RELIABILITY AND SECURITY CHALLENGES FOR DIGITAL AND GREEN TRANSITIONS: UNLOCKING THE POTENTIAL OF DATA SPACES FOR MORE RELIABLE AND SAFER ENERGY SYSTEMS

[1]SHENAE LEE, SHANSHAN JIANG, [2]PER HAKON MELAND, [3]ANDREA NEVERDAL SKYTTERHOLM, [4]MARIT KJOSNES NATVIG

[1,2,3,4]Software Engineering, Safety and Security, SINTEF Digital, Norway
E-mail: shenae.lee@sintef.no

Abstract - The European Union (EU) has introduced the REPowerEU Plan in response to energy market uncertainties caused by the Ukraine war, aiming to reduce reliance on Russian energy imports and achieve climate neutrality by 2050. This initiative promotes renewable energy sources like offshore wind and solar power. However, the digital and green transitions pose significant safety and cybersecurity risks. Addressing these challenges is crucial for ensuring the reliability and security of energy systems and critical infrastructures. Unlike the established safety and security frameworks in the oil and gas industry, green technologies lack robust guidelines. This position paper argues for assessing current digital transformation technologies, identifying gaps in standards, discussing supply chain security, and exploring the benefits of incident data sharing. It also explores the role of digital twin technologies and European data spaces in enhancing safety and interoperability. Despite a tradition of data sharing in the oil and gas sector, similar initiatives are lacking in renewable energy due to missing incentives. Establishing regulations, standards and guidelines for cybersecurity and safety in renewable energy systems is an essential task for future work.

Keywords - Twin Transition,Digitalization of Energy Sector,Common European Energy Data Space

I. INTRODUCTION

The European Union (EU) has been grappling with increasing uncertainties in the energy market, exacerbated by the ongoing Ukraine war. In response, the EU introduced the REPowerEU Plan in 2022, a strategic initiative aimed at reducing the bloc's reliance on Russian energy imports [1]. This plan is not only a geopolitical manoeuvre but also a critical step towards achieving the EU's ambitious climate goal of climate neutrality by 2050[2]. Central to this vision is the promotion of renewable energy sources, such as offshore wind and solar power, which have experienced significant growth over the past decade [3][4][5]. In this context, the European Commission published a formal Communication in 2022 which endorses the 'twin transitions' where the goal is to create synergies between digitalization and the green shift [6].

The "digital transition" refers to the integration of advanced digital technologies into the energy sector to enhance efficiency, reliability, and sustainability. This transition involves the adoption of digital tools such as digital twin technologies, which create virtual models of physical systems to optimize performance and predict maintenance needs. An important enabler of digitalization is Industry 4.0 (I4.0). I4.0 refers to the intelligent networking of machines and processes for industry by means of information and communication technology. Usingthe I4.0 technologies, data exchange can be enabled by digital devices and communication protocols that allow the different stakeholders to communicate and share data of different types [7]. While I4.0 technologies originated from the effort to digitalize manufacturing and production systems, I4.0 technologies can potentially be deployed for various types of systems. For example, the ongoing research project APOS (Automated process for follow-up of safety instrumented systems)[8]aims at developing digital representation of safety systems, to support the energy sector to improve the safety performance. A central concept in I4.0 is asset administration shell (AAS) that digitally represents industrial assets. Another important technology in I4.0 is OPC Unified Architecture (OPC UA), a communication protocol developed by the OPC Foundation [9], which is designed to enable an interoperable, more secure and reliable way of accessing data in industrial applications [10]. The OPC UA framework can be applied for different industrial domains and systems of different types [11]. An example of the application of OPC UA is to provide communication interfaces with manufacturing execution system (MES) and enterprise resource planning (ERP) [12].

On the other hand, the "green transition" refers to the comprehensive shift from fossil fuel-based energy systems to renewable and sustainable energy sources. The green transition is not just about replacing energy sources; it also encompasses the integration of these renewable technologies into existing energy infrastructures, ensuring they operate efficiently and safely [13]. Within the renewables business today, due to the emerging nature of the market, there is less information sharing and high competition compared to traditional energy sources.

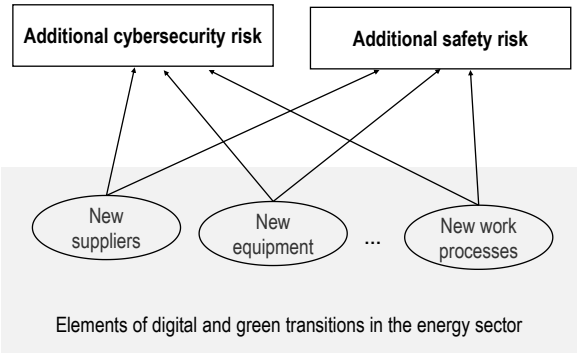

Figure 1. Green and digital transition of energy systems can entail cybersecurity and safety risks.

Green and digital transitions of energy systems will introduce new equipment and new suppliers for renewable technologies, together with new work processes. Furthermore, decentralized energy systems typically use distributed renewable energy sources such as solar and wind power. Such changes can entail risks with respect to cybersecurity and safety, as illustrated in Figure 1. First, more interconnected systemsthrough digital netwroskare more vulnerable to cyberattacks, which poses additional cybersecurity risks. Second, emerging green technologies, like e.g. hydrogen systems, can introduce new safety challenges due to limited knowledge abouthazard characteristics. Lastly, the relationship between safety risks and security risks in high-hazard facilities may need to be addressed, taking into account cyberattacks on operational technology (OT) systems that can lead to severe safety consequences [14]. In a survey among 940 energy professionals, 84% believe that a cyber-attack is likely to cause physical damage to energy assets and 57% anticipate loss of life [15]. For this reason, it is argued in the present paper that ensuring safety and cybersecurity in energy systems are of strategic importance to prevent the adverse impact of twin transitions. Therefore, the main objectives of this paper is to 1) Outline the framework and technologies that can facilitate digital transformation of energy systems 2) Identify gaps in safety and security regulations and standards 3) Discuss supply chain security 4) Explore the opportunity for sharing of incident data related to safety and security. The present study is primarily focuses on twin transitions for the Norwegian energy sector, but the challenges outlined in this paper are relevant for other countries in Europe.

II. CHALLENGES WITH CYBERSECURITY, RELIABILITY AND SAFETY

As energy systems become more interconnected and reliant on digital infrastructure, they become increasingly vulnerable to cyber-attacks. For instance, offshore wind energy is highly distributed, with farms physically at sea, operational data processed in in-house data centres and at larger external centres across Europe. Mission operations are dependent on OT and remote network operations from vendors spread across Europe. Digital disruptions can lead to physical damage to the energy grid and/or loss of energy provision with cascading effects to almost all services in the society.

Based on a comprehensive literature review, Ekechukwu and Simpa [16] argue that the shift towards renewable energy has introduced new vulnerabilities, necessitating the development of advanced cybersecurity measures and standards. According to Dong et al.[17], smart local energy systems (SLES) require robust cybersecurity measures to protect against potential threats and ensure the secure operation of distributed technologies. The orchestration of cyber-physical architectures in SLES necessitates effective detection and management of cybersecurity issues, supported by comprehensive standards and adaptive governance. In the context of virtual power plants (VPPs), Venkatachary et al. [18] highlight the importance of edge computing principles to enhance security. VPPs integrate diverse energy assets into a single virtual entity, which can be targeted by cybercriminals aiming to disrupt operations. The decentralization of energy generation and the increasing use of Internet of Things (IoT) devices further complicate the cybersecurity landscape, requiring innovative solutions to protect data and ensure privacy.

Compared to the oil and gas industry, the regulations and standards governing renewable energy systems involving hazardous substances, such as hydrogen systems and battery energy storage systems (BESS), are less established and less mature. The potential for major accidents involving emerging technologies have beenindicated by recent incidents. For example, the explosion at a hydrogen refuelling station in Norway in 2019 [19] and the battery fire on the ferry MS Brim in 2021 [20] highlight the insufficient knowledge related to the safety aspects of the new renewable energy systems, as well as the lack of detailed regulations and guidance to ensure the safety and reliability of such systems. Experience from such accidentshighlightsthe need for more comprehensive safety regulations, systematic risk management, safer design and safety operating procedures.

Moreover, there is a lack of comprehensive databases for reliability data for renewable systems per today. The oil and gas industry has for decades used OREDA (offshore and onshore reliability data) [21] that reflect the operational experience of different oil and gas installations. The OREDA database is based on agroundwork on reliability data collection, classification, and reliability modelling approaches. Such approaches, despite initially developed for oil and gas application, can be adopted for other application areas like hydrogen systems.

III. RELEVANTREGULATIONS, INIITIATIVES AND STRATEGIES

The future of cybersecurity in renewable energy systems involves addressing the gaps in the previous section by developing comprehensive risk management frameworks and leveraging cutting-edge technologies to mitigate cyber threats, thuscontributing to the realisation of the four key strategies of the European Union's directive on security of network and information systems (NIS directive);managing cyber risk, protection against attacks, detecting cybersecurity events and minimizing the effects of cybersecurity incidents, and the new objectives of NIS2[22] on increasing cyber-resilience in all relevant sectors and improving joint situational awareness and the collective capability to prepare and respond.

These framework and strategies are aligned with the following new and upcoming regulations. The Cybersecurity Act[23]provides a certification framework for ICT products, services and processes to ensure that they meet EU cybersecurity standards. Today, certification is voluntary, however, it might be vital in demonstrating cyber security compliance under other EU laws such as the NIS2 directive and the Cyber Resilience Act. The Cyber Resilience Act{Citation} is a regulation that introduces common cybersecurity rules for manufacturers and developers of products with digital elements, covering both hardware and software. The goal of the Cyber Resilience Act[24] is to ensure that products that are connected to the internet, and software placed on the EU market are more secure. Manufacturers will be kept responsible for the cybersecurity of a product throughout its lifecycle, and lastly, consumers will be properly informed about the cybersecurity of the products they buy and use. The AI Act[25]is a regulation that covers development, deployment, and use of AI systems within the EU. It follows a risk-based approach and classifies AI systems into several risk categories, with different degrees of regulation applying. The Act is created to ensure that AI technologies are developed and used in a way that aligns with fundamental rights, safety and ethical principles. It covers various aspects, including transparency, accountability, and human oversight in AI systems.

Common european data spaces can facilitate secure data sharingfor improved safety and "twin transition". The concept of common European data spaces has been promoted by the European strategy for data [26] as a mechanism to improve European competitiveness through better data availability and control. The concept aims for federated data sharing with increased interoperability, data governance, data sovereignty and value creation based on data, and are built upon sectorial, technical infrastructures for data discovery and trusted data sharing. There are ongoingdata space initivesin many sectors.In the energy sector, existing initiativesare for exampleEnershare[27], EnDaSpace[28], PLATOON[29]. A federated and common European Energy Data Space can support the energy transition towards renewable energy and enable the participation of flexible energy resources as outlined in the EU action plan for digitalizing the energy system [30]. A plan for the realization of the Common European Energy Data Space is developed by the EnTEC report[30]. This report focuses on flexibility in the energy sector where renewables play a key role in the energy flexibility.

Stakeholders in the data space ecosystem include Original Equipment Manufacturers (OEMs), system operators (transmission and distribution), resource aggregators, metered data administrators, customers and third-party service providers. The common European Energy Data Space will be a federated ecosystem where several existing energy data spaces will operate and interoperate between them and across sectors (e.g., with mobility, water and other domains) building upon such common architecture and building blocks. The EU Data Act and Renewable Energy Directive III have provisioned for opening the access to OEM data to enable third parties like technology and component suppliers to provide innovative digital services. One typical use case for energy data spaces is thus related to data access (device, metering and other data), e.g., access to wind power data for predictive maintenance of wind farms/turbines. Another use case to involve small private asset operators in VPPs is related to standardized asset registration process for flexible energy assets to VPPs. There are ongoing initiatives on common architecture descriptions, building blocks and blueprints for federated data spaces (like IDS-RAM[31], GaiaX[32], FIWARE[33] and the iShare Trust Framewor[34]). Reference architectures for energy data spaces are being developed within the EU context such as OMEGA-X[35], ENERSHARE[27] and EDDIE [36] architectures. Data spaces technologies build the basis for data economy and facilitate the onboarding of aorganization to the data ecosystem. Data spaces have a number of technical and non-technical building blocks, such as governance framework, interoperability mechanisms (data models and vocabularies), trust foundations and catalogue for data discovery.

One key technical component is the data space connector, which is the gateway to connect various participants and systems to a data space. A connectorthat facilitateseasy integration of data from systems that implement the OPC UA and AAS into a data spaceis for example implemented[37][38].Organizationsnormally have a number of IT systems that support their business

processes and operations, butthese systems are oftenisolated with no data exchange directly among them. Data space connectors can support data sharing across the internal systems of an organization and streamline itsbusiness activities. On the other hand, the connector canalso facilitate secure data sharing with other data space ecosystem participants incomplient with the data governance framework applied. This will introduce secure opportunities for new business and innovative services. This will also allow third parties to offer new safety-related services using secured access to data that they today do not know and do not have access to.

IV. ISCUSSION AND CONCLUSION

For the improvement of safety for renewable energy systems, we envision that automated safety functions will play a key role. It would therefore be advantageous to establish guidelines that facilitate the application of functional safety standards like IEC 61508 [39] and IEC 61511[40] for the renewable energy systems. IEC 61508 is a standard on functional safety that is used by manufacturers in the development of electrical, electronic, and programmable electronic (E/E/PE) systems. The oil and gas industry has applied IEC 61508/61511 to ensure the demonstration of safety requirements of safety systems on petroleum facilities throughout the lifecycle of the facility. Moreover, in Norway, the Management Regulation by the Norwegian Ocean Industry Authority points to IEC 61508 and IEC 61511,as well as machinery safety standards like IEC 62061 [41] as a basis for petroleum activities. In light of such practices, applying IEC 61508 to hydrogen systems and BESS will offer opportunity to improve safety and reliability of the emerging renewable technologies. For instance, it is advisable to establish requirements for battery management system (BMS) developed based on the approachesin IEC 61511 and IEC 61508. This will include performing hazard and risk analysis considering representative possible accidents like e.g. a fire caused by thermal runaway reaction in the battery modules.

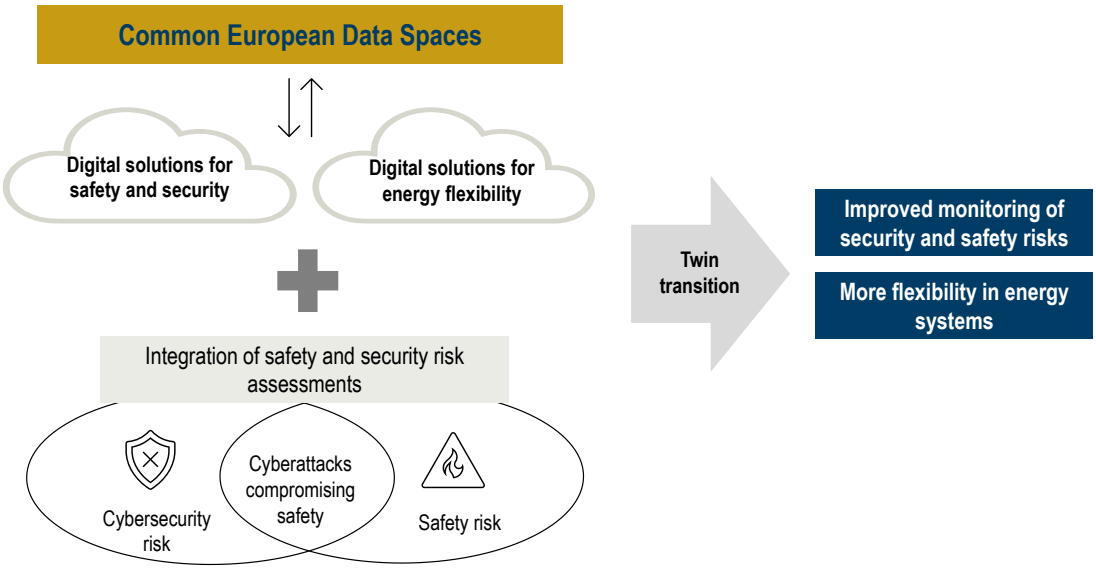

Figure 2. Integration of safety and security assessments, in combination with the possibility to use the data space for better data exchange,for the purpose of facilitating twin transition towards safer, more secure, and more flexible energy systems.

Currently, severaldata spaces implementations exist within the energy sector as well as other sectors, and the energy sector should learn from these initiatives. The mainfocushas been on technical solutions related to data access, data access control, secure data exchange, and data discovery, and cybersecurity and trust have been an active topic in data space technical solutions. General guidelines and solutions for security and trust have also been provided in reference architectures like IDS RAM.

The common European Energy Data Space concept fits well with emerging technologies such as renewable energy, distributed energy production and flexibility markets and provides opportunities for newcomers and third parties to participate and offer new and innovative services using shared data and collaborations via data spaces. Actors with diverse roles and responsibilities can access data from many sources according to a well-defined data governance and sovereignty framework, and the same data can be used to monitor several safety and security related aspects. Suppliers may for example monitor technical installations to ensure timely maintenance and to avoid disruptions. Energy companies can monitor the energy system and detect problems and threats at an early stage, and businesses and citizens can be supported in case of malfunction in their local energy infrastructure (e.g. PV panels or batteries).

Despite of the above, the technical infrastructure needed for a full-scale implementation of a common

European Energy Data Space is still immature.The challengesidentified in this paper and existing literature should be addressed to ensure a smooth twin transition while maintaining safety and security. There is also a lack of real business cases for deployment and operational aspects. The main challenges are related to interoperability as the enormous variety of assets, devices and applications in the energy domain poses a big challenge for semantic interoperability. Safety aspects are so far not specifically addressed in the data space development. The data spaces are designed and implemented to connect different data sources, but no real implementations regarding the connection to safety-related (incident) data is available. Existing databases for incidents and accidents for renewable energy systems could potentially be integrated into acommon data space for enhanced data sharing across EU member states, as illustrated in Figure 2.

The oil and gas industry has a long tradition of cybersecurity frameworks, which can serve as a model for the renewable energy sector. However, as noted ina recent literature review by Imran et al. [42] most of the frameworks, standards and guidelines originate from the US and can be difficult to implement multi- or internationally. Also, voluntary adoption in a non-regulatory environment is questionable. The European Union Agency for Cybersecurity (ENISA) [43] has pointed to a number of shortcoming and problems when it comes to cyber security information sharing in the energy sector. Though there is willingness and commitment among the stakeholders in doing so, there is a lack of time, resources and knowledge to see this through. Animportnat enabler would be practices and tools that can build and maintain trust among the stakeholders, and at the same time comply with different legislation, improve quality of data and create visibility.

ACKNOWLEDGMENTS

We are grateful for the strategic funding from SINTEF Digital to enable this multiplinary study.

REFERENCES

[1] ‘Energy statistics - an overview’. Accessed: Aug. 12, 2024. [Online]. Available: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Energy_statistics_-_an_overview

[2] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS REPowerEU Plan. 2022. Accessed: Aug. 12, 2024. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A230%3AFIN

[3] ‘Energy Statistics 2021’.

[4] ‘The Netherlands - Countries & Regions’, IEA. Accessed: Aug. 02, 2024. [Online]. Available: https://www.iea.org/countries/the-netherlands

[5] ‘EBN-Infographic-2023-A4-Engels.pdf’.

[6] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL 2022 Strategic Foresight Report Twinning the green and digital transitions in the new geopolitical context. 2022. Accessed: Aug. 12, 2024. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0289&qid=1658824364827

[7] M. M. Mabkhotet al., ‘Mapping Industry 4.0 Enabling Technologies into United Nations Sustainability Development Goals’, Sustainability, vol. 13, no. 5, Art. no. 5, Jan. 2021, doi: 10.3390/su13052560.

[8] ‘APOS 2.0 - Automated process for follow-up of safety instrumented systems’, SINTEF. Accessed: Sep. 16, 2024. [Online]. Available: https://www.sintef.no/en/projects/2023/apos-2.0-automated-process-for-follow-up-of-safety-instrumented-systems/

[9] ‘Home Page’, OPC Foundation. Accessed: Sep. 20, 2024. [Online]. Available: https://opcfoundation.org/

[10] R. Drath, E. Barnstedt, B. Fiebiger, and W. Schlögl, ‘Discussion Paper- Interoperability with the Administra9on Shell, OPC UA, and Automa9onML: Target Image and Recommenda9ons for Industrial Interoperability.’.

[11] S.-H. Leitner and W. Mahnke, ‘OPC UA - Service-oriented Architecture for Industrial Applications’, Softwaretechnik-Trends, 2006, Accessed: Sep. 20, 2024. [Online]. Available: https://www.semanticscholar.org/paper/OPC-UA-Service-oriented-Architecture-for-Industrial-Leitner-Mahnke/0ccb58f9a3a9df31ec16c9993285e3e7d7d46aff

[12] Z. Luo et al., ‘OPC UA-Based Smart Manufacturing: System Architecture, Implementation, and Execution’, in 2017 5th International Conference on Enterprise Systems (ES), Sep. 2017, pp. 281–286. doi: 10.1109/ES.2017.53.

[13] Q. Hassan, S. Algburi, A. Z. Sameen, H. M. Salman, and M. Jaszczur, ‘A review of hybrid renewable energy systems: Solar and wind-powered solutions: Challenges, opportunities, and policy implications’, Results in Engineering, vol. 20, p. 101621, Dec. 2023, doi: 10.1016/j.rineng.2023.101621.

[14] S. Parker, Z. Wu, and P. D. Christofides, ‘Cybersecurity in process control, operations, and supply chain’, Computers & Chemical Engineering, vol. 171, p. 108169, Mar. 2023, doi: 10.1016/j.compchemeng.2023.108169.

[15] DNV, ‘The Cyber Priority - The state of cyber security in the energy sector’, 2022. Accessed: Oct. 27, 2022. [Online]. Available: https://www.dnv.com/cybersecurity/cyber-insights/thecyberpriority.html

[16] D. E. Ekechukwu and P. Simpa, ‘The future of Cybersecurity in renewable energy systems: A review, identifying challenges and proposing strategic solutions’, Computer Science & IT Research Journal, vol. 5, no. 6, Art. no. 6, Jun. 2024, doi: 10.51594/csitrj.v5i6.1197.

[17] S. Dong, J. Cao, D. Flynn, and Z. Fan, ‘Cybersecurity in smart local energy systems: requirements, challenges, and standards’, Energy Informatics, vol. 5, no. 1, p. 9, Jun. 2022, doi: 10.1186/s42162-022-00195-7.

[18] S. K. Venkatachary, A. Alagappan, and L. J. B. Andrews, ‘Cybersecurity challenges in energy sector (virtual power plants) - can edge computing principles be applied to enhance security?’, Energy Informatics, vol. 4, no. 1, p. 5, Mar. 2021, doi: 10.1186/s42162-021-00139-7.

[19] Hydrogen Safety Panel, ‘Hydrogen Incident Examples Select Summaries of Hydrogen Incidents from the H2tools.org Lessons Learned Database’, 2020.

[20] ‘NSIA-Brim-Repor-2022_07.pdf’. Accessed: Sep. 24, 2024. [Online]. Available: https://safety4sea.com/wp-content/uploads/2022/07/NSIA-Brim-Repor-2022_07.pdf

[21] OREDA, Offshore Reliability Data Handbook. 2002.

[22] ‘Cybersecurity of network and information systems (2022) | EUR-Lex’. Accessed: Sep. 25, 2024. [Online]. Available: https://eur-lex.europa.eu/EN/legal-content/summary/cybersecurity-of-network-and-information-systems-2022.html

[23] 'The EU Cybersecurity Act | EUR-Lex'. Accessed: Sep. 25, 2024. [Online]. Available: https://eur-lex.europa.eu/EN/legal-content/summary/the-eu-cybersecurity-act.html
[24] 'Cyber resilience act'. Accessed: Sep. 25, 2024. [Online]. Available: https://eur-lex.europa.eu/resource.html?uri=cellar:864f472b-34e9-11ed-9c68-01aa75ed71a1.0001.02/DOC_1&format=PDF
[25] 'Artificial intelligence act'.
[26] 'A European strategy for data | Shaping Europe's digital future'. Accessed: Sep. 25, 2024. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/strategy-data
[27] 'Enershare | The Energy Data Space for Europe'. Accessed: Sep. 25, 2024. [Online]. Available: https://enershare.eu/
[28] 'EnDaSpace - modern data economy in the energy industry', Fraunhofer Institute for Energy Economics and Energy System Technology. Accessed: Sep. 25, 2024. [Online]. Available: https://www.iee.fraunhofer.de/en/presse-infothek/press-media/overview/2021/EnDaSpace-modern-data-economy.html
[29] 'Overview | PLATOON'. Accessed: Sep. 25, 2024. [Online]. Available: https://platoon-project.eu/about-platoon/overview/
[30] 'Common European Energy Data Space - Publications Office of the EU'. Accessed: Sep. 23, 2024. [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/43b8d2d1-6975-11ee-9220-01aa75ed71a1/language-en
[31] 'README | IDS Knowledge Base'. Accessed: Sep. 25, 2024. [Online]. Available: https://docs.internationaldataspaces.org/ids-knowledgebase/v/ids-ram-4/
[32] 'Home - Gaia-X: A Federated Secure Data Infrastructure'. Accessed: Sep. 25, 2024. [Online]. Available: https://gaia-x.eu/
[33] 'FIWARE - Open APIs for Open Minds'. Accessed: Sep. 25, 2024. [Online]. Available: https://www.fiware.org/
[34] 'iSHARE Trust Framework - iSHARE Trust Framework'. Accessed: Sep. 25, 2024. [Online]. Available: https://ishareworks.atlassian.net/wiki/spaces/IS/overview
[35] 'OMEGA-X: Towards a reference architecture model – Omega-X'. Accessed: Sep. 25, 2024. [Online]. Available: https://omega-x.eu/2023/06/20/omega-x-towards-a-reference-architecture-model/
[36] 'EDDIE Architecture'. Accessed: Sep. 25, 2024. [Online]. Available: https://eddie-web.projekte.fh-hagenberg.at/architecture/
[37] M. Neubauer et al., 'Architecture for manufacturing-X: Bringing asset administration shell, eclipse dataspace connector and OPC UA together', Manufacturing Letters, vol. 37, pp. 1–6, Sep. 2023, doi: 10.1016/j.mfglet.2023.05.002.
[38] M. Jacoby, F. Volz, C. Weißenbacher, L. Stojanovic, and T. Usländer, 'An approach for Industrie 4.0-compliant and data-sovereign Digital Twins', Realization of the Industrie 4.0 Asset Administration Shell with a data-sovereignty extension, vol. 69, no. 12, pp. 1051–1061, 2021, doi: 10.1515/auto-2021-0074.
[39] IEC 61508, 'IEC 61508 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems'. 2010.
[40] IEC, 'IEC 61511 Functional safety - Safety instrumented systems for the process industry sector', International Electrotechnical Commission, Geneve, Switzerland, 2016.
[41] IEC 62061. Safety of machinery - Functional safety of safety-related control systems, 2021.
[42] H. Imran, M. Salama, C. Turner, and S. Fattah, 'Cybersecurity Risk Management Frameworks in the Oil and Gas Sector: A Systematic Literature Review', in Advances in Information and Communication, K. Arai, Ed., Cham: Springer International Publishing, 2022, pp. 871–894. doi: 10.1007/978-3-030-98015-3_59.
[43] ENISA, 'Report on Cyber Security Information Sharing in the Energy Sector', ENISA, Report/Study, Nov. 2016. Accessed: Sep. 16, 2024. [Online]. Available: https://www.enisa.europa.eu/publications/information-sharing-in-the-energy-sector

★★★