Enhancing Electricity System Resilience with AI, Digital Twins and Digitalisation Technologies

Dr Aidan Rhodes
Dr Mengxiang Liu
Dr Fei Teng
Imperial College London, Exhibition Road, South Kensington, London, SW7 2AZ
aidan.rhodes@imperial.ac.uk

Extreme weather events such as storms, flooding, and extreme temperatures can cause significant physical and economic damage to energy infrastructure. These events can also disrupt other critical systems such as communications, transportation, and water networks, complicating recovery efforts. Electricity system resilience is defined as the ability of energy systems to withstand and recover from high-impact, low-probability (HILP) events, including extreme weather, cyber-attacks, and equipment failures. Traditional resilience strategies include physical hardening of infrastructure, operational management, and recovery planning. Digital technologies offer new opportunities to enhance energy resilience through improved monitoring, prediction, response and recovery.

Key technologies include advanced modelling techniques and digital twins that can simulate the impact of extreme events and inform proactive measures. Energy Internet-of-Things (EIoT) devices enable real-time monitoring and control of energy systems, improving situational awareness and response capabilities. Machine learning-based techniques (MLBTs) are transforming computational analytics in power systems, offering improvements in reliability management, system stability assessment, frequency analysis, contingency analysis, cyber-attack detection, stability control, and system restoration. Digital twins can bring these component technologies together to provide a real-time overview of systems and assets, providing forecasting and prediction capabilities.

This paper highlights energy systems challenges such as connectivity issues, data privacy, cybersecurity risks, and the need for standardization in implementing digital technologies. Recommendations to utility companies and regulators include investing in digital infrastructure, fostering collaboration and data sharing, and continuously updating resilience and cyber resilience plans to incorporate new technologies and lessons learned from past events.