Rethinking Safety and Security of the Energy System for a Green Future

Roland van Rijswijk-Deij, Gerwin Hoogsteen, and Johann Hurink

University of Twente, Enschede, The Netherlands
{r.m.vanrijswijk, g.hoogsteen, j.l.hurink}@utwente.nl

Abstract. Nations across the world are transitioning their energy systems from fossil fuels to renewable sources at a rapidly accelerating pace. This has huge consequences for how we balance supply and demand in our electricity grid. The shift to renewables also entails a shift from highly centralised production, in large-scale fossil fuel power plants, to vastly distributed renewable sources at scales ranging from photovoltaic home systems to huge offshore wind farms. We argue that this transition requires us to radically rethink the safety and security of the energy grids and the whole supply chain that our modern society depends on. We will move from a well-understood heavily centralised infrastructure to one that is much harder to control, because of physical remoteness (e.g., offshore windfarms), the vast amount of decentralised assets, and because of a much more volatile and dynamic energy production level. This vastly increases our dependence on digital Operational Technology (OT) to control and monitor production for supply and demand balancing, and to, e.g., sense disruptions that require maintenance crews to be sent to remote locations. Couple that with a required change in behaviour of large consumers (industry) and small prosumers (households) to deal with a much more dynamic energy market and it is clear that we face big challenges in safety and security for the energy transition. In this position paper, we argue the need for a research agenda for rethinking how we manage the safety and security of our energy infrastructure.

1 Introduction

Manmade climate change is of grave concern to governments and supranational bodies. To prevent the worst-case outcomes of climate change, the world must urgently reduce the emission of greenhouse gases, mostly caused by burning fossil fuels for heating, electricity production and transport. Switching to the use of electricity from renewable sources plays a key role in reducing humanity's emissions [1]. Nations across the world are spearheading initiatives to increase renewable electricity production. This increase is mostly realised through hydroelectric power, photovoltaics and wind turbines. The latter are also increasingly deployed offshore in countries with a large marine exclusive economic zone.

A key challenge with renewable energy from wind and solar is that production fluctuates depending on the weather and season [2]. These fluctuations can cause

imbalance in the energy grid and currently require operators to use fossil-powered sources (chiefly natural gas) to balance supply and demand in real-time to maintain grid stability. To increase the share of renewables, we must overcome the challenge of shifting this essential balancing task away from fossil sources. This is not the only challenge. The transition extends beyond large-scale production facilities relying on wind and solar; consumers are incentivised – e.g., through tax breaks and feed-in tariffs – to deploy photovoltaics for production. At the same time these consumers are electrifying their demand too, e.g., by installing electric heat pumps. This vastly increases control complexity for grid operators and energy suppliers with millions of new controllable devices being connected to the grid [3]. Lastly, the current physical infrastructure is not designed to cope with the massive increase in electricity usage, resulting in grid congestion and capacity overloading if these novel devices are not properly controlled [4].

Tackling these challenges requires much more fine-grained remote control of millions of production sources. At the same time facilitating this remote control is challenging for, e.g., remote wind turbine farms offshore or in remote locations far from built-up areas to avoid noise pollution. Unfortunately, the challenges do not stop there; the increasingly distributed nature of renewable power production also requires reliable remote sensing. Dispatch of maintenance crews to remote and harsh environments requires careful planning, so production facilities need to be monitored closely to signal a need for maintenance in a timely manner.

If we take a step back and look at this from the digital domain it becomes clear that the energy sector depends on Operational Technology (OT) for the security of supply through novel control systems [5]. Hence, the energy transition must coincide with a control and sensing transition, leading to an increase in communication over vast distances in harsh environments. What might not be immediately obvious is that this also introduces new risks in the safety and security domain [6]. All these new control and sensing systems vastly increase the digital threat surface. Cybercriminals and nation states can leverage this increased attack surface to threaten the safety and stability of the energy grid by attacking communication networks (both in a physical and digital sense), and control and sensor systems. In this paper we argue that this imminent threat combined with the complexity of the changes to the energy production system requires us to rethink the safety and security of our energy system.

2 Problem Statement and Key Challenges

The problem is that threats to the security of supply that emerge from the ongoing energy transition and digitalization are largely unknown due to the vast system complexity. Moreover, the existing complex infrastructure is vital to society, and thus requires a careful transition and phasing out of legacy. We identify a number of key challenges that need to be considered in this transition:

- **Remoteness of infrastructure** – Production facilities for renewable electricity are often in remote locations, e.g., the offshore windfarms discussed

above. This poses significant challenges to availability of long distance communication infrastructure that is vulnerable to breakdowns, both due to targeted attacks and due to natural disasters. Similarly, systems for sensing and control cannot easily be replaced and have strict robustness requirements.

- **Diversity in suppliers of equipment** – Wind turbines are complex systems built by a large variety of producers with long supply chains. Disruptions to these supply chains delay production. Equally, motivated nation-state attackers can nestle themselves anywhere in these supply chains. The opposite of diversity is also a problem. The market for inverters for photovoltaics is dominated by a handful of players. If attackers manage to target one of these suppliers, they can cause havoc on the electricity grid by, e.g., a concerted shutdown of inverters during peak production.
- **Diversity in producers of electricity** – The switch to renewable sources leads to a much increased diversity in producers, in terms of size (from large-scale windfarms down to household PV systems), maturity (from well-meaning but inexperienced citizen collectives to experienced wind farm operators) and modality (wind, PV, hydroelectric, ...).
- **Lack of expertise in IT/OT security** – The industry is in dire need of qualified staff with cybersecurity knowledge on IT/OT systems. Recent attacks on wind turbine manufacturers with severe consequences for large-scale windfarm projects demonstrate the risks this entails [7, 8].
- **Tendency towards siloed solutions** – Manufacturers are catching up with the reality of a shift in energy production. Take, e.g., producers of PV inverters that add features to halt production when market prices are negative (i.e., consumers would need to *pay* a feed-in tariff). Unfortunately, there appears to be a tendency towards siloed solutions, in which manufacturers fail to coordinate across sources and users of electricity (e.g., lack of integration between charge points for electric vehicles and battery energy storage systems, etc.). Attackers can leverage this lack of coordination by, e.g., causing sudden drops in production, or sudden spikes in consumption, eroding consumer trust in both renewables and smart energy management systems.
- **Scale and interconnectedness of the market** – Modern electricity market areas are often vast in scale. Take, e.g., the wide area synchronous grids in North America and the European Continental Synchronous area that supplies hundreds of millions of customers in 24 countries. Revolutionising sensing and control requires coordination on standards, operational processes, security monitoring and incident response, etc., as disruptions in one (small) part of the grid can trigger cascade failures across the entire interconnected grid, potentially leading to a widespread blackout.

3 Research Agenda

To better understand the impact of these challenges on the whole energy system, we propose a multidisciplinary research agenda consisting of five components that need to be investigated. We note that this is not intended as an exhaustive

and definitive list with priorities, rather, it is a first sketch of the most pressing areas where research is needed in our view.

1. We see a prominent role for digital twinning, especially for large-scale systems such as wind farms. These digital twins bridge the physical and digital domain and fulfil the following functions: i) verifying sensor readings from the physical domain against expected system behaviour to detect anomalies indicative of defects or attacks (and distinguishing between these); ii) validating control actions against the digital twin model before transmitting these to actual systems to ensure soundness and viability w.r.t. system stability, power quality and supply continuity; iii) testing the soundness and validity of control signals received from the energy market (e.g., requests to reduce or increase production for grid balancing); iv) modelling boundary condition scenarios to test the impact of automated control actions in these types of situations and the impact these would have on the larger energy grid (compare this to, e.g., the "stresstests" on banks).
2. It is vitally important to guarantee the confidentiality, integrity, authenticity and availability of sensor- and control messages. This brings challenges in terms of the volume of messages, limitations of the ruggedised embedded systems integrated in, e.g., wind turbines and offshore electricity transport systems, and challenges to physically securing long distance data transmission infrastructure in remote locations (e.g., seabed communications).
3. Control of grid infrastructure assets and millions of distributed energy resources requires extensive use of OT systems, which are notoriously vulnerable to cyber threats. We expect a highly heterogenous end situation with a multitude of suppliers of energy production systems, each with complex supply chains. We argue, therefore, that we need to develop an integrated approach that considers the security of entire supply chains. This approach should also consider security throughout the potentially decades-long life cycle of, e.g., wind turbines.
4. Electricity grids are highly integrated systems. We therefore need to improve our understanding of the risks for cascading failures due to attacks on various parts of both the production side of the grid and of the consumption side. This requires building and testing realistic attack scenarios (e.g., "what if an attack turns off all PV inverters of a certain brand?") based on realistic models of complex energy grids.
5. Finally, we argue a need to study how the behaviour of both suppliers and consumers can be influenced in changing market conditions linked to higher volatility of available production capacity. These behavioural changes can be achieved by positive incentives (e.g., negative spot prices when excess capacity is available) as well as negative incentives (e.g., reducing feed-in tariffs to prevent overproduction). We also note that there is a strong link between these behavioural changes and systemic risks; if an attacker can manipulate incentives, producers or consumers may take actions that can ultimately lead to cascading failures (e.g., massively turning off PV inverters or plugging in electric vehicles for charging).

References

1. Core Writing Team. IPCC, 2023: Summary for Policymakers. *Climate Change 2023: Synthesis Report*, pages 1–34, 2023.
2. Shakir D. Ahmed, Fahad S. M. Al-Ismail, Md Shafiullah, Fahad A. Al-Sulaiman, and Ibrahim M. El-Amin. Grid Integration Challenges of Wind Energy: A Review. *IEEE Access*, 8:10857–10878, 2020.
3. Ye Yan, Yi Qian, Hamid Sharif, and David Tipper. A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges. *IEEE Communications Surveys & Tutorials*, 15(1):5–20, 2013.
4. Hanna L. van Sambeek, Marisca Zweistra, Gerwin Hoogsteen, Ivo A. M. Varenhorst, and Stan Janssen. GridShield—Optimizing the Use of Grid Capacity during Increased EV Adoption. *World Electric Vehicle Journal*, 14(3), 2023.
5. Xinghuo Yu and Yusheng Xue. Smart Grids: A Cyber-Physical Systems Perspective. *Proceedings of the IEEE*, 104(5):1058–1070, 2016.
6. Xu Li, Xiaohui Liang, Rongxing Lu, Xuemin Shen, Xiaodong Lin, and Haojin Zhu. Securing smart grid: cyber attacks, countermeasures, and challenges. *IEEE Communications Magazine*, 50(8):38–45, 2012.
7. Eduard Kovacs. Wind Turbine Giant Vestas Confirms Ransomware Involved in Cyberattack. *SecurityWeek*, 2021.
8. Lawrence Abrams. Wind turbine firm Nordex hit by Conti ransomware attack. *Bleeping Computer*, 2022.