Grid Resiliency against Cyber Threats and Wildfires

Sagnik Basumallik, Paroma Chatterjee, Anurag Srivastava, *West Virginia University*

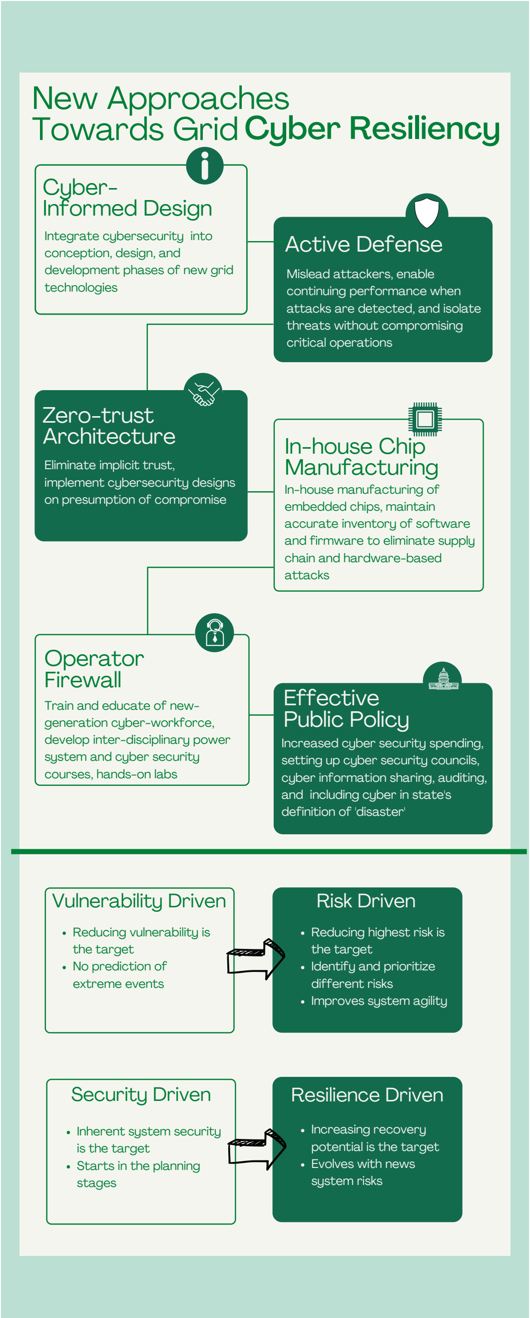
Evolving cyber threats, extreme weather events, and climate change are posing challenge to the reliable and resilient operation of electric power grids. The 2015-2016 Ukraine attack was the first cyber event resulting in a widespread power outage. On the other hand, California continues to bear the brunt of devastating wildfires, where more than 2 million assets are at high to extreme risk.[1] The Department of Energy (DoE) has estimated that power outages cost the U.S. economy 150 billion annually.[2] The impact of prolonged power outages affects interdependent water, gas, communication, and transport networks, undermining national security, and resulting in economic losses to damaged assets to life loss. As a result, the resiliency of the grid has become more important than ever before. The cross-cutting strategies presented in this article allow us to transition from grid security to grid resiliency through technology advancements, efficient operator training, and promoting effective public policy.

Cyber Security

The number of attack surfaces has increased with the digitalization of the electric grid. The biggest challenge in addressing cyber vulnerabilities and their associated risks rise from digital devices not originally designed with security in mind. Currently, there exists more than 196,907 known Common Vulnerabilities and Exposures (CVE) according to the National Vulnerability Database (NVD). The effort and cost associated with 'after the fact' additive security mechanisms, for example, developing patches to these known CVEs, is huge and their impact may be less effective. Further questions arise on how to prioritize and patch such a massive number of vulnerabilities with limited resources.

Modern solutions that address cyber security challenges against critical grid assets need to extend vulnerability-driven approaches to *risk-driven designs* and security-driven approaches to *resiliency-driven plans*.[3] These include *cyber-informed* engineering that integrates cyber security considerations into the very conception, design, and development phases of future grid technologies to limit attack paths and reduce potential cyber vulnerabilities. Building *active defense* mechanisms will mislead attackers towards a honeypot, enable continuing performance when attacks are detected, and develop remediation and isolation schemes to remove attacks without compromising critical grid operations.[4] Future solutions must eliminate 'implicit trusted networks' and implement *zero-trust* architectures. Further, in-house manufacturing of embedded chips and maintaining an accurate inventory (and source) of software and firmware used in grid applications will eliminate supply chain issues for cyber security.[5]

Commitment to creating a diversified cyber-aware workforce through a robust and dynamic education training system is of key importance. Upcoming power systems operators need to develop skills and abilities in both grid operations and computational cyber security. These two fields cannot be kept in silo, and universities need to offer interdisciplinary courses which are team-taught by a cohort of faculties with different expertise. Holistic education cross-cutting cyber, energy, control, artificial intelligence, computing, society, and public affairs, together with the efforts led by the National Initiative for Cybersecurity Education (NICE), will be crucial



towards standardizing cyber security education and creating a strong pipeline of future cyber-aware grid operators.

The Infrastructure Investment and Jobs Act[6] allows better preparedness to be cyber secure through much-needed resources. This bill will enable the Department of Homeland Security (DHS) to provide resources to state and local governments for addressing cybersecurity risks and threats through a $1B funding. A cyber response and recovery fund of $100M also allows the Cybersecurity and Infrastructure Security Agency (CISA) to tap into events of a significant cyber incident when other resources are deemed insufficient. An additional $14.5 M is allocated for research and analysis for technological development. The bill also allows US DOE to get $250M to develop advanced cybersecurity solutions in the energy sector and another $250 M to demonstrate advanced technology working with electric utilities and rural co-ops. The Strengthening American Cybersecurity Act of 2022[7] has proposed to establish a risk-based budget model for cybersecurity spending. Currently, various states have either enacted or passed legislation on cyber security and critical grid infrastructures.[8] Colorado (HB 1236) and Utah (HB 280) have set up cybersecurity councils, North Dakota (SB 2313) now requires cyber information sharing, Alaska (HB 3) and Illinois (HB 3523) include cyberattacks under the state's definition of disaster, Texas (SB 2116) prohibiting foreign-owned companies from electric grid projects and New York (AB 3904) allowing the state public service commission to audit electric corporations.

Wildfires

Driven by climate change and sustained droughts, the number of wildfires has gone up by a significant amount in the last decade. As of Sept. 21, 2022, 51,606 fires have already burned a total of 6,815,741 acres, which is above the 10-year average of 44,111 fires and the average acreage of 6,208,061.[9] Table 1 shows the impact of wildfire on human structures and residences since 2018. Some of the most destructive fires to ravage California caused by power lines faults, failure of aged electrical equipment, or oil-filled power system apparatus explosions are shown in Table 2. The large extent of these fires in the Pacific Gas and Electric (PG&E) Company's service territory in Northern California has unfortunately forced the company to file for bankruptcy when faced with astronomical expected liability.

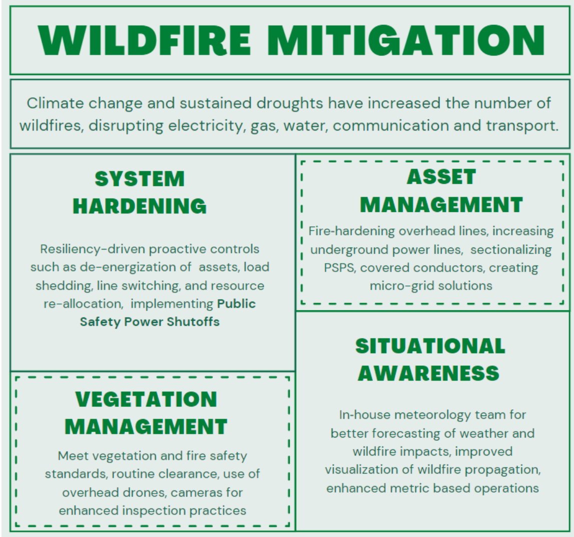
Table 1: *Statistics of Wildfire Impact*[10]

	2018	2019	2020	2021
Structures Burned	25,790	963	17,904	5,972
Residences (%)	70	46	54	60

Proactive steps to minimize the impact of wildfires include resiliency-driven proactive controls that incorporate the de-energization of transmission assets, load shedding, line switching, and resource reallocation as wildfire propagation evolves.[11] Power utilities have implemented stricter wildfire management plans through preliminary solutions such as continued vegetation management activities, enhanced

Table 2: *Most Destructive California Wildfires due to Electrical Issues*[1]

Rank	Fire Name	Date	Acres	Structures	Deaths
1	Camp Fire	Nov, 2018	153,336	18,804	85
2	Tubbs	Oct, 2017	36,807	5,636	22
3	Valley	Sep, 2015	76,067	1,955	4
4	Witch	Oct, 2007	197,990	1,650	2
5	Woolsey	Nov, 2018	96,949	1,643	3



inspection practices, strategic system hardening, increased situational awareness tools, and smarter, smaller, and shorter Public Safety Power Shutoffs (PSPS) during fire seasons. For example, the San Diego Gas and Electric (SDG&E) company's inhouse meteorology team forecasts wildfire impacts to undertake advanced preparations and has pioneered the use of PSPS to ensure public safety. The Southern California Edison (SCE) Company has developed its own Wildfire Risk Reduction Modeling (WRRM) Framework to analyze and quantify wildfire risk. The WRRM is used to estimate risk reduction and help make decisions about wildfire mitigation activities, and prioritize mitigation deployment. Integration of weather data, Vegetation Risk Index (VRI), Circuit Risk Index (CRI), historical wind conditions, and enhanced fault detection via wireless fault indicators can enhance situation awareness and risk assessment. Other solutions include creating micro-grid solutions, use of enhanced recloser protocols with more sensitive relay settings, fire-hardening overhead transmission lines, increasing strategic underground power lines, expansion of covered conductors, the addition of advanced protection capabilities, sectionalizing PSPS, and expansion of the Generator Grant Program to mitigate PSPS impacts. The continued use of the Fire Potential Index (FPI) and the Santa Ana Wildfire Threat Index (WTI) will harden the system and minimize safety risks and potential fire ignitions. Ultimately, prioritizing higher penetration of renewable generation and distributed generation over traditional fossil-fuel-based power generation and bulk transmission in areas with a high risk of forest fires should be the goal for wildfire prevention.

The Infrastructure Investment and Jobs Act allocates $103 million for wildfire risk mitigation efforts, from which $80.9 million will go to accelerating the pace and scale of fuel management (reducing risk through strategic removal of potential wildfire hazards), and about $19.4 million will go towards accelerating the pace and scale of Burned Area Rehabilitation (supporting post-wildfire landscape recovery). Further, the Wildfire Emergency Act of 2021, introduced to reduce the risk of catastrophic wildfires in the western United States, seeks $250 million to conduct large-scale forest restoration projects, $100 million for a new grant program to protect critical infrastructure and allow for greater energy flexibility (by retrofitting key structures like hospitals and police, fire, and utility stations so they can function better without power and expand the use of distributed energy systems, including micro-grids, to reduce the area that power shutoffs affect) and $50 million to help disadvantaged communities plan and collaborate on forest restoration, wildland-urban interface and tribal projects as well as increase equitable access to environmental education and volunteer opportunities.[12] The California legislature has further adopted a set of legislation, specifically passing Senate Bill 901 (Dodd, 2018), Assembly Bill 1054 (Holden, 2019), and AB 111 (Committee on Budget, 2019), that focuses on utility wildfire safety, and establishes requirements for utilities to submit Wildfire Mitigation Plans (WMPs) on an annual basis for review and approval by the California Public Utility Commission (CPUC), describing their initiatives aimed at mitigating wildfire ignition risk from their own infrastructure.

Summary

Moving from a 'secure grid' to a 'resilient grid' requires implementing strategies through multi-disciplinary efforts. Research and development studies on cyber security and wildfires are being carried out in a wide spectrum of science and engineering areas. These include big data analytics and computational tools based on artificial intelligence for improved situational awareness for prediction, prevention, detection, monitoring, and mitigation of impacts due to extreme events. A culture of building grid resiliency needs to be developed by embedding solutions in the design and development process, identifying and prioritizing risks, developing tools and techniques to detect evolving situations and timely patch them while minimally impacting the system operation, assessing risk propagation using system analysis, and most importantly, developing recovery mechanisms when events have already impacted the system. Overall, risks need to be vetted by metrics that track grid impacts considering vulnerability and threats, time taken to identify and respond to events, and resiliency to bounce back. Such proactive solutions need to be further validated on large end-to-end real-life testbeds. Overall, a stronger collaboration of government-regulators-policy makers-solution providers-grid operators-reliability coordinators-national labs, and academia can help come up with innovative solutions and a workforce pipeline to implement them.

References

[1] Insurance Information Institute. Facts + statistics: Wildfires. 2022.

[2] The Pew Charitable Trusts. Distributed generation: Cleaner, cheaper, stronger; industrial efficiency in the changing utility landscape. 2015.

[3] Illia M Diahovchenko, Gowtham Kandaperumal, Anurag K Srivastava, Zoia I Maslova, and Serhii M Lebedka. Resiliency-driven strategies for power distribution system development. *Electric Power Systems Research*, 197:107327, 2021.

[4] The DOE. National cyber-informed engineering strategy, 2022. 2022.

[5] The Government of the USA. The chips and science act. 2022.

[6] The Government of the USA. Infrastructure investment and jobs act. 2021.

[7] The Government of the USA. Strengthening american cybersecurity act of 2022. 2022.

[8] National Conference of State Legislatures. Energy Security State Legislative Review: Cybersecurity and Physical Security. 2021.

[9] CDP. 2022 north american wildfires. 2022.

[10] Congressional Research Service. Wildfire statistics. 2022.

[11] Subir Majumder, Gowtham Kandaperumal, Shikhar Pandey, Anurag K Srivastava, and Clay Koplin. Pre-event two-stage proactive control for enhanced distribution system resiliency. *IEEE Access*, 10:83281–83296, 2022.

[12] Dianne Feinstein. New bill would reduce risk for catastrophic wildfires, increase preparedness. *Press Release*.