# Methods for Increasing the Cyber Resilience of Critical Infrastructures Methods for Increasing the Cyber Resilience of Critical Infrastructures

***Received: 30 January 2023 Accepted: 6 March 2023*** ***Research Article***

Fatih Furkan Bayar
*Cyber Security Directorate*
HAVELSAN
Ankara, Turkey
fbayar@havelsan.com.tr
0000-0003-1157-482X

Sila Sibil Bardak
*Cyber Security Directorate*
HAVELSAN
*Ankara, Turkey*
ssibil@havelsan.com.tr

Ender Saribay
*Cyber Security Directorate*
HAVELSAN
Ankara, Turkey
esaribay@havelsan.com.tr

Ozmen Emre Demirkol, Ph.D.
*Cyber Security Directorate*
HAVELSAN
*Ankara, Turkey*
oedemirkol@havelsan.com.tr

Mert Ozarar, Ph.D.
*Cyber Security Directorate*
HAVELSAN
*Ankara, Turkey*
mozarar@havelsan.com.tr

***Abstract*— Cybersecurity is a critical topic that has become increasingly important in today's world, due to the increasing dependency on technology and interconnected systems. As digitalization increases, the need for cybersecurity measures becomes even more important for several systems that are crucial for society, nuclear facilities, energy systems, finance transportation and healthcare systems. Any damage to critical infrastructures from inside or outside will lead to the deterioration of the social order of countries, the loss of international reputation and the undermining of their credibility. The integration of information technology (IT) and operational technology (OT) within industrial control systems (ICS) has resulted in an expanding attack surface for cyber threats. In order to establish complete cyber-defence solution, innovative artificial intelligence solutions must be utilized alongside traditional cyber security approaches. In the digital transformation process of countries and organizations, the increasing cyber threats are addressed by explaining the five crucial solutions needed, based on international standards. This study aims to provide an overview of strategies to enhance the cyber security maturity level of critical infrastructures, examines both traditional cyber security approaches and artificial intelligence approaches. An architecture is specified to build cyber resilient critical infrastructures.**

***Keywords—Critical Infrastructure, Operational Technology, Industrial Control Systems, Cyber Resilience, Artificial Intelligence***

## I. INTRODUCTION

In the 21st century, technology continues to advance, and people all over the world are becoming more dependent on it. Information technologies (IT) and operational technology (OT) are two examples of the concepts introduced by this discipline, which grew in popularity notably when the internet was discovered. Written sources were replaced by electronic sources when information began to be created, processed, stored, and consumed in an electronic context. As a result, information technologies have emerged as one of the most essential and rapidly evolving technological components of the 21st century. With benefits like quick access and processing power, as well as time and resource savings, information technologies have a significant impact on both the social structure of states and individual usage. Systems utilizing information technology, which are now widely employed in all industries, have become the main focus of evil individuals. Through the utilization of advanced technologies, cybercriminals are now able to engage in illegal acts, including gaining unauthorized access to information systems and compromising or exfiltrating data. It has become a top priority in national and international levels to prevent potential risks from adversarial individuals to information technology systems. Since attacks to cyber systems constantly increase and have more and more impact, the concept of cybersecurity has emerged, and security of technological systems became a fundamental concern. Cybersecurity is the set of all technologies employed by groups or individuals to protect their assets. Any entity having Internet connection naturally causes the attack surface to expand, which makes the protection necessary. Although the foundation of cybersecurity is information technology security, operational technology has continued to advance. Operational technology is the hardware and software that directly monitors and/or controls industrial assets, equipment, processes, and events in order to detect or implement changes [1]. The main reason operational technologies have not received top priority in terms of cybersecurity is that this field of technology typically operates at remote locations without direct Internet access, such as factories, production facilities, energy distribution centers, water treatment plants, or nuclear power plants. The very small attack surface created by the lack of internet connection on the devices operating the equipment in these situations virtually limits the prospect of an assault unless there is physical access. Today, however, the demand for remote equipment monitoring and control has resulted in widespread Internet access by the devices that manage the equipment. Due to this circumstance, the fields of information technology and operational technology have begun to merge into integrated systems. Critical infrastructures including those in the areas of transportation, health, energy, and military all rest on information and operational technology systems that, if they fail, will cause major disruptions to the state and society. It is important to consider national security while evaluating how secure critical infrastructures should be, as well as how resilient they should be to cyberattacks. To ensure the security of critical infrastructures, various cyber

security solutions should be brought together and the necessary infrastructure should be developed. To construct and improve the cyber resilience of critical infrastructures, policies should be created and put into place.

## II. BACKGROUND

In this section, we aim to explain concepts such as cyber security, critical infrastructures, the convergence of technology and critical infrastructures, cyber attacks targeting these infrastructures, and the role of artificial intelligence in these concepts in order to effectively convey the details of our research.

### *A. Cyber Security*

Cyber security is a concept involving ensuring the security of cyber systems, such as mobile phones, computers, websites, and servers. Even though these are the first devices that come into the mind when it is questioned what is tried to be protected in context of cyber security, the amount of devices that are to be protected is much more than those. For instance, it is possible to discuss the cyber security of operational technology devices, particularly those found in critical infrastructure. Therefore, the term cyber security covers a wide range of devices, which also means that ensuring cyber security of a complex environment consisting of many different types of devices is a challenging task.

Nowadays, the term cyber security is much more important than it was, e.g., 20 years ago. Recent developments in technology has shown that cyber environments are now places where the most critical operations are performed, such as money transactions, citizenship procedures, taking exams, submitting documents, which may include sensitive data, for crucial tasks, and many more daily-life cases where the cyber security is the key part for making it possible for these operations to be performed healthily without any dangerous consequences. Since the attackers know that the cyber environments are of great importance for most tasks, they improve their attack vectors more and more as the time goes on. The twenty first century can be referred to as the century of cyber cases since numerous cyber attacks have been performed on numerous organizations and targets, which include critical infrastructures as well.

### *B. Critical Infrastructure*

W.J. Clinton, who was the president of the U.S. at the time, became the first one to use the term critical infrastructure in 1996. The term was first mentioned in the order named as “Executive Order 13010 - Critical Infrastructure Protection” [2]. Based on this executive order, a commission was founded in the U.S. to focus on critical infrastructures' cybersecurity, and related studies had been started. Several distinct pieces of hardware, software, and control equipment in the areas of information and operational technology come to mind when the assets and systems specified in this definition are taken into account. Therefore, physical hardware and virtualized solutions are combined to provide cybersecurity of critical infrastructures.

### *C. Convergence of IT & OT Systems*

Systems for information technology and systems for operational technology were once considered to be independent systems. Information technology teams and operational technology teams were separate within organizations. Teams could only work on systems in which they have expertise. This situation started to alter in the 21st century, and the boundaries between the two disciplines vanished.

The requirements for rapid process execution, real-time execution, and decision tracking have evolved in the 21st century. Therefore, there is an increasing number of OT systems connected to at least one communication network or the Internet. They enable the flow of data into IT environments and the exchange of information between industrial control systems (ICS) components such as sensors and actuators via network connections. With the processing and analysis of this data in information environments, the status and performance of physical devices are monitored and useful statistics that can be used for process management are produced. Remote device configuration for OT systems is possible with IT systems.

It is obvious that combining OT and IT systems has many advantages, but it also carries significant risks. Systems that are not isolated in an environment where all OT and IT networks connected to the Internet are merged are more susceptible to cyberattacks, which can have severe material and physical repercussions.

### *D. Cyber Threats Against Critical Infrastructures*

Industrial control systems are one of the most crucial aspects of the cybersecurity of critical infrastructures. It is feasible to completely halt these physically situated devices' operations and do significant harm with a cyberattack.

Due to newly discovered weaknesses in industrial control systems, which have emerged as a result of the confluence of the information and operational technology domains, these critical infrastructures are now the main target of cyberattacks. The usage of operational technology equipment for 30 to 50 years creates various cybersecurity risks, even while information technology devices are replaced every 3 to 5 years [3]. It is usually not possible to suspend the system and perform an upgrade on it because operational technologies, unlike information technologies, prioritize accessibility and integrity [3]. The attack surface for critical infrastructures has increased significantly due to the convergence of information and operational technology and the ability to access legacy industrial control systems from the virtual world via the Internet.

Since the 21st century, numerous cyberattacks such as the STUXNET attack on Iran's nuclear program, Havex, and Black Energy have been carried out against industrial control systems and critical infrastructures [4]. Some other notable examples of cyberattacks targeting industrial control systems include the Ukraine power grid attack in 2015 and the attack on the Saudi Arabian oil company Aramco. These attacks have utilized various techniques such as malware injection, phishing, and exploitation of vulnerabilities in software and hardware.

One of the most concerning techniques used in these attacks is the ability to gain access to and manipulate industrial control systems through Remote Access Trojans (RATs) and Advanced Persistent Threats (APTs). These types of malware allow attackers to remotely control and manipulate the functionality of industrial control systems, potentially causing damage or disruption to critical infrastructure, as well as collecting sensitive intelligence information. For instance, Havex is a type of RAT used against industrial systems and organizations. It is distributed to target systems by attackers

via phishing e-mails, malicious links, and by injecting the malware inside the software packages presented by ICS software providers through compromised websites [5]. After infecting a system found in a critical infrastructure, Havex downloads and installs its ICS plugin that scans for OPC servers from which it obtains valuable data and transmits the obtained data in an encrypted format to remote servers so that the attackers can gather information regarding the infected infrastructure [5]. Researchers, through reverse engineering and behavioural analysis, have found that Havex malware is vulnerable to honeypots, i.e., it is easily deceivable that a honeypot system is actually among the targets of the malware, by analysing the steps taken by the virus while searching for the targets. This study also shows that improving cybersecurity of critical infrastructures through establishing specialized defenses against known viruses by analyzing vulnerabilities of malwares is possible [5].

Another example of malwares threatening critical infrastructures is, as mentioned above, Stuxnet, which is a complex malware that can provide control of a system to attackers by infiltrating target computers. In case of attack performed on Iran's nuclear program, the malware has disrupted the operation of centrifuges by controlling the electrical current managing the centrifuges so that they change speed in such a rate that they are not designed to be capable of [6]. This provided the attackers a way to slow down Iran's nuclear program without actually needing to perform military attacks on Iran's nuclear systems, and these types of cyberattacks also provide a way for attackers to hide their identities [6].

Additionally, attacks can also leverage social engineering tactics, such as phishing and spear-phishing, to gain access to sensitive information and systems. These attacks seriously harmed the nations' reputation and social order in addition to interfering with the operation of critical infrastructures. As it can also be understood by the cyberattack examples given up to here, one of the biggest dangers to critical infrastructures is the vulnerability of industrial control systems, and cyberattacks on these systems are growing every day [7]. It is now vital to prioritize critical infrastructure cybersecurity at the national level due to the rise in cyberattacks against critical infrastructures and industrial control systems.

### *E. Artificial Intelligence*

Artificial intelligence (AI), is a field of research and engineering that focuses on creating intelligent systems that can perform tasks typically requiring human intelligence, including tasks such as image recognition, natural language processing, speech recognition, decision-making, and language translation. Rule-based systems and machine learning systems are the two basic categories into which AI systems can be split. A branch of artificial intelligence known as machine learning (ML) focuses on creating algorithms and statistical models that let systems get better with practice. ML algorithms can be broken down into three groups: reinforcement learning, unsupervised learning, and supervised learning.

Algorithms under supervision gain knowledge from labeled training data and make assumptions about unobserved data. Unsupervised learning algorithms find significant patterns or structures in unlabeled data by learning from it. Algorithms that use reinforcement learning learn from their interactions with the environment and adjust their behavior to maximize a reward signal. A branch of machine learning named as deep learning focuses on building deep neural networks made up of many layers of artificial neurons. Applications for deep learning techniques include speech recognition, image classification, natural language processing, and game playing. Deep learning algorithms are successful in a wide range of tasks and have been used successfully in various industries such as banking, healthcare and transportation.

While AI solutions are being used at many areas, cyber security starts to become one of the focus areas of artificial intelligence field. Hence, there exists numerous research on detecting cyberattacks by using artificial intelligence techniques. It is possible to use artificial intelligence to support and strengthen cybersecurity solutions to improve cybersecurity of critical infrastructures.

## III. Cyber Security Standards

Many countries and organizations are focusing on critical infrastructure-related cybersecurity issues. Research has led to the emergence of many different, globally accepted models and standards. Organizations develop cyber defense solutions around these criteria to ensure the cybersecurity of critical infrastructures.


Fig. 1. Use of International Cybersecurity Standards

The most preferred cybersecurity standards internationally are ISA / IEC 62443 and NIST CSF as shown in Fig. 1 [8]. Even though the developed standards are meant to provide critical infrastructure cybersecurity, each of them proposes a different cybersecurity strategy. Industrial control systems construct the foundations of critical infrastructures. Standards for information technologies are not applicable for industrial control system cybersecurity since IT have different requirements and criterion [9]. IEC 62443 model contains approaches regarding operational technologies' cybersecurity to provide critical infrastructure cybersecurity. This model defines the procedures that are to be carried out and system-level requirements for ensuring cybersecurity of industrial control systems.

The NIST CSF model essentially outlines the procedures to be followed in order to guarantee cybersecurity and provides examples. The main and sub-categories of functions, as well as informative references, form the basis of the model [10]. NIST defines five functions, namely, identify, protect, detect, respond, and recover. Identifying means to identify and detect the devices and systems to be protected, for which asset management is a crucial task to handle. Protecting describes the act of taking precautions against the cyber threats, such as management of access to the assets and collecting the required logs, which then can be analysed furtherly. Detecting is to recognise cyber threats at the moment they emerge, for which

various tools and technologies can be leveraged. Responding means to take required actions as response to an ongoing cyberattack. Recovering is the process of restoring the system from any damage caused after a cyberattack occurs. The cyber defense solution must perform each function in order to provide cybersecurity in critical infrastructures. As more categories within the functions can be implemented successfully, more cyber-resistance will be offered.

The C2M2 (Cybersecurity Capability Maturity Model) defines various domains, each indicating a defined group of applications related to a certain field [11]. C2M2 model not only focuses on information technologies (IT) security, but it also deals with operational technologies' (OT) cybersecurity. The domains defined by C2M2 are asset, threat, risk, access, situation, response, third-parties, workforce, architecture, and program, as specified by Office of Cybersecurity, Energy Security, and Emergency Response, U.S [11]. The model proposes a different set of objectives for each domain. The asset domain proposes the objectives related to asset management. Threat domain is related to vulnerability management. The risk domain copes with risk management issue, while access domain is about management of access and identity. The situation domain describes the situational awareness of cybersecurity of the system to be protected. The response domain proposes objectives to define how cyber incidents are to be responded once they occur. Third-parties domain is about how to manage risks related to third-parties, while workforce domain is about how to manage workforce. The architecture domain defines objectives regarding how cybersecurity architecture should be designed, and program domain proposes objectives for managing the cybersecurity program as a whole. The C2M2 model also defines three main maturity indicator levels (MILs), namely, MIL1, MIL2, and MIL3. These levels are said to be initiated, performed, and managed, respectively.

Numerous more cybersecurity standards specify templates and/or guidelines for guaranteeing protection against cyber threats. Another cybersecurity standard developed for establishing requirements to guarantee the cybersecurity of critical infrastructure is NERC CIP (Critical Infrastructure Protection). Examination of cybersecurity standards shows that even if they differ from each other, they all address at least the essential elements for a cyber-secure environment: identifying assets, maintaining ongoing protection, and detecting cyberattacks.

## IV. Improving Cyber Resilience in Critical Infrastructures

Creating a robust cyber defense infrastructure is accomplished by integrating various cybersecurity solutions together. There are several techniques that organizations can use to improve cyber resilience in critical infrastructure. The proposed approach uses a methodology comprising of five different solutions in setting up a cyber defense system infrastructure for the underlying infrastructure. Effective management of resources by utilizing suitable technologies and methods for monitoring and controlling assets, vulnerability management systems should be employed to identify assets and potential vulnerabilities, and risk management should be conducted based on the potential impact of these vulnerabilities. Solutions for intrusion detection should be implemented and methods should be established to facilitate incident investigation by maintaining event logs. Artificial intelligence and automation techniques should be applied in the development of the necessary infrastructure.

### *A. Asset Management*

An asset in critical infrastructure refers to any physical or virtual component or system that is essential for the functioning of a critical infrastructure system. Assets are items that an organization needs in order to maintain its operations in a smooth and efficient manner. These assets that are essential for the functioning of a critical infrastructure system include physical devices, software products, information and operational technology assets, and essential information needed for operations. Companies must secure all of their valuable assets against potential threats.

With the rise of the 4th Industrial Revolution, the ability to access and control many IT and OT devices over the internet has made it even more crucial for organizations to also protect these assets in the cyber realm. In order to effectively protect assets, organizations must first identify and manage them.

Asset management is used to identify all the devices, software and systems that are connected to the organization's network and to keep track of assets in order to identify any potential cyber threats that might be brought on by asset weaknesses. Organizations cannot defend against attacks due to their undetectable and unseen existence. To automatically find assets in the network, there are numerous asset discovery techniques. Other than information technology equipment like servers, workstations, and routers, industrial control system hardware like sensors, relays, and actuators should also be automatically found while doing asset discovery in critical infrastructures. During asset detection, information can be gathered via ”active” scanning methods, which transmit network packets to devices, and ”passive” scanning methods, which extract information by observing network traffic . Passive scanning can be a good way to perform safe discovery of networks and devices in industrial control systems [12].

In order to obtain as much information regarding assets found in a critical infrastructure as possible, a study has been performed on the exploration of the hybrid scanning approach, which is the mixture of active and passive scanning techniques [13]. The usage of hybrid scanning method has been shown to make obtaining more thorough information on assets possible, according to research performed.

Asset discovery should be used to gather a variety of crucial data, such as the configuration details of the assets as well as their software and hardware versions, physical location, asset manager, and severity level. Asset data should be digitally archived and accessible via a graphical user interface for viewing and management. By using the asset management approach, it will be possible to spot unauthorized software or configuration changes on assets as well as irregularities in their operation. Vulnerabilities in the assets' current configuration or software will also be discovered, and cyberattacks against the assets will be identified. Asset management in critical infrastructure using artificial intelligence (AI) can involve using AI algorithms and models to automatically identify, classify, and track assets, as well as predict and detect potential vulnerabilities. By using AI algorithms for asset management in critical infrastructure, organizations can improve their ability to identify and prioritize assets that need protection, as well as detect and respond to potential threats in a timely and efficient manner.

The study examines existing machine learning methodologies for developing an effective asset management framework for power distribution systems, as well as for predicting the lifespan and operating stability of electrical equipment [14]. The goal of another article is to showcase the different ways in which Artificial Intelligence (AI) can aid in the management of information assets and enhance the security of enterprise systems. In addition, the research explains that using the Isolation Forest algorithm, it is possible to predict whether an asset in the dataset is rogue or an approved asset [15]. Yawar Rasool Mir tried to analyze the port scan results using artificial intelligence. In this review, they used Artificial Neural Network, Random Forest (RF) and Support vector machine (SVM) calculations to find port scan attempts based on the new CICIDS2017 dataset, with accuracy rates of 98.87%, 99.20% and 72.19%, respectively [16].

### *B. Vulnerability Management*

A cybersecurity vulnerability is a weakness or gap in the security of IT and OT equipment and software, configurations or communication with other assets that can be exploited by attackers to gain unauthorized access, steal sensitive information, or disrupt operations. Each asset within a system can contain its own unique vulnerabilities. Malicious actors can exploit these vulnerabilities to launch attacks such as infiltration, data theft, data alteration, destruction or disruption of system operations.

In order to ensure cybersecurity resilience in critical infrastructures, it is necessary to minimize vulnerabilities in assets. With the convergence of IT and OT fields, the ability to access OT devices via the Internet has expanded the attack surface for industrial control systems attacks on critical infrastructures [17]. 70% of the vulnerabilities created by industrial control systems are network-based vulnerabilities, and organizations should primarily develop vulnerability management solutions to address these vulnerabilities [17].

Data about assets must be gathered and evaluated in order to identify vulnerabilities and fix them. Utilizing asset management, penetration testing, and vulnerability scanning technologies, vulnerability analysis should be carried out. Despite the fact that there are numerous vulnerability detection tools available focusing on information technologies, it is crucial to be careful when applying these tools on ICS (Industrial Control Systems) equipment. The operation of the system may be harmed by network-based brute force scenarios employed during vulnerability scanning because ICS devices have typically not been upgraded or modified for many years [18]. For use on ICS devices, specialized vulnerability scanning tools for the OT field must be created. It is necessary to follow the threat intelligence and analysis reports of the Cybersecurity and Infrastructure Security Agency (CISA) and use the Common Vulnerability Scoring System (CVSS) databases that are accessible online in order to assess the potential impact of vulnerabilities identified in the results of vulnerability scans. In order to determine which vulnerabilities should be fixed first to ensure the security of the system, the vulnerabilities are rated according to their potential impact. Priority risks' vulnerabilities should have action plans made for them, and those vulnerabilities should be fixed as part of these plans.

The increasing number of hardware and software vulnerabilities discovered each year makes manual classification of vulnerability types more difficult [19]. The article investigates algorithms for automatic vulnerability type classification using machine learning. It has been demonstrated in another article that the Gradient Boost Classifier is fully suitable for automatic vulnerability type classification and can be used in practice [20]. In another study, it has been presented that using machine learning algorithms can be an effective way for predicting vulnerabilities [21].

### *C. Risk Management*

Risk management helps identify potentially harmful events, determine their probability of occurrence and predict their potential impact. In other words, it helps identify potential problems and the likelihood of their occurrence and the consequences they cause when they occur [22].

As it is crucial for all kinds of organisations, risk management is an important aspect of ensuring protection and operability of industrial control systems as well. Poor management of risks in an ICS environment may lead to unrecoverable damage as a result of a cyber-attack, a malfunction occurred in the system, a human-error, or many other possible causes. Therefore, identifying risks, determining precautions against them, and defining actions to be taken to mitigate them once they occur are crucial to increase the cyber resilience and reliable operation of critical infrastructures.

Risk management frameworks lay out methodologies and instructions on how to apply risk management in an organized way to ensure risks are treated well enough to mitigate any possible harm to an extent as most great as possible. NIST RMF (Risk Management Framework) is one of existing risk management frameworks, and it consists of 7 main steps, namely, prepare, categorize, select, implement, assess, authorize, and monitor [23].

NIST, in its Guide to Industrial Control Systems (ICS) Security publication, describes how to apply NIST RMF to industrial control systems [24]. Application of NIST RMF on ICS environments is discussed in context of 4 steps, namely, categorize, select, assess, and implement.

NIST advises that systems and network assets should be categorized with a focus on systems used in the ICS environment. The categorization process is advised to be differentiate devices and systems such as PLCs, HMIs, DCS, and SCADAs. Moreover, list of assets in the ICS environment is advised to be updated at least once a year, and each time an asset is added to or removed from the environment [24].

At the select step of risk management for ICS, as advised by NIST, security controls to be applied are to be selected by taking into account ICS environment’s categorization, and selected security controls should be listed in security plan of ICS environment [24].

NIST suggests, at assess step, performing risk assessment by identifying possible impacts -as results of any possible harm to ICS environment- to operations and assets of the organization, as well as to different organizations and to the country. As a result of risk assessment, vulnerabilities causing risks for security of ICS systems, as well as possible mitigation procedures against those risks, may be identified, and risks should be assessed more than several times [24].

At the implement step, it is advised by NIST to sort the risks with respect to size of their impact and to put effort to

mitigate critical risks first. In order to be able to determine the criticalness of the risks, results of risk assessment should be examined in detail [24].

*D. Detection*

The ability to briefly observe the conditions of all the assets present in critical infrastructure systems is one of the most crucial elements in building cyber resilient infrastructures. Monitoring every second the system is in use and every action taken ensures that the defence set up against cyberattacks has the highest level of resistivity. This includes real-time detection of abnormal activities like unauthorized accesses, unauthorized configuration changes, and unusual network traffic that occurs outside of normal operations.
The development of the cyber security field has resulted in the creation of numerous diverse defence systems. As a result, malicious attackers create and employ brand-new attack strategies every day. In the first quarter of 2021, 74% of cyberattacks were zero-day attacks [25]. New cyberattacks that render cyber security measures useless appear every day. Considering the expanding attack surfaces and growing attack channels, enterprises are increasingly at risk from cyberattacks as time goes on.

One cyber defence strategy is insufficient to fend against the evolving and increasingly sophisticated cyberattacks that occur daily. It is necessary to develop a cyber defence infrastructure with a variety of strategies and solutions in order to perform a cyber defence at a high degree of resistivity and maturity. Using various techniques enables the detection of various cyberattack kinds. Establishing cyberattack detection systems for systems in the field of operational technology is equally crucial to constructing cyber defence infrastructures as it is for systems in the field of information technology. To identify cyberattacks conducted on OT devices, various techniques have been developed [26]. Industrial control systems can be kept cyber-secure using solutions for signature and anomaly-based detection that should be positioned inside the network topology, just like in the field of information technologies [26]. By comparing the network traffic with the models built using signatures belonging to known cyberattacks, signature-based solutions can determine whether or not similar attacks have been carried out [27]. While signature-based solutions are effective at identifying known attack types, they are unable to identify zero-day attacks that they come across for the first time. By utilizing anomaly detection tools, which can spot unusual system behavior brought on by zero-day attacks, the range of detectable attack routes should be expanded. Artificial intelligence techniques should be used to develop anomaly detection systems that model the system's usual state and determine whether or not the system deviates from it more than a predetermined rate by tracking network traffic [27]. A complete cyber infrastructure for the detection of cyber-attacks should be developed by using hybrid approaches that combine signature-based and anomaly-based detection technologies.

A variety of assets found across an organization may be the target of cyberattacks. Devices identified in various parts of the organization may therefore serve as the initial point of each attack. Taking control of workstations and endpoints that are running an operating system, causing harm to the system's functionality, or leaking information by altering network traffic, are the basic beginning points for cyberattacks. In order to defend critical infrastructure systems against cyberattacks, developing solutions for endpoint security is just as crucial as developing those that analyze network traffic.

Cyberattacks are less likely to inflict system harm if they are discovered as soon as they occur. To safeguard crucial infrastructures from cyberthreats, endpoint and network traffic security solutions should be created for the fastest possible detection of cyberattacks. Once a cyber-attack starts and becomes successful to penetrate the system, every moment with the intruder inside the system causes a great risk for accessibility, integrity, and confidentiality of cyber systems of an organization. For critical infrastructures, this risk becomes even greater. Therefore, decreasing the probability of a cyber-attack attempt being successful as much as possible in a time interval as narrow as possible is of great importance.

One way to achieve this is to perform access management to make sure that no user has more privilege than they need. This may make it harder for attackers to gain as much access as they need to perform a successful cyberattack, e.g., taking possession of a user with limited access may not be useful for an attacker until a privilege escalation attempt becomes successful, which is a situation that make attackers lose time while making cyber operations centres have more time to interfere with and prevent the cyber-attack attempt. Access management is the management of access privileges assigned to users such that each user has restricted amount of access privileges, just enough to perform the tasks assigned to them. Privileged Access Management (PAM) software technologies should be used to manage the privileges of users, as well as to prevent data breaches [28]. PAM software also makes it possible to monitor activities performed by the users. This is an important information to have for tracking the activities being performed. In case of a cyberattack, if a user account is compromised by an attacker, analyzing the activities performed by the attacker becomes much easier by monitoring the activities done by the compromised user thanks to sophisticated activity monitoring properties of PAM software. Therefore, activity monitoring information gathered from PAM software can be of great importance for SoC teams for interfering with an occurring cyberattack or analyzing a cyberattack after it has happened.

Managing accesses of users is not enough on its own to ensure cyber security of critical infrastructures. Restriction of the incoming and outgoing network traffic is crucial to establish a resistant cyber-secure environment. With the fact that industrial control systems become more and more reachable from outside nowadays for the sake of monitoring them easily, protecting the devices located in critical infrastructure areas from prohibited access incoming through the public network has become an important problem to tackle. It is known that cybersecurity of a contemporary substation can be improved by using a firewall [29]. Firewalls provide protection to a good extent in terms of keeping unwanted traffic outside the internal network of organizations, which is an important factor in preventing attackers from easily communicating with the devices and networks found in the targeted systems. Therefore, using firewall technologies is an important component of ensuring cyber security of critical infrastructures.

Not all of the devices found in a critical infrastructure environment need the same network restrictions and protections. To be able to better manage the communications

within the critical infrastructures and to create a more robust environment in terms of cyber security, network segmentation should be used. Network segmentation is the process of dividing a big computer network into several segments, typically to increase security. This technique, when used appropriately, is one of the most efficient ways to lessen the attack surface of cyber attackers in the event of an infiltration [30]. Network segmentation makes it possible to manage and rule each sub-network separately, e.g., critical devices and servers may be in a tightly restricted sub-network while devices and servers communicating with the public network are located in a sub-network where communication with the public network is possible. Granular network segmentation is a type of network segmentation where devices are located in well-separated networks, and it should be preferred in critical infrastructures to directly prevent almost half of the incoming cyberattacks [30]. Despite all the precautions taken in terms of network and system configurations and cyber security technologies, sophisticated cyber-attacks may still bypass these systems, which means that taking precautions does not guarantee that penetration of the attackers into the system will be avoided. Even though the attackers are avoided before they can penetrate, having information regarding what kind of cyber-attack vectors have been tried on the system is important to know for identifying which parts of the system should be strengthened against cyber threats. Therefore, being able to detect intrusions along with the attempts performed by the attackers is a required skill to have cyber-secured critical infrastructure systems. Intrusion detection systems (IDS) are systems that track and log abnormal network activities along with events occurred in the network by monitoring network traffic. Therefore, they should be used as important components of cyber security systems of critical infrastructures since they provide crucial intelligence to cyber operations centers. Intrusion detection can be performed by using software performing signature-based detection such as Snort [31] and Suricata [32], while machine learning techniques such as Naïve Bayes, Multilayer Perceptron, AdaBoost, etc. can also be applied to perform network intrusion detection, where the detecting intrusion is considered to be a supervised learning problem with nominal and numerical attributes, with the aim of performing multi-class classification [33].

### *E. Security Monitoring*

Events that compromise a system's integrity, accessibility, and efficiency are known as “cyber security events.” These events are those that deviate from a system's normal behavior. A cyber security incident that arises from the routine or expected behavior of a system does not always indicate that a cyberattack has taken place. Each day, an organization creates hundreds of event records. These event logs must be monitored, and it must be decided whether or not they suggest a risk to cyber security. Additionally, necessary safeguards and procedures must be taken to protect against any situations that could provide a threat to cyber security. They should compile and analyze on a centralized management system all asset data and records pertaining to the communications they carried out. Cyber cases may arise from cyber security threat incidents. A cyber case is a cyber incident or series of events that affects or has the potential to affect the assets or services of a critical infrastructure system [34]. In contrary to cyber occurrences, cyber incidents can have negative repercussions on enterprises. As a result, cyber cases must be found as soon as possible, and the required action plan must be developed and put into practice. Systems that contain many cyber security solutions are known as cyber defense substructures, and they are prevalent in critical infrastructures. The cyber defense substructure becomes more complex with each new cyber security solution deployed, making system monitoring more difficult. Given the complexity and multi-stage structure of modern cyberattacks, it becomes clear that in the majority of cases, it is possible to detect these attacks by examining the outputs of many defense solutions. Cyber operation centers should be developed where the defense solutions are regulated and monitored in order to guarantee the cyber security of critical infrastructures. Analysts, operators, and administrators keep an eye on a system's infrastructure, applications, services, and defense mechanisms in cyber operation centers in order to spot and stop cyberattacks, close security gaps, and handle other cyber incidents [35]. Switches, firewalls, servers, IT devices, SCADA systems, PLCs, OT devices, and other critical infrastructure components all generate logs. These logs are frequently kept in the local storage of these devices. This makes it difficult to monitor and track the system from a single location. Collection of logs, which is the first and most crucial stage of monitoring, should be carried out to avoid this issue. Log collection is performed to gather the information stored on local storages together in a collective storage so that the analysis of logs coming from different sources can be carried out in a central manner [35]. It is important that SoC monitors the analyses of collected logs on a regular basis so that any possible cyber threats can be detected while cyber events also get processed before it is too late. Since SoC is the main department responsible for monitoring logs, the log files stored in devices should be transferred to central log storages located in SoC. Choosing methods to follow for collecting logs is an important decision when it comes to performing log collection effectively. There are two main methods to collect logs, namely, agent-based and agentless. It is not possible to assert that one is superior to the other for all possible systems since these methods have different advantages and disadvantages for different systems [36]. Agent-based log collection is performed by installing agent software to servers that are aimed to be monitored, whereas agentless log collection is realized through requests sent from the log collection center to APIs provided by monitored devices. While agent-based log collection method provides much more information than agentless log collection can provide, the latter is much easy to deploy and use than the other since installing agents on each server to be monitored is not always an easy task. Moreover, some devices’ logs cannot be collected using the agent-based log collection method, such as network devices. In those cases, using agentless log collection is a better option, whereas in other cases, agent-based collection solutions are preferable due to large amount of information they can provide. In critical infrastructures, using a log collection environment consisting of both agentless and agent-based log collection techniques seems reasonable since they contain many different types of devices for which the need to collect logs may emerge. So, for components for which it is possible to install agent software easily, using agent-based log collectors is the way to choose, whereas for components for which it is either hard or impossible to use agent-based log collection solutions, using agentless log collectors is the correct option.

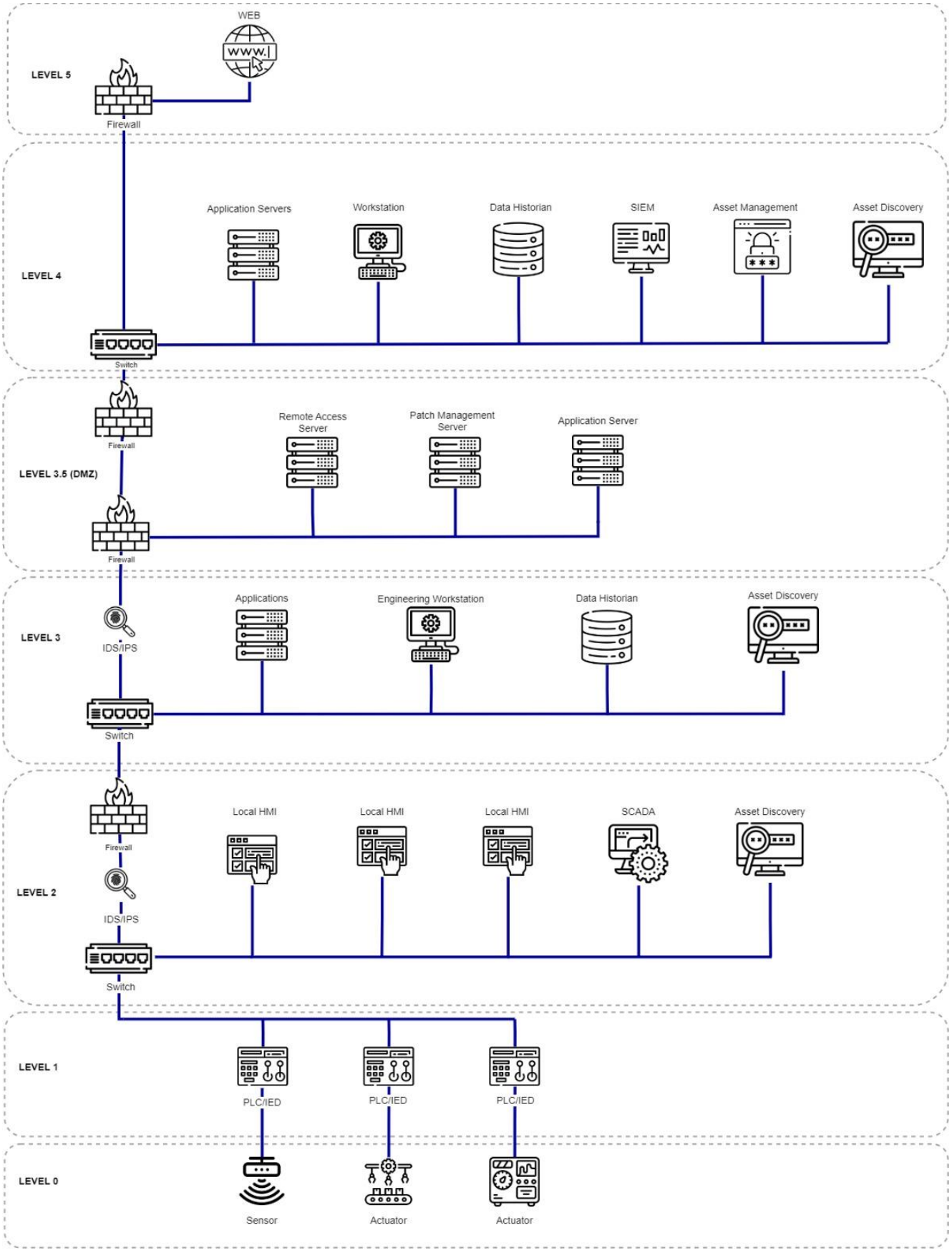


Fig. 2 Architecture of Critical Infrastructure with Cybersecurity Solutions

Collecting logs to a central storage is not enough to detect and mitigate cyber threats on its own. Analysis of the cyber event logs is of crucial importance to detection, mitigation, and prevention of cyber threats since the analysis results obtained from event logs provide the necessary information to be able to deal with cyber threats as much as possible. Manual inspection of these logs is error prone. Moreover, analysis of immense amount of logs, which is the case nowadays, by humans is much far from being possible [35]. In order to make automated analysis of cyber event logs possible, Security Information and Event Monitoring (SIEM) solutions should be used by SoC teams. SIEM solutions aim to identify anomalous events and activities by inspecting and analyzing event logs [37]. For analyzing the logs, there are three main approaches. These are called automated, semi-automated, and hybrid analyses. In automated analysis, only automated tools are used, which implies that humans do not intervene with the analysis of the tool. In semi-automated analysis, both automated and manual analyses take place. On the other hand, hybrid analysis consists of automated analysis where in decision making, humans also take place. Hybrid analysis should be preferred since it provides the best means to perform analysis in the sense that the monitoring can be performed in such a way that it is both uninterrupted and trustable enough in terms of protection that it provides. SIEM solutions can be used together with machine learning algorithms, where the dataset for training the machine learning algorithms are collected from SIEM systems, and the trained machine learning algorithms can be used to produce intrusion predictions, which is useful to predict an attack before it actually occurs [38]. Also, the operators in critical infrastructures can be notified by using machine learning algorithms on whether there is an occurring anomaly and what type of anomaly is predicted to be occurring [39].

## V. ARCHITECTURE OF CYBER RESILIENT CRITICAL INFRASTRUCTURES

Cyber resilience is achieved by integrating several cyber security solutions. Security solutions are organized into several infrastructure segments based on their functions. Cyber resilience in critical infrastructure can be improved by managing all solutions in a single security operation center. Purdue model is a model that describes how the devices in critical infrastructures should be separated into different network segments. In Purdue model, there are 6 levels in total, from level 0 to level 5, and one additional level is actually there to strengthen separation between level 3 and level 4, which is called level 3.5 [40]. IT devices are located at upper levels, whereas OT devices are located at lower levels. The level 0 is the physical process level, where the fundamental physical components of the infrastructure are found, such as actuators. At level 1, intelligent devices that can sense and manipulate physical processes are found, whereas control systems such as SCADA are found at level 2. Level 3 consists of manufacturing operations systems, and level 3.5 is the “demilitarized zone” that is crucial to ensure that communication between IT and OT sides are well separated. Corporate IT is found at level 4, while cloud access is at level 5 [40]. Applying Purdue model is required to strengthen the cybersecurity of critical infrastructures since it is a special type of network segmentation model designed especially for critical infrastructures. First and primarily, it must be determined which assets the critical infrastructure have. To achieve this, asset discovery and management solutions, which will be located separately in the IT and OT segments, can be used to discover assets and monitor their status. This solution can detect changes made to asset configuration by unauthorized users. It will also make it easier to detect system failures. Other procedures such as vulnerability management and risk management will be easier to complete if assets are visible.

Asset management, vulnerability management, and risk management are all passive approaches to increasing cyber resilience. In order to present an effective defense against cyber attacks, active solutions should be used as well as passive methods. For this, IT and OT should be segmented in network topology. A firewall should be used to control the transitions between IT and OT segments. Furthermore, by placing a firewall between Level 2 and Level 3 in the OT segment, it will provide additional protection for the security of the devices in the field, even if attackers infiltrate the OT segment. Also, network traffic analysis can be done with IDS/IPS systems to be placed in front of or behind firewalls. In this way, abnormal network traffic that is not blocked by the firewall and caused by the activity of the attacker can be detected. In addition to traditional signature-based detections on this network traffic, artificial intelligence-based behavior analysis detection systems can be used to provide more advanced protection. With the access management solutions to be used, the authorizations in the IT and OT segments can be controlled from a single point, and access to physical devices in the OT area can be controlled. All cyber security solutions generate event records. These event logs should be collected and stored on a centralized server. As a result, the outcomes of various solutions can be correlated, and analyses can be performed. SIEM solutions should be used for achieving this capability. Administrators can be notified and incident response procedure can be applied by monitoring all event records in SIEM in the case of cyber incidents. The criteria in international cyber security standards for critical infrastructures can be met by the system we suggested on the Purdue model. Different cyber security solutions offer advantages in meeting various criteria. A comprehensive cyber security platform can be established and cyber resilience can be increased by placing all solutions in accordance with the suggested approach shown in Fig. 2.

## VI. CONCLUSION

Critical infrastructures are essential systems that support the continuity of the social and economic system as well as the health and safety of society. Critical infrastructure destruction from either the inside or outside will have a negative impact on a nation's social structure, harm its standing abroad, and undermine its legitimacy. Systems with multiple physical and virtual components from the information and operational technology domains compose critical infrastructures. In the past, closed networks were used to administrate industrial control systems, which include the majority of hardware, devices, and automation tools in the field of operational technology. The disciplines of information and operational technology have converged as a result of the digital transformations performed as of the 21st century, and industrial control systems are now available over the internet. This convergence has revealed industrial control systems' weaknesses, increased the attack surface for cyberattacks on critical infrastructures, and made operational technology systems' vulnerabilities the main target of cyberattacks. Nations should protect their critical infrastructures against cyber threats to guarantee security of critical infrastructures.

Since critical infrastructures are vital to countries and societies, critical infrastructure cyber security should be regarded as a national security issue. Nations should invest adequately in the necessary technologies while developing cyber security policies for their critical infrastructure. To support the security of operational technology devices, the breadth of information technology cyber security solutions must be expanded. Important data in the IT and OT areas, as well as hardware, software, and other resources, must be under the supervision of cybersecurity system that will be placed in critical infrastructures. To identify the assets' vulnerabilities, the data obtained during asset management should be compared to the most recent vulnerability lists. Prioritizing the actions required to address the vulnerabilities is crucial due to dangers that they present. To identify cyberattacks in real time, solutions based on signature and anomaly-based attack detection should be developed in addition to the system's current vulnerabilities. To avoid management issues that could develop as a result of each new solution making the cyber defense platform more complex, the complete cyber defense platform should be controllable from a single center. Thus, cyber risks can be better studied, cyber attack detection times can be reduced, and cyber cases can be handled faster by combining visualization, control, analysis, and management from a single operation center.

## REFERENCES


[1] "Operational Technology (OT)." Gartner, Gartner, www.gartner.com/en/information-technology/glossary/operational-technology-ot. Accessed 15 Jan. 2023.

[2] Clinton, William Jefferson. "Executive order 13010-critical infrastructure protection." Federal register 61.138 (1996): 37347-37350.

[3] Shah, Rajiv. Protecting critical national infrastructure in an era of IT and OT convergence. Australian Strategic Policy Institute, 2019.

[4] Hemsley, Kevin E., and E. Fisher. History of industrial control system cyber incidents. No. INL/CON-18-44411-Rev002. Idaho National Lab.(INL), Idaho Falls, ID (United States), 2018.

[5] Rrushi, Julian, et al. "A quantitative evaluation of the target selection of havex ics malware plugin." Industrial control system security (ICSS) workshop. 2015.

[6] Farwell, James P., and Rafal Rohozinski. "Stuxnet and the future of cyber war." Survival 53.1 (2011): 23-40.

[7] "Threat Landscape for Industrial Automation Systems in H1 2021." Securelist, Kaspersky Lab, securelist.com/threat-landscape-for-industrial-automation-systems-in-h1-2021/104017/. Accessed 17 Jan. 2023.

[8] Bristow, Mark. "A SANS 2021 Survey: OT/ICS Cybersecurity." eng. In (2021).

[9] "Understanding IEC 62443." IEC, International Electrotechnical Commission, www.iec.ch/blog/understanding-iec-62443.

[10] Cybersecurity, Critical Infrastructure. "Framework for improving critical infrastructure cybersecurity." URL: https://nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP 4162018 (2018).

[11] "Cybersecurity Capability Maturity Model (C2M2)." Energy.gov, U.S. Department of Energy, 2023, www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2. Accessed 18 Jan. 2023.

[12] Wedgbury, Adam, and Kevin Jones. "Automated asset discovery in industrial control systems-exploring the problem." 3rd International Symposium for ICS & SCADA Cyber Security Research 2015 (ICS-CSR 2015) 3. 2015.

[13] Mytilinaios, Artemis, Michel van Veen, and Pavlos Lontorfos. "Real time asset inventory in ICS." (2021).

[14] Lal Rajora, Gopal, Miguel A. Sanz-Bobi, and Carlos Mateo Domingo. "Application of Machine Learning Methods for Asset Management on Power Distribution Networks." Emerging Science Journal 6.4 (2022): 905-920.

[15] Adebayo, Abimbola, Mhd Saeed Sharif, and Wael Elmedany. "The Role of Artificial Intelligence in Asset Management of Enterprise Systems." 2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT). IEEE, 2022.

[16] Mir, Yawar Rasool, and Navneet Kaur Sandhu. "Port Scan Detection using AI." (2019).

[17] Guevara, Isaac, and Chen Fradkin. "Growing ICS vulnerabilities mandate prioritization: Use vulnerability management at the convergence of information and operational technologies to lower risk to industrial control systems." Control Engineering 68.2 (2021): 31-34.

[18] "The Ultimate Guide to OT Vulnerability Management." Verve Industrial, verveindustrial.com/resources/guide/the-ultimate-guide-to-ot-vulnerability-management/. Accessed 20 Jan. 2023.

[19] Yosifova, Veneta, Antoniya Tasheva, and Roumen Trifonov. "Predicting vulnerability type in common vulnerabilities and exposures (CVE) database with machine learning classifiers." 2021 12th National Conference with International Participation (ELECTRONICA). IEEE, 2021.

[20] Yosifova, Veneta. "Vulnerability Type Prediction in Common Vulnerabilities and Exposures Database with Ensemble Machine Learning." 2021 International Conference Automatics and Informatics (ICAI). IEEE, 2021.

[21] Khan, Saad, and Simon Parkinson. "Review into state of the art of vulnerability assessment using artificial intelligence." Guide to Vulnerability Analysis for Computer Networks and Systems: An Artificial Intelligence Approach (2018): 3-32.

[22] Kaplan, Stanley, and B. John Garrick. "On the quantitative definition of risk." Risk analysis 1.1 (1981): 11-27.

[23] "About Risk Management Framework (RMF)." NIST Computer Security Resource Center, National Institute of Standards and Technology, csrc.nist.gov/projects/risk-management/about-rmf. Accessed 12 Mar. 2023.

[24] National Institute of Standards and Technology. "Guide to Industrial Control Systems (ICS) Security." NIST Special Publication 800-82 Revision 2, U.S. Department of Commerce, 1 May 2015, doi: 10.6028/nist.sp.800-82r2.

[25] "Zero-Day Malware: Q1 2021." Help Net Security, 29 June 2021, www.helpnetsecurity.com/2021/06/29/zero-day-malware-q1-2021. Accessed 20 Jan. 2023.

[26] Murray, Glenn, et al. "Detection techniques in operational technology infrastructure."(2018).

[27] Fernandes, Gilberto, et al. "A comprehensive survey on network anomaly detection." Telecommunication Systems 70 (2019): 447-489.

[28] Purba, Anton, and Mohammad Soetomo. "Assessing Privileged Access Management (PAM) using ISO 27001: 2013 Control." ACMIT Proceedings 5.1 (2018): 65-76.

[29] Anderson, Dwight, and Nathan Kipp. "Implementing firewalls for modern substation cybersecurity." proceedings of the 12th Annual Western Power Delivery Automation Conference, Spokane, WA. 2010.

[30] Korman, Matus, et al. "Analyzing the effectiveness of attack countermeasures in a scada system." Proceedings of the 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids. 2017.

[31] "Snort." Snort.org, snort.org. Accessed 21 Jan. 2023.

[32] "Suricata." Suricata, suricata.io. Accessed 21 Jan. 2023.

[33] Hamid, Yasir, M. Sugumaran, and Ludovic Journaux. "Machine learning techniques for intrusion detection: a comparative analysis." Proceedings of the International Conference on Informatics and Analytics. 2016.

[34] Klaver, Marieke, and Eric Luiijf. "Analyzing the cyber risk in critical infrastructures." Issues on Risk Analysis for Critical Infrastructure Protection. IntechOpen, 2021.

[35] Onwubiko, Cyril. "Cyber security operations centre: Security monitoring for protecting business and supporting cyber defense strategy." 2015 international conference on cyber situational awareness, data analytics and assessment (cybersa). IEEE, 2015.

[36] Pandey, Himanshu, and Er Kushagra Mittal. "Analogy between Agent Less Monitoring and Agent Based Monitoring." Reliability: Theory & Applications 15.3 (2020): 117-124.

[37] Wenge, Olga, et al. "Security information and event monitoring as a service: a survey on current concerns and solutions." PIK-Praxis der Informationsverarbeitung und Kommunikation 37.2 (2014): 163-170.

[38] Anumol, E. T. "Use of machine learning algorithms with SIEM for attack prediction." Intelligent Computing, Communication and Devices: Proceedings of ICCD 2014, Volume 1. Springer India, 2015.

[39] Hindy, Hanan, et al. "Improving SIEM for critical SCADA water infrastructures using machine learning." Computer Security: ESORICS 2018 International Workshops, CyberICPS 2018 and SECPRE 2018, Barcelona, Spain, September 6–7, 2018, Revised Selected Papers 2. Springer International Publishing, 2019.

[40] Garton, D. "Purdue Model Framework for Industrial Control Systems & Cybersecurity Segmentation." U.S. Department of Energy, 14 Oct. 2022, www.energy.gov/sites/default/files/2022-10/Infra_Topic_Paper_4-14_FINAL.pdf. Accessed 21 Jan. 2023.