# Editor-in-Chief's Letter

Richard M. Krieg, PhD

This double issue of JCIP includes both new articles and an archival section which provides a curated revisit to some of the pioneering articles that helped to shape *JCIP*'s trajectory to date. The criteria used to select the archived contributions are presented along with commentary on each of the articles in my Archival Section Overview.

The current issue begins with our **Editor's Interview with Mateo Jaramillo**, CEO of Form Energy ("Revolutionizing the Global Electricity System through Multi-Day Battery Storage"). A vanguard in the energy storage industry, Form Energy is carving a niche with its groundbreaking iron-air battery technology, which boasts an impressive electricity storage capacity of up to 100 hours. This positions it as a viable and cost-efficient adjunct to conventional power plants. The company's vision leverages Jaramillo's rich experience at Tesla, where he pioneered their stationary energy storage program. His journey from Gaia Power Technologies to Tesla and now to Form Energy underscores a consistent trajectory toward innovative energy solutions. With the iron-air battery, Form Energy introduces a "multi-day storage" (MDS) concept, aiming to fortify grid reliability against the backdrop of increasingly frequent extreme weather events, a challenge underscored by the Texas power crisis during Winter Storm Uri.

Form Energy's strategic underpinnings are bolstered by strong public policy support, illustrated by the company's collaboration with federal and state governments, such as the Inflation Reduction Act and state-level incentives. This support has catalyzed the company's trajectory, enabling the construction of its first state-of-the-art battery factory in West Virginia and a significant pilot project in New York. The federal and state endorsement not only accelerates the commercialization of Form Energy's transformative technology but also signifies a commitment to grid decarbonization and a transition to clean energy. With leadership that I describe as a "dream team," Form Energy's culture is steeped in mutual respect and a collective mission to address climate change—a mission that is now translating into tangible economic benefits and job creation, particularly in the communities hosting their operations.

Between our last edition and now, Artificial Intelligence (AI) has emerged as a transformative force, heralding what could be the next major technological revolution. In his editorial: "Artificial Intelligence—A Perspective," **Pramode Verma** offers a reflective perspective on AI's evolution and potential, comparing it to historical technological leaps such as the printing press and the steam engine. Verma articulates the dual nature of AI's expansion: the incredible capability to

 doi: 10.18278/jcip.4.1.1

extend human intellect, and the imperative to harness such growth responsibly to mitigate potential harm. He explores the generative aspects of AI that have begun to challenge the boundaries between human creativity and machine learning, raising questions about the future of this human-machine continuum.

The discussion moves to the ethical and practical challenges presented by AI, particularly in the realms of misinformation and the necessity for regulation. Verma suggests that AI's growth, powered by sophisticated algorithms and extensive data, is inevitable, yet must be regulated with awareness of the rights and protections for those it could harm. The author proposes solutions for regulating the spread of misinformation, advocating for the positive identification of information sources online, akin to the Know Your Customer (KYC) policies in financial institutions. He also addresses the need for oversight in broadcast media and public databases to ensure the authenticity and accuracy of information disseminated, especially in sensitive areas like healthcare.

In the broader context of AI, Verma's editorial echoes a global conversation about the integration of AI into the fabric of society. While AI's capabilities inch ever closer to human intelligence, surpassing it in some areas, the editorial raises profound questions about the essence of human consciousness and emotion, which AI has yet to touch. It acknowledges the transformative potential of AI on employment and digital literacy, and the consequential widening of the socio-economic divide. The editorial serves as a call to navigate the AI revolution with a conscious effort to balance technological prowess with ethical foresight, ensuring that AI serves as a benefactor rather than a disruptor to the collective human experience.

In "Cybersecurity Preparedness of Critical Infrastructure: A National Review," **Maryam Roshanaei** notes that critical infrastructures, such as transportation networks, power grids, water systems, telecommunications, and financial systems, are the bedrock of modern society, integral to the daily operations of governments, businesses, and communities. The U.S., while heavily reliant on these systems, faces challenges in safeguarding them against increasingly sophisticated domestic and international threats. The article discusses the challenges modern societies face in protecting critical infrastructures, emphasizing the need for robust cybersecurity readiness to ensure that systems can withstand and recover from disruptive events.

The article continues to underscore the importance of collaborative, comprehensive strategies that integrate Information, Communication, and Technology (ICT) platforms with innovative technologies for enhanced protection. With critical infrastructures becoming more interconnected and digitized, they are more susceptible to cyber threats, making cybersecurity readiness an essential aspect of national security. Furthermore, it highlights the varying security needs of IT and Operational Technology (OT) within critical infrastructures, particularly emphasizing the unique requirements of OT systems for safety and reliability. The

need for resilient strategies that protect against all types of threats and the urgency of developing such measures are central themes of the discussion.

The article's analytic findings illuminate the stark reality that CI installations have been recurrently compromised. The Energy and Transportation sectors are particularly vulnerable, having faced a substantial number of incidents over the years. The data suggest a trend of escalating sophistication in cyberattacks, with a notable spike in disruptions due to ransomware and malware—underscoring an urgent call for reinforced cybersecurity readiness. By charting the landscape of past breaches, the article serves as a clarion call for a fortified stance against potential future threats. It is buttressed by Grubbs et al. in "Evolution and Trends of Industrial Control System Cyber Incidents Since 2017," which is presented in the Archival Section.

In "PJM: Charting the Path to the Grid of the Future," **Kenneth Seile**r notes that the electric grid stands as one of the most crucial yet complex systems in modern society, a silent enabler of our daily lives and economic activities. He summarizes the electric grid's evolving landscape from the perspective of planning for a grid operator that services an extensive region, including 13 states and the District of Columbia. He explores the challenges and transformations the grid is undergoing, delving into the intersection of customer preferences, clean energy goals, policy choices, and technological advancements, painting the picture of an industry at a pivotal point of change.

Seiler's article is timely, as it addresses the escalating need to balance reliability and innovation in the face of retiring conventional energy generators and the increasing frequency of extreme weather events. The piece highlights PJM Interconnection's important role in managing these challenges while maintaining an uninterrupted power supply, a task that is becoming increasingly complex and urgent. The discussion revolves around not just the need for effective operation but also the need for strategic planning and market adaptations to ensure the resilience and reliability of the grid in unprecedented scenarios. Seiler's perspective is particularly valuable given PJM's position as the largest regional transmission organization in the United States, emphasizing the scale and impact of the issues discussed.

The article further explores the practical aspects and implications of transitioning to a grid that increasingly relies on renewable energy sources, such as wind and solar. This transition, while important for a sustainable future, presents unique challenges in maintaining the reliability of the power supply. The author examines these challenges in depth, including the need for new planning processes, the impact of regulatory and market structures, and the critical role of policy in facilitating this transition.

**Andrew Bochman's** "In the Polycrisis Era, Infrastructure Defenders Need to Broaden, Not Tighten, Their Focus," delves into the complexity of our current

period, characterized by overlapping and interlinked crises that collectively threaten global infrastructure. The author highlights the need for a strategic rethink in infrastructure protection, emphasizing the interdependencies between operational technology cybersecurity and climate-induced physical risks. Acknowledging the evolving and compound nature of threats, from climate change to rapid technological advancement, the paper underscores the urgency of holistic resilience planning and intersectoral collaboration.

In detailing the components of the Polycrisis Era, the author reflects on historical precedents, current vulnerabilities, and the inadequacies of existing frameworks to address multifaceted challenges. A particular focus is placed on the systemic failures to manage complex social, ecological, and technological systems, and the consequent economic and societal repercussions. The article argues for a shift from siloed defense strategies to integrated approaches that recognize the cascade of impacts from climate events and cyber threats.

The article introduces the concept of Critical Function Assurance (CFA), advocating for proactive risk management and preparedness for "black sky events"—extreme, prolonged outages affecting multiple states—and "black swan" events—unpredictable, catastrophic occurrences. It proposes a cross-disciplinary strategy that leverages diverse expertise and calls for enhanced communication among infrastructure defenders. By examining both cyber and physical climate risks, the paper suggests that shared knowledge and coordinated defenses can bolster resilience in the face of unprecedented global challenges.

The vast majority of U.S. critical infrastructure is owned by private sector companies. In "New SEC Cybersecurity Disclosure Protocols: Enhanced Transparency, Short Deadlines," **Brian Walker** discusses the final rule issued by the SEC on Cybersecurity Risk Management, Strategy, Governance, and Incident Response. Finalized on July 26, 2023, the rule requires SEC-regulated companies to disclose significant cybersecurity incidents and their cyber risk management processes. It aims to provide investors with more transparency into the cyber risks and mitigation strategies of SEC-regulated companies. The rulemaking process, which lasted eighteen months and began in March 2022, involved heated debate and divergent viewpoints. Walker highlights the challenges companies will face in adapting to these new regulations, particularly those with less structured cyber risk management approaches.

In outlining the new rules for annual cyber risk disclosures, the article focuses on two areas: Cyber Risk Management and Cyber Risk Governance. Under rule provisions, affected companies must describe strategies and processes for managing cyber risk, and the roles and responsibilities of those involved in monitoring and managing such risk. In addition to annual disclosures, companies must also report significant cyber-related incidents within four business days of determining their materiality. Companies will need to focus on foundational capabili-

ties like incident classification, response, crisis response plans, and regular testing to comply effectively with the SEC's new cybersecurity rules. While the finalized rules do not provide detailed guidance on these disclosures, they emphasize transparency, leaving the specifics to each company's leadership.

[Editor's note: in terms of some of its climate change disclosures, the SEC's current posture is part of a broader global trend towards integrating environmental, social, and governance (ESG) factors in financial reporting. However, it highlights the ongoing debate in the United States about the role of regulators in addressing climate change and the extent to which companies should be held accountable for disclosing climate-related risks. The contentious nature of this rulemaking reflects broader societal divisions over climate policy and the role of business in mitigating environmental impacts.]

**Stanley Forczyk**, in "National Infrastructure Bank: A Permanent Solution and Timely Budget Workaround," highlights the critical state of America's public infrastructure, which is strained by both underinvestment and the impacts of climate change. The recent Infrastructure Investment and Jobs Act (IIJA) of 2021, while a substantial measure, only covers a fraction of the nation's vast, unfunded infrastructure needs. The proposed solution is the establishment of a $5 trillion National Infrastructure Bank (NIB), outlined in HR4052, which would address this funding gap without additional taxes or debt, by using private sector Treasury swaps for equity in the bank.

The article underscores the role of robust infrastructure in economic vitality and social equity. It illustrates the negative consequences of inadequate investment in public infrastructure—hampering efficiency, innovation, and disproportionately affecting disadvantaged communities. It also details how a well-funded and modernized infrastructure is crucial for businesses, particularly for supply chain efficiency and overall national competitiveness.

The proposed NIB is intended to complement existing federal programs and to catalyze economic growth by providing low-cost loans for critical infrastructure projects. This would facilitate strategic, sustainable investments across diverse sectors such as transportation, water management, and housing. The author posits that the Bank's self-sustaining model, which mirrors successful historical precedents, is intended to appeal across the political spectrum, emphasizing infrastructure investment as a bipartisan priority that could drive America's future prosperity and international competitiveness.