HYGCEL

WP6 Task 6.3

Operational risks and cybersecurity

ABSTRACT

Task 6.3 had two main research questions. Research question 1 was dedicated to operational risks of hydrogen production value chain: What are the primary operational risks associated with transitioning from small-scale to large-scale hydrogen production and distribution, and how can these risks be effectively mitigated? Research question 2 focused on cybersecurity in hydrogen infrastructure: What are cybersecurity vulnerabilities in the hydrogen production and distribution value chain, particularly in regions with advanced smart grid systems like Finland and how can they be identified and mitigated?

The first research question was analysed by reviewing past accidents and incidents within the hydrogen value chain, focusing on learning from recorded events and identifying the root causes associated with hydrogen-related risks. The second question analysed historical cyberattacks in the energy market, with a focus on understanding the types of cyberattacks, their motives, and the stakeholders targeted. This analysis also examined the potential consequences of such attacks to suggest and develop strategies for preventing or mitigating future threats. In this context, the work involved collaboration with HYGCEL WP 4 task 3 on "Cybersecurity in the Hydrogen Economy: Enhancing Safety and Resilience with IoT and Edge Computing," where we proposed a suggested solution to improve cyber safety and resilience using IoT systems. The findings from these studies emphasises the importance of robust safety and cybersecurity measures as hydrogen infrastructure scales up and becomes more integrated into energy systems.

MOTIVATION

The rapid growth of the hydrogen economy, driven by the global aim to achieve net-zero emissions by 2050, highlights the need for thorough safety and risk assessments, especially as large-scale hydrogen infrastructure is being planned, but is still relatively new and untested. This study is motivated especially by the urgent necessity to address safety concerns that could for example impact public acceptance, a critical factor in the successful deployment of hydrogen technologies. Additionally, as the hydrogen sector increasingly relies on digital systems, the study focuses on identifying ways to enhance cybersecurity to protect against potential threats that could jeopardize both safety and the reliability of energy supply. By addressing these challenges, the study aims to support the secure and sustainable development of the hydrogen economy, crucial for achieving long-term environmental and economic goals.

RESULTS

Results regarding safety and risks

The findings from the safety studies present a detailed analysis of hydrogen-related incidents and accidents, with a particular focus on the critical areas of storage, distribution, and human factors within the hydrogen value chain. This investigation also addresses the aspects related to transition from small-scale to large-scale hydrogen usage and drawing valuable lessons from historical events.

The analysis covered 82 pcs of hydrogen-related events. Based on the results, most accidents occur during the storage and distribution phases of the hydrogen value chain.

The hydrogen value chain consists of multiple components, and each component presents unique risks that require targeted safety measures. Specifically, components such as piping, valves, fittings, and other connection points were identified as particularly vulnerable, frequently contributing to these incidents. These findings can be explained, for example, by the known physical properties of hydrogen, such as high diffusivity and low molecular weight, which make hydrogen prone to leaks and failures at connection points and containers. This is further explained in **Error! Reference source not found.**, where the gaseous distribution (40%)

and gaseous storage (24%) stages are highlighted as critical points where most hydrogen-related events occur.

Despite the high energy and pressure involved in compression, this phase accounted for 11% of the incidents (see supplementary material of Alfasfos et al. 2024[1]), suggesting better management practices compared to storage and distribution. Incidents related to electrolysis were minor (9%), possibly reflecting the early stage of hydrogen production through this method. The study underscores the vulnerability of gaseous hydrogen distribution components i.e., the pipelines (22%) and storage facilities (18%), suggesting a need for enhanced safety measures in these areas.

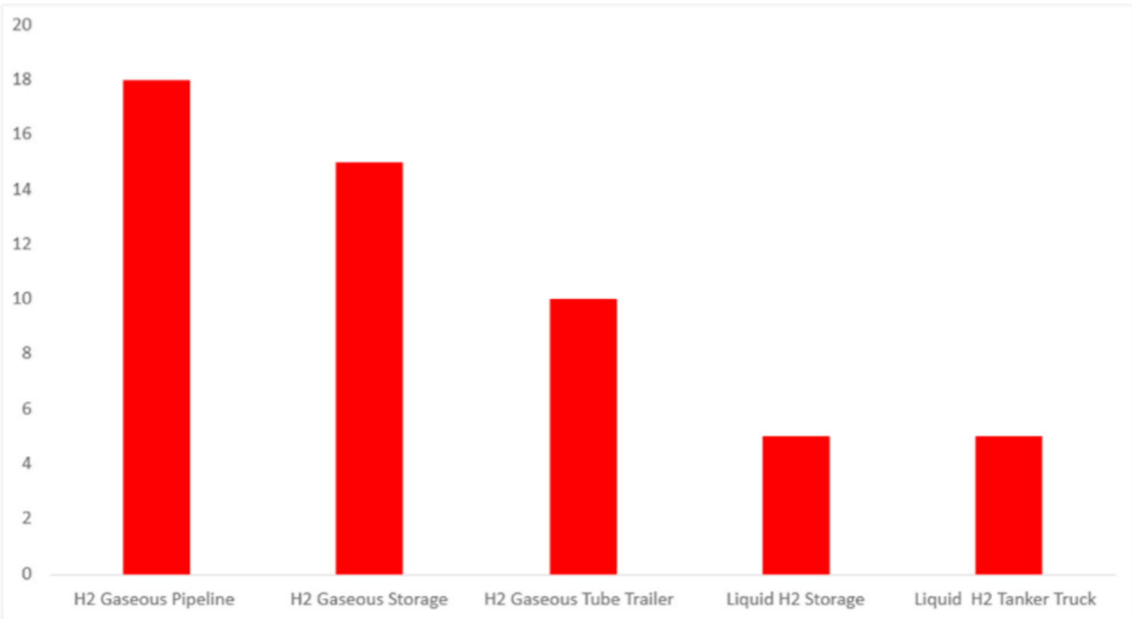

Figure 1 Gaseous and liquid hydrogen events occurring in the storage and distribution stages (number of events).

A significant portion of hydrogen-related incidents can be traced back to human error (Figure 2 parts 1 and 3), which were found to be the predominant root cause of accidents within the hydrogen value chain. Human errors are often linked to insufficient training, inadequate safety procedures, and poor operational oversight, highlighting the critical need for continuous education and training for all personnel involved. Organizational and managerial shortcomings also play a substantial role in these incidents. Common issues include deficiencies in safety management, poor maintenance practices, and a general failure to adhere to established safety standards (lack of standards is discussed in later paragraphs).

To summarise, the study found that human and organizational errors account for 87% of the incidents analyzed, as illustrated in Figure 2, with maintenance operations being a particularly significant factor. Equipment failures, especially in piping, valves, and storage systems, are frequent and often result in dangerous hydrogen leaks. These leaks can escalate into explosions or fires, leading to severe economic and social impacts. For instance, a hydrogen leak at an ammonia plant caused a fire that resulted in substantial equipment damage and financial losses. The findings underscore the urgent need for enhanced safety training, improved maintenance protocols, censors and better design and materials for critical components to mitigate these risks.

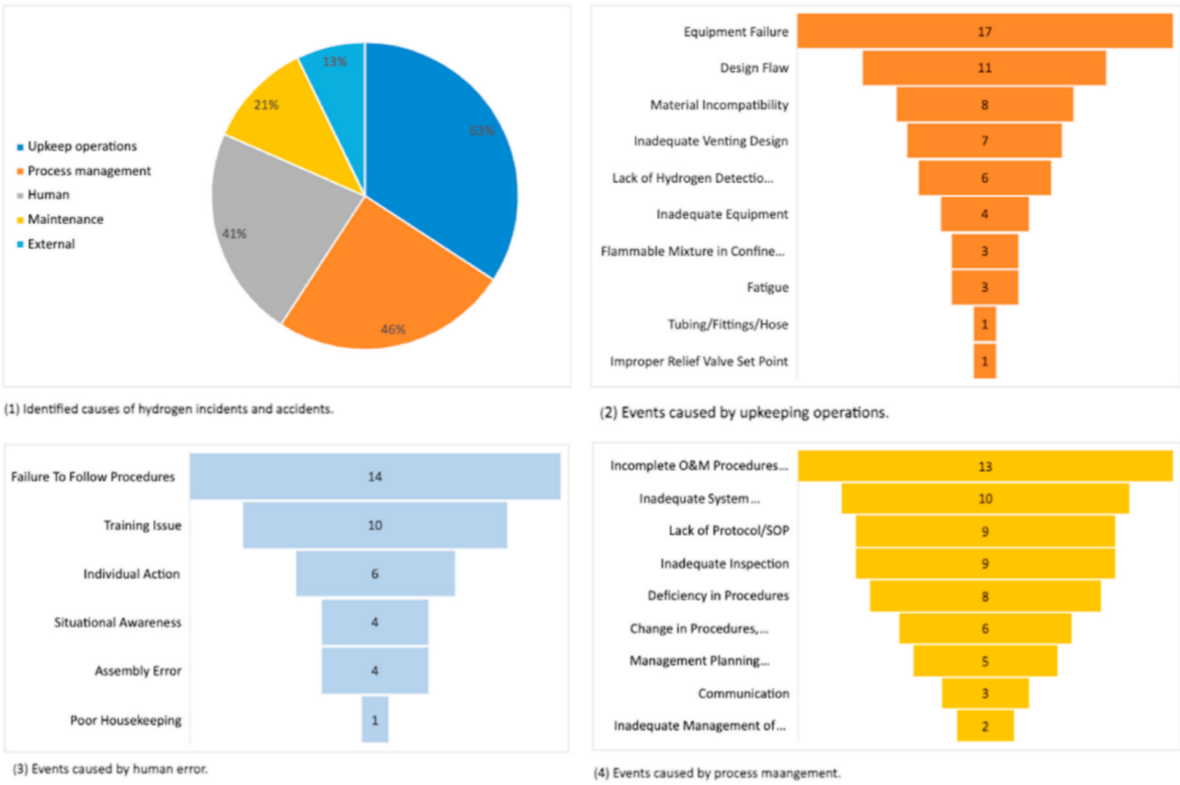

Figure 2 Identified causes of hydrogen incidents and accidents.

The study further highlighted the increased risks associated with transitioning from small-scale to large-scale hydrogen usage. While hydrogen has a long history of safe use in smaller, controlled environments, scaling up its production, storage, and distribution amplifies the potential for accidents. This escalation in risk is particularly evident in the increased operational challenges associated with managing large quantities of highly pressurized Hydrogen with more personnel handling it. Other studies indicate similar findings [2].

Moreover, the study identifies gaps in the current safety legislation and regulatory framework for hydrogen. While regulations like ATEX (Atmosphères Explosibles) provide a foundational framework for safe hydrogen handling, they are not sufficiently comprehensive to address all the unique risks associated with hydrogen, especially as its use scales up. The research points out the need for more specific and stringent regulations that cater to the unique challenges posed by hydrogen and its specific applications [3], including storage, distribution, and integration into existing energy infrastructures.

The analysis of past hydrogen incidents provides valuable lessons for the future development of the hydrogen economy, leading to several key recommendations.

First, enhancing safety training and education is crucial, given that human error is a leading cause of hydrogen incidents. Ongoing, comprehensive training programs are necessary to cover both the technical aspects of hydrogen handling and the importance of adhering to safety protocols.

Second, improving maintenance and inspection practices is essential to prevent incidents. The study recommends the implementation of stricter maintenance schedules and the adoption of advanced monitoring technologies to detect potential issues before they lead to accidents.

Third, as the hydrogen economy scales up, conducting thorough safety assessments and developing management strategies to effectively mitigate the risks associated with large-scale hydrogen storage and distribution are critical steps for ensuring safety and public confidence in hydrogen technologies. It should be noted that with proper safety management and good practices the risks can be mitigated.

Fourth, there is a clear need for more robust safety regulations specifically tailored to the risks associated with hydrogen. This includes updating existing frameworks like ATEX and developing new standards suited to the hydrogen economy. Additionally, addressing these issues requires not only improving individual competencies but also strengthening the overall safety culture and processes within organizations. Beyond technical measures, creating a proactive approach to risk management and safety innovation is essential.

Results regarding cyber security

The findings from the study on hydrogen-related incidents and the broader energy sector underscore the critical importance of addressing not only the physical and human factors but also the growing cybersecurity threats that could severely impact the hydrogen economy. The year 2010 marked a pivotal moment in the cybersecurity threat landscape against the energy sector, signalling the urgent need for initiative-taking measures to ensure a secure energy transition. Notably, cyberattacks such as the Stuxnet worm deployment on Iran's Natanz uranium enrichment facility demonstrated the capability of cybercriminals to inflict physical damage on energy infrastructure. This attack, along with others analysed, highlighted the devastating potential of cyberattacks as tools in political conflicts and emphasized the need for resilient cybersecurity systems.

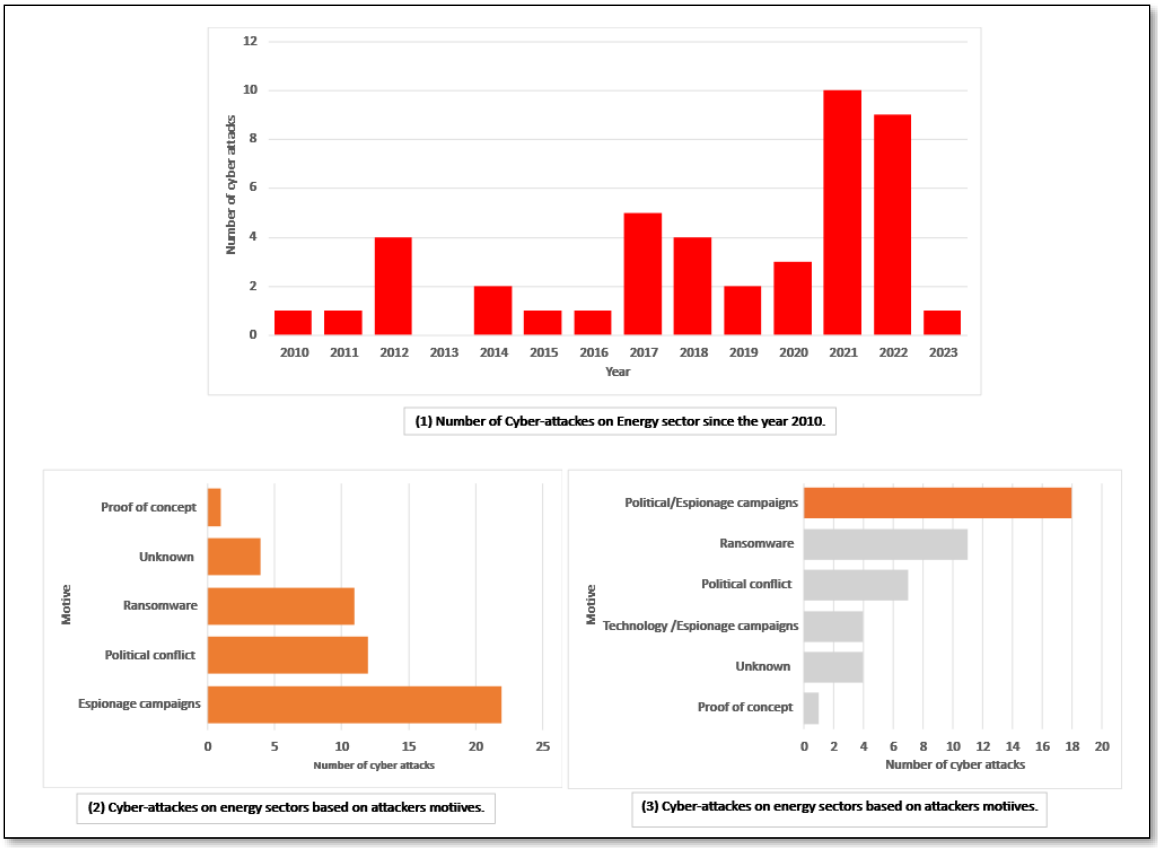

Figure 3 Analysis of 44 major cyberattacks on energy sector since the year 2010, numbers and motives.

An analysis of 44 major cyberattacks on the energy sector since 2010 reveals a consistent increase in such incidents, peaking in 2021 and 2022, as shown in **Error! Reference source not found.**. The predominant motivations behind these attacks were political and espionage efforts, although other motives such as ransomware and proof-of-concept demonstrations were also identified.

Major energy companies, particularly in the electricity and oil sectors, have been the primary targets, with severe consequences including widespread power outages, data destruction, and significant economic disruptions. For instance, the 2015 cyberattack on Ukraine's electricity grid, which used the BlackEnergy malware, resulted in a power outage affecting over 220,000 people, underscoring the perilous implications of cyberattacks on public well-being. The integration of cybersecurity into the hydrogen value chain is increasingly vital as the energy sector becomes more digitized, particularly with the adoption of smart grids and IoT technologies as **Error! Reference source not found.** illustrates.

Finland, with its advanced smart grid infrastructure, exemplifies the heightened risk of cyberattacks in the energy sector. However, these risks can be mitigated through well-designed safety procedures, increased awareness and education among workers, and effective communication among stakeholders across the value chain. Cybersecurity risk assessments were conducted in collaboration with HYGCEL WP 4task 3, have identified the importance of limiting the consequences of attacks and ensuring robust data communication to protect the hydrogen economy.

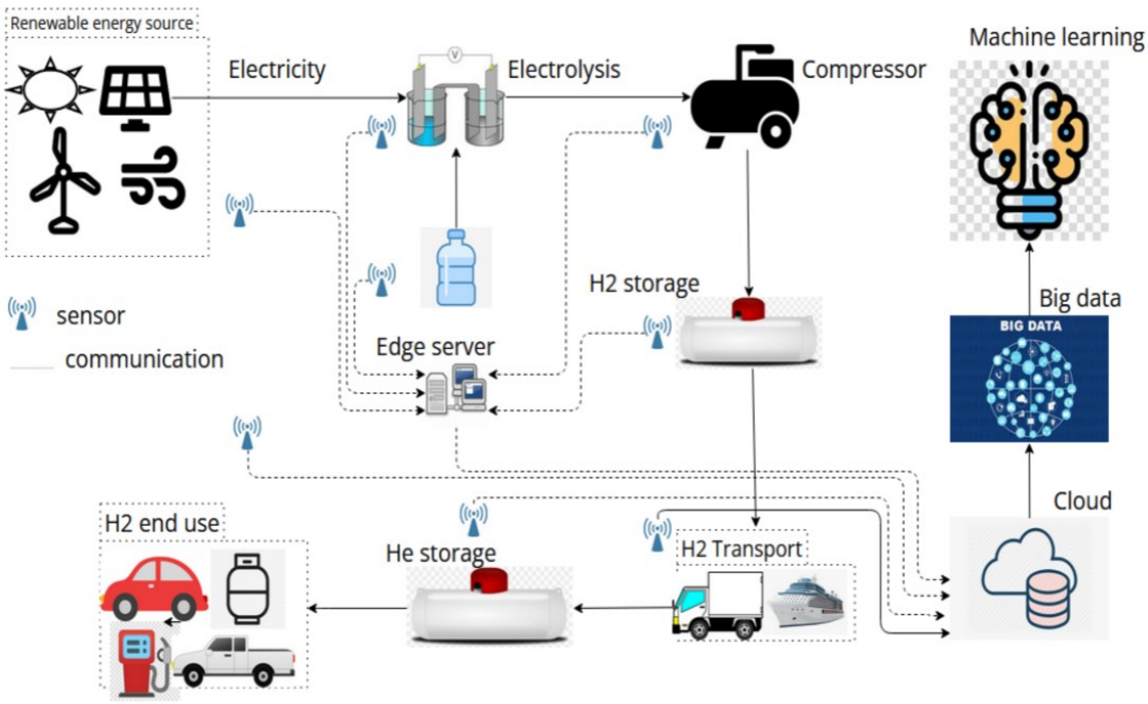

Figure 4 Hydrogen process from generation, storage, transportation to end use, using the renewable energy sources.

As the hydrogen economy continues to expand, integrating cybersecurity measures into all aspects of the energy transition is not just advisable but necessary. Efforts are ongoing to quantify the costs of risk mitigation, with preliminary literature suggesting that these could constitute 5% to 10% of total investments, depending on the value chain.

The role of cybersecurity in safeguarding the future of energy, particularly in hydrogen production and distribution, cannot be overstated, and proactive measures must be prioritized to prevent catastrophic disruptions

APPLICATIONS/IMPACT

The findings emphasize the critical need for integrating robust safety and cybersecurity measures as the hydrogen economy scales up. The transition to large-scale hydrogen usage and the increasing digitization of the energy sector highlight vulnerabilities that could have severe consequences if not properly managed. The impact of this research is evident in the call for enhanced safety protocols and comprehensive training programs due to high share of human factor as a root cause of hydrogen events. In addition, strengthened cybersecurity frameworks to protect both physical infrastructure and data integrity is needed. Ensuring that these measures are in place will be crucial for gaining public trust and securing investment, which are essential for the successful development and expansion of hydrogen facilities globally.

MAIN CONTACT

Jani Sillman and Risto Soukka, LUT Energy systems

AUTHORS

WP 6 authors: Rami Alfasfos (main author in HYGCEL safety research), Jani Sillman, Esa Vakkilainen, Risto Soukka

REFERENCES

[1] Alfasfos, R., Sillman, J., Soukka, R. 2024. Lessons learned and recommendations from analysis of hydrogen incidents and accidents to support risk assessment for the hydrogen economy. International Journal of Hydrogen Energy. 60, 1203-1214. https://doi.org/10.1016/j.ijhydene.2024.02.226

[2] Patel, P., Garaniya, V., Baalisampang, T., Arzaghi, E., Abbassi, R., Salehi, F. 2024. A technical review on quantitative risk analysis for hydrogen infrastructure. Journal of Loss Prevention in the Process Industries. 91, 105403. https://doi.org/10.1016/j.jlp.2024.105403

[3] OECD, 2023. Risk-based Regulatory Design for the Safe Use of Hydrogen, OECD Publishing, Paris, https://doi.org/10.1787/46d2da5e-en.