

Regular Article

A New Framework for Cyber Risk Assessment for Industry 4.0 and Recommendations for Vietnam

Correspondence: ...

Communication: received July 2022

Online publication: ..., Digital Object Identifier: ...

The associate editor coordinating the review of this article and recommending it for publication was

Abstract– Industry 4.0 encompasses smart manufacturing and Internet of Things, which has brought huge benefits to a wide range of industries. This development, however, has raised more cyber security risks for both Information Technology (IT) and Operational Technology (OT) systems. In this paper, potential cyber vulnerabilities and threats in manufacturing in Industry 4.0 are briefly reviewed based on the architecture and operating principle of the manufacturing system in Industry 4.0. Criteria for cyber risk assessment for both IT and OT are reviewed via different standards. We then provide recommendations for cyber risk assessment and discuss a new framework for IT/OT risk assessment in Vietnam.

Keywords– Internet of things (IoT), cyber security, Industry 4.0, industrial control system, operational technology system, manufacturing.

1 INTRODUCTION

Industry 4.0 has made advancements to manufacturing in optimizing supply chains and assets, analyzing and predicting maintenance problems by applying new technologies such as Internet-of-Things (IoT) and cloud computing [1]. Such development, however, faces an increase in cyber attacks (CBAs) since manufacturing systems are exposed to the Internet; also, new types of CBAs appear. It was estimated that CBAs cost the global economy up to 400 billion USD a year [2]. For smart manufacturing, CBAs are even more severe since it would lead to system failure. Therefore, organizations should pay more attention to cyber risk management to mitigate the consequence of CBAs.

Cyber risks assessment (RAS) has an important role in cyber risk management, which helps a security system to make accurate decision on risk treatment. Outcomes of an RAS process are determined based on vulnerabilities, threats, and assets. According to ISO/IEC 27005:2008 [3], a vulnerability is a weakness or hole of a security program that threats can exploit to gain illegitimate access to the assets of an organization. A threat is identified as what impact each vulnerability will have on the assets. Threats may arise from objective or subjective reasons and be intentional

or unintentional attacks. Risks refer to potential consequences when threats can cause damage to the assets of an organization.

Typically, a manufacturer consists of information technology (IT) and operational technology (OT) systems. The former consists of computers and telecommunication for storing, recovering, transmitting, manipulating, protecting data or information, and exchanging data among different organizations. The latter is defined as a system of software and hardware to manage/monitor physical devices, machines, as well as processes and product segments in the operation of an enterprise [4].

Numerous international standards and frameworks have been developed for RAS. For examples, NIST SP 800-30 and ISO/IEC 27001:2005 for IT are published by the National Institute of Standards and Technology (NIST) and the International Standards Organization (ISO), respectively. For OT, ISA/IEC 62443 series is jointly published by the International Society for Automation (ISA) and the International Electrotechnical Commission (IEC). It presents a process-based approach for deploying, implementing, operating, and maintaining security.

Previous studies propose practical approaches and models for RAS of IT [5], [6], of OT [7], [8], and of IoT [9]. However, they looked at RAS for IT, OT, and IoT separately and did not consider new vulnerabilities, threats, and assets (VTA) in Industry 4.0.

Further, existing RAS frameworks have been created

in each organizational perimeter [10]. They mainly deal with information security [11] and are based on antivirus software, firewall, intrusion detection, and malware protection tools to detect vulnerabilities and corresponding threats at the entry of the perimeter. However, the boundaries between the physical world and the cyber world, and among companies are blurred when IoT is applied in Industry 4.0. Data and intellectual property is now shared on the Internet across partner companies. Also, IT and OT networks can be accessed from many points via smart sensors, IoT devices, and clouds. Hence, the existing RAS frameworks may not be sufficient and need to be upgraded.

The contributions of this paper are the follows:

- We provide a brief review of methodologies and existing standards used for cyber RAS, primarily focusing on OT and recommendations for improving Cyber RAS for IT and OT systems in Industry 4.0 in Vietnam.
- We propose a possible framework for IIoT risk assessment in Vietnam. The proposed framework considers IT, OT, and IIoT system. We build an experiment that simulates an IIoT network and compare with several existing frameworks. The results show that our method gives the same severity level as OWASP.

2 ARCHITECTURE, OPERATING PRINCIPLE, VULNERABILITIES AND THREATS OF MANUFACTURING IN INDUSTRY 4.0

This section will discuss the architecture and operating principles of manufacturing. It is the basis for determining vulnerabilities and threats in Industry 4.0.

2.1 Architecture and Operating Principle

A manufacturing system in Industry 4.0 combines a cyber-physical system (CPS) with IoT technology. A cybersystem represents entities and functions related to IT, while physical systems include production processes and applications. CPS combines IoT technology in production processes and other services [12].

The architecture of a CPS in Industry 4.0 is illustrated in Figure 1 [13]. In the architecture, sensor networks connect directly to the Internet. The interconnection of sensors and actuators, and computing provide the ability to collect raw data from a real-world environment via sensors and exchange the data across platforms for analysis and processing. Monitoring, planning, and controlling can be performed via the Internet. A large amount of collected data from sensor networks can be used to predict issues of maintenance and improve productivity and risk management by giving back control data to the physical world [14]. That process will provide a self-optimizing capability of the system.

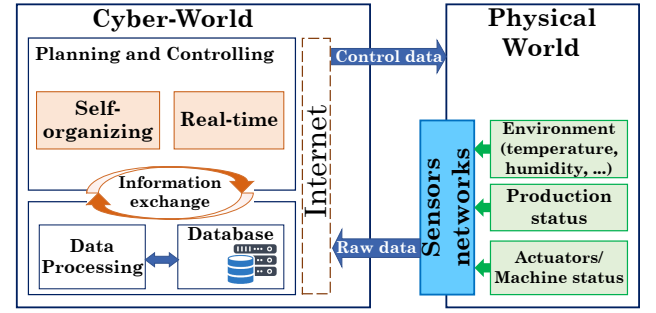


Figure 1: Cyber-Physical Systems leveled architecture.

The operation principle of a manufacturing system in Industry 4.0 is illustrated in the workflow in Figure 2 [15]. The figure illustrates the whole process of production with supportive technologies such as robotics, cloud computing, data analytics, IoT, and smart sensors. Communication technologies for exchanging data from sensors to clouds, such as OPC-UA [17], wireless sensor networks, and Web services, maintain the communication between humans and machines. The production process is operated by IT and OT systems. From designing to the production stage, data are stored and exchanged via the Internet for processing by cloud computing.

2.2 Vulnerabilities and Threats of IT Systems

The advancements of the Internet and the IoT Internet have made an impact on IT systems in Industry 4.0 in terms of cyber threats.

Some main types of threats are grouped in Table I. Firstly, when most of the devices can connect to the Internet, IT systems have to face cyber attacks more frequently. However, operating systems and software used to operate hardware may no longer be supported because factories rarely stop operations to upgrade IT systems. Hence, the system cannot be maintained and supported and could be exploited by old variants of network malware. Secondly, autorun.inf related cyber risks have been detected significantly in manufacturing as compared to in other industries. The common practice of using USB drives to copy and transfer information between computers and networks could be an ideal way of malware propagation, e.g., Stunex. Thirdly, companies and technical teams now tend to use clouds to share their work. Hackers can perform targeted campaigns that aim to steal intellectual prop-

Table I: Common threats in IT systems

Vulnerabilities	IT Threats
Long replacement cycle in operating system	Old variant malware
Software is no longer be supported	Pervasiveness of network worms
Using USB drives to copy and transfer information	Auto-run
The importance of industry	Targeted campaigns

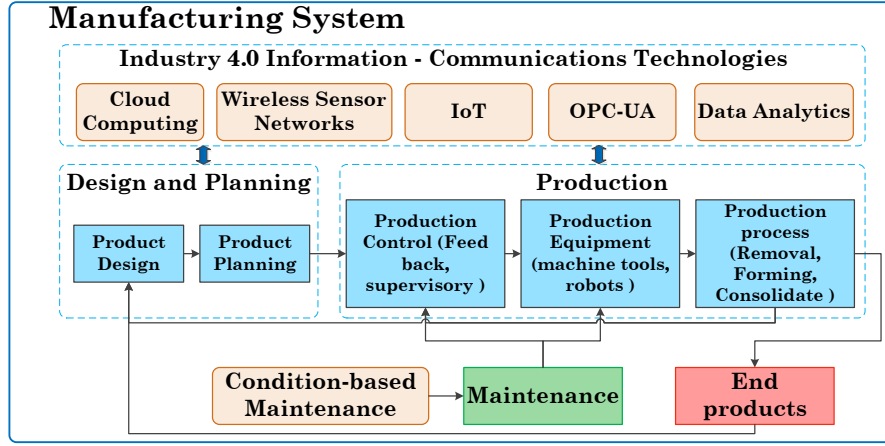


Figure 2: Manufacturing workflow in Industry 4.0 [16].

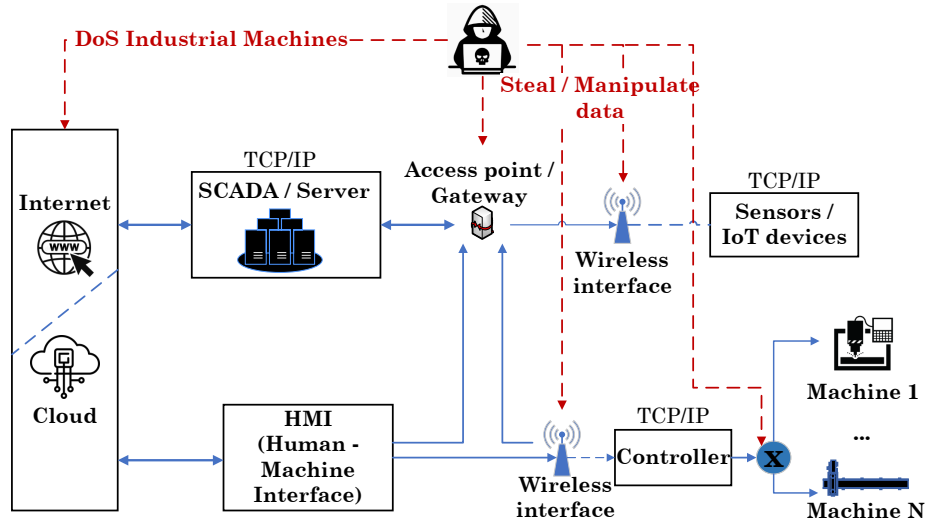


Figure 3: Example of threats in OT system.

erty or critical information. Potential threats come from insecure clouds [18].

2.3 Vulnerabilities and Threats of OT Systems

The main vulnerabilities and threats of OT systems are presented in Table II. Human-machine interfaces (HMIs) allow operators and engineers to monitor and control the equipment while programmable logic controllers are used to program logic into several pieces of equipment. However, industrial malware can access HMIs when exchanging data via the Internet or the USB. Figure 3 illustrates an example of the OT system in Industry 4.0 with threats from an attacker. OT devices and industrial control systems (ICS) can connect to the Internet using Web-based protocols [19], increasing the possibility of cyber attacks. Most attacks have exploited insecure communications between hardware and software of OT systems. A hacker can access the

Table II: Common threats in OT systems

Vulnerabilities	OT Threats
Modern Human-Machine Interfaces (HMIs) expose to the Internet	Unauthorized tampering
Manufacturing equipment is not designed with security	Industrial malware
Insecure communications from sub-systems to higher-level systems	Illegitimate reconfigure sub-systems
Data breach from IT systems to ICS devices	Malware targeting ICS

network and perform an interception to steal data and manipulate the system.

2.4 Vulnerabilities and Threats of IIoT Systems

While IIoT and Industry 4.0 are separate concepts, they should not be viewed that way when introduc-

ing greater efficiency and automation in manufacturing [20].

From the reference model of the open systems interconnection (OSI), an IIoT system contains perception/physical, network, service, and application layers [13]. Thereby, cyber threats will be examined from each layer. In the perception layer, unauthorized access is the most concern because hackers can use malicious sensors or unauthorized IIoT devices to gain information exchanging among the entities of the system. Attackers can manipulate the system from the received data, makes it stop working, or damage them. In the network layer, threats include Denial of Services (DoS), routing, man-in-the-middle attacks, and data breaches. In the service layer, attackers mainly use malicious information to manipulate users, which can be seen in spoofing or phishing attacks. They try to get user or system information by pretending to be legitimate businesses or partners. The application layer is the layer closest to users and faces numerous attack interfaces. Attackers can exploit poor security applications through the HMI connecting internet interface. They can perform malicious code injection, illegitimate configuration, and phishing attacks.

From the IIoT perspective, previous works propose different layers for IIoT [21]–[23]. In [23], the authors classified the IIoT network into five layers including business layer, application layer, middleware layer, network layer and perception layer. These layers can cover nearly all purposes and technical architecture of IIoT as well as IIoT networks. In this work, we focus on the following three layers of an IIoT network: perception, edge, and cloud/data, as described in Figure 4.

- **Perception layer:** This layer includes an enormous number of sensors, cameras, controllers, and smart devices. These devices play a crucial role in an

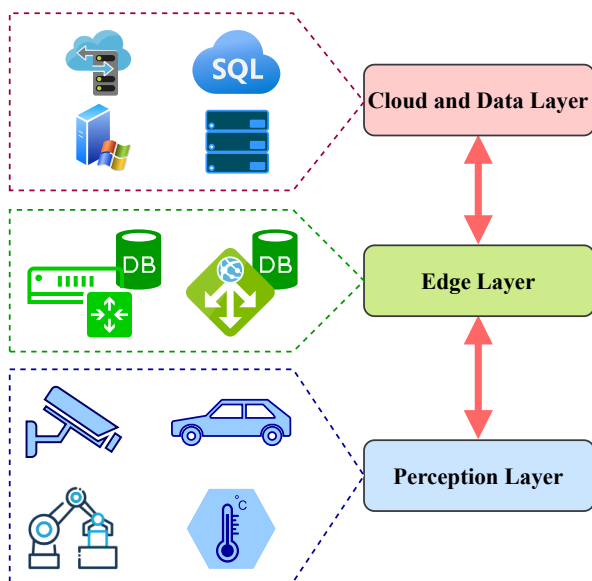


Figure 4: Architecture of the IIoT network.

IIoT system by collecting information from the system and the environment such as temperature, humidity, power, and state, as well as executing the decision from other layers. Through these devices, the other layers can have information about the working system and perform analysis to find out the abnormal behavior of the system and make decisions. The decisions are then sent back to these layers to be implemented.

- **Edge layer:** This layer, as the edge gateway, receives and collects data from the perception layer. It also can perform some slightly additional functions such as edge analysis, storage, data aggregation, or making quick decisions for some authorized tasks.
- **Cloud and data layer:** This layer is the heart of an IIoT system. The functions of this layer are management, processing, and monitoring of a large amount of data collected from the perception layer. In addition, this layer applies novel technologies, e.g., machine learning to learn the historical data and then predict or identify abnormal behaviors in the network. After analysis, the data are also stored in the storage system of this layer.

3 CYBER RISK ASSESSMENT

3.1 RAS Methodologies

An RAS process contains two steps: risks analysis and risks evaluation [24]. The former uses information systems to identify sources and estimate risks. The latter compares the estimated risks with an acceptable risk level to determine the severity of the risks (ISO/IEC 27001:2013). Hence, RAS is a non-trivial task since it involves all kinds of platforms, operating systems, application programs, networks, people, processes, and inter-dependencies. Based on the analysis of the scenario and the target of the organization in assessing risks, cyber risks can be evaluated in the main approaches as seen in Table III. Among them, appraisal is widely used in organizations. It is divided into three categories (quantitative, qualitative, and hybrid) as presented in Table IV.

3.2 RAS for IT

There is a wide range of laws and regulations worldwide to manage and assess cyber risks, including NIST

Table III: Risks evaluation approaches

Appraisalment	Perspective	Resource Valuation	Risk Measurement
Quantitative	Asset-driven	Vertical View	Non-Propagated
Qualitative	Service-driven	Horizontal View	Propagated
Hybrid	Business-driven		

Table IV: Appraisalment: quantitative, qualitative, and hybrid

Methods	Advantages	Disadvantages
Quantitative: (monetary value or percentages) - Inputs and outputs can be monetary and non-monetary	- The levels of estimated risks can be identified in monetary terms - The levels of estimated risks can be illustrated in numerical results	- Difficult to estimate probabilities of threats - Expensive and time-consuming since the calculation of risks level will take much of time to monitoring and recording the events
Qualitative: (non-numerical methods) - Inputs and outputs are linguistic and range or rank variables respectively	- Threat likelihood information may not be required - Can perform quickly - Cost effective - Risk assessment can be performed by operators that not are experts on security or computers	- Monetary and probabilities are not achieved - Lack of sufficient measurable detail - Highly depend on the knowledge of operators and may not accurate
Hybrid (NIST SP 800-30r1): Using both quantitative and qualitative	Flexibility	

Table V: NIST and ISO Comparison

NIST	ISO 27001
First intent built to help the United States of American organizations manage risks	Internationally recognized approach for ISMS
Three key components: core, implementation tiers, and profiles with categories	Not focus on details of technical methods, concentrate on ISMS and provide recommendations
Control catalogs, 5 functions, 21 categories, and 78 subcategories	Annex A has 14 Control Domains, with 114 total controls
Voluntary, self-certification mechanism, and not certifiable	Relies on independent audit and certification bodies

and ISO/IEC 27001. NIST Cyber Security Framework (CSF) and NIST Risk Management Framework (RMF) were created to acknowledge and standardize specific controls and processes. ISO/IEC 27001 is widely used for managing information security. It outlines a method for performing an information security management system (ISMS) of an organization and then certifies the method. It also introduces general security techniques that help governments and organizations solve problems of information security. Both ISO and NIST standards are created for ISMS and RAS from different aspects and involve different scopes, as demonstrated in Table V [25], where ISO/IEC 27001:2005 and NIST SP 800-30r1 are the two frameworks that provide guidance for RAS.

3.3 RAS for OT

The difference between RAS for OT systems compared to RAS for IT systems can be seen in information assets, in which RAS is evaluated in terms of confidentiality (C), integrity (I), and availability (A) measures. Though criteria of information security in OT and IT systems include confidentiality, integrity and availability altogether, these measures are not given the same priority, as illustrated in Figure 5 [25].

The IT system considers confidentiality the most important in the group of the three measures. In contrast, the OT system complements control and prioritizes control and availability. Their order in IT systems is CIA (confidentiality, integrity and availability) while in OT systems is CAIC (control, availability, integrity and confidentiality), respectively. That difference will significantly affect the cyber security frameworks.

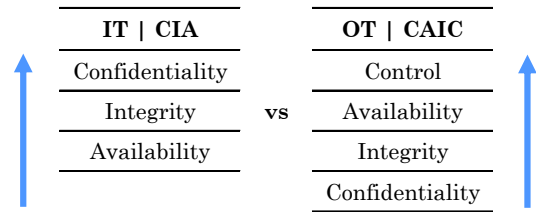


Figure 5: Different priorities of OT and IT in terms of cyber security.

The ISA/IEC 62443 standards, first created by ISA and then developed by IEC, deal with security issues unique to OT systems and specifically for ICS. It consists of four main areas: general basics, operators and service providers, requirements for automation systems, and automation component requirements. ISA/IEC 62443 and ISO 27001 standards have some similarities in contents related to policies such as management commitments and organization responsibilities.

Figure 6 illustrates the frameworks and standards that adapt to the IT and OT environments. The arrow from the left to right presents the decrease in the levels of confidentiality, where the ISA/IEC 62443 standards are considered as “made for OT”, such as standard IEC 62443-3-2 suggests is the guidance of RAS for system design. There are frameworks used for risks managements for OT systems and ICS that are included in NIST, such as NIST Special Publication 800-82 R2.

Standards	ISO 27001	NIST CSF	NIST CSF + Special publications	ISA 62443	ISA 62443 + Technical References
Confidential level	Ultra high	High	Medium	Low	Low
Usage	Rework needed	Need work for OT	Can work for OT	Made for OT	Made for OT

IT OT

Figure 6: Different standards for OT and IT in term of cyber security.

Table VI: Vietnam National Standards for Cybersecurity and corresponding ISO standards

Vietnam National Standards	ISO
TCVN ISO/IEC 27001:2009	ISO/IEC 27001:2005 – IT - ISMS - Requirements
TCVN ISO/IEC	ISO/IEC 27002:2005 – IT - Security techniques - Code of practice for ISMS
TCVN 10295:2014	ISO/IEC 27005:2011 – IT - Security techniques - ISMS
TCVN 8709-1:2011	ISO/IEC 15408-1:2008 – IT - Security Techniques - Part 1
TCVN 8709-2:2011	ISO/IEC 15408-2:2008 – IT - Security Techniques - Part 2
TCVN 8709-3:2011	ISO/IEC 15408-1:2008 – IT - Security Techniques - Part 3
TCVN 11386: 2016	ISO/IEC 18045:2008 – IT - Security techniques - Methodology for IT security evaluation
TCVN 11930:2017	NIST SP 800-53r4 – IT - Basic requirements for security information system according to security levels
TCVN ISO/IEC 27002:2020	ISO/IEC 27002:2013 – IT - Security techniques - Code of practice
TCVN ISO/IEC 27002:2020	ISO/IEC 27002:2013 – IT - Security techniques - Code of practice
TCVN 10295:2014	ISO/IEC 27005:2011 – IT - Security techniques - Information security risk management
TCVN 11239:2015	ISO/IEC 27035:2011 – IT - Security techniques - Information security incident management

4 VIETNAMESE STANDARDS FOR CYBER RAS

Vietnamese agencies and organizations implement information security risk management that is based on the following principles (stated in standard TCVN 10295:2014):

- 1) Risk management must be conducted regularly and continuously in accordance with the regulations, policies, processes, and procedures to ensure the information security of agencies and organizations;
- 2) Risk treatment should be conduct feasibility and guarantee the balance between the cost and the efficiency.
- 3) Decentralize risk, and avoid transferring the risk to reduce the consequences.

Measures for ISMS and RAS are promulgated by the Authority of Information Security (AIS) based on the ISO/IEC 27005:2011 framework, the deployment of the ISO/IEC 27001. Vietnam's National Standards for Cybersecurity (VSC) and their corresponding ISO standards are presented in Table VI. Since VSC is based on ISO/IEC 27001, they are *mainly* applied to IT systems. Regarding RAS, there are several standards for IT systems but none for OT systems. RAS for OT needs to be consulted by the government or experts in that area. The information security for ICS is only mentioned in Circular 03/2017/TT-BTTTT of the Ministry of Information and Communications of Vietnam.

VSC standards for securing OT systems should

be established in a systematical and synchronous way, among organizations, assurances, governance, and technical measures.

5 RECOMMENDATIONS FOR CYBER RAS FOR IT AND OT SYSTEMS IN VIETNAM

In this part, we provide recommendations for RAS for IT and OT systems that are illustrated in Figure 7.

For IT systems, the system assets are evaluated based on the security measures of C, I and A mentioned above, representing the importance and the necessity of the information levels of each organization. For example, the values of C, I, and A are 4, 3, and 2, respectively. The total value of the asset is the sum of those values, which is 9. The organization should follow Decree 85/2016/ND-CP of the government to determine the level of the IT system and the corresponding values of C, I and A. The vulnerabilities of the system can be detected by a scanner or set of questionnaires. The questionnaires are established based on RAS for IT following TCVN 10295:2014 (ISO/IEC 27005:2011).

For OT systems, since the priority levels are CAIC or AIC, the measures of assets need to be re-evaluated as mentioned in Section 3.3. The organization should follow the guidance of RAS for OT, such as ISA/IEC 62443-3-2 or NIST 822-82, to build practical questionnaires or checklists for determining the vulnerabilities. Measuring risks can be conducted by a scoring system such as the Common Vulnerability Scoring System

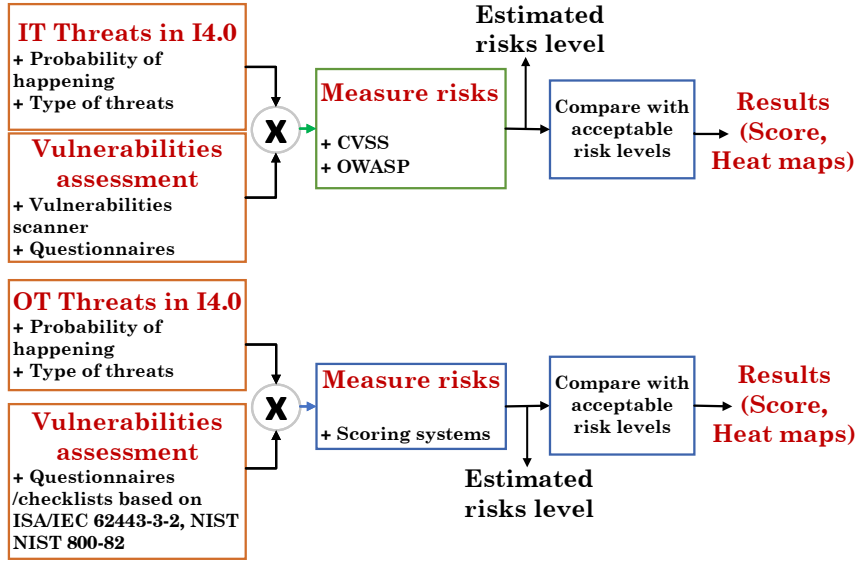


Figure 7: Recommendation of RAS for IT and OT systems.

Table VII: OWASP scoring system

Overall Risk Severity				
Impact	High	Medium	High	Critical
	Medium	Low	Medium	High
	Low	Note	Low	Medium
		Low	Medium	High
Likelihood				

(CVSS) [26]. The estimated risk is compared with the acceptance risks, which are defined by the organization or by referring to scoring systems such as the Common Vulnerabilities and Exposures (CVE) database [27]. Consequently, the levels of risks, such as low or high, are given and demonstrated on a heat map table or table of the levels.

6 PROPOSED RAS FRAMEWORK IN VIETNAM

In this section, we propose a new RAS framework for IT, OT and IIoT systems.

For simplicity of scanning cybersecurity for the end-user IT devices, we build an open-source Web application namely RASVN. Our application provides a high-end framework to scan IT risks and a set of TCVN-based questions about OT risks. The architecture is shown in Figure 8.

In detail, each device in the IoT system is scanned for IT risks by the proposed system namely UET.SoC in [6] to get a single report. Our proposed system uses vScanner software to scan the vulnerability of IT devices. This software uses the data of the list of vulnerabilities and exposures from CVE security vulnerability database [27], which uses CVSS [26] to mark the scoring system. CVSS is a well-known scoring system which

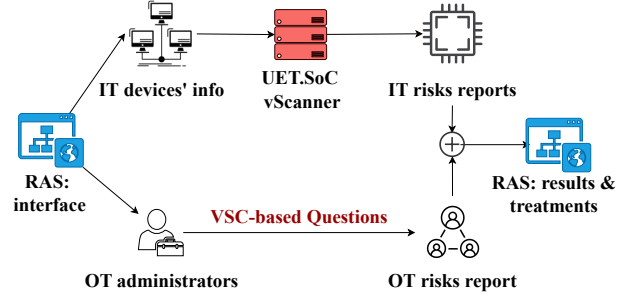


Figure 8: Proposed framework for RAS of IIoT.

Table VIII: CVSS Scoring system

Score ranges	Level
0.0 - 3.9	Low
3.9 - 6.9	Medium
7.0 - 10.0	High

classifies the vulnerabilities based on the severity levels of the heat map ranging from 0 as lowest to 10 as highest, as given in Table VIII. To quantify the severity levels of the heat map, CVSS uses exploitability and impact measures including confidentiality (C), integrity (I), and availability (A) to identify the base score as follows [28]:

$$Severity_level = 1 - [1 - A] * [1 - I] * [1 - C]. \quad (1)$$

As described in Figure 4, the IIoT systems include a large number of IT devices which perform different tasks in the network. The result from scanning these IT devices provides weights for individual IT devices. The weight of an IT device is indicated by the number of other devices which are affected when this IT device is under attacks. For example, a device at the edge layer which is a gateway for four sensors at the perception

Table IX: Proposed set of questions used for determining vulnerabilities of OT systems.

Group	Number of questions
Access Control	8
Account Management	2
Communication Protection	35
Continuity	6
Environmental Security	10
Incident Response	1
Personnel	4
Physical Security	36
Portable/Mobile/Wireless	3
Remote Access Control	2
Software	1
System Integrity	4
System Protection	4
Training	1

layer will have the weight of 4. A device is responsible for more devices will have higher points because they have more data and affect the IIoT system more seriously. In the proposed method, the severity level is accompanied to the weight of the devices:

$$Device_severity = Severity_level * Device_weight. \quad (2)$$

The total risk of the IT system can then be calculated as

$$IT_severity = \frac{\sum Device_severity}{\sum weight}. \quad (3)$$

Table IX summarizes our proposed set of question to evaluate OT systems. These questions provide guidance on how to secure ICS. It follows NIST SP-800-82-r2, including Supervisory Control and Data (SCADA) systems, distributed control systems, and other control system configurations such as PLC, while addressing their unique performance, reliability, and safety requirements. The standard provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.

The level of risks of an OT system after having the answers of all questions are shown in Table IX. Each question is represented for a vulnerability of OT systems. Thus, the number of unanswered questions or questions with “No” as answer are described as flaws of the system. From these flaws, the risk of the OT system is determined as

$$OT_severity = \frac{Q_{total} - Q_{yes}}{Q_{total}}, \quad (4)$$

where Q_{total} is the total number of questions and Q_{yes} is the number of “Yes” answers. After that, we map the result to the CVSS scoring system to find the severity level of the OT system.

IT and OT systems can play an equal role for the security of IIoT systems [29]. Having obtained RAS for the IT and OT systems above, we can now calculate the

Table X: The summary Risk scoring for IT devices

IT Devices	Risk scoring	Number of slave devices
Server 1	7.5	5
Server 2	0	5
IoT Gateway CPS200 RE	4.9	4
IoT Gateway Adlink 212	9	4
BeagleBone Wireless	9.3	1

total severity of the complete IIoT systems by

$$Total_severity = \frac{IT_severity + OT_severity}{2}. \quad (5)$$

7 RESULTS

7.1 Proposed method

Next, we present our results in evaluating the cybersecurity risks of IT, OT, and IIoT systems. To evaluate the results of our proposed method, we build an experiment that simulates a real IIoT system as in Figure 9. In this experiment, there are 8 sensors at the perception layer, 2 IoT gateways at the edge layer, and 2 servers at the cloud and data layer. Each IoT gateway connects with 4 sensors by different industrial communication standards. The servers can connect with each other by a network, e.g., blockchain or local area network. This system is set up to work as a real IIoT system with real-time monitoring. After setting up the system, we assess the risk of this system by our proposed method and compare it with other state-of-the-art methods, i.e., CVSS and OWASP.

To assess the IT system, we first need to scan the vulnerabilities of all configurable devices in our network. However, most of the sensors are purely physical devices, they can not be scanned to find vulnerabilities. Thus, we scan the following devices in different layers to find the vulnerabilities: a BeagleBone wireless module, two IoT gateways and two servers. The risk scoring and the number of slave devices for each IT device are described in Table X. From Equations 2 and 3, we found a the risk level of 5.9, which is medium, according to CVSS.

To assess the OT system, we first need to answer a list of OT security questions in detail. Each question identifies a risk of an OT system. In our experimental system, after carefully checking each question, we identified a risk of 7.4, which is high according to CVSS.

Finally, the total risk can be identified by Equation (5). In our experimental system, we obtained a total risk of 6.65, which is medium, according to CVSS.

7.2 RAS by CVSS

The CVSS scoring system assesses the risks of a system based on three parts: base metrics, temporal

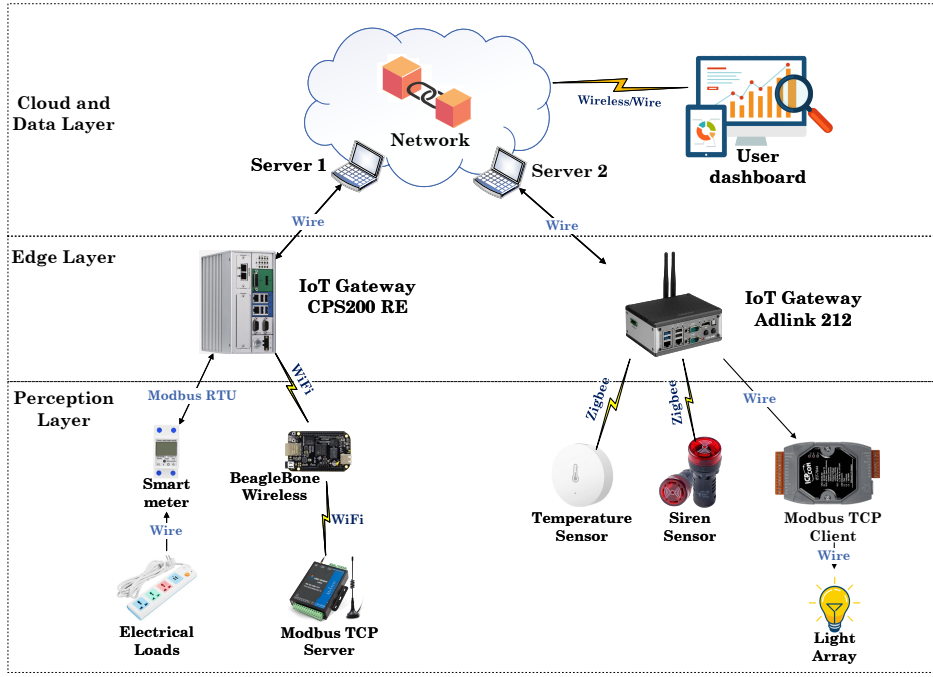


Figure 9: Our experimental model to simulate a real IIoT system.

metrics, and environmental metrics. The base metrics evaluate the internal system quality facing vulnerability, the temporal metrics evaluate the evolution characteristics over the lifetime of vulnerability, and the environmental metrics evaluate the vulnerability based on the environment or implementation. An example of using CVSS to assess the risk of a system is described in Figure 10.

We use CVSS as a baseline to compare with our RAS framework. The results of CVSS scoring are described in Table XI. With these results, our experimental IIoT system identified the risk as high. It can be seen that CVSS rates our experimental system with a higher level of risk, in comparison with our proposed method. However, as described in the previous section, CVSS includes some common questions, and thus it is difficult for CVSS to understand the specified IT, and OT systems of the overall IIoT system, unlike our proposed method.

Table XI: CVSS results from our system

	Base	Temporal	Environmental
Score	8.3	7.7	7.7
Level	High	High	High

7.3 RAS OWASP

Unlike CVSS, OWASP [30] uses likelihood and impact scores to assess the risks of the system. While the likelihood score gives an estimate of a successful attack from a group of attackers, the impact score gives the impact of an attack on technical and business factors. The likelihood and impact scores are categorized into three levels corresponding to the severity of a system, namely low, medium, and high. The answers to the corresponding questions and the results of OWASP are presented in Figure 11. The risk levels are determined by combining the levels of impact and likelihood, as seen in Table VII. Figure 11 also provides the results of

Figure 10: An example of CVSS risk evaluation.

OWASP Risk Assessment Calculator

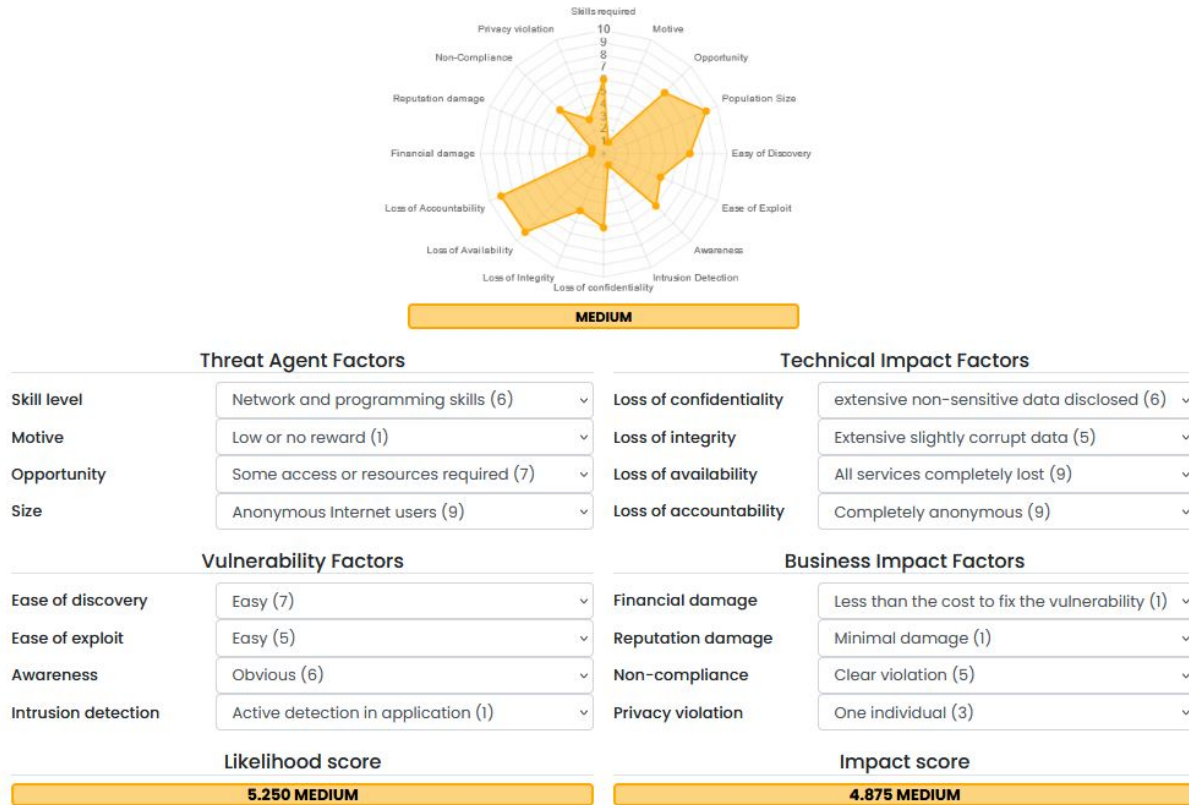


Figure 11: The evaluation results obtained by OWASP.

the likelihood score of 5.25 (medium) and impact score of 4.875 (medium) of our system. The risk level of our system was assessed as medium, according to Table VII. Thus, it can be seen that our proposed method provides a similar risk severity as OWASP, even if our proposed method focuses on the IT and OT systems for an IIoT network.

7.4 Risk assessment web-service for Vietnam

A risk assessment web-service¹ for Vietnam (RASVN) is built based on the proposed framework as mentioned in Section 6. Figure 12 shows the sequence diagram of RASVN, which includes three objects: the website interface (front-end), the UET.SoC vScanner, and the website back-end.

In detail, the users need to provide RASVN with some identifying information (e.g., name, email), information on IT devices in the user system (e.g., public IP address, number of slave devices), and answer a list of OT questions. The rest of the processes are all automated, i.e., RASVN will create new scanning tasks on UET.SoC system based on IT devices' information. After the UET.SoC system has scanned all devices and reported IT risks of the devices, the RASVN back-end

gets and sends them together with OT answers to the user interface. At the RASVN web interface, the IT and OT severity levels are used to calculate the total risk of the overall IIoT system. Finally, RASVN visualizes RAS results of the user system. Moreover, the full report is in raw type, which includes all detailed results of the RAS session, being available for download.

An example of results of RASVN is shown in Figure 13. Since we do not have enough public IPv4 addresses, we only assessed risks in the edge and perception layers of our experimental model as shown in Figure 9 (with an IoT Gateway CPS200RE, an IoT Gateway Adlink 212, a BeagleBone Wireless, and the other unscannable IoT devices/sensors). The first three devices were scanned to produce IT risk report. 117 OT questions are then answered, as shown in Table XII, for the OT risk report. In Figure 13a and 13b, the IT score of each device and OT score for each device are visualized side by side; this helps users compare and find out the risky device/OT area. The final score results of the system are given in Figure 13c, in which the IT, OT, and Overall risk scores are 7.2, 7.3, and 7.3, respectively. All of them are at the high level of risk. Users may then download our detailed report to check and treat system vulnerabilities.

¹<http://rasvn.systems>

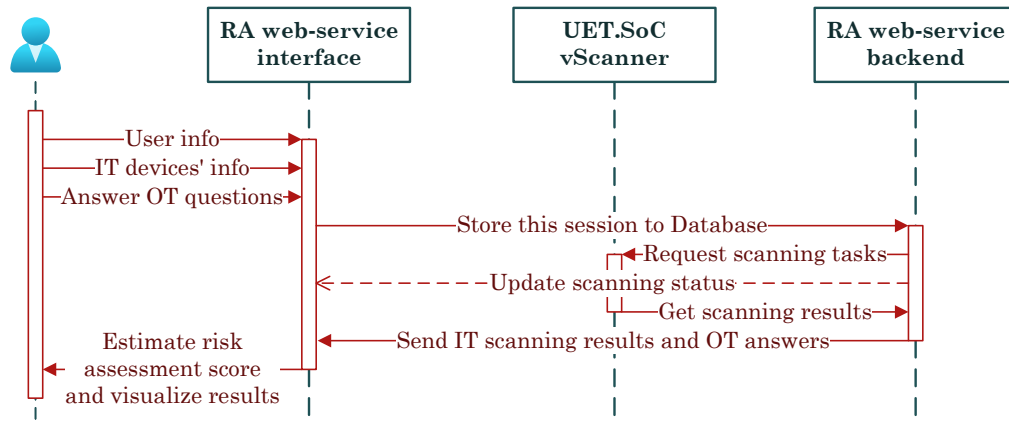


Figure 12: Sequence diagram of RA web-service for Vietnam.

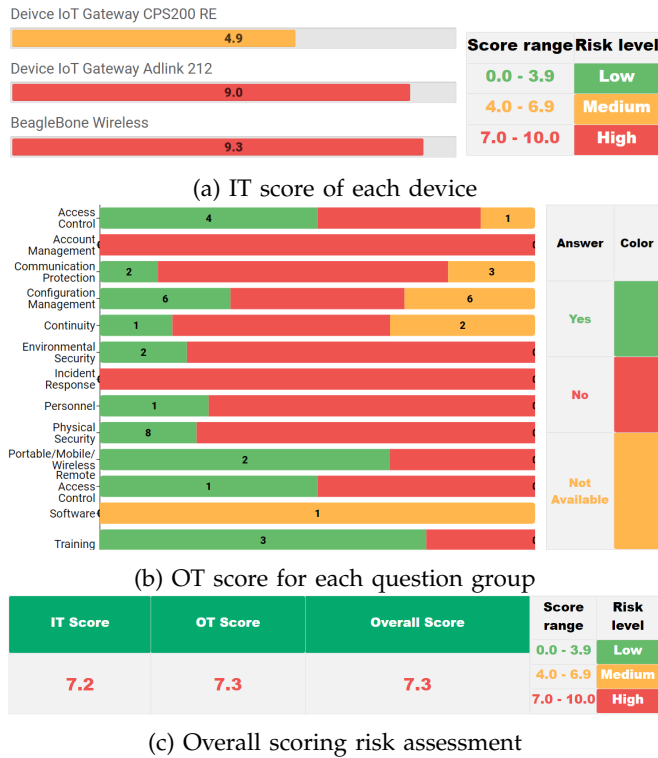


Figure 13: An example of risk assessment result using RA web-service for Vietnam.

8 CONCLUSION

This paper has provided an overview of potential cyber risks in Industry 4.0. We also review some standards for RAS in IT and OT systems. The cyber security standards used in Vietnam and their corresponding ISO and NIST standards are also showed in this paper. Further, we recommend an approach for RAS and give a possible framework of RAS for OT systems. Finally, we propose a new framework for RAS in an IIoT system

that can provide the total risk level of the system.

For future study, we realize that some issues need to be investigated related to RAS in Industry 4.0. Firstly, although vulnerabilities can be detected online, most of the existing RAS approaches or frameworks are conducted offline. It is difficult to deal with real-time processing that requires a dynamic risk assessment. Secondly, probabilities of given threats only hold with frequent attacks but may not hold with new types of threats or threats that rarely happen. Thus, the results of RAS will not be accurate. Lastly, acceptance risk levels in each organization are different, and they highly depend on their scale and function. Finding the scheme to determine the suitable acceptance risk levels is essential.

REFERENCES

- [1] B. C. Ervural and B. Ervural, "Overview of cyber security in the industry 4.0 era," in *Industry 4.0: managing the digital transformation*. Springer, 2018, pp. 267–284.
- [2] "Gartner says by 2020, more than half of major new business processes and systems will incorporate some element of the internet of things." Gartner, 2016, accessed: Feb. 14, 2022. [Online]. Available: <https://www.gartner.com>
- [3] "Information technology — security techniques — information security risk management," International Organization for Standardization, Standard ISO/IEC 27005:2008, 2008.
- [4] "Operational technology (ot)," Gartner, accessed: Feb. 14, 2022. [Online]. Available: <https://www.gartner.com/en/information-technology/glossary/operational-technology-ot>
- [5] M. Le, H. D. Huu, T. N. Ngoc, and et al., "An assessment model for cyber security of vietnamese organization," *VNU Journal of Science: Policy and Management Studies*, vol. 33, no. 2, pp. 97–103, 2017.
- [6] L. V. Ha, P. V. On, and N. N. Hoa, "Information security risk management by a holistic approach: a case study for vietnamese e-government," *IJCSNS International Journal of Computer Science and Network Security*, vol. 20, no. 6, pp. 72–88, 2020.
- [7] Y. Zheng and S. Zheng, "Cyber security risk assessment for industrial automation platform," in *2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Adelaide, SA, Australia, 2015, pp. 341–344.

- [8] X. Lyu, Y. Ding, and S.-H. Yang, "Safety and security risk assessment in cyber-physical systems," *IET Cyber-Physical Systems: Theory & Applications*, vol. 4, no. 3, pp. 221–232, 2019.
- [9] I. Lee, "Internet of things (iot) cybersecurity: Literature review and iot cyber risk management," *Future Internet*, vol. 12, no. 9, p. 157, 2020.
- [10] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A review of cyber security risk assessment methods for scada systems," *Computers & Security*, vol. 56, pp. 1–27, 2016.
- [11] G. Culot, F. Fattori, M. Podrecca, and M. Sartor, "Addressing industry 4.0 cybersecurity challenges," *IEEE Engineering Management Review*, vol. 47, no. 3, pp. 79–86, 2019.
- [12] H. Well, "The 4th industrial revolution," *Report*, 2018, accessed: Feb. 14, 2022. [Online]. Available: <https://kemptechnologies.com/>
- [13] J. Lee, B. Bagheri, and H.-A. Kao, "A cyber-physical systems architecture for industry 4.0-based manufacturing systems," *Manufacturing letters*, vol. 3, pp. 18–23, 2015.
- [14] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.
- [15] A. Ustundag and E. Cevikcan, *Industry 4.0: managing the digital transformation*. Springer, 2017.
- [16] M. Ghobakhloo, "The future of manufacturing industry: a strategic roadmap toward industry 4.0," *Journal of Manufacturing Technology Management*, vol. 29, no. 6, pp. 910–936, 2018.
- [17] "Unified Architecture," OPC Foundation, accessed: Feb. 14, 2022. [Online]. Available: opcfoundation.org/about/opc-technologies/opc-ua
- [18] A. Mishra, N. Gupta, and B. B. Gupta, "Security threats and recent countermeasures in cloud computing," in *Modern principles, practices, and algorithms for cloud security*. IGI Global, 2020, pp. 145–161.
- [19] J. Prinsloo and et al., "A review of industry 4.0 manufacturing process security risks," *Applied Sciences*, vol. 9, no. 23, p. 5105, 2019.
- [20] A. Gilchrist, *Industry 4.0: the industrial internet of things*. Springer, 2016.
- [21] "The industrial internet of things volume g1: Reference architecture," in *Industrial Internet Consortium*, 2019.
- [22] "Itu internet of thing report, 2005," <https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf>.
- [23] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: The internet of things architecture, possible applications and key challenges," in *2012 10th International Conference on Frontiers of Information Technology*, 2012, pp. 257–260.
- [24] A. Shamel-Sendi, R. Aghababaei-Barzegar, and M. Cheriet, "Taxonomy of information security risk assessment (isra)," *Computers & Security*, vol. 57, pp. 14–30, 2016.
- [25] P. P. Roy, "A high-level comparison between the nist cyber security framework and the iso 27001 information security standard," in *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications*, Durgapur, India, 2020, pp. 1–3.
- [26] "Common Vulnerability Scoring System (CVSS)," Forum of Incident Response and Security Teams, accessed: Feb. 14, 2022. [Online]. Available: <https://www.first.org/cvss/>
- [27] "CVE security vulnerability database. Security vulnerabilities, exploits, references and more," MITRE Corporation, accessed: Feb. 14, 2022. [Online]. Available: <https://www.cvedetails.com/>
- [28] M. U. Aksu, M. H. Dilek, E. İ. Tatlı, K. Bıçakçı, H. İ. Dirik, M. U. Demirezen, and T. Aykır, "A quantitative cvss-based cyber security risk assessment methodology for it systems," in *2017 International Carnahan Conference on Security Technology (ICCST)*. IEEE, 2017, pp. 1–8.
- [29] "Architecture alignment and interoperability," in *Industrial Internet Consortium*, 2019.
- [30] B. Mburano and W. Si, "Evaluation of web vulnerability scanners based on owasp benchmark," in *2018 26th International Conference on Systems Engineering (ICSEng)*. IEEE, 2018, pp. 1–6.

Table XII: Risk assessment web-service for Vietnam: OT questions

No.	ID in CSET	Group	Question
1	239	Access Control	Are periodic reviews conducted of existing authorized physical and electronic access permissions to ensure they are current?
2	245	Access Control	Do electronic monitoring mechanisms alert system personnel when unauthorized access or an emergency occurs?
3	248	Access Control	Does the system enforce assigned authorizations for controlling electronic access to the system?
4	249	Access Control	Are access control policies and associated access mechanisms to control access to the system?
5	258	Access Control	Is a device verified against a pre-defined list of authorized devices before a connection is established? (e.g., Active Directory policy or firewall rules.)
6	259	Access Control	Does the system authenticate devices before establishing remote network connections using bi-directional authentication between devices that are cryptographically based?
7	263	Access Control	If your authentication encryption module fails can you still authenticate without creating a denial of service that impacts operational performance of system?
8	279	Access Control	Does the system prevent further access to the system by initiating a session lock after a defined time period of inactivity or a user initiated session lock?
9	226	Account Management	Are users required to take, and devices implement, specific measures to safeguard authenticators?
10	230	Account Management	Are unique authenticators required to be provided by vendors and manufacturers of system components?
11	384	Communication Protection	Do the system components separate telemetry/data acquisition services from management port functionality?
12	391	Communication Protection	Is the unauthorized release of information outside the system boundary or any unauthorized communication through the system boundary prevented when an operational failure occurs of the boundary protection mechanisms?
13	395	Communication Protection	Does the system prevent remote devices that have established connections (e.g., PLC, remote laptops) with the system from communicating outside that communications path with resources on uncontrolled/unauthorized networks?
14	398	Communication Protection	Have you evaluated the latency issues introduced by the use of cryptographic mechanisms to ensure that they do not impact operational performance?
15	406	Communication Protection	Are collaborative computing devices (e.g., video and audio conferencing) restricted on your control system network?
16	407	Communication Protection	Are collaborative computing devices disconnected and powered down when not in use?
17	409	Communication Protection	Are collaborative computing devices disabled or removed from systems in secure work areas?
18	410	Communication Protection	Does the system reliably associate security labels and markings with information exchanged between the enterprise systems and the control system?
19	413	Communication Protection	Is the use of VoIP authorized, monitored, and controlled?
20	416	Communication Protection	Are the system devices that collectively provide name/address resolution services for an organization fault tolerant?
21	417	Communication Protection	Does the use of secure name/address resolution services avoid adverse impacts to the operational performance of the system?
22	427	Communication Protection	Does the system enforce dynamic information flow control based on changing conditions or operational considerations?
23	431	Communication Protection	Does the system enforce defined one-way flows using hardware mechanisms (i.e., data diode)?
24	437	Communication Protection	Are automated or manual mechanisms (e.g., roles and responsibilities as defined by Active Directory) used as required to assist authorizing users in making the correct information sharing/collaboration decisions?
25	439	Communication Protection	Are communications limited to only the devices that need to communicate?
26	524	Configuration Management	Is the delivery and removal of system components limited, authorized, and recorded?
27	529	Configuration Management	Is there an inventory of systems and critical components and is it maintained?
28	534	Configuration Management	Is a baseline configuration for the development and test environments maintained and managed separately from the operational baseline?
29	540	Configuration Management	Are configuration changes tested, validated, and documented before installing them on the operational system, and has testing been ensured to not interfere with system operations?
30	546	Configuration Management	Is there physical security to restrict data devices, serial ports, network ports, USB, and secure digital memory card?
31	548	Configuration Management	Are the security settings configured to the most restrictive mode consistent with system operational requirements?
32	550	Configuration Management	Are exceptions from the mandatory configuration settings identified, documented, and approved based on explicit operational requirements?
33	551	Configuration Management	Are the configuration settings for all components of the system enforced?
34	552	Configuration Management	Are changes to the configuration settings monitored and controlled in accordance with policies and procedures?

35	557	Configuration Management	Has an inventory of the components of the system been developed, documented and maintained that accurately reflects the current system?
36	558	Configuration Management	Has an inventory list of the components of the system been developed, documented, and maintained that is consistent with the system boundary?
37	559	Configuration Management	Has an inventory list of the components of the system been developed, documented, and maintained that is at the level of granularity deemed necessary for tracking and reporting?
38	560	Configuration Management	Has an inventory of the components of the system been developed, documented, and maintained that includes defined information deemed necessary to achieve effective property accountability?
39	561	Configuration Management	Is the inventory of system components and programming updated as an integral part of component installation, replacement, and system updates?
40	562	Configuration Management	Are automated mechanisms used to help maintain an up-to-date, complete, accurate, and readily available inventory of system components, configuration files and set points, alarm settings and other required operational settings?
41	563	Configuration Management	Are automated mechanisms used to detect the addition of unauthorized components/devices/component settings into the system?
42	568	Configuration Management	Are critical digital assets (CDA) in security areas destroyed on removal from operations, or are they inspected and subject to an approved documented sanitization procedure on being removed from service (e.g., lifecycle plan)?
43	569	Configuration Management	Are all factory default authentication credentials changed on system components and applications upon installation?
44	570	Configuration Management	Does legacy equipment with known authentication deficiencies have compensatory access restrictions?
45	573	Configuration Management	Are the legacy components identified, tested, and documented to verify that the compensatory measures are effective?
46	642	Continuity	Is normal operation of the system resumed in accordance with its policies and procedures after a security event?
47	646	Continuity	Is the alternate storage site configured to facilitate timely and effective recovery operations?
48	647	Continuity	Are alternate command/control methods identified, and are agreements in place to permit the resumption of operations within a defined time period when the primary system capabilities are unavailable?
49	652	Continuity	Are necessary communications for the alternate control center identified, and are agreements in place to permit the resumption of system operations for critical functions within a defined time period when the primary control center is unavailable?
50	656	Continuity	Is the alternate control center fully configured to be used as the operational site supporting a minimum required operational capability?
51	663	Continuity	Are backup copies of the operating system and other critical system software stored in a separate facility or in a fire-rated container that is not collocated with the operational software?
52	511	Environmental Security	Is the emergency power shutoff protected from unauthorized activation?
53	512	Environmental Security	Is the emergency power-off capability protected from accidental and intentional/unauthorized activation?
54	513	Environmental Security	Is there a short-term uninterruptible power supply to be used for orderly system shutdown?
55	514	Environmental Security	Is there a long-term alternate power supply that is capable of maintaining minimally required operational capability?
56	515	Environmental Security	Is there a long-term alternate power supply that is self-contained and not reliant on external power generation?
57	517	Environmental Security	Are there fire suppression and detection devices/systems?
58	518	Environmental Security	Do fire detection devices/systems activate automatically and notify the organization and emergency responders in the event of a fire?
59	519	Environmental Security	Do fire suppression devices/systems provide automatic notification to the organization and emergency responders?
60	527	Environmental Security	Is the system power equipment and power cabling protected from damage and destruction?
61	528	Environmental Security	Are redundant power equipment and parallel power cabling paths provided for the system?
62	582	Incident Response	Are cyber and control system security incident information promptly reported to authorities?
63	177	Personnel	Are all required controls for employees terminated for cause completed within 24 hours?
64	179	Personnel	Are electronic and physical access permissions reviewed when individuals are reassigned or transferred?
65	180	Personnel	Are electronic and physical access permissions reviewed within 7 days when individuals are reassigned or transferred?
66	185	Personnel	Are periodic reviews of physical and electronic access conducted to validate terminated account access was removed?
67	470	Physical Security	Are lists of personnel with authorized access developed and maintained, and are appropriate authorization credentials issued?
68	471	Physical Security	Are the access list and authorization credentials reviewed and approved at least annually and those no longer requiring access removed?
69	472	Physical Security	Is physical access to the facility authorized based on position or role?
70	473	Physical Security	Are two forms of identification required to gain access to the facility?
71	474	Physical Security	Are physical access authorizations enforced for all physical access points to the facility?
72	475	Physical Security	Are individual access authorizations verified before granting access to the facility?
73	476	Physical Security	Is entry to the facility controlled by physical access devices and/or guards?

74	477	Physical Security	Are the areas officially designated as publicly accessible controlled in accordance with the organization's assessment of risk?
75	478	Physical Security	Are keys, combinations, and other physical access devices secured?
76	479	Physical Security	Are physical access devices inventoried on a periodic basis?
77	480	Physical Security	Are combinations and keys changed on a defined frequency, and when keys are lost, combinations compromised, or individuals are transferred or terminated?
78	481	Physical Security	Is physical access to distribution and communication lines controlled and verified?
79	482	Physical Security	Is physical access to output devices controlled?
80	483	Physical Security	Is physical access to the system controlled independently of the facility access controls?
81	484	Physical Security	Are security checks at physical boundaries performed for unauthorized removal of system components?
82	485	Physical Security	Is every physical access point to the facility guarded or alarmed and monitored 24 hours per day, 7 days per week?
83	486	Physical Security	Are lockable physical casings used to protect internal components of the system from unauthorized physical access?
84	487	Physical Security	Is physical access monitored to detect and respond to physical security incidents?
85	489	Physical Security	Are results of reviews and investigations coordinated with the organization's incident response capability?
86	490	Physical Security	Are real-time physical intrusion alarms and surveillance equipment monitored?
87	491	Physical Security	Are automated mechanisms used to recognize potential intrusions and initiate designated response actions?
88	492	Physical Security	Is physical access controlled by authenticating visitors before authorizing access?
89	493	Physical Security	Are visitors escorted and monitored as required in the security policies and procedures?
90	494	Physical Security	Are two forms of identification required for access?
91	495	Physical Security	Are visitor access records maintained, and are all physical access logs retained for as long as required by regulations or per approved policy?
92	496	Physical Security	Do visitor records include name and organization of the person visiting?
93	497	Physical Security	Do visitor records include the signature of the visitor?
94	498	Physical Security	Do visitor records include a form of identification?
95	503	Physical Security	Are automated mechanisms employed to facilitate the maintenance and review of access records?
96	504	Physical Security	Is cryptographic hardware protected from physical tampering and uncontrolled electronic connections?
97	505	Physical Security	Are all external system and communication connections identified and protected from tampering or damage?
98	506	Physical Security	Are asset location technologies used to track and monitor the movements of personnel and vehicles to ensure they stay in authorized areas?
99	507	Physical Security	Are asset location technologies used to identify personnel needing assistance?
100	508	Physical Security	Are asset location technologies used to support emergency response?
101	509	Physical Security	Is hardware (cages, locks, cases, etc.) used to detect and deter unauthorized physical access to system devices?
102	510	Physical Security	Is the ability to respond to an emergency not hindered by using tamper-evident hardware?
103	300	Portable / Mobile / Wireless	Are usage restrictions and implementation guidance established for organization-controlled mobile devices?
104	315	Portable / Mobile / Wireless	Is authentication and encryption used to protect wireless access to the system and the latency induced does NOT degrade the operational performance of the system?
105	324	Portable / Mobile / Wireless	Is peer-to-peer wireless networking capability disabled except for explicitly identified components in support of specific operational requirements?
106	293	Remote Access Control	Is remote access for privileged commands and security-relevant information authorized only for compelling operational needs and is the rationale for such access documented?
107	294	Remote Access Control	Is Bluetooth wireless networking capability disabled except for explicitly identified components in support of specific operational requirements?
108	379	Software	Are system components used that have no writable storage that is persistent across component restart or power on/off cycles?
109	449	System Integrity	Does the use of automated flaw remediation processes NOT degrade the operational performance of the system?
110	455	System Integrity	Is the correct operation of security functions verified upon system startup and restart, upon command by user with appropriate privilege, periodically, and at defined time periods?
111	463	System Integrity	Is tamper-evident packaging used during transportation from vendor to operational site, during operation, or both?
112	469	System Integrity	Is the output from the system handled and retained in accordance with applicable regulations, standards, and organizational policy as well as operational requirements?
113	332	System Protection	Are the operational system boundary, the strength required of the boundary, and the respective barriers to unauthorized access and control of system assets and components defined?
114	336	System Protection	Does the system design and implementation protect the integrity of electronically communicated information?
115	339	System Protection	Does the use of public key certificates avoid degrading (i.e., latency) the operational performance of the system?
116	351	System Protection	Has legacy equipment been updated with current or custom developed system components?
117	197	Training	Are simulated events incorporated into continuity of operations training to facilitate effective response by personnel in crisis situations?