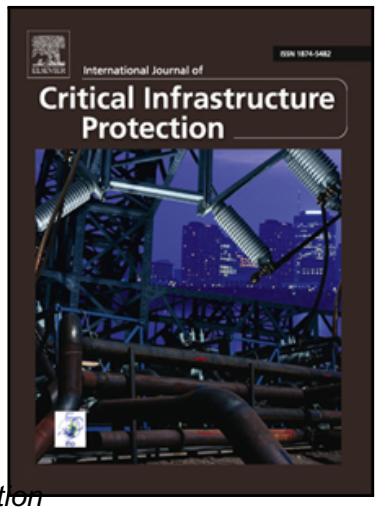

Building resilience against cyber threats in the energy sector

Janne Hagen

PII: S1874-5482(17)30202-0
DOI: 10.1016/j.ijcip.2017.11.003
Reference: IJCIP 233

To appear in: *International Journal of Critical Infrastructure Protection*

Please cite this article as: Janne Hagen , Building resilience against cyber threats in the energy sector, *International Journal of Critical Infrastructure Protection* (2017), doi: 10.1016/j.ijcip.2017.11.003

Building resilience against cyber threats in the energy sector

Janne Hagen
Norwegian Water Resources and Energy Directorate, P.O. Box 5091, Majorstuen, N-0301 Oslo, Norway

Digitalization and the expansion of Internet-based services offer new opportunities for efficient power grid operation. Meanwhile, automation, real-time data, big data analytics and the Internet of Things are beginning to penetrate the energy sector. Technology provides improved situational awareness and faster, more efficient recovery after outages and failures. Innovations in industry and market dynamics push these developments, while regulatory authorities attempt to promote cyber security as increased technological dependence and emergent cyber risks become a reality. The Norwegian Water Resources and Energy Directorate (NVE) regulates security in Norway's hydroelectric and thermal power industries, as well as in the national grid. NVE promotes energy security and infrastructure resilience by improving regulations, guidelines and methods for revision.

Hydropower is the dominant energy source in Norway. Norway's mountainous regions have numerous interconnected water reservoirs. Regulating reservoir water levels and throughput are important to balancing electricity production and consumption, enhancing energy security, managing flood risks and preserving ecosystems and wildlife. Hydropower contributes about 142 000 GWh, 96% of Norway's total energy production while the remaining 4% is provided by thermal and wind power.

Water from Norway's reservoirs flows through tunnels inside mountains. The torrents move turbines that transform kinetic energy to electricity in massive generators located in power stations inside mountains or in the valleys below the reservoirs. Transmission lines crisscross valleys, mountains and fjords, connecting electricity generation sources to consumers. Norway's energy consumers comprise about 5.3 million inhabitants and nearly half a million public and private enterprises.

Statnett SF, the Norwegian transmission system operator (TSO), is responsible for maintaining the balance of the nation's power grid. Managing the transmission grid involves solving an

optimization problem that delivers energy to consumers while maintaining the 50 Hz frequency, planning maintenance activities, reducing the risk of outages, keeping water levels in reservoirs within the mandated thresholds, preserving ecosystems and wildlife, and delivering economic performance – all in real time. While supervisory control and data acquisition (SCADA) and information technology systems help manage water levels, balance power generation and consumption, and operate transformers and circuit breakers in the transmission grid, the planned rollout of smart meters – the first phase in the implementation of Norway's "smart grid" – will provide unprecedented situational awareness and efficient and reliable operations of the electric power grid.

The digitalization of the Norwegian power grid has been underway for years. It has created digital value chains that cross national jurisdictions, including Europe, Asia and the United States, even space (GPS). Operating the electric power grid is complex enough today – grid complexity and the risk of digital failures will increase significantly as intelligence and automation give rise to smart grids and smart cities.

The rollout of smart meter infrastructures will enable new services, including safety, surveillance, energy management and security. It will also prepare the energy infrastructure for the full-duplex transfer of energy from the grid to consumers and from consumers (who inject surplus renewable energy) to the grid.

But the flip side of smart meter infrastructures and the smart grid are many cyber security challenges. First, the smart grid will have numerous, constantly-evolving attack entry points. Second, the Norwegian rollout mandates the remote disabling functionality in all smart meters, which renders a system failure or attack that disconnects large numbers of consumers a strategic risk. The dilemma is that the remote functionality was intended to enhance operational effectiveness, but this becomes a serious threat in an adversary's hands. A scary scenario is the targeted disconnection of millions of homes, key institutions and industries. At this time, regulations permit distribution grid operators to disconnect only one customer at a time. Could this requirement be maintained in the face of a system failure or attack?

A third challenge is posed by the continual integration of new and old systems with and without appropriate security mechanisms. It is extremely arduous to ensure the proper

application and maintenance of configuration, access control and authentication mechanisms, patching regimes, encryption policy administration and key management. Global enterprises deliver their devices and systems to a host of industries, causing the same vulnerabilities and hard-coded passwords to be encountered across the critical infrastructure sectors. The software industry does not deliver secure products, so constant patching is needed. However, a patched version may not work well with the rest of the system. Indeed, patches must be thoroughly tested before they are applied in the critical infrastructure.

Mother Nature has historically imposed the greatest challenges to the Norwegian energy supply. However, cyber crime is moving to a close second place. Norway is a small, but highly digitalized country – this fact has changed the security equation significantly. In 2016, a Norwegian cyber crime and data breach survey revealed that 27% of the 1,500 responding enterprises had experienced unwanted data security incidents; the worst reported incidents were malware infections.

Cyber attacks have impacted every critical infrastructure sector in Norway. However, the attacks on Ukrainian electric utilities in December 2015 and 2016 remind us that the energy sector has inherent vulnerabilities that can be targeted to wreak havoc to the Norwegian economy and society.

What can the Norwegian authorities do about this?

In November 2015, the Norwegian Governmental Committee on Digital Vulnerabilities delivered an assessment in the form of an Official Norwegian Report (NOU) to the Ministry of Justice and Public Security. The report, which covered several critical infrastructure sectors, including the energy sector, incorporated 50 recommendations. Six recommendations were directed at the energy sector:

1. Improve cyber security skills in the supervisory authority for the energy sector (NVE).

2. Assess the types of information in the digital value chain that should be under national control.

3. Explore the robustness of communications in the energy sector and the dependence of the energy sector on the public telecommunications infrastructure.

4. Conduct risk analyses of the integration of SCADA systems and new energy distribution management systems.

5. Stimulate the creation of strong information and communications environments in critical energy grid operators.

6. Require energy enterprises and grid operators to interact closely with the sector KraftCERT or other similar computer security incident response teams (CSIRTs).

Norway has comprehensive security regulations for the energy sector, much more than other European countries. The regulations build on the relevant NIST guidelines, FERC recommendations and the ISO/IEC-27001/2 standard. The regulations share many similarities with ISO/IEC 27001/2, but have different wording. The regulations emphasize the protection of critical SCADA systems and sensitive information.

Cyber-criminal activity and anticipated technological trends have influenced a broad cyber protection regime in Norway. This includes baseline security for all information technology systems, including regulations on storing critical energy data outside the country. Proactive cyber security measures must be accompanied by effective detection and mitigation as well as emergency preparedness. Indeed, emergency preparedness is already covered by the current regulations. Meanwhile, efforts are underway to establish an incident response ecosystem for the energy sector through the establishment of KraftCERT and a national framework for cyber incident handling.

Without question, energy is the most critical infrastructure sector. Cyber threats and digital vulnerabilities will affect energy security to a much greater degree in the future than they do today. Therefore, it is imperative that Norwegian authorities – and the relevant entities in other countries – weave technical, legislative and regulatory themes to craft robust solutions that ensure that the global smart grid will be safe, secure and resilient.

Biography

Dr. Janne Hagen is a Head Engineer at the Norwegian Water Resources and Energy Directorate, Oslo, Norway. She previously served as Principal Scientist at the Norwegian Defence Research Establishment, conducting research on societal security and critical infrastructure protection. Dr. Hagen has been a member of several expert groups, including the Norwegian Governmental Committee on Digital Vulnerabilities in Society, which delivered an Official Norwegian Report (NOU 2015:13) to the Ministry of Justice and Public Security in November 2015. Her research interests include SCADA security, digital society vulnerabilities and emergency preparedness.

Email address: janh@nve.no