A MODEL FOR DYNAMIC CYBER SECURITY RISK ASSESSMENT IN THE INDUSTRIAL IOT ENVIRONMENT

Mirjana D. Stojanović[1]*,
Jasna D. Marković-Petrović[2]

[1]University of Belgrade,
Faculty of Transport and
Traffic Engineering,
Belgrade, Serbia

[2]Public Enterprise Electric Power
Industry of Serbia,
Belgrade, Serbia

Abstract:

This paper considers cyber security risk assessment, as a vital part of the risk management process, in the industrial Internet of Things (IIoT) systems. A general model for IIoT dynamic risk assessment (DRA) is proposed, starting from the definition of IIoT context. Several risk calculation algorithms are surveyed, with an emphasis on artificial intelligence and machine learning-based methods. The model is illustrated in the example of IIoT-based supervisory control and data acquisition (SCADA) system in a hydropower plant.

Keywords:

Cyber Security, Dynamic Risk Assessment, Industrial Internet of Things, Machine Learning, SCADA.

INTRODUCTION

The Internet of Things (IoT) concept promotes the idea of everyday physical objects (things) being connected to the Internet and being able to identify themselves to other devices. As a subset of IoT, the Industrial IoT (IIoT) refers to machine-to-machine and industrial communication technologies with automation applications, in order to enable more efficient and sustainable production [1]. Since many IIoT systems belong to critical infrastructure, cyber security is one of the key issues that have to be solved to achieve their wide implementation and deployment. Security solutions require equal emphasis upon the system's view, specific mechanisms and their applications, development of the appropriate test-beds, and standardization efforts in the field [2]. Apart from evolving threats, the complexity of the problem increases due to the heterogeneity of physical objects, networking technologies and applications that should be able to communicate and collaboratively provide immutable and verifiable data. The main security risk factors include: real-time and complex interactions; security flaws in certain parts of the system; poor integration of security subsystems; insecure network connections and communication protocols; shared technology issues; multiple points of

Correspondence:
Mirjana D. Stojanović

e-mail:
m.stojanovic@sf.bg.ac.rs

DOI: 10.15308/Sinteza-2022-230-237

entry and failure; the use of open software platforms together with commercial off-the-shelf hardware and software components; and the lack of protection for legacy systems with long operational life [3].

This paper addresses IIoT cyber security risk assessment (as a core part of the risk management process), which includes risk identification, analysis and evaluation [4]. The need for a dynamic risk assessment (DRA) approach is explained, and a general model is proposed together with a brief survey of suitable risk calculation methods. The proposed approach is illustrated in the example of IIoT-based supervisory control and data acquisition (SCADA) system in a hydropower plant.

The rest of the paper is organized as follows. Section 2 briefly surveys the background and related works. Section 3 proposes the general concept for DRA risk assessment in the IIoT environment and surveys the algorithms for risk assessment with the emphasis on machine learning-based methods. Section 4 illustrates the proposed approach on a hybrid cloud-based SCADA system. Finally, Section 5 concludes the paper.

2. BACKGROUND AND RELATED WORKS

In the context of industrial control systems (ICSs) security, the U.S. National Institute of Standards and Technology (NIST) defines risk assessment as "the process of identifying risks to operations, assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact" [5]. Figure 2 illustrates the process of ICS cyber security risk assessment.

For general-purpose networks, the objective is to maintain balanced protection of confidentiality, integrity and availability (CIA triad), with data confidentiality as the main concern. Protection of industrial control networks assumes the AIC triad, which means that the availability is given the highest priority. The reversed order of priorities makes difference in terms of security policies and mechanisms, with the main goal to preserve the availability of critical infrastructure systems on a 24/7 basis. Cyber security threats exploit system vulnerabilities and possibly cause incidents, which may further cause damage to assets and have an impact on security infrastructure. Therefore, threats, vulnerabilities, and impacts should be combined together to provide a qualitative or quantitative measure of the risk [6]. Examples of qualitative risk assessment are experts' assessment, rating estimates, checklists of risk sources, method of analogies, etc. According to [7], quantitative risk assessment methods can be classified as follows: (1) analytical methods such as sensitivity analysis, scenario analysis, method of the risk-adjusted discount rate; (2) probabilistic theoretical methods, which include simulation, game theory, tree constructing methods and (3) unconventional methods such as modelling with fuzzy logic and machine learning.

DRA (also known as continuous risk assessment) relies on data that are collected and processed in real time, and encompasses the three basic components: assets management, attack modelling and risk calculation [8]. Assets management refers to material goods (devices, communication links, hardware and software), their performances (including upgrading and updating) and their valuation in terms of impact to AIC triad, criticality,

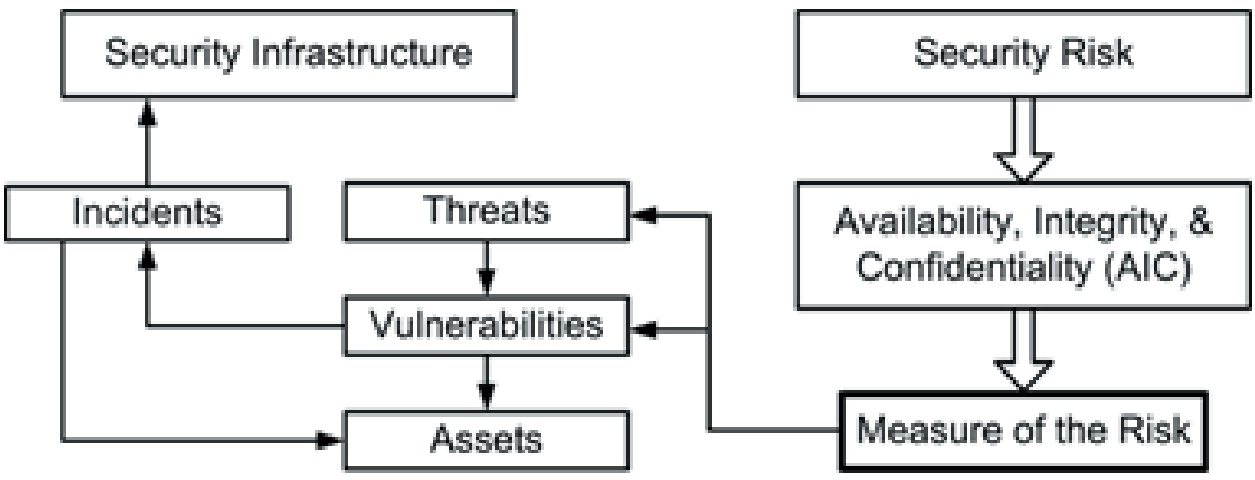

Figure 1 - Security risk assessment process in industrial control systems.

sensitivity and security expenses. Attacks can be modelled by means of different techniques such as: hidden Markov models, graph-based techniques, hierarchical modelling using attack trees, clustering, fuzzy logic, etc. Risk calculation takes into account likelihood (frequency) and the impact of all possible attacks, while the algorithm may depend on attack modelling method.

Measure of the risk can be updated continuously or periodically, and expressed quantitatively or qualitatively. The Industrial Internet Consortium (IIC) implies the need for DRA by considering risk assessment in the context of overall security measures and emphasizing the need to adapt to continually changing threats and attacks, to provide responses that will minimize the impact on the IIoT system, and to enable cooperation of different organizations to ensure the early identification of security threats [9].

Recent trends in DRA techniques have been surveyed in [8] together with a proposal of decision guide to choosing the most suitable technique considering general-purpose networks, IoT environments and ICSs. A general description of a solution that has the potential towards IIoT continuous risk assessment is presented in [10]. The solution makes use of different data sources to analyse cyber risks on a continuous basis, integrating this activity with the operational process. The method is illustrated in the example of environmental control in a data centre. A quantitative DRA approach intended for smart grids is proposed in [11], and relies on attack defence trees and computation of the predefined risk attributes that are being propagated through the tree nodes.

An architectural view of continuous security risk assessment in IIoT is presented in [12], followed by a survey of machine learning-based solutions used for risk calculation. Applicability of deep learning approaches for DRA in IIoT systems is discussed in [13].

3. PROPOSAL OF A MODEL FOR DRA IN IIOT SYSTEMS

The main novelty of this paper is the proposal of a general model for DRA in the heterogeneous IIoT systems. The model relies on identification of the IIoT context for risk assessment, and is completely applicable to different attack models and risk calculation algorithms.

3.1. EXPLANATION OF THE MODEL

Figure 2 shows the proposed model of dynamic cyber security risk assessment in the IIoT environment. It comprises the following steps:

- *Definition of the IIoT context*, depending on risk aspect and involved entities [14]. Risk aspects may differ for sensor/actuator manufacturers; platforms, applications and industrial systems; customers (industry, healthcare, smart cities), or for system integrators, service providers and end users. Examples of entities are humans, hardware, software, communication and cloud infrastructure, and they determine the information flow. Identification of IIoT context is required for two main reasons:
  - Multiplication of cyber-physical attack points is possible in the IIoT system due to the integration of sensors, actuators, platforms, applications and users. This means that the attack performed in a single point may have impact on the whole system; and
  - The same entity can be used in different IIoT contexts, which require different security levels, depending on specific risk factors.
- *Identification of attack points* refers to the recognition of assets that can be targeted by cyber or cyber-physical attacks;
- *Attack modelling* refers to the creation of cyber attack models in order to identify and simulate attacks against security environments, using likely adversary techniques and attack paths. This block is not mandatory, since the risk engine (depending on the applied algorithm) can rely only on monitoring results obtained from security mechanisms;
- *Risk calculation engine* implements a suitable algorithm, taking into account a number of static and dynamic inputs. Static parameters are stored in the knowledge repository; they encompass records such as asset register, asset values, history of incidents, as well as previous risk measures and the risk mitigation plan [12]. Dynamic parameters are obtained from attack modelling (if present) and monitoring tools. The output of risk calculation engine is a qualitative or quantitative risk measure;

- *Risk mitigation plan* specifies techniques and methods to be used to avoid, reduce, and control the probability of risk occurrence, for different risk levels. It also includes selection of security tools such as logs monitoring, antivirus software, firewalls, intrusion detection and prevention systems, malware detection, network traffic monitoring and analysis; and
- *Continuous monitoring of attacks and security mechanisms* provides loopbacks for modification of attack points, revision of attack models and tuning of the risk calculation engine. Security tools capture and process inputs from the IIoT system in a real time and generate notifications about potential threats and suspicious events. The security information and event management (SIEM) software imports information from security tools, performs correlation of the corresponding events and prepares appropriate dynamic inputs for the risk assessment tool.

3.2. RISK CALCULATION ALGORITHMS

Several traditional algorithms that can be used for continuous risk calculation in industrial environments are described in [15], including Bayesian methods, bow-tie analysis and risk barometer. Recent trends show that artificial intelligence (AI) and machine learning (ML) bring substantial benefits for DRA implementation in the IIoT environment due to their suitability for edge computing, big data processing, predictive risk management and efficient decision-making [12], [13], [16].

There are several mainstream machine learning-based approaches, namely supervised and unsupervised learning, deep learning, reinforcement learning and deep reinforcement learning [17]. Table 1 contains a brief summary of these approaches, regarding their suitability for edge computing.

Supervised and unsupervised learning are widely used for data classification and clustering. Supervised learning assumes prior knowledge of the output values for given data samples. The goal is to learn a function that maps an input to an output based on example input-output pairs. Support vector machines (SVMs), decision tree and naive Bayes are typical algorithms that are commonly used for discrete valued classification. Unsupervised learning does not have labelled outputs; its task is to infer a function that describes the structure of unlabeled data. One of the most widely used algorithms is K-means, which splits data whose category is unknown into several disjoint clusters. Certainly, different types of artificial neural networks (ANNs) can be supervised and unsupervised.

Deep learning is a class of ML techniques that is inspired by the structure of a human brain. The algorithms attempt to draw similar conclusions as humans would by using a multi-layered structure of neural networks (e.g., convolutional neural networks, CNNs). The computational model can automatically extract features needed for prediction or classification from massive raw data. Deep learning can be easily integrated into edge computing-based systems and used for traffic and behaviour prediction, as well as for fault and incidents detection.

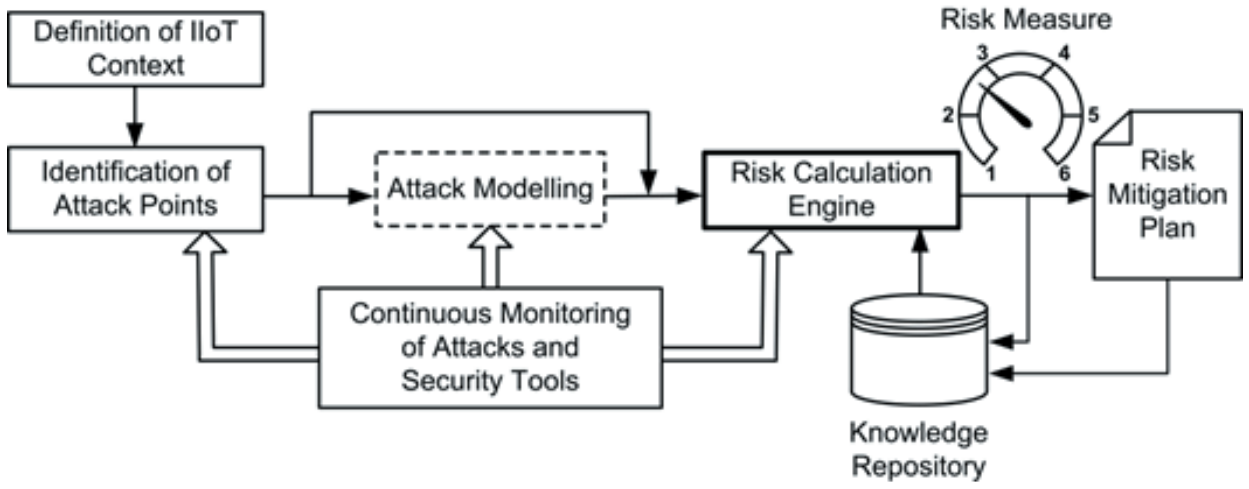

Figure 2 – Proposed model of dynamic cyber security risk assessment in the IIoT system.

Method	Algorithms	Application	Advantages	Limitations
Supervised learning Unsupervised learning	ANN, SVM ANN, K-means	Classification and clustering	Easy and quick to deploy	Sensitive to data, massive data, performance bounds
Deep learning	CNN	Prediction, detection	End-to-end learning features	Long training time, massive data, training tricks, black-box
Reinforcement learning	Markov decision, Q-learning	Decision making	Learning without a priori knowledge	Curse of dimensionality
Deep reinforcement learning	Deep Q-network	Feature extraction and decision making	End-to-end reinforcement learning	Very long training time in large discrete state space

Table 1 - Methods, algorithms and application of machine learning in edge computing

Reinforcement learning, inspired by behavioural psychology, enables an agent to learn in an interactive environment by trial and error using feedback from its own actions and experiences. It assumes rewards and punishments as indicators of positive and negative behaviour. Reinforcement learning is suitable for automatic control and decision making issues in highly dynamic environments. Typical representatives are Markov decision process and Q-learning algorithms.

Deep reinforcement learning (e.g., deep Q-network) combines ANNs with reinforcement learning that are goal-oriented algorithms. In other words, it brings together function approximation and target optimization by mapping state-action pairs to expected rewards. This feature makes deep reinforcement learning suitable for both feature extraction and decision making.

4. CASE STUDY

The case study considers an IIoT SCADA system in the hydropower plant, based on a hybrid cloud infrastructure, as illustrated in Figure 3. Such architecture can easily be extended to support other smart grid applications. Hybrid cloud allows companies to combine their own data centre and/or private cloud setup with public cloud resources such as Software-as-a-Service (SaaS), Data-as-a-Service (DaaS), etc. One of the most common applications of hybrid cloud is to keep sensitive, mission-critical data and applications in the private cloud, and to use public cloud when capacity is needed for less sensitive development or testing activities [18]. The basic idea is to take advantage of cost benefits of public cloud services, while preserving high level of security for critical applications that are executed in the private cloud [19], [20].

In the SCADA system, controllers process signals from field devices and generate appropriate commands for these devices. They encompass remote terminal units (RTUs), programmable logic controllers (PLCs) and intelligent electronic devices (IEDs) that perform local control of actuators and sensor monitoring. Controller network is connected via secure communication links to SCADA application (master terminal unit, MTU) that is executed in the private cloud [18]. SCADA application makes use of the private Platform-as-a-Service (PaaS) model to perform the following functions: (1) Preparing and sending command and control messages to controllers; (2) Collecting and analysing real-time process and historical data obtained from field sites, and generating actions based on detected events; (3) Preparing inputs for hydroinformatics system; (4) Preparing data to be presented on the HMI (human-machine interface) consoles; and (5) Preparing and sending relevant data to be stored on a historian server. Private PaaS allows support of different software platforms that can be tailored to other critical applications in the power utility.

Public SaaS is used for provisioning of publicly available information about the water level of the inflow. Public DaaS can optionally be used for storage of less sensitive data. Hydroinformatics system determines operation of aggregates for optimal consumption of hydropower potential based on the water level, the data obtained from SCADA system and the energy production requirement.

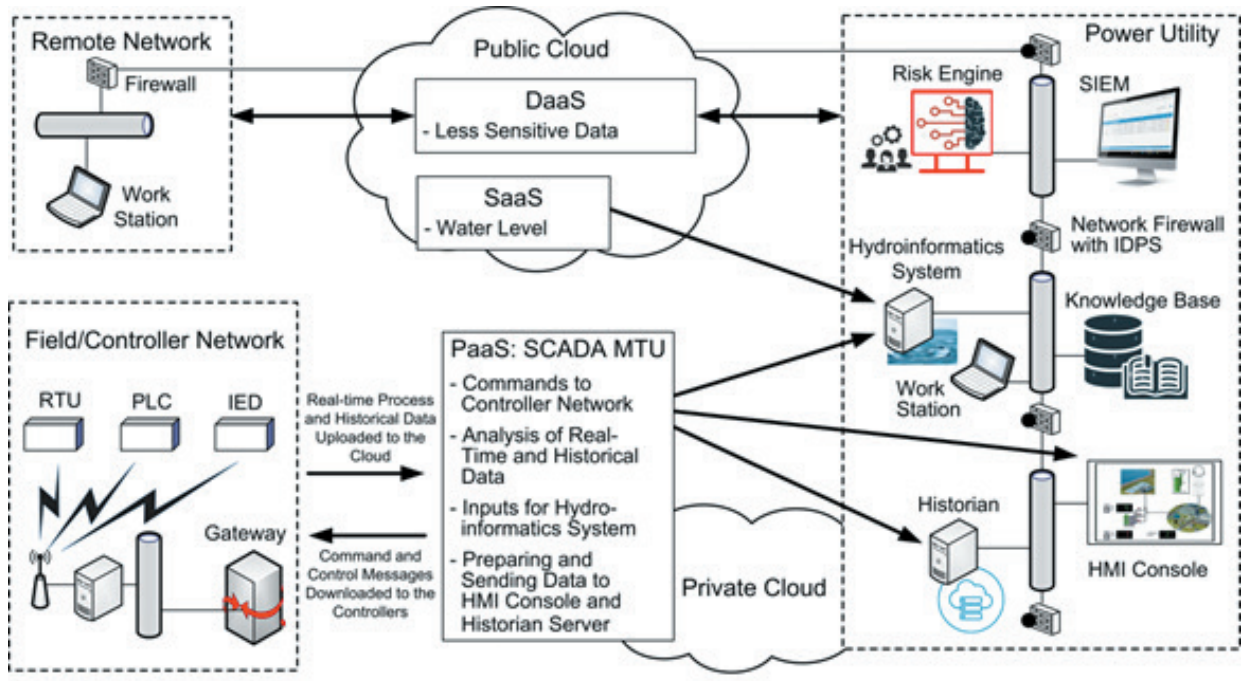

Figure 3 - Architecture of the secured IIoT SCADA system using a hybrid cloud infrastructure.

Based on the previous description, the following IIoT contexts can be identified:

- Real-time communication between the SCADA MTU and field sites;
- Communication between the SCADA MTU and the hydroinformatics systems;
- The use of public cloud services; and
- Communication with the historian server and HMI application.

SCADA control centre performs its actions based on the data received from field sites. Attacks that jeopardize process control focus on modifying control data or blocking the data transfer. Primary threats to SCADA systems are command/response injection, various forms of denial of service (DoS) attacks, including distributed DoS (DDoS), and man-in-the-middle (MITM) attack. Detailed considerations about cyber threats and attacks on SCADA systems can be found in the literature [2], [18], [21].

Achieving high level of security and privacy assumes implementation of complex security measures [2]. Securing the private cloud is complete responsibility of the power company, and it starts from the definition of security objectives and associated policies, followed by implementation of mechanisms that ensure the AIC triad; authentication and access control; intrusion detection and prevention, as well as a set of other preventive measures. Regarding public cloud services, the most important step is the careful choice of cloud service provider with a well defined service level agreement for each service [2].

Following initial risk assessment (in the system design phase), four inline network-based intrusion detection and prevention systems (IDPSs) are installed together with firewalls at network's vulnerability points to cyber attacks, as indicated in Figure 3. IDPSs monitor the traffic in specific network segments and observe the activities of network and application layer protocols to identify and stop suspicious activities and events. They also typically record information about these activities, notify the administrator about important events with warnings and alarms, and generate reports. SIEM software collects and aggregates security-related logs, generated throughout the private cloud infrastructure, performs correlation of the corresponding events, and prepares dynamic inputs to the risk engine.

As mentioned earlier, different algorithms can be applied to perform dynamic risk calculation. However, hybrid approach which takes into account experts' assessment is strongly recommended. The role of experts' opinion is fundamental in the initial phase (system design) as well as for tuning the risk engine and interpretation of the obtained results.

This particularly stands for ML-based algorithms in order to mitigate their shortcomings, primary regarding high error susceptibility and possibly wrong interpretation of results.

Interpretation of results poses questions how to consider risk knowledge, particularly in quantitative risk assessment (e.g., considering two-dimensional or three-dimensional risk matrices), and how these results contribute to system evolution? Calibration and correction based on new evidence would possibly allow risk analysis to consider evolving conditions and improve system knowledge [16].

5. CONCLUSION

Although different qualitative and quantitative approaches, methods and tools for risk assessment in industrial control systems can be found in the literature, only a few of them deal with the models for dynamic cyber security risk assessment in the IIoT environment. The model proposed in this paper starts from identification of the IIoT context, assuming that one entity can be used in different contexts with different security requirements. The model is general enough to allow different attack models and risk calculation algorithms.

Machine learning-based approaches offer a strong potential for DRA, particularly if combined with the experts' opinion. Continuous monitoring of attacks and security tools, followed by a correlation analysis of the observed data, provides feedback for the risk calculation engine. The proposed approach is illustrated in the example of IIoT-based SCADA system that uses a hybrid cloud infrastructure. Finally, our future work is twofold. First, we are planning to develop DRA architectural views for other IIoT applications, particularly smart grids. Second, we are investigating hybrid risk calculation approaches that combine experts' assessment with deep learning based methods.

6. ACKNOWLEDGEMENTS

This work was partially funded by the Ministry of Education, Science and Technological Development of Serbia.

7. REFERENCES

[1] E. Sissini, A. Saifullah, S. Han, U. Jennehag and M. Gidlund, "Industrial Internet of Things: Challenges, Opportunities, and Directions," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, p. 4724–4734, 2018.

[2] M. D. Stojanović and S. V. Boštjančič Rakas, Eds., Cyber Security of Industrial Control Systems in the Future Internet Environment, Hershey, PA: IGI Global, 2020.

[3] S. Nazir, S. Patel and D. Patel, "Assessing and Augmenting SCADA Cyber Security: A Survey of Techniques," *Computers & Security,* vol. 170, p. 436–454, 2017.

[4] International Organization for Standardization (ISO), *Risk Management – Guidelines, Standard ISO 31000:2018*, 2018.

[5] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams and A. Hahn, "*Guide to Industrial Control Systems (ICS) Security", NIST Special Publication 800-82 Rev. 2*, Gaithersburg, MD: U.S. National Institute of Standards and Technology, 2015.

[6] T. Tsiakis, "Information Security Expenditures: A Techno-Economic Analysis," *International Journal of Computer Science and Network Security,* vol. 10, no. 4, p. 7–11, 2010.

[7] M. Kalinin, V. Krundyshev and P. Zegzhda, "*Cybersecurity Risk Assessment in Smart City Infrastructures," Machines*, vol. 9, no. 4, 2021.

[8] O. Mirzaei, J. Maria de Fuentes and L. G. Manzano, "Dynamic Risk Assessment in IT Environments: A Decision Guide," in *Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution*, Z. Fields, Ed., Hershey, PA, IGI Global, 2018, p. 234–263.

[9] Industrial Internet Consortium (IIC), *Industrial Internet of Things Volume G4: Security Framework, IIC:PUB:G4:V1.0:PB:20160919*, 2016.

[10] C. Adaros Boye, P. Kearney and M. Josephs, "Cyber-Risks in the Industrial Internet of Things (IIoT): Towards a Method for Continuous Assessment," in *Information Security, ISC 2018. Lecture Notes in Computer Science*, vol. 11060, L. Chen, M. Manulis and S. Schneider, Eds., Cham, Springer, 2018, pp. 502-519.

[11] E. Rios, A. Rego, E. Iturbe, M. Higuero and X. Larrucea, "Continuous Quantitative Risk Management in Smart Grids Using Attack Defense Trees," *Sensors,* vol. 20, no. 16, 2020.

[12] M. Stojanović and J. Marković-Petrović, "Application of Machine Learning for Cyber Security Risk Assessment in Industrial IoT Systems: A Review," in *Proceedings of the 7th Virtual International Conference on Science, Technology and Management in Energy – eNergetics 2021*, Niš, Serbia, 2021.

[13] M. Stojanović and J. Marković-Petrović, "Deep Learning for Cyber Security Risk Assessment in IIoT Systems," in *Encyclopedia of Data Science and Machine Learning*, J. Wang, Ed., Hershey, PA, IGI Global, 2022.

[14] E. T. Nakamura and S. L. Ribeiro, "A Privacy, Security, Safety, Resilience and Reliability Focused Risk Assessment Methodology for IIoT Systems," in *Proceedings of the 2018 Global Internet of Things Summit (GIoTS)*, Bilbao, Spain, 2018.

[15] V. Villa, N. Paltrineri and V. Cozzani, "Overview on Dynamic Approaches to Risk Management in Process Facilities," *Chemical Engineering Transactions*, vol. 43, p. 2497–2502, 2015.

[16] N. Paltrinieri, L. Comfort and G. Reniers, "Learning about Risk: Machine Learning for Risk Assessment," *Safety Science*, vol. 118, p. 475–486, 2019.

[17] B. Cao, L. Zhang, Y. Li, D. Feng and W. Cao, "Intelligent Offloading in Multi-Access Edge Computing: A State-of-the-Art Review and Framework," *IEEE Communications Magazine*, vol. 57, no. 3, p. 56–62, 2019.

[18] M. Stojanović, S. Boštjančič Rakas and J. Marković-Petrović, "SCADA Systems in the Cloud and Fog Environments: Migration Scenarios and Security Issues," *FACTA UNIVERSITATIS Series: Electronics and Energetics*, vol. 32, no. 3, p. 345–358, 2019.

[19] G. Aryotejo, D. Y. Kristiyanto and M. Mufadhol, "Hybrid Cloud: Bridging of Private and Public Cloud Computing," *Journal of Physics: Conference Series*, vol. 1025, 2018.

[20] I. Lee, "An Optimization Approach to Capacity Evaluation and Investment Decision of Hybrid Cloud: A Corporate Customer's Perspective," *Journal of Cloud Computing: Advances, Systems and Applications*, vol. 8, no. 15, p. 1–13, 2019.

[21] A. Sajid, H. Abbas and K. Saleem, "Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges," *IEEE Access*, vol. 4, p. 1375–1384, 2016.