Methodological insights for the prevention of cyber-attacks risks in the energy sector: An Empirical Study

Jean Bertholat, Myriam Merad, Johann Barbier

Methodological insights for the prevention of cyber-attacks risks in the energy sector: An Empirical Study

Jean Bertholat

UMR LAMSADE, Dauphine University PSL, France; Innovation Department, Alten SA, France. E-mail: jean.bertholat@atlen.com*

Myriam Merad

UMR LAMSADE, Dauphine University PSL, France. E-mail: myriam.merad@lamsade.dauphine.fr*

Johann Barbier

Innovation Department, Alten SA, France. E-mail: johann.barbier@atlen.com

As the reliance on technology and virtualization grows, the vulnerability to cyber-attacks increases, necessitating specialized approaches to analyze and understand these risks. This research focuses on developing a comprehensive framework for the identification, analysis, and management of cyber risks in the energy industry, with the goal of enhancing the resilience of sociotechnical systems against known and emerging cyber threats. This paper provides a first critical analysis of existing methodologies and cyber risk assessment practices, identifies gaps in current approaches, and outlines a roadmap for the development and implementation of a cyber risk study methodology and a digital tool tailored to the energy sector. The proposed methodology incorporates the development of knowledge databases for cyber risk analysis, encompassing data on energy industry environment and past cyber incidents and accidents. This information will facilitate the identification of attack scenarios and enable a comprehensive categorization of risks. The paper also discusses the practical application of the developed methodology applied to a first case study within the energy industry, illustrating its potential for enhancing cyber resilience. Finally, the paper reflects on the implications of the findings for the broader field of cyber risk analysis and management, as well as avenues for future research and development.

Keywords: Cybersecurity – risk analysis, risk management - Methodology - Programming - Software

1. Introduction

The increasing dependence on technology and on virtualization has led to a corresponding increase in vulnerability to cyber-attacks, and the need for specialized approaches to analyze and understand these risks. While current risk management standards provide some guidance (e.g. ISO 31000 and 27000), there is a lack of clear and consistent methods commonly shared for assessing the effectiveness of cyber risks management systems. Comprehensive and well-designed cyber risk analyses can provide valuable insights into organizations' vulnerabilities and potential strategies for mitigating risks.

Our research is focusing on cyber risk analysis and management in the energy industry and sector. Our goal is to suggest a framework for the identification, the analysis, and the management of cyber risks for sociotechnical systems in the energy industry and sector. This framework aims at improving the resilience of these systems to known and emerging cyber-attacks.

One of our main tasks is to organize an adequate and accurate database for cyber risk analysis. This will include data on past cyber incidents, near misses, and cyber accidents, which will enable the identification of attack' scenarios and a detailed categorization of risks. Based on this information, relevant methods for cyber risk analysis and management will be proposed and applied to case studies.

To address the challenges and objectives laid out in our research project, this paper is organized as follows. Section 1 provides a first comprehensive overview and critical analysis of existing methodologies and cyber risk assessment practices in the literature to understand their strengths and limitations as well as identifying potential gaps that our proposed framework seeks to address. In Section 2, we outline the roadmap and objectives established for future research, detailing the steps we believe are necessary to develop a holistic and adaptable approach. To address the issues linked to the identification, the analysis, and the management of cyber risks in sociotechnical systems located in ever-evolving cyber threat landscape. In Section 3, we will focus on the application of our proposed roadmap to a fictive simplified use case within the energy sector. This will serve to demonstrate the potential accuracy and effectiveness of the roadmap, as well as its potential for further refinement and adaptation in real-world scenarios. Finally, in Section 4, we engage in discussions and perspectives, reflecting on the implications of our findings for the broader field of cyber risk analysis and management, as well as potential avenues for future research and development.

By following this structure, our paper aims to provide a clear and coherent overview of the current state of cyber risk analysis in the energy sector, the proposed framework, and its potential impact on the resilience of sociotechnical systems.

2. Critical Analysis

In the realm of scientific literature concerning cyber risk specifically in the energy sector, which encompasses around thirty papers, there are three primary schools of thought. These perspectives concentrate on known risks by assuming the predictability of an attack and center the focus of cyber risk studies on the presence of vulnerabilities (Peterson, Haney, and Borrelli 2019). These methodologies, which are the least costly in terms of finances and social investment, enable the generation of swift quantitative conclusions (Gourisetti, Mylrea, and Patangia 2020) and facilitate the establishment of risk mitigation procedures or insurance policies (Lau et al. 2021). This approach can indeed be employed when the threat cannot be identified; however, when the risk is known, it represents only a sub-component of a broader risk study, which is what is pursued in our research.

Specifically, our goal of identifying the interdependencies between existing risks to dynamically refine the risk study aligns more closely with the second school of thought, which is the examination and the consideration of threat behavior (Zografopoulos et al. 2021). This practice is more resource-intensive, as it emphasizes the cyber ecosystem - a rapidly evolving and unpredictable environment. It necessitates the analysis of hazards and their correlation with the vulnerable system to evaluate response behavior (Wang et al. 2021) and the potential consequences. Some solutions, which approach cyber risk studies from this angle, attempt to develop detection technologies (Papastergiou, Mouratidis, and Kalogeraki 2021) to counter threats in real-time. Meanwhile, others explore the long-term evolution of threats (Borenius et al. 2022) without suggesting a methodology to respond as effectively as possible before they materialize.

The final school of thought strives to address risk assessment from the perspective of regulations and standards. Papers that discuss regulatory and standards aspects soon recognize

that these are insufficient (Erdogan et al. 2022), (Bajramovic and Gupta 2017) and therefore propose approaches akin to the current mentioned in the preceding paragraph (Liatifis et al. 2022). Compliance with regulatory aspects is a prerequisite for any risk study, making it crucial to concentrate on this aspect. However, similar to the analysis of a system's vulnerability, compliance study is part of a more comprehensive scope that is encompasses in cyber risk study. Our research is conducted within this perspective of integrating these diverse schools of thought.

In conclusion, shedding light on risk assessment approaches applied to the energy sector highlights the importance of understanding the various schools of thought and their implications for industry. This analysis underscores the necessity of sharing and structuring data in order to comprehend the intricate cyber ecosystem that interacts with the energy sector industries. By fostering collaboration and effectively organizing data, researchers and industry professionals can better address the complex and evolving cyber risks that these industries face, ultimately enhancing security and resilience in the energy sector.

3. RoadMap – Methodology

The objectives of this roadmap presentation are multifaceted, as it aims to provide a comprehensive overview of the long-term vision of the research project, focusing on the development of a cyber risk assessment methodology tailored to the energy industry. By presenting this roadmap to researchers in the field, we hope to receive valuable feedback and guidance on our proposed approach, enabling us to refine and enhance our research trajectory. The presentation will highlight the key milestones and stages involved in the project, illustrating how they build upon one another to form a cohesive and robust framework for cyber risk assessment. Furthermore, the presentation seeks to facilitate collaboration and knowledge exchange among experts, fostering a productive dialogue that will contribute to the advancement of the field and ensure the development of a well-rounded, impactful thesis. Ultimately, the roadmap presentation will serve as a foundation for the project, guiding its progress and evolution in response to the feedback and insights gained from the wider research community.

3.1. Development of Knowledge Bases

The development of knowledge bases is crucial for enhancing cyber resilience, as they serve as repositories of vital information, best practices, and lessons learned from past incidents. More specifically, a collaborative knowledge database can foster information sharing and cooperation between organizations, industries, and governments, allowing for a more comprehensive understanding of the ever-evolving cyber threat landscape. While organizations such as CISA have initiated efforts to create such knowledge bases (Enhancing resilience through cyber incident data sharing and analysis, CIDAWG ,2015) the tangible results have been limited, partly due to the insufficient details provided in incident declarations (Incident Reporting System, CISA). By encouraging collaboration and more detailed reporting, a robust and informative knowledge base can be established, leading to improved decision-making, risk management, and ultimately, cyber resilience. This collaborative approach will empower stakeholders to learn from one another's experiences, identify emerging threats, and develop proactive mitigation strategies to counteract the constantly evolving cyber risks that affect the energy industry and other critical sectors.

3.1.1. The Environment Surrounding the Energy Industry

Understanding the environment in which the energy industry operates is crucial for assessing the cyber risks it faces. This includes identifying defensive actors (e.g., policymakers, industry

stakeholders, researchers, and think tanks) and threat actors (e.g., cybercriminals, state-sponsored hackers) that could target the industry. Additionally, we will explore the trends in cyber incidents and potential impacts on the industry.

3.1.2. The Specific Targeted Industry

Within the energy industry, we will map the key organizational actors and their relationships, identify regulations and standards governing cybersecurity, and analyze the industry's vulnerabilities and potential attack vectors. This information will be gathered through interviews with industry professionals, document analysis, and review of relevant literature.

3.1.3. The Cyber Incidents and accidents

To assess cyber risks effectively, we need to understand the types of cyber incidents and accidents that can occur in the energy industry. We will develop a knowledge database around cyber incidents and accidents by examining existing databases, analyzing regulatory criteria and indicators proposed in scientific papers and identifying relevant cyber events. This will allow us to create a structured database that can be used in cyber risk study.

3.2. Development of Cyber Risk Study Methodology

Based on the knowledge base developed, we will create a comprehensive cyber risk study methodology tailored to the energy industry. This will involve:

(i) Reviewing existing risk analysis methods and identifying their strengths and weaknesses in the context of cyber risk analysis for the energy industry.

(ii) Modelling complex systems in the energy industry and identifying the limitations of these models (e.g., data availability, budget constraints, and study time).

(iii) Developing a fictive case-study that encompasses the various stages of the risk assessment process, including identification, analysis, evaluation, and risk management. This will involve the application of appropriate risk study methods at each stage and the consideration of various risk scenarios.

3.3. Implementation of Cyber Risk Study Methodology

The Implementation of the Cyber Risk Study Methodology section focuses on the practical aspects of applying the developed risk study methodology within real-world scenarios. This involves the creation and implementation of a digital tool designed not only to gather and populate data from a diverse range of sources and structures (RetEx, press articles, or ATT&CK descriptions) but also to apply the risk study methodology to the collected data. This integrated tool will enable efficient and effective analysis of cyber risks in complex environments.

To ensure the validity and effectiveness of the developed methodology and digital tool, case studies within the energy industry will be utilized as a means of testing and refining the approach. These case studies will provide valuable opportunities to assess the practicality and relevance of the methodology in a real-world context, allowing for any necessary adjustments or improvements to be made.

The results and insights obtained from the application of the methodology to these case studies will be a crucial component of the thesis. They will not only demonstrate the efficacy of the developed cyber risk study methodology but also contribute to the collective understanding of cyber risks within the energy industry. By showcasing the successful implementation of the methodology, this section will emphasize the potential value and impact of the research on enhancing cyber resilience in the targeted industry.

4. Case Study

The case study section of this paper aims to apply the developed cyber risk study roadmap, focusing on hydroelectric infrastructures. These infrastructures are characterized by their distributed architecture with numerous sensors, automation and the age and complexity of their networks, making them particularly vulnerable to cyber threats. In this case study, we will specifically examine a French dam, demonstrating the practical application of the proposed cyber risk study methodology in addressing the unique challenges and vulnerabilities associated with electrical infrastructures within the energy industry.

4.1. Case Study Approach

The case study section applies the various steps of the thesis methodology to a simplified real infrastructure. The modeling is intentionally simplified due to the lack of easily accessible data and the focus on evaluating the methodology rather than obtaining fully accurate data. The risk scenarios developed in this section are framed based on reality but adapted in this fictive case-study (EuRepoC, TiSafe, Incident Hub database).

A deliberately simplistic and not necessarily relevant risk study methodology is applied to the case study, as the primary objective is to evaluate the methodology itself rather than the relevance of the study. The data presented are derived from a shallow analysis of the environment, with a more detailed examinations of the databases planned for future research. This will include connecting and inferring data to automate the analysis process, while further refining the methodology.

4.2. Hydroelectric Power Plant and Surrounding Environment

In this case study, the focus is on a French hydroelectric dam involved in water collection, treatment (3600Z), and power generation (3511Z). The surrounding environment includes 19 operators, thousands of hectares of land, and numerous contracts with various stakeholders. The dam is managed by the company “Société du Canal de Provence” and is connected to various infrastructures, such as treatment plants, micro-electric power stations, and reservoirs.

In terms of cyber threat actors, Russian groups, North Korean groups, and hacktivists pose potential risks for the system, especially with the use of ransomwares that being a dominant threat trend (X-Force Threat Intelligence Index 2022 IBM Full Report).

4.3. The Bimont Dam Infrastructure

The case study examines a French hydroelectric dam, the Bimont Dam, located in Aix-en-Provence. Established in 1957, the dam generates 9 GWh of electricity annually and provides water to 150,000 hectares of agricultural land. It employs around 50 people and competes with companies like Veolia Water.

The dam's IT/OT systems comprise traditional ICS components, including SCADA and production network components, often with outdated software versions. Employee awareness of cyber risks remains low.

Additionally, the Bimont Dam shares a concerning history with the Malpasset Dam, suggesting possible vulnerabilities that could be triggered by various hazards.

Regulatory actors, Figure. 1, also play a vital role in overseeing the dam's operations, and understanding their expectations and connections is crucial for addressing potential risks effectively.

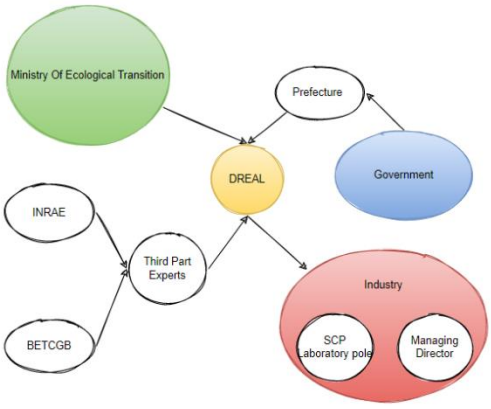

Fig. 1. Regulatory actors interacting with the industry for the case study modeling.

These data from different public sources, will be valuable for assessing the various criteria essential for the risk analysis conducted within the context of the Bimont Dam case study.

4.4. Analyzing Cyber Risk Scenarios and Their Consequences on a Hydroelectric Dam

The case study delves into the risk study methodology by firstly identifying various attack scenarios and analyzing their potential impact on the Bimont Dam. Two attack types, Table 1, are chosen for analysis. Ransomware, the most prevalent today and Advanced Persistent Threat (APT) characterized by long-term and targeted objectives such as espionage or destruction/destabilization, exemplified by the case of Sony (Lehu 2018). It generally requires a higher level of complexity and investment of resources. Three scenarios are modeled statically using the MITRE ATT&CK framework, for instance Sc.1; “Phishing (IA) - Valid Account (P) - Default Credentials (LM) - Commonly Used Port (C&C) - Loss of control (I)”. The framework outlines a sequence of causes and effects, Figure 2, involving exploitation of vulnerabilities, installation of remote access software, and other steps leading to loss of control on the turbine. The ATT&CK framework is utilized to illustrate cyber-attack scenarios following the cyber kill chain concept. Each individual attack technique within a scenario corresponds to a specific metric in the CVSS vector, allowing for a comprehensive representation of the attack's characteristics. The scenarios employed in this study are derived from expert judgement and are based on historical cyber-attacks such as Stuxnet and Triton.

Table 1. Some attributes of Attack scenarios

Attack SC	Attack Type	Kinetic
Sc.0	Ransomware (Eternity Ransomware)	Moderate
Sc.1	Ransomware (Conti)	Moderate
Sc.2	APT	Slow

A systemic approach is taken to understand the attack, avoiding siloed treatment of threats. Literature analysis demonstrates an increased level of abstraction when considering cyber threats, shifting focus from specific targets to more abstract categories.

In this study, the Common Vulnerability Scoring System (CVSS) score is expanded[a] to apply to attack behavior rather than just vulnerability.

For instance, the Sc.1 mentioned above can be evaluated with the following CVSS v3.1 Vector: [AV:N/AC:L/… /MA:H]. The scenarios are assessed based on their characteristics, consequences, kinetic and probability of occurrence.

Consequences of the attacks are considered, with varying levels of financial loss and operational impact for each scenario. The potential impact on stakeholders, such as EDF and households depending on the dam's electricity, is also examined.

The case study emphasizes the importance of data from public and private sources in understanding the environment and the potential

[a]CVSS, generally used to rate vulnerabilities, is there applied to evaluate cyber attack's impacts, from a global perspective, considering characteristics like attack vector and complexity, as well as its effects on confidentiality, integrity, and availability.

for developing a tool to collect and aggregate this information for improved risk assessment.

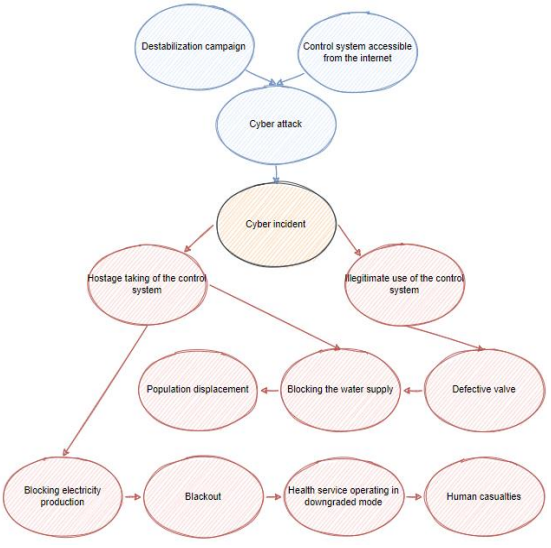

Fig. 2. Causes-consequences diagram.

4.5. Evaluating risk scenarios

The evaluation phase of the case study involves ranking the risk levels associated with the different attack scenarios and aggregating the results to create a probability-consequence matrix.

Ransomware attacks are found to have the highest likelihood of occurrence (Tenable 2022 Threat Landscape Report) The consequences focus is on the potential financial losses for the company, which could be as follows (reflection on public data as French water price): In Sc.0, there could be a €4 million operational loss per day (3.5% of turnover) and a €2 million ransom (average ransom demand). Sc.1 might include a €4 million operational loss, damaged reputation leading to a 1% loss of agricultural customers (€15 million/year), and a €7 million ransom. For Sc.2, the consequences could be a €12 million operational loss over three days, €200,000 in repair costs and partial drainage of the lake, as well as reputational damage. The scenarios are therefore ranked according to an expert's judgment and their probability and severity, as shown in Figure 3.

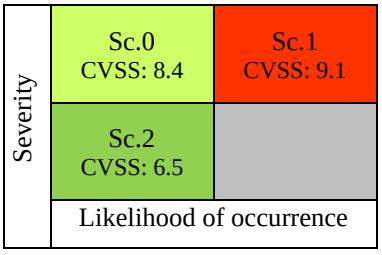

Fig. 3. Probability - Severity matrix of the 3 scenarios

4.6. Managing risk scenarios

In the context of critical infrastructure, managing cyber risks entails the establishment of technical, organizational, and human safeguards to minimize the risks previously characterized.

For example, implementing a strong password policy and a software update policy (cf. MITRE D3FEND) for public-facing applications in Sc.1 could decrease the CVSS score to 7.3.

4.7. Case study conclusion

In conclusion, the purpose of this case study was to apply the methodology outlined earlier in the previous section. The relevance of the results is strongly influenced by the quality of the data provided at the beginning of the study. Various system modeling methods can be employed to enhance the accuracy of the analysis, a simplified one was used in this study. Additionally, numerous techniques (Seda-Sanabria, Morgeson, and Dechant 2023), the NCISS from CISA, or the CRS from the NIST and tools like IT Security Risk Management from Archer or Nucleus from Nucleus security, are available for studying, quantifying and prioritize, aggregate data from the various components of an attack.

This case study demonstrates that more precise data on the infrastructure and the cyber ecosystem in which it operates significantly impacts the level of detail in modeling target and source systems, ultimately affecting the results obtained.

5. Conclusion

This paper has outlined the development of a cyber risk study methodology tailored to the energy industry, specifically for plant operators and inspection agencies. By conducting a comprehensive review of the literature and considering various aspects such as the academic contribution, selection of an activity domain, development of a knowledge base of the target environment, cyber incidents, modeling of complex systems, and risk study methodologies, we have proposed a robust and effective cyber risk study methodology.

The proposed methodology encompasses multiple stages, including identification, analysis, evaluation, and risk management, taking into account the unique characteristics of the energy industry and the specific challenges it faces in terms of cybersecurity. Through the integration of collaborative efforts and continuous improvement, the methodology can be adapted to address the evolving cyber risk landscape and emerging technologies.

Future research should focus on expanding the methodology to other critical energy infrastructure, with expanded data and investigating the impact of emerging technologies, developing advanced monitoring tools, and exploring the role of human factors in cybersecurity. By pursuing these research directions, we can contribute to the overall resilience and security of critical infrastructure sectors, safeguarding them from the ever-growing threat of cyberattacks.

References

Bajramovic, Edita, and Deeksha Gupta. 2017. "Providing Security Assurance in Line with National DBT Assumptions." In , edited by AA Mohamed, FM Idris, AH Husin, and NA Hamid. Vol. 1799. https://doi.org/10.1063/1.4972939.

Borenius, Seppo, Pavithra Gopalakrishnan, Lina Bertling Tjernberg, and Raimo Kantola. 2022. "Expert-Guided Security Risk Assessment of Evolving Power Grids." *ENERGIES* 15 (9). https://doi.org/10.3390/en15093237.

Erdogan, Gencer, Inger Anne Tondel, Shukun Tokas, Michele Garau, and Martin Gilje Jaatun. 2022. "Needs and Challenges Concerning Cyber-Risk Assessment in the Cyber-Physical Smart Grid." In , edited by HG Fill, M VanSinderen, and L Maciaszek, 21–32. https://doi.org/10.5220/0011137100003266.

Gourisetti, Sri Nikhil Gupta, Michael Mylrea, and Hirak Patangia. 2020. "Cybersecurity Vulnerability Mitigation Framework Through Empirical Paradigm (CyFEr): Prioritized Gap Analysis." *IEEE SYSTEMS JOURNAL* 14 (2): 1897–1908. https://doi.org/10.1109/JSYST.2019.2913141.

Lau, Pikkin, Lingfeng Wang, Zhaoxi Liu, Wei Wei, and Chee-Wooi Ten. 2021. "A Coalitional Cyber-Insurance Design Considering Power System Reliability and Cyber Vulnerability." *IEEE TRANSACTIONS ON POWER SYSTEMS* 36 (6): 5512–24. https://doi.org/10.1109/TPWRS.2021.3078730.

Lehu, Jean-Marc. 2018. "Cyberattaque : la gestion du risque est-elle encore possible ?Analyse et enseignements du cas Sony Pictures." *La Revue des Sciences de Gestion* 291–292 (3–4): 41–50. https://doi.org/10.3917/rsg.291.0041.

Liatifis, Athanasios, Pedro Ruzafa Alcazar, Panagiotis Radoglou Grammatikis, Dimitris Papamartzivanos, Sofianna Menesidou, Thomas Krousarlis, Molinuevo Martin Alberto, et al. 2022. "Dynamic Risk Assessment and Certification in the Power Grid: A Collaborative Approach." In , edited by A Clemm, G Maier, CM Machuca, KK Ramakrishnan, F Risso, P Chemouil, and N Limam, 462–67. https://doi.org/10.1109/NetSoft54395.2022.9844034.

Papastergiou, Spyridon, Haralambos Mouratidis, and Eleni-Maria Kalogeraki. 2021. "Handling of Advanced Persistent Threats and Complex Incidents in Healthcare, Transportation and Energy ICT Infrastructures." *EVOLVING SYSTEMS* 12 (1): 91–108. https://doi.org/10.1007/s12530-020-09335-4.

Peterson, John, Michael Haney, and R. A. Borrelli. 2019. "An Overview of Methodologies for Cybersecurity Vulnerability Assessments Conducted in Nuclear Power Plants." *NUCLEAR ENGINEERING AND DESIGN* 346 (May): 75–84.

https://doi.org/10.1016/j.nucengdes.2019.02.025.

Seda-Sanabria, Yazmin, James D Morgeson, and Jason A Dechant. 2023. “An Integrated Approach for Physical and Cyber Security Risk Assessment:”

Wang, Shuang, Lei Ding, He Sui, and Zhaojun Gu. 2021. “Cybersecurity Risk Assessment Method of ICS Based on Attack-Defense Tree Model.” *JOURNAL OF INTELLIGENT & FUZZY SYSTEMS* 40 (6): 10475–88. https://doi.org/10.3233/JIFS-201126.

Zografopoulos, Ioannis, Juan Ospina, Xiaorui Liu, and Charalambos Konstantinou. 2021. “Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies.” *IEEE ACCESS* 9: 29775–818. https://doi.org/10.1109/ACCESS.2021.3058403.