*INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC*

## DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/MIS-22-67165-Revision-0

# Enhancing Resilience of our Nations Critical Infrastructure

**Ronald Earl Fisher, Celia Helene Porod**

**November 2023**

**Idaho National Laboratory**
**Idaho Falls, Idaho 83415**

**http://www.inl.gov**

**Prepared for the**
**U.S. Department of Energy**
**Under DOE Idaho Operations Office**
**Contract DE-AC07-05ID14517**

## CHAPTER 11

# Enhancing resilience of our Nation’s critical infrastructure

**Ron Fisher and Celia Porod**
Idaho National Laboratory, Idaho Falls, ID, United States

### Contents

## 11.1 Introduction

In February 2013, *Presidential Policy Directive—Critical Infrastructure Security and Resilience* (PPD-21) was released to advance “a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure” [1]. Since then, substantial effort has been applied to the advancement of research and development focused on critical infrastructure security and resilience to support infrastructure owners and operators. Even with the progress made to date, there is an ongoing need for multidisciplinary, cross-discipline support to provide end-to-end solutions to enhance the resilience of critical infrastructure nationwide. To address this gap, Idaho National Laboratory (INL) created the Resilience Optimization Center (IROC) as a national center for systems resilience and risk management. This center brings together multidisciplinary subject matter experts internally across the laboratory, as well as from public and private entities, other national laboratories, and academia, to address some of the Nation’s more challenging infrastructure problems. These experts are working to provide easier access to subject matter experts; providing feasible, optimized solutions that yield observable results; and creating collaborative teams that apply a cyber-physical dependencies approach.

*Risk-informed Methods and Applications in Nuclear and Energy Engineering*
https://doi.org/10.1016/B978-0-323-91152-8.00002-8

To gain a better understanding of resilience as it relates to critical infrastructure assets and systems, this chapter reviews resilience terminology to establish a common taxonomy. Then an overview of the need for a comprehensive and collaborative approach is addressed, along with a look at some current and ongoing research initiatives. Enhancing the resilience of the Nation cannot be done with a siloed approach; experts must come together from various fields and backgrounds and work collaboratively in a way that bridges the gap between cyber and physical infrastructure through applying necessary research, analysis, testing, and validation.

## 11.2 Resilience terminology

The Nation depends on critical infrastructure assets and systems to carry out daily life. The disruption or incapacitation of such assets and systems could have devastating impacts on the ability to perform essential tasks, even tasks as simple as turning on the lights, having access to running water, or driving across a bridge. As defined in PPD-21, "the term 'critical infrastructure' has the meaning provided in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)), namely systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" [1]. As of 2019, current U.S. Critical Infrastructure Sectors include the following: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waster; transportation systems; and water and wastewater systems [2].

Critical infrastructure is often interconnected, depending on other infrastructure to be able to perform certain functions, representing a dependent or interdependent relationship. Infrastructure dependency is "a linkage or connection between two infrastructures, through which the state of one infrastructure influences or is correlated to the state of the other" [3]. Infrastructure interdependency is "a bidirectional relationship between two infrastructures through which the state of each infrastructures influences or is correlated to the state of the other. More generally, two infrastructures are interdependent when each is dependent on the other" [3] (Fig. 1). Being able to identify and understand these relationships is one of the most challenging, but also most important steps in infrastructure analysis. As stated by

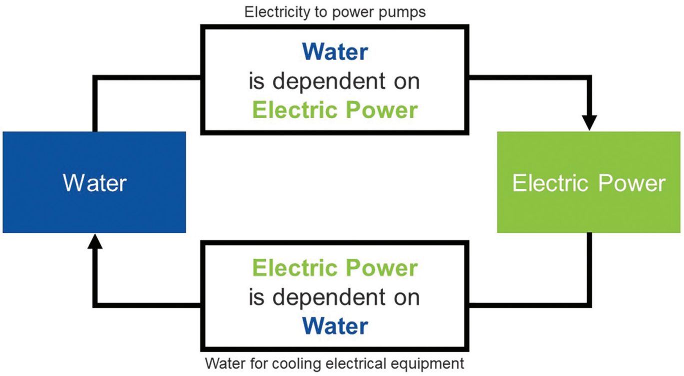

**Fig. 1** Example of water and electric power dependency.

Rinaldi et al. [3], "what happens to one infrastructure can directly and indirectly affect other infrastructure, impact large geographic regions, and send ripples throughout the national and global economy" [3].

Resilience is defined as "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" [1]. Similarly, the National Infrastructure Advisory Council (NIAC) defines resilience as "the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends on its abilities to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event" [4]. For an infrastructure asset or system to increase their resilience, there must be a comprehensive understanding of the interconnectedness with other assets and systems to support planning, response, and recovery efforts. This effort takes focused analysis to be able to not only identify these relationships but also to be able to provide solutions to improve overall resilience no matter what scale—local, regional, or national.

## 11.3 Taking a comprehensive and collaborative approach

Significant progress has been made to date to advance the resilience of critical infrastructure; however, there is still a great amount of work left. To address the gaps in infrastructure resilience research and development, INL created the IROC, which implements a new paradigm of operating as a highly effective, collaborative, and strategic team. IROC brings together multidisciplinary teams to leverage cyber-physical dependencies capabilities to increase resilient critical infrastructures. Through employing this operating model, IROC connects internally with experts from across the laboratory, as well as with external stakeholders, to leverage their capabilities for an even more holistic operating picture. Examples of IROC support include but are not limited to assessing resilience gaps; defining how current resilience postures affect operational success; mapping and validating system interdependencies; exploring mitigation options; and leveraging existing best practices from public and private entities.

There is no one-size-fits-all approach to resiliency. Resilience planning should be scaled and bound to an asset owner's finite resources, such as time, budget, and staffing, as well as operation criticality and risk profile. By ensuring assessments and recommendations fit within the scope of an organization's operational limitations, IROC can provide optimized solutions that are realistic and implementable. Leveraging extensive laboratory capabilities, IROC offers expertise in cyber systems; full-scale infrastructure testing; intelligent instrumentation and control; emergency planning and response; vulnerability/risk analysis; integrated energy solutions; modeling/simulation; and visualization/scientific computing [5]. The IROC targets the development of innovative solutions to wicked critical infrastructure problems. These solutions aim to help mitigate disruptions from natural disasters and man-made attacks, while also identifying gaps and proposing new research, capabilities, and investments.

## 11.4 Ongoing research efforts

Innovative research is taking place at INL to bring about these state-of-the-art resilience solutions to infrastructure challenges. A few of these examples are outlined:

**Cyber-physical testbeds.** INL has the premier national cyber-physical testbed for research, analysis, testing, and validation. The four pillars this is based on are the following:

**(1)** Cyber: Pure modeling and simulation (including high-performance computing and physics-based modeling).

**(2)** Virtualization: Virtualizing cyber systems and representing their infrastructure dependencies and interdependencies.

**(3)** Small-scale physical: Small-scale representations of physical and cyber-physical systems (includes the Department of Homeland Security (DHS) Controls Environment Laboratory Resource (CELR) and other control system laboratories).

**(4)** Full-scale physical: Full-scale test ranges for electric power, wireless communications, water infrastructure, and their respective dependencies, including cyber-physical linkages.

The pillars provide a unique cyber-physical testbed capability for the Nation.

**Advanced battery test lab.** *A limiting factor of any electric vehicle is the quality of its battery, which is of particular concern for consumers. As electric vehicles transition from "the car of the future" to "the car of now," consumers need to know they can trust the vehicle manufacturers' claims about the quality and lifetime of the car's battery* [6].

**Electric Vehicle Infrastructure Lab (EVIL).** *INL's Electric Vehicle Infrastructure Lab (EVIL) develops and evaluates solutions for EV charging infrastructure integration with the electric grid. The research activities include high-power EV charging grid interaction, cyber-physical security, EM-field safety, and operational performance characterization. These research areas primarily focused on conductive charging and wireless charging technologies designed for electrified transportation* [7].

**Real-time power and energy systems.** *Advanced modeling capabilities can incorporate real-world data, hardware, and software into real-time simulations. At the INL Power and Energy Real-Time Laboratory (PERL), there is diverse expertise and the ability to co-simulate electrical, thermal, and mechanical systems. The laboratory also can integrate with microgrid test beds and simulation resources at other national laboratories. Augmenting PERL capabilities in real-time simulation are RTDS and Opal-RT assets located at the INL campus* [8].

**Cybersecurity and resilience.** In 2020, INL researchers conducted a study that looked at cyber risk reporting trends based on Securities and Exchange Commission (SEC) filings from 2005 to 2018 of U.S. publicly traded companies. Even with the continual increase in cyberthreats and successful cyberattacks over time, it was found that there is a lack of consistency in reporting cyber risks and breaches in SEC filings. In 2017, only 2.8% of companies identified cyber risk as one of their business risk concerns in their financial reporting (Form 10-K) [9]. This limiting reporting is concerning; better reporting of cyber risks and attacks will help all stakeholders better understand and value the cyber risk component of business risk [9].

**Applying artificial intelligence and machine learning.** INL is also applying artificial intelligence and machine learning to tackle resilience challenges through automated infrastructure and dependency detection

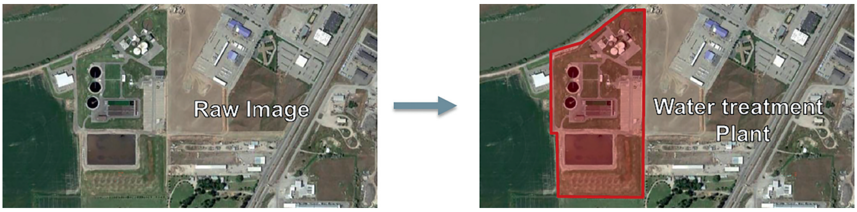

**Fig. 2** Example of detection via satellite imagery.

via satellite imagery and dependency profiles. The goals of this effort are to (1) develop computer vision models that can detect critical infrastructure features within satellite imagery and (2) incorporate dependency profiles from INL's All Hazards Analysis Framework (AHA) into the data pipeline. Identifying and understanding the dependencies that exist among infrastructures can enhance the planning and preparedness for both man-made and natural disasters (Fig. 2).

**Custom geospatial application development.** Research continues to expand on the topic of infrastructure interdependencies. One example of INL's research areas is a focus on custom geospatial application development to address data access, visualization, sharing, and analytical needs through stand-along, web-based, and enterprise-level systems. In addition, these applications aim to provide geospatially based analytical capabilities to enhance data integration and visualization related to situational awareness.

## 11.5 Conclusions

Enhancing the resilience of critical infrastructure will be an ongoing effort that will only be successful with a comprehensive and collaborative approach. Through the creation of the IROC, multidisciplinary experts can come together to conduct detailed research and develop innovative solutions that will address the needs of infrastructure across the Nation.

## References

[1] The White House, Office of the Press Secretary, Presidential Policy Directive – Critical Infrastructure Security and Resilience, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[2] Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), Critical Infrastructure Sectors. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.

[3] S.M. Rinaldi, J.P. Peerenboom, T.K. Kelly, Identifying, understanding, and analyzing critical infrastructure interdependencies, IEEE Control. Syst. Mag. 21 (6) (2001) 11–25, https://doi.org/10.1109/37.969131. https://ieeexplore.ieee.org/document/969131.

[4] National Infrastructure Advisory Council (NIAC), A Framework for Establishing Critical Infrastructure Resilience Goals: Final Report and Recommendations by the Council, 2010. https://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf.

[5] https://resilience.inl.gov/about-inl-resilience-optimization-center/.

[6] https://inl.gov/360-tour/battery-test-center-lab/.

[7] DHS CISA, A Guide to Critical Infrastructure Security and Resilience, 2019. https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf. https://cet.inl.gov/SitePages/Evaluation%20of%20Conductive%20and%20Wireless%20Charging%20Systems.aspx.

[8] https://renewableenergy.inl.gov/Conventional%20Renewable%20Energy/SitePages/RTDS.aspx.

[9] R. Fisher, J. Wood, C. Porod, L. Greco, Evaluating cyber risk reporting in US financial reports, Cyber Security: A Peer-Reviewed Journal 3 (3) (2020) 275–286.