Journal of
Cybersecurity and Privacy

MDPI

Article

A Risk Assessment Analysis to Enhance the Security of OT WAN with SD-WAN

Van Joshua Abergos and Faiza Medjek *

Department of Computer Science and Creative Technologies, University of the West of England, Frenchay Campus, Bristol BS16 1QY, UK; van2.abergos@live.uwe.ac.uk
* Correspondence: faiza.medjek@uwe.ac.uk

Abstract: This paper introduces a comprehensive risk assessment of various wide area network (WAN) technologies as applied to Operational Technology (OT) infrastructures, thus uncovering which WAN technology is best suited for OT to mitigate the risks of Denial of View (DoV), Denial of Control (DoC), and Denial of Service (DoS). A new risk weight-based evaluation approach is proposed following NIST CSF and ISA/IEC 62443 standard risk scoring (RS). In this approach, RS was modified by introducing new risk metrics, namely, risk (Rn), mitigation (Mm), risk prioritization (WRn), and mitigation prioritization (WMm) to create a specialized probability formula to assess risks on OT WAN infrastructure. The proposed formula has been implemented to automate data analysis and risk scoring across nine WAN technologies. The obtained results demonstrated that software-defined wide area network (SD-WAN) has the best security features that even overshadow its vulnerabilities to perform not just as a WAN solution but as a security solution against DoV, DoC, and DoS. Furthermore, this paper identifies and highlights what to prioritize when designing and assessing an SD-WAN setup. In addition, this paper proposes an SD-WAN-based architecture to reduce DoV, DoC, and DoS risks.

Keywords: operational technology (OT); industrial control systems (ICS); cyber physical systems (CPS); risk assessment; prioritization; software-defined wide area network; SD-WAN; OT security

check for updates

Citation: Abergos, V.J.; Medjek, F. A Risk Assessment Analysis to Enhance the Security of OT WAN with SD-WAN. *J. Cybersecur. Priv.* **2024**, *4*, 910–937. https://doi.org/10.3390/jcp4040042

Academic Editor: Christos Bouras

Received: 25 August 2024
Revised: 2 October 2024
Accepted: 7 October 2024
Published: 10 October 2024

1. Introduction

The adoption of Industry 4.0 marks a new phase of digital transformation in manufacturing companies. This change involves using new technologies and innovations to improve manufacturing processes through automation and smart technologies [1] (pp. i-412). The benefit of this industrial transformation is that it offers better performance and scalability in manufacturing industries. Small to large enterprises yield an increase in efficiency, productivity, and quality of output, which in turn directly or indirectly help in cost management for manufacturing companies [2] (pp. 1415–1420). What entices the move to adopt Industry 4.0 are the benefits of seamless integration of physical and digital components using technologies like cyber-physical systems (CPSs), the Internet of Things (IoT), and robotics. This integration provides better predictability allowing more control and easier data management. This is made possible by technologies like big data analytics, cloud computing, and cybersecurity to optimize operations and decision-making further. The adoption of this emerging technology shows how important data are and how critical it is for the industry revolution. The increasing connectivity and data exchange in Industry 4.0 systems emphasize security to data privacy being crucial [3] (pp. 2797–2810). Sensitive data can be stolen or be rendered unusable if left unprotected. While improved connectivity and real-time data exchange between operational technology (OT) and IT systems enhance the OT availability, they also expand the threat landscape, exposing these systems to new security risks [4].

OT differs in security priorities compared to IT which focuses on safety, availability, and integrity (SAI) as opposed to the CIA Triad [5]. The SAI has been derived from the security lifecycle for Industrial Automation and Control Systems (IACS) [6]. Given that it shows how critical availability is, failing it imposes risk on both the safety and integrity of the industrial control systems (ICS)and cyber physical systems (CPS) [7]. Thus, it is important to understand how denial on ICS and CPS works. There are three denial attacks on ICS and CPS based on MITRE | ATT&CK which are Denial of Control (DoC), Denial of Service (DoS), and Denial of View (DoV) [8–10]. DoV disrupts the monitoring of ICS and CPS environments. This attack remains unnoticeable and recovers to normal once the adversary has completed the motive [11]. DoC prevents ICS and CPS operators from interacting with the process controls, leaving it momentarily unmanageable during the said attack [12] (pp. 249). The most crucial is DoS, which disrupts expected or natural device functionality and, in the worst case, would lead to ICS and CPS Permanent Denial of Service (PDoS) since IPS/ICS devices are sensitive to environmental change and can easily be manipulated [13,14].

To achieve near 100% availability, ICS and CPS will need to implement several critical strategies and best practices developed from established standards. For example, ensure that important components have backups that can take over in case of failure through the use of redundant systems and data storage, as well as the use of redundant pathways of communication to avert a single point of failure [15]. Additionally, the design of fault-tolerant systems results in continuous operation even if some of the components fail; this makes the network resilient to unanticipated downtime [16]. Equipment downtime can be significantly minimized with regular maintenance checks, this ensures that systems are maintained with up-to-date security patches against known vulnerabilities [17,18] (pp. (437–465). Another best practice is to divide a network into segments so it can contain breaches and limit their impact [16,19–24]. Network segmentation should isolate critical systems from IT networks, thus further limiting the adversary's entry-point to OT either on public or corporate IT networks [8–10,25]. Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs) deployments do provide consistent tracking of system activity and network traffic [26,27] (pp. 18–28). High system availability can be maintained by effectively responding to and mitigating incidents by utilizing a well-prepared and -maintained incident response plan, which is also frequently updated based on past incident resolutions [19]. Access to systems having critical information can also be restricted by deploying strong access controls, including role-based access controls (RBACs) [28,29] (pp. 185–233). For instance, multi-factor authentication (MFA) is what helps to limit access to any data-sensitive systems by authorizing only a few individuals who are truly required to access the device, thus enhancing security and minimizing the risk of unauthorized access and other possible disruptions [19,28,29] (pp. 185–233). Ongoing security training for employees should include policies, procedures, and incident response in relation to security. Promoting security awareness also makes sure that all staff members are aware of their responsibilities for upholding security and are knowledgeable of prominent threats [30,31] (pp. 133–144), [32] (pp. 289–296).

1.1. Existing Limitations

Manufacturing businesses operate in remote areas, which makes status visibility and data backup difficult. When exploited, these vulnerabilities may result in DoV (Technique T0815), DoC (Technique T0813), and, worse, DoS [8–12]. Threats include possible natural disasters and other unfavorable events in addition to cyberattacks, which could prevent the provisioning of manufacturing services. Available options at this time, such as integration with third-party networks, are reliant on the provider's accessibility in the region and may require the private entity's willingness to give up control over OT traffic management to a third party or vendor. Data integrity may be jeopardized by possible third-party issues [33] (pp. 47–54), [34] (pp. 4543–4572), [35] (pp. 680–693).

The research community has been actively exploring both software-defined network (SDN)-based network security and the security of the SDN architecture, as highlighted in [36]. Additionally, cybersecurity mechanisms within software-defined wide area networks (SD-WAN) architectures have been examined, comparing private and open-source solutions [37,38]. However, to the best of our knowledge, and as will be discussed in the Related Works Section, existing research primarily focuses on the CIA triad and IT infrastructure, without adequately assessing the effectiveness of SD-WAN in mitigating prevailing cybersecurity risks within OT infrastructure. Moreover, current studies rely on simulation tools to evaluate the security capabilities of SDN and SD-WAN, focusing on their functionalities rather than mapping them to OT-specific risks. Most SDN studies concentrate on LAN traffic analysis, whereas this paper emphasizes SAI and the risks associated with extending OT infrastructure using WAN technology. In other words, this paper highlights the importance of analyzing a reliable and secure OT WAN infrastructure for data management and visibility across remote manufacturing sites.

1.2. Contributions

The purpose of this paper is to investigate the risks and current mitigation (mitigation is defined as risk mitigation for OT WAN mitigating risks on DoV, DoC, DoS) efficiency of using SD-WANs, a manufacturing-owned cloud network, to increase the security and availability of OT Networks with a focus on DoV, DoC, and DoS attacks. In this paper:

1. A new risk assessment approach is introduced based on NIST CSF and ISA/IEC 62443 standards. The proposed risk-scoring approach allows for predicting risk based on security standard requirements and present vulnerabilities.
2. A program has been implemented to automate the scrutinization of eight different WAN technologies against SD-WAN to understand the possible gaps of an OT WAN infrastructure and highlight the security advantages of using SD-WAN to secure such infrastructure. The selected technologies are Satellite WAN, LoRaWAN, Private LTE/5G Networks, MPLS (Multiprotocol Label Switching), Leased Line, DMVPN (Dynamic Multipoint Virtual Private Network), IPSec VPN (Internet Protocol Security Virtual Private Network), and VPLS (Virtual Private LAN Service).
3. The suitability of all studied WAN technologies in terms of risks and mitigations related to DoC, DoV, and DoS attacks is highlighted.
4. Two designs of an OT-WAN-based network using SD-WAN and following the PURDUE model are introduced.

1.3. Paper Organization

The rest of this paper is organized as follows: Section 2 discusses the related works and highlights the gap in the literature pertaining to SD-WAN's actual effectiveness compared to existing OT WAN, with a focus on security. Section 3 describes the background underpinning the OT risk-assessment framework and contributes to the proposed approach. Section 4 explains the methodology of how our proposed risk-scoring mechanism tests and calculations have been carried out to compare the nine selected OT WAN technologies. Section 5 illustrates the findings. Finally, Section 6 concludes the paper.

2. Related Works

SD-WAN is recognized in OT networks since it is among the major enablers of IT infrastructures [39] (pp. 1–9). SD-WAN ensures safe, uninterrupted operations while providing protection against cyber threats [40]. As a result, it enhances the availability of ICS and CPS, which is essential for advancing along the Industry 4.0 path. A key advantage of SD-WAN is its ability to provide centralized security management, enabling consistent application and real-time monitoring of security policies across all network segments. This ensures that there is no extended exposure to potential threats [40,41] (pp. 14–76). Further, SDN, a parent category of SD-WAN, eases network segmentation by isolating critical ICS/CPS components, helping contain lateral attackers' movement in line with industry standards [42]. This includes integrating security features into SD-WAN, such as next-generation firewalls, secure web gateways, and anomaly traffic detection for comprehensive security coverage [43]. SD-WAN also offers advanced threat detection and response capabilities, including IDS, IPS, and real-time threat intelligence, enabling effective cyber-attack detection and prevention. Additionally, SD-WAN platforms provide real-time analytics and access to threat intelligence feeds, facilitating proactive threat management [23,24]. Data-in-transit are further secured with encrypted tunnels and a zero-trust model, ensuring only authenticated and authorized entities can access resources or network traffic. To safeguard against tampering, SD-WAN employs authentication certificates and mutual TLS encryption, strengthening communication security and ensuring network integrity. Furthermore, SD-WAN configurations are secured through profiles managed by a cloud controller, preventing unauthorized configuration changes on physical or edge devices. This ensures that only centrally authorized and managed configuration modifications are allowed, effectively mitigating the risk of local tampering [21,22].

2.1. SDN-Related Research

Most existing SDN papers have explored or demonstrated the capabilities of SDN in modern networks.

2.1.1. SDN Non-Security Related

A study on SDN emphasized the use of SDN programmability to achieve network traffic redundancy by connecting multiple data centers for high availability, rather than relying on numerous links from different internet service providers, and by establishing a centralized controller [44] (pp. 479–484). Another paper proposed utilizing a multipath routing technique within an SDN, which was simulated on a small network to demonstrate SDN's faster reaction time and programmability compared to static routes, dynamically responding to network topology changes during unexpected events or disasters [45] (pp. 478–483). Additionally, the study in [46] (pp. 1–6) focused on SDN-based communication in Smart Grids, highlighting features such as global/local traffic management and application-aware routing. This research introduced the concept of intelligent electronic devices to facilitate efficient data exchange in power line communication distribution networks.

2.1.2. SDN Security Related

The study in [47] (p. 258) focused on the security features of SDN and its deployment in IT/OT-converged networks, particularly IoT environments. The authors explained how SDN responds to DDoS attacks by utilizing dynamic network routing and programmability to assist in decision-making during such incidents [47] (p. 258). Another notable paper proposed to construct an SDN backup and restoration solution to enhance the readiness of organizations to recover from cyber-attacks. The SDN solution was configured within a local area network (LAN), and the backup scheme was simulated using Ryu Controllers within local network premises, with plans to improve it for future applications in wide area and cloud networks [48] (pp. 241–246).

2.2. SD-WAN-Related Research

2.2.1. SD-WAN Non-Security Related

As SDN gained popularity, the need arose to extend the network design to cloud environments and expand its reach across wider WANs. This demand led to the development of SD-WAN, which has since become the focus of numerous studies examining its performance and compatibility with evolving networks. Through a systematic review, the authors in [36] compared the architecture of SD-WAN with that of legacy WANs, providing insights into how SD-WAN overcomes the limitations of traditional networks in response to market demands and emerging network techniques and protocols. Another paper introduced a backup and recovery mechanism utilizing SD-WAN, proposing a method for Distributed Data Backup and Recovery (DDBR). The suggested SD-WAN configuration is implemented across multiple network switches for backing up control plane data [49]. Another backup scheme examines load-balancing optimization of WAN links through OpenNetMon, an open-source dashboard, to enhance bandwidth utilization and facilitate traffic engineering. This article provides an in-depth analysis of SD-WAN features and showcases its effective data backup capabilities [50]. With the increasing demand for cloud networks, the application of SD-WAN in these environments has become widespread. Consequently, one study examined how effectively SD-WAN can enhance network connectivity through its flexibility, scalability, and improved security related to traffic-routing optimization. Another study evaluated the efficiency of SD-WAN in resource provisioning and green energy scheduling within multi-cloud environments [48,51] (pp. 5645–5656).

2.2.2. SD-WAN Security Related

The authors in [36] compared two SD-WAN solutions—Flexiwan and Fortinet—to evaluate their cybersecurity mechanisms in response to common attacks such as man-in-the-middle, DoS, and brute force. The paper concludes that commercial solutions provide superior cybersecurity mechanisms and mitigations. On the other hand, the authors in [37] compared various open-source SD-WAN solutions—Flexiwan, OPNSense, and pfSense—and found that while all three provide comprehensive security features, they also have vulnerabilities that can be addressed. The study in [52] (pp. 1981–1986) explored the applications of SD-WAN within an OT network, emphasizing the use of physical isolation, symmetric key encryption, automated data transfer, and VPNs. The authors underscore the importance of network segregation, point out that certain servers and computers contain sensitive information, and highlight the roles of symmetric key encryption and dynamic data routing in automated data transfer.

2.3. Analysis

While the above- mentioned studies offer valuable insights that contribute to today's research, there is a significant gap in comprehensively analyzing SD-WAN and assessing its effectiveness as a security solution for OT infrastructure, rather than merely viewing it as a network device. Moreover, the existing research primarily employs simulations using various tools to analyze SD-WAN. This paper will evaluate whether SD-WAN is sufficiently efficient as a security solution for OT networks through a security risk assessment, considering the advantages and disadvantages of an extended OT infrastructure in a cloud environment. Additionally, this paper includes a systematic evaluation of selecting a risk management framework tailored to OT, which will be used to test multiple WAN security solutions and identify key variables to consider when choosing a network security solution to enhance the OT WAN infrastructure and bolster security for ICS and CPS.

2.4. Existing Risk-Scoring Techniques

We summarized the different risk-scoring methods in Table 1. This evaluation aims to identify the effectiveness and gaps in current risk-scoring techniques that can be adapted for extending OT WANs. The comparison focuses on different risk-assessment functionalities, including the availability of a ready-to-use formula, existing risk-score-scaling techniques, the incorporation of risk with mitigation scoring, asset-specific assessments, and predictive risk analysis.

Table 1. Comparison of the different related risk-scoring techniques.

Technique	Advantages	Disadvantages	Application in OT	Formula Granularity and Approach	Risk Score Scaling	Includes Risk and Mitigation Scoring	Per Asset Assessment	Predictive Risk Score Analysis
Proposed Risk Scoring (OT WAN Risk Scoring)	Provides comprehensive and granular approach in identifying risk severity and mitigation effectiveness present per WAN device when used in OT.	Focus only on the OT WAN devices.	Efficiently calculate the risks in WAN technologies when used in OT.	Yes— (Detailed in the next sections).	Yes	Yes	Yes	Yes
FTA/ETA	Identifies root causes and potential failure sequences which is good for incident prediction and risk reduction.	Requires detailed knowledge of failure probabilities, which may be hard to quantify.	Applied in OT for predictive analysis of failures and to model cascading impacts on operations.	No— Probability of Top Event = Product of probabilities of all contributing events	Yes	Yes	Yes	Yes

FMEA	Structured, systematic approach; helps prioritize risks based on severity, occurrence, and detectability; useful for identifying critical failure modes.	Can be subjective;
		requires detailed analysis;
		time-consuming to implement across large systems.
			Used in OT to assess potential failure modes of equipment and processes.	Yes—
				RPN = Severity × Occurrence × Detectability.
					Yes	No	Yes	No

QRA	Provides numerical results that support cost–benefit analysis and decision-making; useful in high-risk industries for precise risk quantification.	Requires substantial data and statistical expertise; can be time-consuming and resource intensive.	Applied in safety-critical OT environments such as oil and gas, chemical, and nuclear sectors.	Yes— Probability of Occurrence × Impact; uses statistical models and probabilistic analysis.	Yes	No	No	Yes
CVE-Based Scoring (CVSS)	Widely recognized; standardized scoring; adaptable for OT with environmental modifications.	May not fully capture OT-specific risks like physical safety or operational impact without modification.	Used to evaluate vulnerabilities with environmental modifications to better reflect OT-specific impacts.	No— CVSS Score = Base Score × Temporal Score × Environmental Score	Yes	No	Yes	Yes

Table 1. *Cont.*

Technique	Advantages	Disadvantages	Application in OT	Formula Granularity and Approach	Risk Score Scaling	Includes Risk and Mitigation Scoring	Per Asset Assessment	Predictive Risk Score Analysis
Threat Likelihood and Impact Matrix (Risk Matrix)	Simple visualization of risk; easily understood; allows for prioritization.	Can oversimplify risk; subjective scoring may lead to inconsistencies in results.	Commonly used in OT for its straightforward approach to evaluating and prioritizing risks.	Yes— Risk Score = Likelihood × Impact	Yes	No	No	Yes
HAZOP	Identifies potential hazards and operability issues systematically; highly detailed and structured; widely recognized in process industries.	Requires expert knowledge; can be labor-intensive; qualitative, making numerical comparisons hard.	Commonly used in chemical, oil and gas, and other process industries for hazard analysis.	No— Uses guide words to identify deviations; no direct scoring formula.	No	Yes	No	No
Bow-Tie Analysis	Provides clear visualization of threats and mitigation paths; focuses on prevention and mitigation measures.	Time-consuming to create and interpret; lacks numerical scoring, making comparisons difficult.	Useful in OT for visually mapping cause-effect relationships and mitigation measures in critical systems.	No— Scoring based on risk scenario analysis with predefined preventive and mitigative measures (No direct formula)	No.	Yes	No	No
MITRE ATT&CK for ICS Framework	Maps specific OT attack vectors; highly granular; assists in identifying targeted threats.	No standard numerical scoring; qualitative; requires expert knowledge to interpret results.	Highly specific to OT, providing detailed insights into attack vectors and security control gaps.	No— Scoring based on observed tactics, techniques, and procedures (TTPs) using a scoring rubric.	No	No	No	No

Fault Tree Analysis (FTA) and Event Tree Analysis (ETA) method can predict failures based solely on design, without the need for physical components, by analyzing single failure paths for each asset or event [53] (pp. 83781–83793), [54].

Failure Modes and Effects Analysis (FMEA) prioritizes risks using risk priority numbers but primarily focuses on identifying failures rather than mitigating events. While it performs detailed analysis per asset, it tends to be retrospective and is not typically employed for predictive risk assessments [55] (p. 106480), [56].

Quantitative risk analysis (QRA) applies numerical scaling to assess probability and impact, concentrating on quantifying risk rather than detailing mitigation. QRA usually evaluates scenarios that encompass more than single assets while offering predictions using statistical and probabilistic models [57] (pp. 127–139).

CVE-based scoring or CVSS assigns scores ranging from 0 to 10, with higher scores indicating greater risk. This method evaluates vulnerabilities specific to each asset without considering mitigations, making it suitable for predictive analysis based on known vulnerabilities, which may be vendor-dependent [58] (pp. 353–356), [59] (pp. 4486–4495).

The Risk Matrix is a threat likelihood and impact matrix that operates on a scale from 1 to 25. It primarily assesses risks without explicit mitigation and can be applied for predictions in hypothetical scenarios [60] (pp. 29775–29818).

Hazard and Operability Study (HAZOP) is used for qualitative risk assessment, classifying risks descriptively instead of numerically. It includes safeguard ratings but is generally applied at a system-wide level rather than for individual assets and is not suited for predictive analytics without modifications [61] (pp. 266–279), [62].

Bow-Tie Analysis does not provide direct scoring; instead, it visually represents threats and mitigation measures, displaying them graphically. It broadly maps threats rather than focusing on individual assets, making it more appropriate for mapping existing systems rather than for predictive analysis [63].

The MITRE ATT&CK for ICS Framework does not offer numerical scores, but it does provide a qualitative or descriptive severity scale for various attack techniques. It does not aim to assess the vulnerability of specific assets but rather offers mitigation strategies for identified attack techniques. Designed for operational scenarios, it is not ideally suited for predictive modeling without further component analysis [64] (pp. 1–6), [65] (pp. 1–6).

In summary, current risk-scoring techniques lack a detailed approach for calculating risk while accounting for mitigation factors specific to each WAN device. Most existing methods do not offer predictive risk scoring to evaluate risks and mitigations when a WAN device is deployed in OT, which is crucial during the planning phase before acquiring such devices. This paper proposes a new risk-scoring method to address these limitations. While FTA/ETA is the closest existing technique, it does not provide guidance on how to compute probability variables or how mitigation factors influence risk scoring. This paper will also rectify these issues through the proposed risk-scoring method.

3. Background

3.1. OT Risk Management Frameworks

Critical systems have several notable risk management frameworks in the OT cybersecurity field, which are structured methodologies for securing ICS and CPS. The most popular include the NIST Cybersecurity Framework (CSF), ISO/IEC 27001, ISA/IEC 62443, and NERC CIP. Each of these frameworks has distinct strengths in terms of what aspects of cybersecurity they are designed to help with; in the case of OT environments, NIST CSF and ISA/IEC 62443 are quite popular since they are considered broad and detailed [66] (p. 101677), [67] (pp. 59–72).

The NIST Cybersecurity Framework allows for a broad and flexible approach to cybersecurity by equally covering IT and OT environments. It structures five major core components around the actions of Identify, Protect, Detect, Respond, and Recover. This ensures that risks are well understood and managed in a comprehensive manner and permits an organization to adjust the framework to suit its needs. This allows NIST CSF to be very flexible and have a very wide acceptance base in different industries. These elements also position NIST CSF as applicable in diverse and ever-evolving threats found in OT environments, where flexibility and comprehensiveness in risk management can serve well [17,68].

ISO/IEC 27001 is an internationally accepted standard that gives a rigorous, structured approach to managing information security. Its core component, the Plan–Do–Check–Act cycle, maintains a uniform process of managing and enhancing information security. While ISO/IEC 27001 is largely IT-oriented, its vast documentation depth and compliance requisites can be applied to OT through large efforts. Compliance with several global regulations makes it widely applicable for organizations seeking international compliance. However, its concentration on IT and implementation complexity make the framework less liked by OT users compared to NIST CSF and ISA/IEC 62443 [69].

ISA/IEC 62443 is specifically tailored to address the challenges associated with securing OT (ICS/CPS) systems, which come with unique requirements. The framework is divided into several parts that offer guidelines on various security aspects in ICS, including general concepts, policies and procedures, system requirements, and component requirements. This level of detailed technical guidance ensures that the security requirements for individual components and overall systems are thoroughly developed and robust. The lifecycle approach of ISA/IEC 62443 facilitates ongoing security enhancements from design through operation and maintenance, making it particularly effective for the OT environment, which necessitates specialized security controls. Another notable strength of this framework is its strong sectoral focus, making it highly valued in industries that utilize OT [70].

NERC CIP standards are applicable and mandatory for the whole North American energy sector, focusing on the security of electric utilities. The scope of the standards involves everything from identification of assets to the management of security, personnel training, electronic and physical security, system security management, and even incident reporting. While NERC CIP provides detailed and specific directives regarding its guidelines, its functionality and mandates are exclusively applicable to the energy sector. This targeted nature makes the framework less suitable for use in other OT environments. However, its prescriptive compliance guarantees high levels of security and reliability specifically within its designated sector [71].

In summary, NIST CSF and ISA/IEC 62443 are more inclined toward industrial systems, making them inclusive, flexible, and better suited in an OT environment. While it is broad in applicability and has an emphasis on betterment, NIST CSF allows itself to be tailored toward various industries. In turn, ISA/IEC 62443 elaborates on detailed technical standards, arming it with solid security protocols meant explicitly for OT. Lastly, even though ISO/IEC 27001 is globally accepted and has a structured approach, its best application is when IT environments are addressed alone. In turn, NERC CIP is more sector-specific, relating solely to the energy sector, and it lacks such broad applicability as NIST CSF and ISA/IEC 62443. Table 2 summarizes the differences between the above-mentioned frameworks.

Table 2. Comparison of the different frameworks.

Feature	NIST CSF	ISO/IEC 27001	ISA/IEC 62443	NERC CIP
Focus	Broad, includes IT and OT	Primarily IT, with some OT applications	Specific to ICS and OT	Specific to the energy sector
Core Components	Five Functions: Identify, Protect, Detect, Respond, Recover	Plan-Do-Check-Act (PDCA) cycle	Various parts for different aspects of ICS security	CIP Standards
Industry Adoption	Widely adopted across multiple industries	Widely adopted, especially in IT	Increasing adoption in industrial sectors	Mandated for North American electric utilities

Table 2. *Cont.*

Feature	NIST CSF	ISO/IEC 27001	ISA/IEC 62443	NERC CIP
Flexibility	High, adaptable to various industries and organizations	Moderate, less tailored for OT	Moderate, tailored for ICS but can be complex	Low, highly specific to the energy sector
Regulatory Alignment	Aligns with various regulations and standards	Aligns with ISO standards and some regulations	Aligns with IEC standards and some regulations	Aligns with energy sector regulations
Implementation Complexity	Moderate, with clear guidelines and best practices	Moderate to high, requires significant documentation	High, detailed and technical	High, detailed and sector-specific
Support for ICS/OT	Strong, with NIST SP 800-82 providing specific guidance	Limited, more IT-focused	Strong, specifically designed for ICS/OT	Strong, but specific to the energy sector
Continuous Improvement	Emphasizes continuous improvement through core functions	Emphasizes continuous improvement through PDCA	Supports continuous improvement through lifecycle approach	Emphasizes compliance and periodic review
Documentation and Resources	Extensive, including detailed guidelines and case studies	Extensive, but often more general	Extensive, technical focus	Extensive, but very specific
Global Recognition	High, especially in the U.S. and globally	High, globally recognized	Growing, recognized in industrial sectors	High, but limited to the energy sector

3.2. OT WAN Device Risk Identification and Mitigation

Availability risks in WAN devices with respect to OT infrastructure must be identified and mitigated. This section gives a description of the several techniques to identify and mitigate OT WAN device risks. One of the major vulnerabilities in WAN devices, according to NIST, includes firmware exploits. Under ID.RA-1 in the NIST Cybersecurity Framework, it is stated that vulnerabilities to known threats should be collected, correlated, and communicated [19]. Similarly, ISA/IEC 62443 stipulates that systems should be designed to minimize exposure to these device vulnerabilities. Another notable risk is through attack surfaces caused by unrecorded devices, nonstandard configurations, enabled unused protocols, and external access exposure. NIST CSF ID.AM-2 indicates the need for an inventory of software platforms and applications in an organization [19]. ISA/IEC 62443 3-3 SR 7.3 also emphasizes the importance of reducing attack surfaces to a minimum [6]. Zero-day vulnerabilities can also be directly attributed to the firmware or software of devices. NIST CSF DE.CM-4 emphasizes the importance of the device's ability to detect malicious code, and ISA/IEC 62443 4-1 SR 1.4 establishes the same security management in mitigating this risk [6,19].

Additional considerations include the incident impact when a device is down. NIST CSF ID.BE-5 addresses the identification of resilience requirements to support critical services [19]. ISA/IEC 62443 2-1 SR 2.6 suggests that an analysis of the consequences of such incidents should be conducted as part of the process [6]. Third-party dependency, where an organization may depend on external software or hardware, can also be a risk. NIST CSF ID.SC-1 implies that identifying and evaluating suppliers and partners should be included in the risk assessment process [19]. A similar recommendation from ISA/IEC 62443 2-4 SR 1.1 is that dependencies on third parties should be documented or recorded [6]. Hardware failure risks must be considered, and NIST CSF PR.DS-4 proposes that there should be enough capacity to support availability in case of hardware failure [19]. Similarly, ISA/IEC 62443 3-3 SR 7.4 states that system designs should be resistant to hardware failures [6]. Physical protections against environmental risks, such as the ability of the device to withstand temperature and humidity, are addressed in NIST CSF PR.PT-5 and ISA/IEC 62443 3-3 SR 5.1, respectively [6,19].

Another notable risk is human error, such as misconfigurations, which can be mitigated through response and recovery plan testing guided by NIST CSF PR.IP-9 and ISA/IEC 62443 2-4 SR 3.1, and effective training [6,19]. Software-related risks must be patched to prevent firmware complications. According to both NIST CSF PR.IP-12 and ISA/IEC 62443 3-3 SR 7.5, this requires support for vulnerability and update management [6,19]. Access control risks are associated with the management of user access and permissions. NIST CSF PR.AC-1 involves the identity and credential management process [19], while ISA/IEC 62443 3-3 SR 1.1 ensures capabilities for user authentication are in place [6]. Communication network risks, which depend on both the availability and integrity of information, can be mitigated through NIST CSF PR.PT-3 and ISA/IEC 62443 3-3 SR 3.2 to protect system access and communications [6,19]. These mitigation strategies involve deploying security devices and solutions, including firewalls and encryption, which are addressed in NIST CSF PR.IP-3 and ISA/IEC 62443 3-3 SR 3.1 [6,19]. Implementing redundancy and failover capabilities as stated in NIST CSF PR.DS-4 and ISA/IEC 62443 3-3 SR 5.2 [6,19] are crucial to OT infrastructure. The effectiveness of policy and configuration management is observed in NIST CSF PR.IP-1, along with ISA/IEC 62443 3-3 SR 1.8, providing guidelines for maintaining baseline configurations [6,19]. Staying up to date with current threat intelligence is essential, as implied by both NIST CSF DE.DP-4 and ISA/IEC 62443 4-1 SR 1.8, which is necessary for effective threat management. Security awareness training, guided by NIST CSF PR.AT-1 and ISA/IEC 62443 2-4 SR 3.1, aim to reduce human errors [6,19]. This is further supported by various NIST CSF and ISA/IEC 62443 guidelines in implementing resource budget management, compliance with regulations, business continuity, and backup solutions.

In summary, assessing risks and mitigating risks for WAN devices in OT infrastructure involves a comprehensive approach guided by frameworks like NIST CSF 2.0 and ISA/IEC 62443. These frameworks provide detailed guidelines to identify vulnerabilities, minimize risks, and ensure robust security measures, contributing to the overall resilience and reliability of OT systems. Those frameworks provide clear guidelines about the identification of weaknesses, risk reduction, and ways to assure strong security levels among other resiliency features and dependability of OT systems. Table 3 summarizes OT WAN device risks identification and mitigations per framework. The identified risks and mitigations serve as the factors used in the proposed risk scoring calculation.

Table 3. OT WAN device risks identification and mitigations per framework.

Category	Risks/Mitigations	NIST CSF	ISA/IEC 62443
OT WAN Device Risk	Vulnerability Risks	ID.RA-1	3-3 SR 7.7
	Attack Surface Risks	ID.AM-2	3-3 SR 7.3
	Zero Day Existing Risks	DE.CM-4	4-1 SR 1.4
	Incident Risk Impact when Down	ID.BE-5	2-1 SR 2.6
	Third-Party Dependencies	ID.SC-1	2-4 SR 1.1
	Hardware Failure Risks	PR.DS-4	3-3 SR 7.4
	Environmental Risks	PR.PT-5	3-3 SR 5.1
	Human Error Risks	PR.IP-9	2-4 SR 3.1
	Software Update Risks	PR.IP-12	3-3 SR 7.5
	Access Control Risks	PR.AC-1	3-3 SR 1.1
	Communication Network Risks	PR.PT-3	3-3 SR 3.2

Table 3. *Cont.*

Category	Risks/Mitigations	NIST CSF	ISA/IEC 62443
OT WAN Risk Mitigation	Security Measures within the Device	PR.IP-3	3-3 SR 3.1
	Network Configuration Fault Tolerance	PR.DS-4	3-3 SR 5.2
	Policy Management and Configuration Management	PR.IP-1	3-3 SR 1.8
	Capability for Threat Intelligence and Updates	DE.DP-4	4-1 SR 1.8
	Security Awareness	PR.AT-1	2-4 SR 3.1
	Resource Budget	ID.GV-2	2-1 SR 2.3
	Regulatory Environment Compliance	ID.GV-3	4-2 SR 1.1
	Business Continuity	PR.IP-4	3-3 SR 5.3
	Detection of Attack Attempts	DE.CM-1	4-2 SR 2.7
	Backup and Recovery Solutions	PR.IP-4	3-3 SR 5.5
	Access Control Policies	PR.AC-3	3-3 SR 1.6
	Encryption and Data Protection Measures	PR.DS-1	3-3 SR 4.3
	Patch Management Processes	PR.IP-12	3-3 SR 7.5
	Compatibility with SIEM Systems	DE.DP-4	4-2 SR 2.7
	Network Segmentation	PR.AC-5	3-3 SR 3.1
	Redundancy and Failover Mechanisms	PR.DS-4	3-3 SR 5.2
	Third-Party Vendor Risk Management	ID.SC-1	2-4 SR 1.1

4. Proposed Risk-Assessment Approach

The first aim of this paper is to raise the availability of OT infrastructure and secure it against DoV, DoC, and DoS attacks by extending it to a WAN technology. The second aim is to evaluate the risks associated with the proposed extension and highlight which WAN technology is more appropriate in terms of security. The proposed risk-scoring (*RS*) method is based on a military risk management called Composite Risk Management (CRM), which identifies hazards from assets and develops controls prioritization to be supervised and reviewed in a cycle process [72]. NIST is the main framework to be used in the proposed RS method, which independently calculates WAN technology risk score instead of assessing the infrastructure as a whole (details are in Section 4.3). The proposed methodology is intended to complement, rather than replace, the existing risk metric calculation standards by specifically focusing on OT WAN risk assessment. The proposed risk scoring (*RS*) calculation method incorporates both qualitative and quantitative values. Qualitative values are derived from risk variables, as each OT infrastructure will experience different occurrences of risk, which also applies to mitigation variables [60] (see Section 4.2 for more details). The quantitative aspect of the calculation represents the actual risk score, which is the total value of risk determined based on the qualitative variable assumptions. Equation (1) represents the proposed *RS* calculation approach, where *RS* is the average sum of the total weighted risks *(WRt)* and the total weighted mitigations *(WMt*).

$$RS = \frac{WRt + WMt}{2} \tag{1}$$

WRt is calculated as the sum of the weight assigned to a risk factor multiplied by the risk factor value, as depicted in Equation (2). On the other hand, *WMt* is calculated as the sum of weight assigned to a mitigation factor multiplied by the mitigation factor value, as depicted in Equation (3). Details about *Rn* and *Mn* variables are in Section 4.2.

After substitution, *RS* is calculated according to Equation (4), where n and m represent the risk and mitigation factors, respectively. *n* and *m* variables track the number of existing risks in the given WAN solution and their corresponding mitigation features designed to counteract those risks.

$$WRt = \sum_{n=1}^{x} (WRn)(Rn) \tag{2}$$

$$WMt = \sum_{m=1}^{y} (WMm)(1 - Mm) \tag{3}$$

$$RS = \frac{1}{2}\left[\sum_{n=1}^{x} (WRn)(Rn) + \sum_{m=1}^{x} (WMm)(1 - Mm)\right] \tag{4}$$

In the following sections, we will present details for every component in Equation (4).

4.1. OT Risks and Mitigations Prioritization and Priority Weighting

Prioritizing the risks to implement the mitigation process chronologically based on severity is essential. This is needed to properly scale implementation progress and to measure effectively the efficiency of the deployed solution. It is best to align it with the recommendations in NIST SP 800-82 Rev. 3, which provides guidance on securing OT systems while addressing unique performance, reliability, and safety requirements. It also incorporates the principles from ISA/IEC 62443, which focuses on securing industrial automation and control systems by managing risks associated with these environments [19,73]. Tables 4 and 5 provide OT risks and mitigations prioritization, respectively, which are based on NIST SP 800-82 and ISA/IEC 62443. This will be used in the RS computation defining both risk and mitigation variables based on their priority level, and showing how OT WAN devices or solutions will be assessed before they can be deployed in the OT Infrastructure. The prioritized risks and mitigations are the ones identified in Table 3 mapping the NIST and ISA/IEC standards considered for OT WAN.

Tables 4 and 5 illustrate the distribution of priority weights for risks and mitigations, respectively, which will be utilized in Equations (2) and (3) for calculating the risk score (RS) as shown in Equation (4). The weights range from 0 to 1, with a total sum of 1 for the overall weight, signifying that a higher weight value indicates greater priority in risk and mitigation calculations. Both risk and mitigation weights are based on qualitative and quantitative assumptions informed by NIST CSF and ISA/IEC 62443. They are qualitative because each OT infrastructure will prioritize risks differently, but since the proposed method is based on the OT risk-assessment standard framework, it is also quantitative in nature. The scoring is influenced by the priorities outlined by NIST and ISA/IEC 62443. However, the weight values may vary in actual OT environments based on expert assumptions and real occurrences.

A risk/mitigation value is attributed to every attack (S_{DoV}, S_{Doc} , and S_{Dos}). The values are associated with a priority level (1 to 5) that can be high (4 or 5), medium (3) or low (1 or 2) (see Tables 4 and 5). The values assigned to *DoV*, *DoC*, and *DoS* are based on how the risk affects its occurrence. The same is expressed in mitigation but to emphasize how effective it can prevent DoV, DoC, and DoS. A combined score multiplying the 3 values is then calculated following Equation (5). The weight for every risk (i.e., *WRn*)/mitigation (i.e., *WMm*) is then calculated by dividing the combined score for a given risk/mitigation factor by the sum of all combined scores as depicted in Equations (6) and (7), respectively.

The calculation concept is inspired from NIST (see Section 4.3), but the scaling is based on the proposed approach.

$$Combined\ Score = S_{DoV} * S_{Doc} * S_{DoS} \tag{5}$$

$$WRn = \frac{Risk_{Combined\ Score}}{\sum Risk_{Combined\ Score}} \tag{6}$$

$$WMm = \frac{|Mitigation_{Combined\ Score}}{\sum Mitigation_{Combined\ Score}} \tag{7}$$

Table 4. OT WAN risks prioritization and weight values.

Priority Level	**Risks**	S_{DoV}	S_{DoC}	S_{DoS}	**Combined Score**	**Weight (WRn)**	**Description**
High Priority	Access Control Risks	5	5	4	100	0.1484	Crucial in preventing the unauthorized access to systems and devices, which can make way for serious security breaches.
High Priority	Communication Network Risks	5	5	5	125	0.1855	It is necessary to provide safe and reliable paths for communication in OT settings.
High Priority	Vulnerability Risks	5	4	5	100	0.1484	The top responsibility is the identification and addressing of known vulnerabilities that attackers can exploit.
High Priority	Zero Day Existing Risks	4	4	4	64	0.095	There could be unknown vulnerabilities that may be exploited by new attacks, which are unexpected; this unverified vulnerability is in urgent need of fixing.
High Priority	Incident Risk Impact when Down	4	4	5	80	0.1187	Ensuring minimal disruption and quick recovery during incidents to maintain operational continuity.
Medium Priority	Software Update Risks	4	5	2	40	0.0593	This is important for the management of risks associated with applying software updates, which can add new vulnerabilities or incompatibility issues.
Medium Priority	Hardware Failure Risks	2	5	5	50	0.0742	Addressing potential failures in hardware that could disrupt operations or compromise security.
Medium Priority	Attack Surface Risks	4	4	3	48	0.0712	Reducing the number of potential entries points that attackers can exploit.
Medium Priority	Third-Party Dependencies	3	3	3	27	0.0401	Managing risks associated with reliance on external vendors and service providers.
Medium Priority	Human Error Risks	4	4	2	32	0.0475	Mitigating risks arising from human mistakes that can lead to security incidents.
Low Priority	Environmental Risks	2	2	2	8	0.0119	Consideration to environmental factors that may affect the physical and operational integrity of OT systems.
					674	1	

Table 5. OT WAN mitigations prioritization and weight values.

Priority Level	**Mitigations**	S_{DoV}	S_{DoC}	S_{DoS}	**Combined Score**	**Weight (WMm)**	**Description**
High Priority	Business Continuity	5	5	5	125	0.1394	Capability to support continuity plans of the business during and after security-related incidents.
High Priority	Access Control Policies	5	5	4	100	0.1115	It is critical for preventing unauthorized access to critical systems.
High Priority	Network Segmentation	4	4	5	80	0.0892	It helps contain breaches, hence limiting the spread of cyber incidents within the network.

Table 5. *Cont.*

Priority Level	Mitigations	S_{DoV}	S_{DoC}	S_{DoS}	Combined Score	Weight (WMm)	Description
High Priority	Security Measures within the Device	4	4	5	80	0.0892	It ensures the integrity of devices operating within the OT environment.
High Priority	Patch Management Processes	4	4	4	64	0.0713	Ensures that systems are up to date and able to validate the latest security patches to mitigate vulnerabilities.
High Priority	Encryption and Data Protection Measures	5	5	4	100	0.1115	Critical for maintaining the confidentiality and integrity of data in transit and at rest.
Medium Priority	Detection of Attack Attempts	3	3	4	64	0.0713	Implementing mechanisms to detect and respond to security incidents.
Medium Priority	Backup and Recovery Solutions	3	4	5	60	0.0669	This ensure that data and system states can be restored in the case of an event.
Medium Priority	Network Configuration Fault Tolerance	3	3	5	45	0.0502	It enhances the network's fault tolerance, therefore enabling it to sustain and recover from faults quickly.
Medium Priority	Redundancy and Failover Mechanisms	3	4	5	60	0.0669	Ensures continuity of operations in the event of system failures.
Medium Priority	Capability for Threat Intelligence and Updates	4	4	3	48	0.0535	Keeping the system updated with the newest threat intelligence to help prevent an attack.
Low Priority	Policy Management and Configuration Management	3	4	1	12	0.0134	Manages the security policies and configuration enforcement.
Low Priority	Security Awareness	4	4	1	16	0.0178	Training difficulty (adaptability) to employees to identify and respond to potential security threats.
Low Priority	Third-Party Vendor Risk Management	3	3	2	18	0.0201	Manages the risk positioned by third-party vendors; escalates so that they do not turn into a weak link in the process.
Low Priority	Regulatory Environment Compliance	2	2	2	8	0.0089	Ensuring that operations are operating in accordance with relevant regulations and standards.
Low Priority	Compatibility with SIEM Systems	3	3	1	9	0.01	Ensures integration with Security Information and Event Management (SIEM) tools for better monitoring and analysis.
Low Priority	Resource Budget	2	2	2	8	0.0089	Cost allocation of appropriate budget to support the security measures.
					897	1	

4.2. Risk and Mitigation Values per Selected Technology

Tables 6 and 7 represent the qualitative risks and mitigations assumptions based on the current OT infrastructure setup (i.e., related to WAN technology extension). The values are based on the metric scaling shown in Table 8, which is meant to follow NIST scoring. The values will be used in Equations (8) and (9) to calculate Rn and Mm, respectively. As Rn and Mm are probabilities that take values between 0 and 1, risk and mitigation are normalized. Weighted risk and weighted mitigation will then be calculated using Equations (2) and (3), respectively. The scores in Tables 6 and 7 are not standard or fixed values; for clarity and simplicity, they were assigned based on research insights into WAN technology and were guided by NIST and ISA/IEC frameworks. In a real scenario, this will be based on experts' assumptions or most effectively based on the existing risk assessment framework. The values were decided based on OT WAN environments considering their location, technology setup, and availability of the said technology.

Table 6. Risks when using WAN technology to extend OT.

Technology	Access Control Risks	Communication Network Risks	Vulnerability Risks	Zero Day Existing Risks	Incident Risk Impact when Down	Software Update Risks	Hardware Failure Risks	Attack Surface Risks	Third-Party Dependencies	Human Error Risks	Environmental Risks	References
SD-WAN	2	2	3	3	3	3	3	3	3	2	2	Proposed work
Satellite WAN	3	4	3	3	5	3	4	4	5	3	5	[74,75]
LoRaWAN	3	4	4	3	4	3	3	4	4	3	4	[76,77]
Private LTE/5G Networks	3	4	3	3	5	3	3	5	3	3	5	[78,79]
MPLS	2	2	2	2	4	2	3	2	3	2	2	[80–83]
Leased Line	2	2	2	2	5	1	3	2	3	2	2	
DMVPN	3	2	3	3	4	3	3	3	3	4	2	[84,85]
IPSec VPN	3	2	3	3	4	3	4	3	3	4	2	[86–88]
VPLS	3	3	3	2	4	2	3	2	4	3	2	[89,90]

Table 7. Risks mitigations when using wan technology to extend OT.

Technology	Access Control Policies	Network Segmentation	Security Measures within the Device	Patch Management Processes	Encryption and Data Protection Measures	Detection of Attack Attempts	Backup and Recovery Solutions	Network Configuration Fault Tolerance	Redundancy and Failover Mechanisms	Capability for Threat Intelligence and Updates	Policy Management and Configuration Management	Security Awareness	Third-Party Vendor Risk Management	Regulatory Environment Compliance	Business Continuity	Compatibility with SIEM Systems	Resource Budget	References
SD-WAN	4	4	4	4	5	4	4	4	4	4	4	3	4	4	4	4	3	Proposed work
Satellite WAN	3	3	3	2	3	3	2	2	3	3	3	2	3	3	3	3	2	[74,75]
LoRaWAN	3	3	3	2	4	3	2	2	2	2	3	2	3	3	2	2	2	[76,77]
Private LTE/5G Networks	3	4	3	3	2	3	3	3	3	3	3	3	3	3	3	3	2	[78,79]
MPLS	4	5	4	4	3	3	3	4	4	3	3	3	4	4	4	3	2	[80–83]
Leased Line	4	5	4	4	3	3	3	4	4	3	3	3	4	4	4	3	2	
DMVPN	4	4	3	3	5	2	3	3	3	2	3	3	4	4	4	3	4	[84,85]
IPSec VPN	4	4	3	3	5	2	2	2	2	2	3	3	4	4	2	4	5	[86–88]
VPLS	4	5	4	3	4	2	3	3	4	2	3	3	4	4	4	3	3	[89,90]

Table 8. Metric scaling and RS.

Metric Scaling		Mm/5 and Rn/5 Values	
1	Very Low	RS < 0.2	Very Low
2	Low	RS < 0.4	Low
3	Moderate	RS < 0.6	Moderate
4	High	RS < 0.8	High
5	Very High	RS $\geq$ 0.8	Very High

The proposed method will help estimate the risks during the decision phase, before procuring and installing a WAN solution. The computation is designed to be compatible with the manufacturing existing risk scoring.

$$Rn = \frac{Risk}{5} \tag{8}$$

$$Mm = \frac{Mitigation}{5} \tag{9}$$

4.3. RS Derivation from NIST

The concept for RS (Risk Score) computation is based on the NIST model, which defines risk as the product of Threat, Vulnerability, and Impact as illustrated in Equation (10), where:

- Threats considered are DoV, DoC, and DoS—known attacks that are consistently exploited along the OT ICS/CPS kill chain [8–12].
- Vulnerability refers to the risks associated with using a WAN device to extend OT infrastructure and the likelihood of its mitigation features successfully addressing DoV, DoC, and DoS. In other words, it is equal to the probability of risk and probability of mitigation to succeed
- Impact is represented by a weight that prioritizes the OT infrastructure, ranking the risks and mitigations based on their current relevance to the specific OT environment. Precisely, the impact equals the weight of risk and the weight of mitigation.

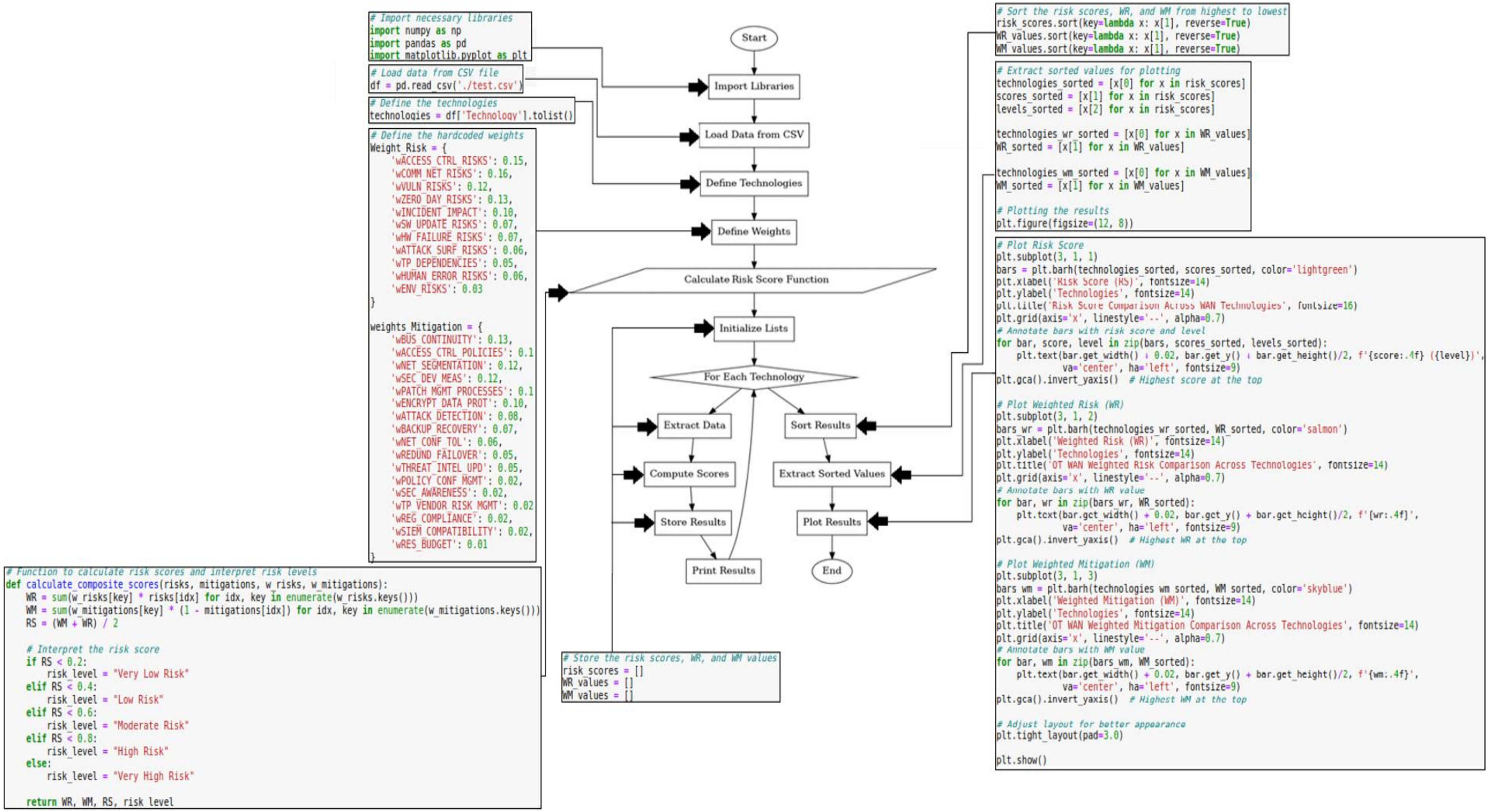
$$R_{NIST} = Threat \ast Vulnerability \ast Impact \tag{10}$$

By substituting the relevant values, Equation (1) will be formulated, representing the average risk from both the risk associated with each device used in the OT WAN and the probability of mitigation failure.

5. Implementation, Results, and Analysis

5.1. Automation

The proposed risk evaluation has been implemented using Python, as depicted in Figure 1. A program was developed to automate the graphical presentation and calculation of the nine WAN technologies which have 56 variables: 11 risk variables (Table 6), 17 mitigation variables (Table 7), and 28 priority weight values (Tables 4 and 5). The automation was made possible by declaring the risk values and mitigation values in a CSV file. The priority weights are hardcoded in the Python code since of the said variables, it is the least likely to change because it will be the standard prioritization of the said OT infrastructure. All variables are not fixed; the program is flexible enough to be modified whenever adjustment is needed or if changes in design are made. The flowchart in Figure 1 is straightforward, explaining the code in layman's terms thus directly representing the whole code.



```
# Import necessary libraries
import numpy as np
import pandas as pd
import matplotlib.pyplot as plt
```

```
# Load data from CSV file
df = pd.read_csv('./test.csv')
```

```
# Define the technologies
technologies = df['Technology'].tolist()
```

```
# Define the hardcoded weights
Weight_Risk = {
    'wACCESS_CTRL_RISKS': 0.15,
    'wCOMM_NET_RISKS': 0.16,
    'wVULN_RISKS': 0.12,
    'wZERO_DAY_RISKS': 0.13,
    'wINCIDENT_IMPACT': 0.10,
    'wSW_UPDATE_RISKS': 0.07,
    'wHW_FAILURE_RISKS': 0.07,
    'wATTACK_SURF_RISKS': 0.06,
    'wTP_DEPENDENCIES': 0.05,
    'wHUMAN_ERROR_RISKS': 0.06,
    'wENV_RISKS': 0.03
}

weights_Mitigation = {
    'wBUS_CONTINUITY': 0.13,
    'wACCESS_CTRL_POLICIES': 0.1
    'wNET_SEGMENTATION': 0.12,
    'wSEC_DEV_MEAS': 0.12,
    'wPATCH_MGMT_PROCESSES': 0.1
    'wENCRYPT_DATA_PROT': 0.10,
    'wATTACK_DETECTION': 0.08,
    'wBACKUP_RECOVERY': 0.07,
    'wNET_CONF_TOL': 0.06,
    'wREDUND_FAILOVER': 0.05,
    'wTHREAT_INTEL_UPD': 0.05,
    'wPOLICY_CONF_MGMT': 0.02,
    'wSEC_AWARENESS': 0.02,
    'wTP_VENDOR_RISK_MGMT': 0.02
    'wREG_COMPLIANCE': 0.02,
    'wSIEM_COMPATIBILITY': 0.02,
    'wRES_BUDGET': 0.01
}
```

```
# Function to calculate risk scores and interpret risk levels
def calculate_composite_scores(risks, mitigations, w_risks, w_mitigations):
    WR = sum(w_risks[key] * risks[idx] for idx, key in enumerate(w_risks.keys()))
    WM = sum(w_mitigations[key] * (1 - mitigations[idx]) for idx, key in enumerate(w_mitigations.keys()))
    RS = (WM + WR) / 2

    # Interpret the risk score
    if RS < 0.2:
        risk_level = "Very Low Risk"
    elif RS < 0.4:
        risk_level = "Low Risk"
    elif RS < 0.6:
        risk_level = "Moderate Risk"
    elif RS < 0.8:
        risk_level = "High Risk"
    else:
        risk_level = "Very High Risk"

    return WR, WM, RS, risk_level
```

```
# Store the risk scores, WR, and WM values
risk_scores = []
WR_values = []
WM_values = []
```

```
# Sort the risk scores, WR, and WM from highest to lowest
risk_scores.sort(key=lambda x: x[1], reverse=True)
WR_values.sort(key=lambda x: x[1], reverse=True)
WM_values.sort(key=lambda x: x[1], reverse=True)
```

```
# Extract sorted values for plotting
technologies_sorted = [x[0] for x in risk_scores]
scores_sorted = [x[1] for x in risk_scores]
levels_sorted = [x[2] for x in risk_scores]

technologies_wr_sorted = [x[0] for x in WR_values]
WR_sorted = [x[1] for x in WR_values]

technologies_wm_sorted = [x[0] for x in WM_values]
WM_sorted = [x[1] for x in WM_values]

# Plotting the results
plt.figure(figsize=(12, 8))
```

```
# Plot Risk Score
plt.subplot(3, 1, 1)
bars = plt.barh(technologies_sorted, scores_sorted, color='lightgreen')
plt.xlabel('Risk Score (RS)', fontsize=14)
plt.ylabel('Technologies', fontsize=14)
plt.title('Risk Score Comparison Across WAN Technologies', fontsize=16)
plt.grid(axis='x', linestyle='--', alpha=0.7)
# Annotate bars with risk score and level
for bar, score, level in zip(bars, scores_sorted, levels_sorted):
    plt.text(bar.get_width() + 0.02, bar.get_y() + bar.get_height()/2, f'{score:.4f} ({level})',
             va='center', ha='left', fontsize=9)
plt.gca().invert_yaxis()  # Highest score at the top

# Plot Weighted Risk (WR)
plt.subplot(3, 1, 2)
bars_wr = plt.barh(technologies_wr_sorted, WR_sorted, color='salmon')
plt.xlabel('Weighted Risk (WR)', fontsize=14)
plt.ylabel('Technologies', fontsize=14)
plt.title('OT WAN Weighted Risk Comparison Across Technologies', fontsize=14)
plt.grid(axis='x', linestyle='--', alpha=0.7)
# Annotate bars with WR value
for bar, wr in zip(bars_wr, WR_sorted):
    plt.text(bar.get_width() + 0.02, bar.get_y() + bar.get_height()/2, f'{wr:.4f}',
             va='center', ha='left', fontsize=9)
plt.gca().invert_yaxis()  # Highest WR at the top

# Plot Weighted Mitigation (WM)
plt.subplot(3, 1, 3)
bars_wm = plt.barh(technologies_wm_sorted, WM_sorted, color='skyblue')
plt.xlabel('Weighted Mitigation (WM)', fontsize=14)
plt.ylabel('Technologies', fontsize=14)
plt.title('OT WAN Weighted Mitigation Comparison Across Technologies', fontsize=14)
plt.grid(axis='x', linestyle='--', alpha=0.7)
# Annotate bars with WM value
for bar, wm in zip(bars_wm, WM_sorted):
    plt.text(bar.get_width() + 0.02, bar.get_y() + bar.get_height()/2, f'{wm:.4f}',
             va='center', ha='left', fontsize=9)
plt.gca().invert_yaxis()  # Highest WM at the top

# Adjust layout for better appearance
plt.tight_layout(pad=3.0)

plt.show()
```

Figure 1. OT WAN risk assessment automation flowchart.

5.2. Testing and Discussion

The comparison results of the implemented RS approach indicate that SD-WAN has the lowest risk score based on mitigation to risk averaging (as highlighted in Equation (1)), which is presented in Figure 2, and this is supported by Figure 3 (OT WAN-weighted risk) and Figure 4 (OT WAN-weighted mitigation). The results also indicate that the weighted mitigation score (complimentary percentage, the lower the better) of SD-WAN outweighs its risks. SD-WAN score has a marginal gap compared to its predecessors which are MPLS, leased line, and VPLS because of the security features SD-WAN innately has.

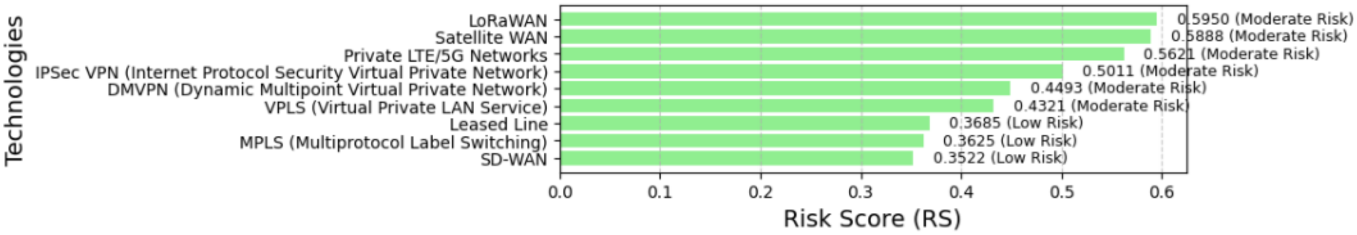


Figure 2. Risk score comparison across WAN technologies.

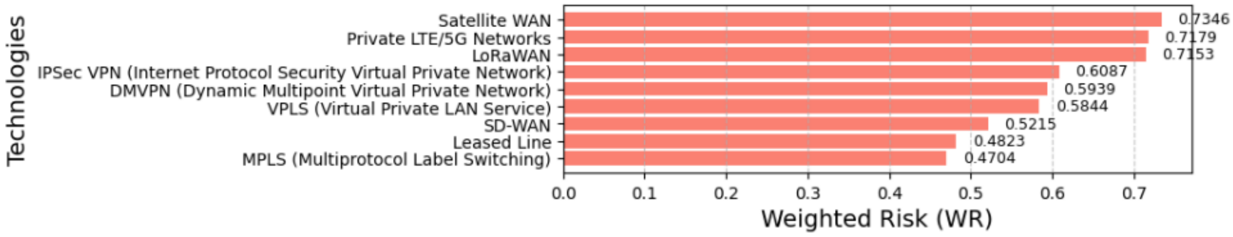


Figure 3. OT WAN weight risk comparison across technologies.

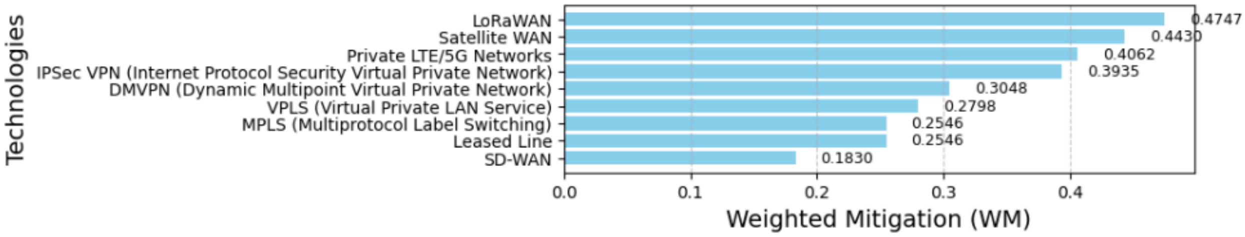


Figure 4. OT WAN weighted mitigation (equivalent risk) comparison across technologies.

RS presented in Figure 2 shows that SD-WAN, MPLS, and leased line have the lowest risk scores, meaning these technologies will provide a better and secure OT WAN connectivity avoiding DoV, DoC, and DoS attacks and ensuring more availability. On the other hand, VPLS, DMVPN, IPSec VPN, LTE/5G, Satellite, and LoraWAN technologies fall behind in terms of their mitigation capabilities, like network visibility, network management, and threat intelligence, which in turn makes the OT infrastructure more susceptible to risk, which can be seen in both Figures 3 and 4, yielding to a higher risk score as presented in Figure 2.

The weighted risks which can contribute to DoV, DoC, and DoS attacks as presented in Figure 3 show that MPLS, leased line and SDWAN have the lowest risk. The risk heat map graph in Figure 5 highlights the risk breakdown, showing what risk variables contributed the most to Figure 3 values. For example, from Figure 5, we see that SD-WAN has multiple moderate risk scores, which are zero-day, incident impact when down, software, hardware, attack surface, recorded vulnerabilities, and, lastly, third-party dependencies. These risk variables show what can be improved in SD-WAN and can be mapped on its mitigation features if this has been remediated. Although SD-WAN has multiple moderate risks, it is visible in Figure 5 that other WAN technologies, other than MPLS and leased line, have higher risks which is also highlighted in Figure 3.

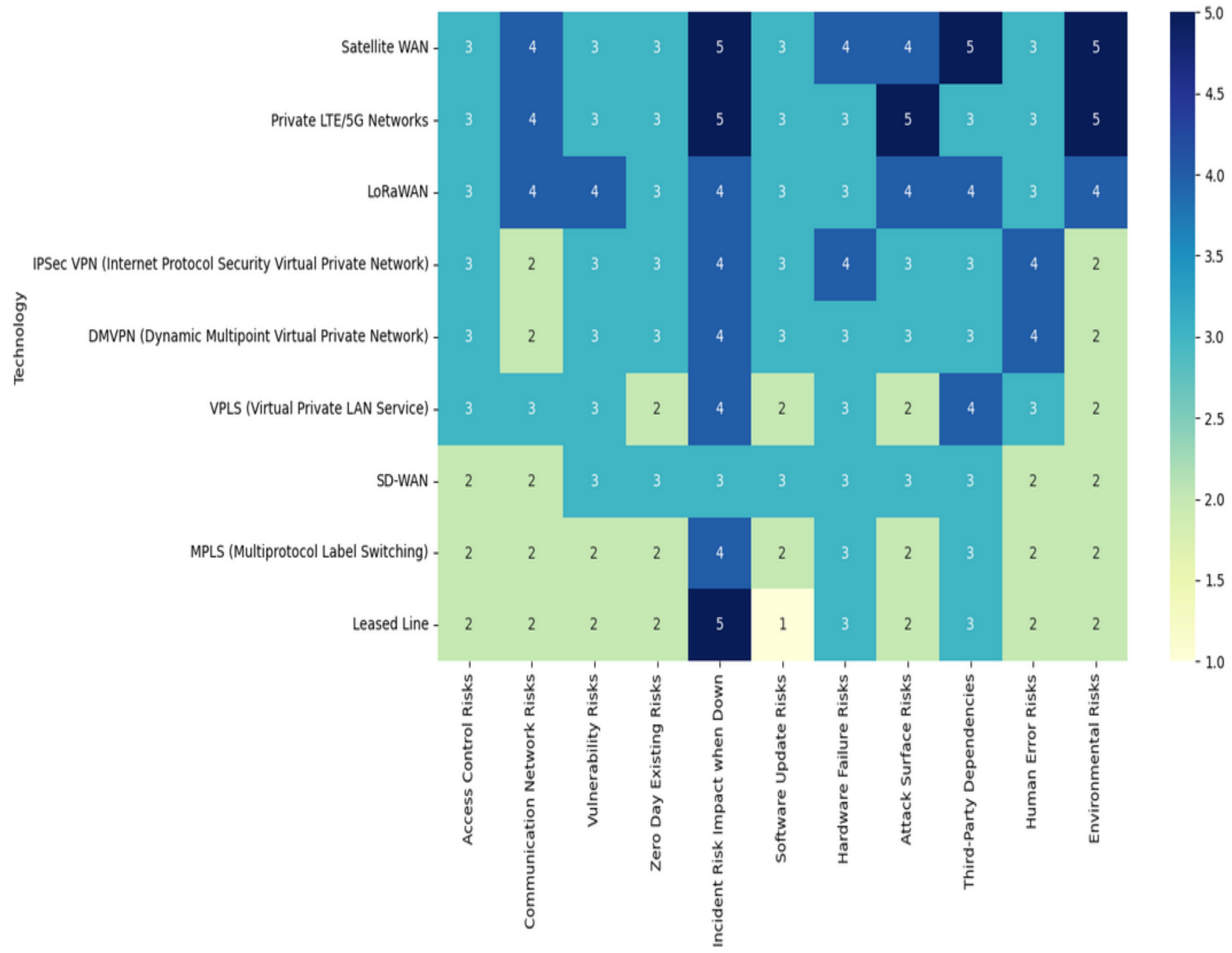


Figure 5. Heatmap of risk across technologies (sorted by highest risk).

The weighted mitigations which will help on preventing DoV, DoC, and DoS attacks as presented in Figure 4 show what technologies have the best mitigation features. SD-WAN, MPLS, and leased line have the top-three best mitigation features. This is supported by the mitigation heat map, in Figure 6, which can also be used in assessing a specific technology against a predefined feature requirement to have in each OT infrastructure. Figure 6 also shows that, among all nine OT WAN technologies, SD-WAN has the best mitigation features, which only falls behind on security awareness, which means engineers will need further training to adapt to this technology and resource budget, meaning it is moderately costly to implement.

If future changes are made to the OT infrastructure, the severity of risks and the effectiveness of mitigations may fluctuate based on the cybersecurity posture of the OT WAN. This could lead to either higher mitigation weights and lower risk weights if the security has been enhanced through continuous improvement, or higher risk weights and lower mitigation weights if an unforeseen vulnerability has been introduced due to the WAN modification. It is important to note that this paper focuses solely on the WAN aspect of the OT infrastructure, meaning any changes beyond the WAN (such as internal traffic) are outside the scope, as the weights are specifically assigned to WAN devices managing inbound and outbound external traffic.

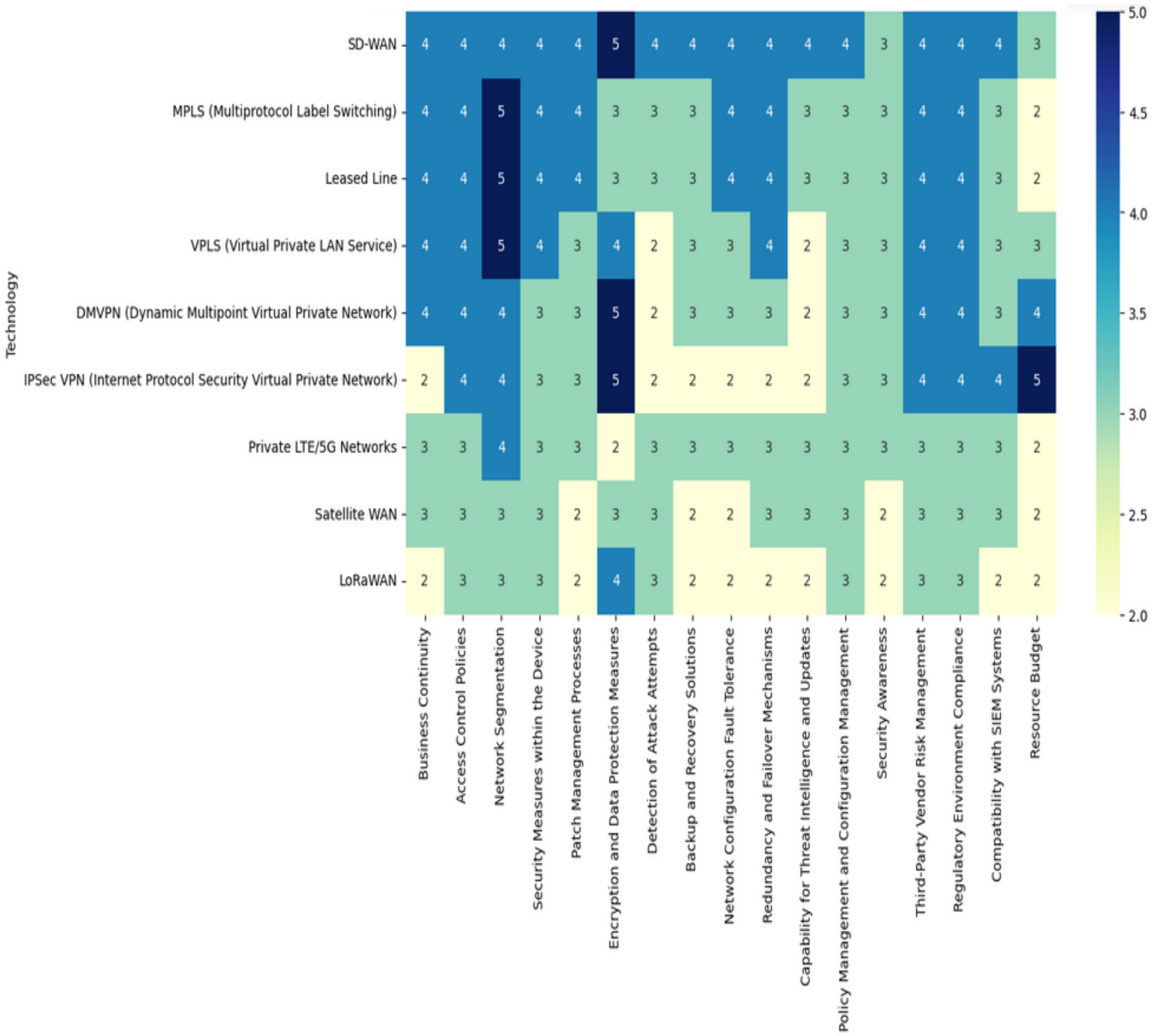


Figure 6. Heatmap of security measures across technologies (sorted by highest mitigation).

5.3. SD-WAN Design Based on the Proposed OT WAN Risk Assessment

In this section, we propose an SD-WAN based design to secure OT infrastructure following our proposed RS approach. Aligning to the obtained results, SD-WAN has been selected to be deployed on the IT side of the network where it is part of the layered security design. SD-WAN is integrated into the OT Purdue model (The Purdue Enterprise Reference Architecture (PERA) model is a hierarchical framework for designing and securing industrial control systems by organizing operations from physical processes to business planning [91] (pp. 12–44)) as depicted in Figures 7 and 8. The design is based on NIST CSF and ISA/IEC 62443 standards, which incorporate a zero-trust architecture to segregate the IT network from the OT network. In the proposed design, the zero-trust next-generation firewall is implemented with IPS/IDS modules installed and perimeter DMZ firewalls to isolate OT from IT network. Traditionally, OT environments are designed as air-gapped facilities which necessitates a robust segregation method on the extended OT network to replicate it. Based on the proposed setup (see Figure 7), policies must be implemented on both SD-WAN and firewalls ensuring that proper logging and threat intelligence are available both locally and remotely. This setup enhances security by monitoring and responding to potential threats in real time. It is important to note that traffic management is one of the key features of SD-WAN, which allows it to monitor and apply policing in either inbound or outbound traffic, allowing only one-way traffic, which is OT to IT and not bidirectional and should also be imposed on the firewalls.

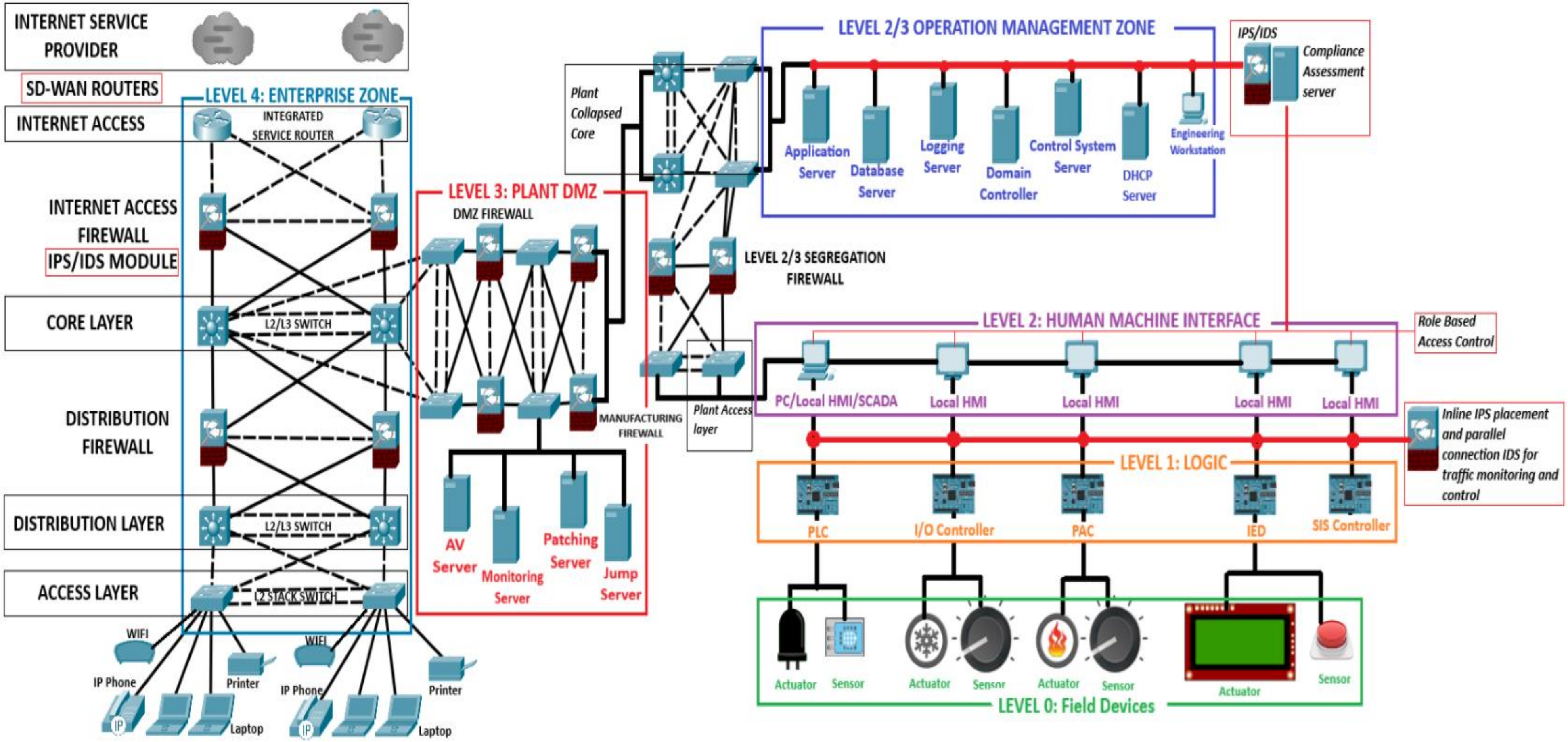


Figure 7. OT branch site low-level design.

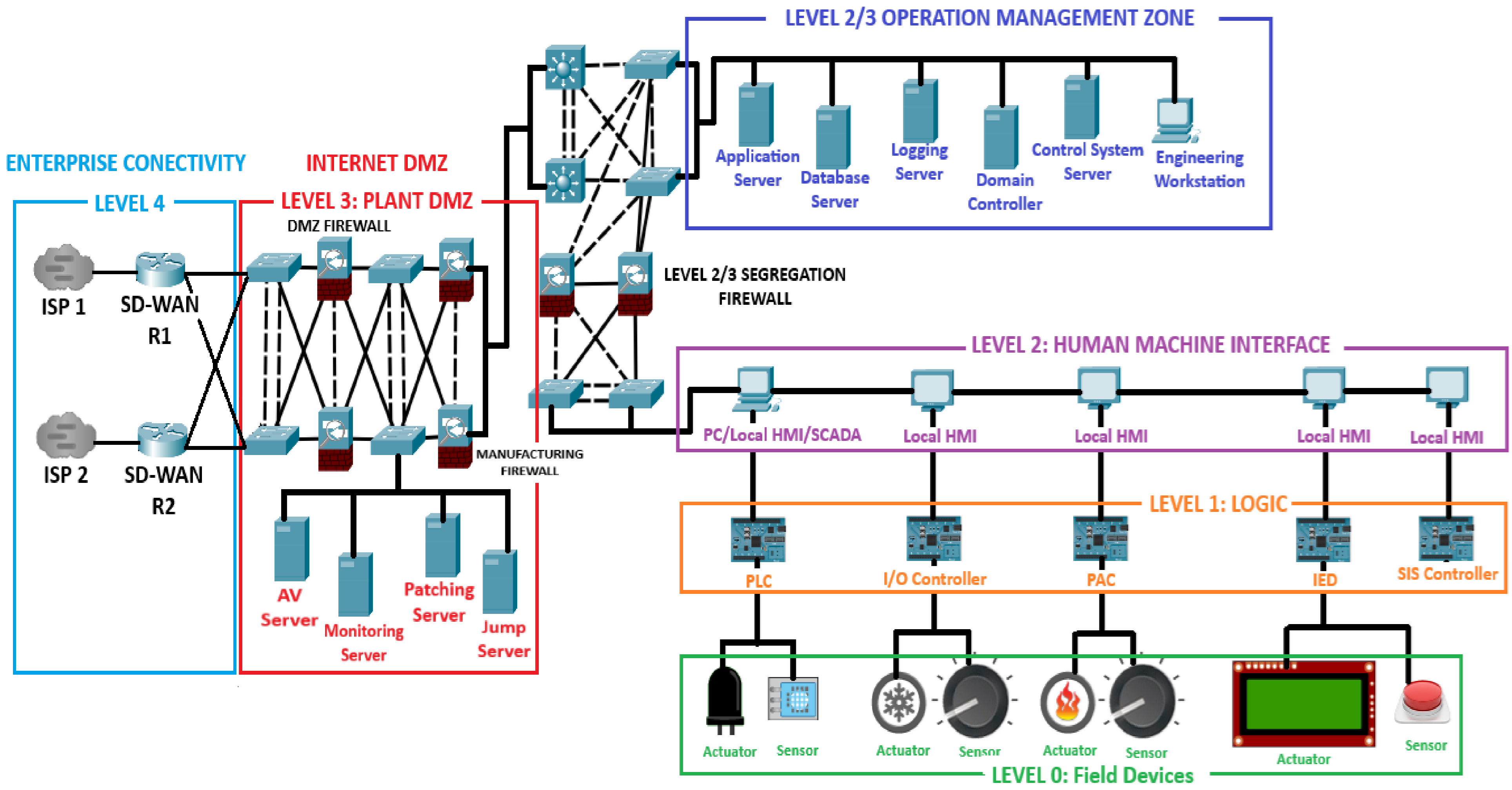


Figure 8. OT remote site low-level design.

Figure 8 illustrates how SD-WAN can be configured as a medium for out-of-band connectivity, a management connection utilized in both IT and OT network designs. Focusing on OT, the design shows that SD-WAN can be placed in the DMZ, dedicated to managing traffic, which enhances security for remote patching of OT servers, out-of-band maintenance connections, and hardens third-party remote access for ICS and CPS. This setup is also applicable to smaller OT infrastructures, where IT networks are connected remotely over WAN.

To prevent loss of availability in ICS and CPS, data backups (i.e., M0953 as outlined in MITRE | ATT&CK) can be secured over the WAN via SD-WAN, which also enables logging and monitoring of OT infrastructure. This can be achieved through a management connection or out-of-band communication (i.e., M0810 in MITRE | ATT&CK) using SD-WAN's ability to encrypt and segregate network segments with multi-VPNs. Another mitigation for availability loss is service redundancy (i.e., M0811 as presented in MITRE | ATT&CK), which can be implemented over WAN for ICS and CPS. SD-WAN's compatibility with various WAN technologies allows for secure and redundant options.

6. Conclusions and Future Directions

The key conclusion of this paper is that SD-WAN is the most effective WAN technology for enhancing the availability of OT infrastructure, particularly in ICS and CPS environments. This conclusion is supported by the proposed risk assessment approach, where SD-WAN achieved the lowest risk score of 0.3522, outperforming MPLS at 0.3625 and Leased Line at 0.3685, both widely recognized WAN connectivity options. Other WAN technologies exhibited moderate to high-risk values, ranging from 0.4321 to 0.5950, indicating that SD-WAN provides the best risk-to-mitigation ratio. The findings emphasize SD-WAN's superior mitigation capabilities. It can prevent vulnerabilities such as Denial of View (Technique T0815), Denial of Control (Technique T0813), and Denial of Service (DoS) in OT WAN environments by selecting the WAN technology with the lowest risk score, thus minimizing exposure to threats.

This paper demonstrated that by assessing potential SD-WAN risks alongside its integrated mitigation features, a risk score can be calculated. This scoring aligns with NIST and ISA/IEC risk and mitigation prioritization frameworks, offering an evaluation of how effectively SD-WAN can prevent OT WAN vulnerabilities. Additionally, this paper conducted a comprehensive OT risk analysis of various WAN technologies, including Satellite WAN, LoRaWAN, LTE/5G, MPLS, leased line, DMVPN, IPSec VPN, and VPLS, providing a detailed approach to assessing WAN technology risks.

By calculating the risk score for each WAN technology, considering their inherent risks and mitigation capabilities, the exploitable vulnerabilities of these technologies when applied in OT infrastructure are clearly identified. As a result, the probabilities of Denial of View (DoV), Denial of Control (DoC), and Denial of Service (DoS) can be estimated and minimized.

A limitation of this paper is the absence of a comprehensive network simulation for the proposed designs in Figures 7 and 8. Therefore, it would be beneficial for future studies to test the proposed design by implementing it within an actual OT infrastructure. This would allow for the fine-tuning of IPS/IDS anomaly detection settings, as well as monitoring and tagging network traffic over SD-WAN. Simulations should specifically involve actual OT devices, particularly focusing on unidirectional traffic from OT to IT, and examine the behavior of SD-WAN multi-VPN during secure remote monitoring (such as ICS and CPS status updates) and redundancy backup drills for ICS and CPS data (including historical logs and configuration backups).

Author Contributions: Conceptualization, V.J.A. and F.M.; methodology, V.J.A. and F.M.; software, V.J.A.; validation, V.J.A. and F.M.; formal analysis, V.J.A.; investigation, V.J.A.; resources, V.J.A.; writing—original draft preparation, V.J.A.; writing—review and editing, F.M.; visualization, V.J.A. and F.M.; supervision, F.M.; project administration, V.J.A. and F.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Matt, D.T.; Modrák, V.; Zsifkovits, H. (Eds.) *Industry 4.0 for SMEs: Challenges, Opportunities and Requirements*; Springer Nature: Cham, Switzerland, 2020; p. i-412. [CrossRef]
2. Villa, A.; Taurino, T. SME Innovation and Development in the Context of Industry 4.0. *Procedia Manuf.* **2019**, *39*, 1415–1420. [CrossRef]
3. Rikalovic, A.; Suzic, N.; Bajic, B.; Piuri, V. Industry 4.0 implementation challenges and opportunities: A technological perspective. *IEEE Syst. J.* **2022**, *16*, 2797–2810. [CrossRef]
4. Deloitte. Industry 4.0 and Cybersecurity: Managing Risk in an Age of Connected Production. Deloitte Insights. 2018. Available online: https://www2.deloitte.com/content/dam/insights/us/articles/3749_Industry4-0_cybersecurity/DUP_Industry4-0_cybersecurity.pdf (accessed on 24 August 2024).
5. ISAGCA (International Society of Automation Global Cybersecurity Alliance). Security Lifecycles Whitepaper. 2020. Available online: https://anapur.de/wp-content/uploads/2020/10/ISAGCA-Security-Lifecycles-whitepaper-FINAL.pdf (accessed on 24 August 2024).
6. ISA. ISA/IEC 62443 Series of Standards. 2024. Available online: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards (accessed on 24 August 2024).
7. Hahn, A.; Ashok, A.; Sridhar, S.; Govindarasu, M. Cyber-Physical Systems Security. 2019. Available online: https://www.cybok.org/media/downloads/Cyber-Physical_Systems_Security_issue_1.0.pdf (accessed on 24 August 2024).
8. MITRE. MITRE ATT&CK for ICS. 2024. Available online: https://attack.mitre.org/techniques/ics/ (accessed on 24 August 2024).
9. MITRE. Mitigations ICS. 2024. Available online: https://attack.mitre.org/mitigations/ics/ (accessed on 5 July 2024).
10. MITRE. Network Segmentation (M0930). 2024. Available online: https://attack.mitre.org/mitigations/M0930/ (accessed on 24 August 2024).
11. Assante, M.J.; Lee, R.M. The Industrial Control System Cyber Kill Chain. SANS Institute. 2015. Available online: https://sansorg.egnyte.com/dl/HHa9fCekmc (accessed on 24 August 2024).
12. Macaulay, T.; Assante, M.J.; Lee, R.M. RIoT Control: Understanding and Managing Risks and the Internet of Things. In *Security and Privacy in the Internet of Things*; Gupta, M., Walrand, B., Eds.; Morgan Kaufmann: Cambridge, UK, 2015; p. 249. Available online: https://books.google.co.uk/books/about/RIoT_Control.html?id=oXIYBAAAQBAJ&redir_esc=y (accessed on 24 August 2024).
13. Cybersecurity and Infrastructure Security Agency (CISA). ICS Alert (ICS-ALERT-17-102-01A): BrickerBot Permanent Denial-of-Service Attack. 2017. Available online: https://www.cisa.gov/news-events/ics-alerts/ics-alert-17-102-01a (accessed on 24 August 2024).
14. Cybersecurity and Infrastructure Security Agency (CISA). Advisory (ICSA-15-202-01): Siemens SIPROTEC Denial-of-Service Vulnerability. 2018. Available online: https://www.cisa.gov/news-events/ics-advisories/icsa-15-202-01 (accessed on 24 August 2024).
15. National Institute of Standards and Technology (NIST). Manufacturing Sector: Cybersecurity Recovery Framework Project. NIST NCCoE. 2022. Available online: https://www.nccoe.nist.gov/sites/default/files/2022-12/mfg-recovery-project-description-final-r1.pdf (accessed on 24 August 2024).
16. Stouffer, K.; Pillitteri, V.; Lightman, S.; Abrams, M.; Hahn, A. Guide to Industrial Control Systems (ICS) Security (NIST Special Publication 800-82 Revision 3). National Institute of Standards and Technology. 2022. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf (accessed on 24 August 2024).
17. National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity. 2018. Available online: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (accessed on 24 August 2024).
18. Maurushat, A.; Nguyen, K. The legal obligation to provide timely security patching and automatic updates. *Int. Cybersecur. Law Rev.* **2022**, *3*, 437–465. [CrossRef] [PubMed]
19. National Institute of Standards and Technology (NIST). *The NIST Cybersecurity Framework (CSF) 2.0*; NIST Cybersecurity White Paper; Department of Commerce: Gaithersburg, MD, USA, 2024. [CrossRef]
20. Cisco. *Secure Access Service Edge (SASE)*; Cisco Systems, Inc.: San Jose, CA, USA, 2020. Available online: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-sd-wan-secur-aag-cte-en.pdf (accessed on 24 August 2024).
21. Cisco. Harness the Power of Networking to Secure Industrial Operations. Cisco White Paper. 2023. Available online: https://www.cisco.com/c/en/us/products/collateral/security/industrial-security/harness-power-networking-secure-industrial-operations-wp.html (accessed on 6 August 2024).
22. Cisco. Security Overview. 2024. Available online: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-17/security-book-xe/m-security-overview.html (accessed on 24 August 2024).
23. Palo Alto Networks. Network Segmentation Solution Brief. Palo Alto Networks White Paper. 2023. Available online: https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/techbriefs/network-segmentation-solution-brief (accessed on 24 August 2024).

24. Palo Alto Networks. Prisma SD-WAN. 2024. Available online: https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/prisma-sd-wan-aag (accessed on 24 August 2024).
25. North American Electric Reliability Corporation (NERC). Zero Trust Architecture for Electric Operational Technology (OT). NERC White Paper. 2023. Available online: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/White_Paper_Zero_Trust_For_Electric_OT.pdf (accessed on 24 August 2024).
26. Scarfone, K.; Mell, P. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication. 2020. Available online: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-94.pdf (accessed on 24 August 2024).
27. Garcia-Teodoro, P.; Diaz-Verdejo, J.; Macia-Fernandez, G.; Vazquez, E. Anomaly-based network intrusion detection: Techniques, systems and challenges. *Comput. Secur.* **2021**, *28*, 18–28. [CrossRef]
28. Hu, V.C.; Ferraiolo, D.F.; Kuhn, D.R. Assessment of Access Control Systems. NIST Special Publication. 2020. Available online: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=926756 (accessed on 24 August 2024).
29. Dasgupta, D.; Roy, A.; Nag, A. Multi-Factor Authentication. In *Advances in User Authentication*; Springer Publication: Berlin/Heidelberg, Germany, 2021; pp. 185–233. Available online: https://link.springer.com/book/10.1007/978-3-319-58808-7 (accessed on 24 August 2024).
30. CyBOK. Introduction to the Cyber Security Body of Knowledge (CyBOK). 2019. Available online: https://www.cybok.org/media/downloads/Introduction_to_CyBOK.pdf (accessed on 24 August 2024).
31. Siponen, M.; Pahnila, S.; Mahmood, A. Employees' Adherence to Information Security Policies: An Empirical Study. In *New Approaches for Security, Privacy and Trust in Complex Environments*; Venter, H., Eloff, M., Labuschagne, L., Eloff, J., von Solms, R., Eds.; Springer: Boston, MA, USA, 2007; pp. 133–144. [CrossRef]
32. Kruger, H.A.; Kearney, W.D. A prototype for assessing information security awareness. *Comput. Secur.* **2021**, *25*, 289–296. [CrossRef]
33. Rong, C.; Nguyen, S.T.; Jaatun, M.G. Beyond lightning: A survey on security challenges in cloud computing. *Comput. Electr. Eng.* **2013**, *39*, 47–54. [CrossRef]
34. Mavoungou, S.; Kaddoum, G.; Taha, M.; Matar, G. Survey on threats and attacks on mobile networks. *IEEE Access* **2016**, *4*, 4543–4572. [CrossRef]
35. Jin, H.; Jiang, H.; Zhou, K. Dynamic and Public Auditing with Fair Arbitration for Cloud Data. *IEEE Trans. Cloud Comput.* **2018**, *6*, 680–693. [CrossRef]
36. Bustamante, J.R.; Avila-Pesantez, D. Comparative analysis of Cybersecurity mechanisms in SD-WAN architectures: A preliminary results. In Proceedings of the 2021 IEEE Engineering International Research Conference (EIRCON), Lima, Peru, 27–29 October 2021; pp. 1–4. [CrossRef]
37. Hama Amin, R.; Ahmed, D. Comparative Analysis of Flexiwan, OPNSense, and pfSense Cybersecurity Mechanisms in MPLS/SD-WAN Architectures. *Passer J. Basic Appl. Sci.* **2023**, *6*, 27–32. [CrossRef]
38. Ozgur Yurekten, O.; Demirci, M. SDN-based cyber defense: A survey. *Future Gener. Comput. Syst.* **2021**, *115*, 126–149. [CrossRef]
39. Yang, Z.; Cui, Y.; Li, B.; Liu, Y.; Xu, Y. Software-Defined Wide Area Network (SD-WAN): Architecture, Advances and Opportunities. In Proceedings of the 2019 28th International Conference on Computer Communication and Networks (ICCCN), Valencia, Spain, 29 July–1 August 2019; IEEE: Valencia, Spain, 2019; pp. 1–9. [CrossRef]
40. Borgianni, L.; Troia, S.; Adami, D.; Maier, G.; Giordano, S. From MPLS to SD-WAN to ensure QoS and QoE in cloud-based applications. In Proceedings of the 2023 IEEE 9th International Conference on Network Softwarization (NetSoft), Madrid, Spain, 19–23 June 2023; pp. 366–369. [CrossRef]
41. Kreutz, D.; Ramos, F.M.V.; Verissimo, P.E.; Rothenberg, C.E.; Azodolmolky, S.; Uhlig, S. Software-Defined Networking: A Comprehensive Survey. *Proc. IEEE* **2015**, *103*, 14–76. [CrossRef]
42. Etxezarreta, X.; Garitano, I.; Iturbe, M.; Zurutuza, U. Software-Defined Networking approaches for intrusion response in Industrial Control Systems: A survey. *Int. J. Crit. Infrastruct. Prot.* **2023**, *42*, 100615. [CrossRef]
43. Fortinet. Fortinet Secure SD-WAN. 2023. Available online: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortinet_secure_sdwan.pdf (accessed on 24 August 2024).
44. Fressancourt, A.; Gagnaire, M. A SDN-based network architecture for cloud resiliency. In Proceedings of the 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2015; IEEE: Las Vegas, NV, USA, 2015; pp. 479–484. [CrossRef]
45. Izumi, S.; Edo, A.; Abe, T.; Suganuma, T. An Adaptive Multipath Routing Scheme Based on SDN for Disaster-Resistant Storage Systems. In Proceedings of the 2015 10th International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA), Kraków, Poland, 4–6 November 2015; IEEE: Krakow, Poland, 2015; pp. 478–483. [CrossRef]
46. Aydeger, A.; Akkaya, K.; Cintuglu, M.H.; Uluagac, A.S.; Mohammed, O. Software defined networking for resilient communications in Smart Grid active distribution networks. In Proceedings of the 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 23–27 May 2016; IEEE: Kuala Lumpur, Malaysia, 2016; pp. 1–6. [CrossRef]
47. Foschini, L.; Mignardi, V.; Montanari, R.; Scotece, D. An SDN-enabled architecture for IT/OT converged networks: A proposal and qualitative analysis under DDoS attacks. *Future Internet* **2021**, *13*, 258. [CrossRef]
48. Umar, R.; Kusuma, R.S. Recovery System using SDN Technology for Cyber Attack Solution. In Proceedings of the 2021 8th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Jakarta, Indonesia, 28–30 November 2015; IEEE: Semarang, Indonesia, 2021; pp. 241–246. [CrossRef]

49. Zhang, Y.; Xu, C.; Muntean, G. A Novel Distributed Data Backup and Recovery Method for Software Defined-WAN Controllers. In Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 7–11 December 2021; IEEE: Madrid, Spain, 2021; pp. 1–6. [CrossRef]
50. Attia, A.; Khalifa, N.E.; Kotb, A. Data Backup Approach using Software-defined Wide Area Network. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*, 309–316. [CrossRef]
51. Wen, Z.; Garg, S.; Aujla, G.S.; Alwasel, K.; Puthal, D.; Dustdar, S.; Zomaya, A.Y.; Rajan, R. Running Industrial Workflow Applications in a Software-Defined Multicloud Environment Using Green Energy Aware Scheduling Algorithm. *IEEE Trans. Ind. Inform.* **2021**, *17*, 5645–5656. [CrossRef]
52. Saxena, M.C.; Bajaj, P. A Novel Method of End-to-End Data Security using Symmetric Key-based Data Encryption and SDWAN Networking. In Proceedings of the 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Noida, India, 14–16 December 2022; IEEE: Noida, India, 2022; pp. 1981–1986. [CrossRef]
53. Babeshko, I.; Giandomenico, F.D. Safety and cybersecurity assessment techniques for critical industries: A mapping study. *IEEE Access* **2023**, *11*, 83781–83793. [CrossRef]
54. Domínguez, R.; Gomez, C.; Cerezo, O. Risk Analysis Based on ETA, FTA and Bowtie Methodologies for the Bulk Coal Discharge Process. In *Advances in Safety Management and Human Performance*; AHFE 2021. Lecture Notes in Networks and Systems; Arezes, P.M., Boring, R.L., Eds.; Springer: Cham, Switzerland, 2021; Volume 262. [CrossRef]
55. Park, C.; Kontovas, C.; Yang, Z.; Chang, C.-H. A BN driven FMEA approach to assess maritime cybersecurity risks. *Ocean. Coast. Manag.* **2023**, *235*, 106480. [CrossRef]
56. Edu, A.S.; Agoyi, M.; Agozie, D. Digital security vulnerabilities and threats implications for financial institutions deploying digital technology platforms and application: FMEA and FTOPSIS analysis. *PeerJ Comput. Sci.* **2021**, *7*, e658. [CrossRef]
57. Goerlandt, F.; Khakzad, N.; Reniers, G. Validity and validation of safety-related quantitative risk analysis: A review. *Saf. Sci.* **2017**, *99*, 127–139. [CrossRef]
58. Ushakov, R.; Doynikova, E.; Novikova, E.; Kotenko, I. CPE and CVE based Technique for Software Security Risk Assessment. In Proceedings of the 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Cracow, Poland, 22–25 September 2021; pp. 353–356. [CrossRef]
59. Falco, G.; Caldera, C.; Shrobe, H. IIoT Cybersecurity Risk Modeling for SCADA Systems. *IEEE Internet Things J.* **2018**, *5*, 4486–4495. [CrossRef]
60. Zografopoulos, I.; Ospina, J.; Liu, X.; Konstantinou, C. Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies. *IEEE Access* **2021**, *9*, 29775–29818. [CrossRef]
61. Dallat, C.; Salmon, P.M.; Goode, N. Risky systems versus risky people: To what extent do risk assessment methods consider the systems approach to accident causation? A review of the literature. *Saf. Sci.* **2019**, *119*, 266–279. [CrossRef]
62. Fares, B. *An Integrated Risk Analysis Framework for Safety and Cybersecurity of Industrial SCADA Systems*; University of Stavanger: Stavanger, Norway, 2021.
63. Progoulakis, I.; Rohmeyer, P.; Nikitakos, N. Cyber physical systems security for maritime assets. *J. Mar. Sci. Eng.* **2021**, *9*, 1384. [CrossRef]
64. Gourisetti, S.N.G.; Lee, A.; Reddi, R.; Isirova, K.; Touhiduzzaman, M.; Sebastian-Cardenas, D.J.; Lambert, K.; Cali, Ü.; Mylrea, M.; Rahimi, F.; et al. Assessing Cybersecurity Resilience of Distributed Ledger Technology in Energy Sector Using the MITRE ATT&CK® ICS Framework. In Proceedings of the 2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain), Irvine, CA, USA, 7–11 November 2022; pp. 1–6. [CrossRef]
65. Ekisa, C.; Ó Briain, D.; Kavanagh, Y. Leveraging the MITRE ATT&CK Framework for Threat Identification and Evaluation in Industrial Control System Simulations. In Proceedings of the 2024 35th Irish Signals and Systems Conference (ISSC), Belfast, UK, 13–14 June 2024; pp. 1–6. [CrossRef]
66. Bhamare, D.; Zolanvari, M.; Erbad, A.; Jain, R.; Khan, K.; Meskin, N. Cybersecurity for industrial control systems: A survey. *Comput. Secur.* **2020**, *89*, 101677. [CrossRef]
67. Kriaa, S.; Bouissou, M.; Pietre-Cambacedes, L. Modeling the Stuxnet attack with BDMP: Towards more formal risk assessments. *Int. J. Crit. Infrastruct. Prot.* **2015**, *10*, 59–72. [CrossRef]
68. Cybersecurity and Infrastructure Security Agency (CISA). Commercial Facilities Sector Cybersecurity Framework Implementation Guidance. CISA. 2021. Available online: https://www.cisa.gov/sites/default/files/publications/Commercial_Facilities_Sector_Cybersecurity_Framework_Implementation_Guidance_FINAL_508.pdf (accessed on 24 August 2024).
69. International Organization for Standardization (ISO). ISO/IEC 27001:2022 Information Technology—Security Techniques—Information Security Management Systems—Requirements. 2022. Available online: https://ia600500.us.archive.org/6/items/iso27001/iso27001.pdf (accessed on 24 August 2024).
70. Heinl, M.P.; Pursche, M.; Puch, N.; Peters, S.N. From standard to practice: Towards ISA/IEC 62443-conform public key infrastructures. In *Computer Safety, Reliability, and Security*; Springer: Berlin/Heidelberg, Germany, 2023. [CrossRef]
71. Francia, G. Mapping of the NERC-CIP Standards with the NIST CSF. Presented at the 2022 CAE in Cybersecurity Symposium. 2022. Available online: https://www.caecommunity.org/sites/default/files/Copy%20of%2002%20Francia_NERC-CIP_Presentation.pdf (accessed on 24 August 2024).
72. US Department of the Army. Risk Management. ATP 5-19. 2014. Available online: https://www.armyresilience.army.mil/ard/images/pdf/Policy/ATP%205-19%20Risk%20Management.pdf (accessed on 24 August 2024).

73. National Institute of Standards and Technology (NIST). Guide for Conducting Risk Assessments. Special Publication 800-30 Revision 1. 2012. Available online: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (accessed on 24 August 2024).
74. Yan, Y.; Han, G.; Xu, H. A survey on secure routing protocols for satellite network. *J. Netw. Comput. Appl.* **2019**, *145*, 102415. [CrossRef]
75. Wu, X.; Du, Y.; Fan, T.; Guo, J.; Ren, J.; Wu, R. Threat analysis for space information network based on network security attributes: A review. *Complex Intell. Syst.* **2023**, *9*, 3429–3468. [CrossRef]
76. Pospisil, O.; Fujdiak, R.; Mikhaylov, K.; Ruotsalainen, H.; Fujdiak, R. Testbed for LoRaWAN security: Design and validation through man-in-the-middle attacks study. *Appl. Sci.* **2021**, *11*, 7642. [CrossRef]
77. Qadir, J.; Cabus, J.E.U.; Butun, I.; Lagerström, R.; Gastaldo, P.; Caviglia, D.D. Analysis of LPWAN: Cyber-security vulnerabilities and privacy issues in LoRaWAN, Sigfox, and NB-IoT. In *Low-Power Wide-Area Networks: Opportunities, Challenges, Risks and Threats*; Butun, I., Akyildiz, I.F., Eds.; Springer: Cham, Switzerlnad, 2023; pp. 139–170. [CrossRef]
78. Suomalainen, J.; Julku, J.; Vehkaperä, M.; Posti, H. Securing Public Safety Communications on Commercial and Tactical 5G Networks: A Survey and Future Paper Directions. *IEEE Open J. Commun. Soc.* **2021**, *2*, 1590–1615. [CrossRef]
79. Nguyen, V.-L.; Lin, P.-C.; Cheng, B.-C.; Hwang, R.-H.; Lin, Y.-D. Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2384–2428. [CrossRef]
80. Alouneh, S.; En-Nouaary, A.; Agarwal, A. MPLS security: An approach for unicast and multicast environments. *Ann. Telecommun.* **2009**, *64*, 391–400. [CrossRef]
81. Alouneh, S.; Al-Hawari, F.; Hababeh, I.; Ghinea, G. An Effective Classification Approach for Big Data Security Based on GMPLS/MPLS Networks. *Secur. Commun. Netw.* **2018**, *2018*, 8028960. [CrossRef]
82. Zhipeng, Z.; Chandel, S.; Jingyao, S.; Shilin, Y.; Yunnan, Y.; Jingji, Z. VPN: A Boon or Trap?: A Comparative Study of MPLS, IPSec, and SSL Virtual Private Networks. In Proceedings of the 2018 Second International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 22–23 February 2018; pp. 510–515. [CrossRef]
83. Sllame, M. Performance Evaluation of Multimedia over MPLS VPN and IPSec Networks. In Proceedings of the 2022 IEEE 2nd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA), Sabratha, Libya, 23–25 May 2022; pp. 32–37. [CrossRef]
84. Cisco Systems, Inc. Dynamic Multipoint VPN (DMVPN). 2024. Available online: https://www.cisco.com/c/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/data_sheet_c78-468520.html (accessed on 24 August 2024).
85. Marah, H.M.; Khalil, J.R.; Elarabi, A.; Ilyas, M. DMVPN Network Performance Based on Dynamic Routing Protocols and Basic IPsec Encryption. In Proceedings of the 2021 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), Kuala Lumpur, Malaysia, 12–13 June 2021; pp. 1–5. [CrossRef]
86. Frankel, S.; Kent, K.; Lewkowski, R.; Orebaugh, A.D. Guide to IPsec VPNs. NIST Special Publication 800-77. 2005. Available online: https://csrc.nist.rip/library/NIST%20SP%20800-077%20Guide%20to%20IPsec%20VPNs,%202005-12-01%20(Final).pdf (accessed on 24 August 2024).
87. Xu, Z.; Ni, J. Paper on network security of VPN technology. In Proceedings of the 2020 International Conference on Information Science and Education (ICISE-IE), Sanya, China, 4–6 December 2020; pp. 539–542. [CrossRef]
88. Pudelko, M.; Emmerich, P.; Gallenmüller, S.; Carle, G. Performance Analysis of VPN Gateways. In Proceedings of the IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Virtual, 9–12 November 2020; pp. 1–8. Available online: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=andarnumber=9142755 (accessed on 24 August 2024).
89. Liyanage, M.; Ylianttila, M.; Gurtov, A. Secure Hierarchical VPLS Architecture for Provider Provisioned Networks. *IEEE Access* **2015**, *3*, 967–984. [CrossRef]
90. Gaur, K.; Kalla, A.; Grover, J.; Borhani, M.; Gurtov, A.; Liyanage, M. A Survey of Virtual Private LAN Services (VPLS): Past, Present and Future. *Comput. Netw.* **2021**, *196*, 108245. [CrossRef]
91. Rathwell, G.A.; Williams, T.J. Use of the Purdue Enterprise Reference Architecture and Methodology in industry (the Fluor Daniel example). In *Modelling and Methodologies for Enterprise Integration*; IFIP—The International Federation for Information Processing; Bernus, P., Nemes, L., Eds.; Springer: Boston, MA, USA, 1996; pp. 12–44. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.