Journal of *Cybersecurity and Privacy*

MDPI

Review

Safety and Security Considerations for Online Laboratory Management Systems

Andrea Eugenia Pena-Molina *,† **and Maria Mercedes Larrondo-Petrie** †

Electrical Engineering and Computer Science Department, College of Engineering and Computer Science, Florida Atlantic University, 777 Glades Road, Boca Raton, FL 33431, USA; petrie@fau.edu

* Correspondence: a.e.molina@ieee.org

† These authors contributed equally to this work.

Abstract: The pandemic forced educators to shift abruptly to distance learning, also referred to as e-learning education. Educational institutions integrated new educational tools and online platforms. Several schools, colleges, and universities began incorporating online laboratories in different fields of education, such as engineering, information technology, physics, and chemistry. Online laboratories may take the form of virtual laboratories, software-based simulations available via the Internet, or remote labs, which involve accessing physical equipment online. Adopting remote laboratories as a substitute for conventional hands-on labs has raised concerns regarding the safety and security of both the remote lab stations and the Online Laboratory Management Systems (OLMSs). Design patterns and architectures need to be developed to attain security by design in remote laboratories. Before these can be developed, software architects and developers must understand the domain and existing and proposed solutions. This paper presents an extensive literature review of safety and security concerns related to remote laboratories and an overview of the industry, national and multinational standards, and legal requirements and regulations that need to be considered in building secure and safe Online Laboratory Management Systems. This analysis provides a taxonomy and classification of published standards as well as security and safety problems and possible solutions that can facilitate the documentation of best practices, and implemented solutions to produce security by design for remote laboratories and OLMSs.

Keywords: security; safety; privacy; e-learning; remote labs; online laboratory management systems

check for updates

Received: 27 February 2025
Revised: 12 April 2025
Accepted: 5 May 2025
Published: 13 May 2025

Citation: Pena-Molina, A.E.; Larrondo-Petrie, M.M. Safety and Security Considerations for Online Laboratory Management Systems. *J. Cybersecur. Priv.* **2025**, *5*, 24. https://doi.org/10.3390/jcp5020024

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Different technologies have developed continuously in recent decades for e-learning education, leading to considerable progress and innovation in several fields, including industry, business, finance, healthcare, management, education, and other educational services. Consequently, e-learning frameworks and tools have expanded and incorporated rapidly as new concepts of e-learning tools and remote laboratories [1]. The COVID-19 pandemic significantly advanced the transition to e-learning, establishing it as a worldwide central component of modern education. Educational institutions adopted Online Laboratory Management Systems (OLMSs) to allow students to interact with professional engineering tools and gain real-world experiences through web-based platforms. OLMSs include features that help manage laboratory experiments, schedule experiments, deliver assignments, control remote experiments, generate experiment reports, and automatically grade laboratory experiments [2].

The Latin American and Caribbean Consortium of Engineering Institutions (LACCEI) [3] is a non-profit organization that collaborates with the Organization of American States (OAS) [4], supporting initiatives by the Ministers of Science and Technology of OAS member countries. The LACCEI research team is currently developing Smart Adaptive Remote Laboratories (SARLs) [5], which are a type of OLMS. SARL is an e-learning system that incorporates an adaptive approach based on student academic profiles, allowing SARL to adapt the activities and challenges of laboratory experiments accordingly. Remote laboratory stations utilize Raspberry Pi microcontrollers, which are connected to laboratory equipment and receive and execute SARL commands transmitted by students through a browser interface. In addition, laboratory stations are equipped with webcams to capture and stream the current state of the laboratory to the user. SARL developers actively engage in multiple Institute of Electrical and Electronic Engineers (IEEE) standard development working groups to ensure the integration of best practices and standards within their e-learning platforms. They consistently incorporate emerging standards into their platforms [6], including the IEEE Standard 1876-2019 on Networked Smart Learning Objects for Online Laboratories [7], IEEE P2834 Standard for Secure and Trusted E-Learning Systems [8], and IEEE P7004.1 Standard for Safe and Secure Virtual Classroom [9]. In addition, ongoing efforts are underway to develop additional IEEE and International Organization for Standardization (ISO) standards, such as the IEEE P2881 Standard for Learning Metadata [10] and ISO 2700x Information Security Standard [11].

This paper comprehensively analyzes safety and security solutions for OLMS and remote laboratories, highlighting seven key focus areas, including general security concerns, security frameworks, access control and authentication, threats and vulnerabilities, integrity and monitoring, communication security, and safety. Several researchers presented safety and security solutions for remote laboratories. However, gaps are unresolved, including the technical complexity of developing secure systems, the absence of standardized architecture, and the need for specialized security patterns. Addressing these issues could enhance scalability, promote broader adoption, and strengthen the overall security of remote laboratories by implementing a "security by design" approach.

This paper is structured as follows: Section 2 describes the research methodology, including the taxonomy and the systematic literature review process. Section 3 outlines the field's state of the art, focusing on the history of the remote laboratories, the progression of computer safety and security, relevant legal frameworks and regulations, specific safety and security challenges, and the solutions proposed for OLMS environments. Section 4 details the results of the literature analysis and the remaining gaps. Section 5 addresses the conclusion and future work. Lastly, Appendix A presents the tables that organized the literature review on safety and security regulations and standards, the classification of security attacks, and the articles related to safety and security in remote laboratories.

2. Research Methodology

2.1. Taxonomy

The purpose of this taxonomy is to deliver a systematic classification of the main concepts in OLMS's safety and security. In addition, it gives a historical perspective, standard terminology, identification of seminal papers, and highlights gaps in this field, and it will serve as a foundation for future research.

A comprehensive feature diagram is used to present the taxonomy (Figure 1) that resulted from the literature analysis. The feature diagram for Safety and Security in OLMS organizes the key elements into a hierarchical structure, ensuring a precise classification of mandatory and optional aspects. At the top, safety and security in OLMS branches into major areas: Remote Laboratories, Computer Safety and Security Evolution, Legal

Requirements and Regulations, Security in Remote Laboratories and OLMS, and Proposed Solutions. The Remote Laboratories section includes the first implementations and the different types of remote laboratories. The Computer Safety and Security Evolution sections involve security, safety history, and evolution. The Legal Requirements and Regulation section consists of the safety and health regulations and the governmental agencies, the consumer products acts, prevention by design, privacy regulations, and safety and security standards. The Security in Remote Laboratories and OLMS section entails data security, instrument security, and the classification of security attacks and their consequences. Finally, the Proposed Solutions are divided into general security concerns, security frameworks, access control and authentication, communication security, threats and vulnerabilities, and integrity and monitoring. In the feature diagram, the mandatory elements are marked with a black circle, while optional elements are marked with a white circle, providing flexibility in different regulatory and security contexts. This structured approach helps define a taxonomy for understanding and analyzing OLMS's safety and security concerns.

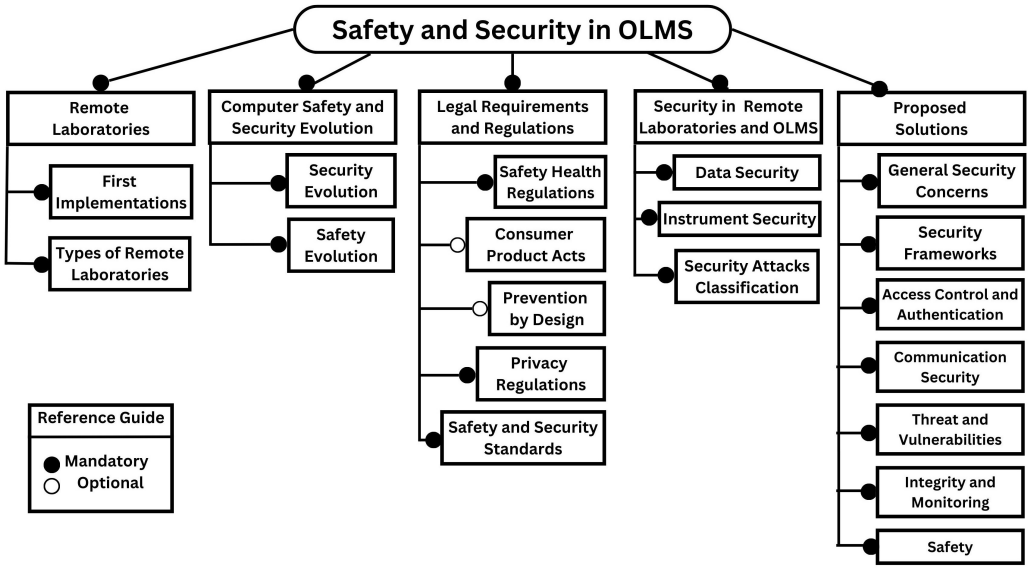


Figure 1. Feature diagram of the taxonomy.

2.2. Method

The search strategy for this systematic literature review (SLR) incorporated the Scopus and Research Rabbit AI tools. We selected Scopus because it is a valuable resource for citation tracking and research analysis to identify key publications within the defined scope. On the other hand, Research Rabbit is an AI web-based tool designed to discover and explore academic papers. It uses citations from seed papers to find connections between them and authors using visual maps, making it easier to understand how different pieces of research are connected.

We used the following search queries in the Scopus database:

- Query 1 (Q1): TITLE-ABS-KEY ((safety OR security) AND (online AND laboratory AND management AND systems) OR (remote AND laboratories)).
- Query 2 (Q2): TITLE-ABS-KEY (first AND implementation AND remote AND laboratories) AND (history).
- Query 3 (Q3): TITLE-ABS-KEY (legal AND safety AND security AND requirements AND regulations).
- Query 4 (Q4): TITLE-ABS-KEY (computer AND safety AND security AND evolution).
- Query 5 (Q5): TITLE-ABS-KEY ((threat OR vulnerabilities) AND (remote AND laboratories)).

The findings for each query are summarized in Table 1, which outlines the total number of papers identified, the number of papers considered relevant, and the categorization of papers as potentially related or unrelated. From the Scopus searches, we gathered 381 papers. Subsequently, the Research Rabbit query, employing the keywords Safety, Security, Online Laboratory Management Systems, and Remote Laboratories, returned 58 papers in total. After the removal of duplicates, the subsequent title, abstract, and keyword screening yielded 37 papers for the SLR. From this subset, 21 papers were chosen to analyze the proposed solutions.

Table 1. Number of papers in each query.

Query	Total Number	Related	Possible Related	Not Related
Q1	381	32	93	256
Q2	215	5	25	185
Q3	148	0	3	145
Q4	223	1	28	194
Q5	233	31	8	184
Research Rabbit	58	10	7	41

3. Literature Review

3.1. Remote Laboratories

The development of laboratory stations controlled remotely began in the 1990s when Aburdene et al. [12] presented an innovative solution for laboratory equipment shared through online platforms to improve hands-on learning in education. In 1996, the University of Oregon introduced the "Second Best to Being There" (SBBT) approach. The principal objective was to extend the accessibility of existing equipment to a larger number of students accessing the physical laboratory through the Internet, using User Datagram Protocol/Internet Protocol (UDP/IP) for communication. The primary focus of its application was on teaching control systems. The experience achieved was found to be very similar to the experience using the real equipment. Numerous distance-learning scenarios included virtual classrooms, establishing a feeling of actual presence or telepresence. The SBBT approach replicates the local laboratory environment for students participating remotely. A successful distance-learning application is built on three essential components: active engagement in learning, data collection capabilities, and adherence to safety guidelines [13]. It marked the first time undergraduate students could fully engage with a virtual laboratory setup [14]. After that, several proposals for remote laboratories emerged, incorporating advanced techniques such as virtual reality (VR), digital twins, and robotics. Additionally, the scope of virtual laboratories expanded to new fields like chemistry, physics, cybersecurity, and engineering, among others [15].

Based on the technology applied to design the laboratory experiment, remote laboratories can be classified into physical, online, and hybrid laboratories. Physical labs include on-site and mobile setups, while online labs consist of remote and virtual configurations. A hybrid laboratory may combine physical labs (such as on-site and mobile variants) or online labs (such as remote and virtual options) or even integrate elements from both physical and online labs [16]. Online laboratories can be further categorized as follows:

- Remote laboratories based on client–server applications: Users access the laboratory remotely by identifying themselves, allowing them to participate in experiments and record their activities. A common disadvantage is installing specific software on client devices, which some educational institutions may restrict to prevent potential virus infections or security vulnerabilities.

- Remote laboratories based on Internet technologies: This category includes remote labs that only require a web browser on the client side, with a web server on the server side to facilitate communication with the laboratory hardware [17].

3.2. Computer Safety and Security Evolution

3.2.1. Security

In October 1967, the US Department of Defense (DoD) [18] created a working group to tackle security issues concerning classified data in computer systems intended for remote access and resource sharing. In collaboration with the National Computer Security Center (NCSC) [19], they released a set of security evaluation criteria known as the *Orange Book*, or *Trusted Computer System Evaluation Criteria* (TCSEC) [20]. The NCSC's role was to conduct product evaluations based on these criteria. The objective of the *Orange Book* was to specify the functionalities at assurance levels to mitigate defined levels of risk. This framework supported the creation of operating systems that ensured compliance with US government standards [21]. The *Orange Book* is part of a series of documents published by the DoD, known as the *Rainbow Series*, which were issued in 1983, updated in 1985, and later replaced by the Common Criteria international standard in 2005 [22].

In the United Kingdom, a similar initiative emerged in 1982 when the Communications-Electronics Security Group (CESG) [23] was appointed as the national authority overseeing government systems handling classified information. CESG developed a comprehensive set of criteria for evaluating complete systems, including physical, personnel, and administrative aspects. Their evaluation framework became operational in 1984. In 1987, the Department of Trade and Industry (DTI) [24] established the Commercial Computer Security Centre (CCSC) [25] to advance the UK industry's interests. The CCSC developed globally recognized security evaluation criteria for various product categories and market sectors to achieve this. The CCSC recognized the value of refining the *Orange Book* by separating its security functionality requirements from its assurance prerequisites. CESG and many other countries supported this approach, including France, Germany, the Netherlands, and Canada. The goal was to enable the creation of both straightforward, highly secure products, like cryptographic devices, and more complex systems, such as databases, with appropriately scaled assurance levels. Additionally, the Commission of European Communities [26] published the *Information Technology Security Evaluation Criteria* (ITSEC) [27], which incorporated security evaluation standards from France, Germany, the Netherlands, CESG, and the CCSC. These countries also developed the *Information Technology Security Evaluation Manual* (ITSEM), which provided the technical foundation for the evaluation process and its certification [21].

On the other hand, in 1990, the US Computer Security Act [28] granted authority to the US National Institute for Standards and Technology (NIST) [29], mirroring the powers held by the UK's DTI. As a result, NIST formed a similar partnership with the National Computer Security Center (NCSC) [30], akin to the DTI's collaboration with CESG. Meanwhile, as the ITSEC and ITSEM frameworks evolved, NIST initiated the US Federal Criteria. At the same time, Canada introduced its criteria, distinguishing between functionality and assurance while identifying key security functional components and offering guidance on their integration. The US viewed ITSEC as the first step toward an international standard, with the Canadian criteria following as the subsequent development [21].

3.2.2. Safety

Safety and security have evolved into different disciplines for several years, even when they have shown a close relationship and shared numerous common traits. In 1989, Anderson [31], in his paper "Safe and Secure Computer Systems", suggested that

reliability, safety, and security hold a significant meaning and importance beyond mere semantic distinctions within their respective domains. However, there are also valuable similarities between them that can be beneficial to explore and utilize. In addition, in the early 90s, Jonsson [32] and Brewer [21] also shared similar concepts. However, they started to emphasize the interrelation between both concepts. Pietre-Cambacedes et al., in their paper "Cross-fertilization between safety and security engineering" [33], discuss the methods, models, tools, and techniques developed in the field of safety engineering and their application in security engineering and vice versa. Later, Uckelmann et al. [34], in their paper "Safety and Security in Federated Remote Labs—A Requirement Analysis", expressed the need to look jointly at safety and security because separate research efforts can be time-consuming and very expensive. They also highlighted that the topic of safety for security in the context of cyber–physical systems is currently an area of research.

The safety of a system is the probability that it will either perform its intended function correctly or cease its processes in a manner that does not disrupt the overall functioning of the system or put at risk the well-being of individuals associated with it [35].

The security of a computer system is the capability to defend against unauthorized access, intentional disruptions, or attacks directed at its assets, such as data, hardware, and software. This safety concept operates based on aggressive functions initiated by individuals, also known as attackers, who want personal benefits through illegal activities. Security is typically characterized by fundamental aspects of the CIA triad, which consist of confidentiality (the computing system's capacity to safeguard system assets by blocking unauthorized access, ensuring that information remains undisclosed to unapproved parties), integrity (the computer system's capability to protect data and other assets from unauthorized tampering, deletion, or destruction), and availability (the system's ability to provide uninterrupted services to authorized users, even when faced with potential attacks) [32].

3.3. Legal Safety and Security Requirements and Regulations

3.3.1. Safety and Security Regulations

Safety rules and protocols vary in counties and regions. Legal standards are required to protect products, work places, and public health [34]. The most important professional safety and health rules include instructions in the European Union 89/391 [36], Vocational Safety and Health Administration in the United States (OSHA) [37], Health and Safety Guidance 65 (HSG 65) [38] United Kingdom, Work Health and Safety (WHS) [39] in Australia, and others. Table A1 compares the main aspects of the most known safety and security regulations (See Appendix A).

3.3.2. Safety Consumer and Product Acts

In 1972, the US Congress adopted the Consumer Product Safety Act (CPSA) [40], which created the Consumer Product Safety Commission (CPSC) [41]. This federal law grants the CPSC the authority to create safety standards for consumer products, assess potential hazards, issue recalls for products that present unreasonable risks of injury to the public, and protect consumers from unsafe products, including toys, appliances, and furniture. Other countries have taken similar steps. For example, the Canada Consumer Product Safety Act was implemented on 14 December 2010, which replaced Part I of the Hazardous Products Act (HPA) [42]. This Act intends to safeguard the consumer's safety by managing or preventing risks associated with human health. The primary legislation for consumer protection in the UK, the Consumer Rights Act [43], mandates that goods, services, and digital content comply with quality standards while protecting consumers from deceptive business practices and unfair contract terms. It also gives consumers the

right to refunds, repairs, or replacements for defective products. In the EU, the General Product Safety Regulation (GPSR) [44] was passed on 12 December 2024, and stipulates that all companies must verify that their products are safe under normal usage by conducting risk assessments, clearly labeling them with safety information, and keeping a tracking system linking them to their original producers. In Australia, the Australian Consumer Law (ACL) [45] includes provisions regarding product safety, liability, and consumer protections while granting the Australian Competition and Consumer Commission (ACCC) [46] the authority to regulate and oversee product safety regulations.

3.3.3. Prevention Through Design

Prevention through design (PtD) [47], also called safety by design in Europe, involves employing strategies to mitigate occupational hazards at the initial stages of the design process. The primary focus is optimizing employees' well-being and safety throughout the entire life cycle of materials and processes. This concept and movement advocates for architects, engineers, and product designers to preemptively address health and safety risks during the developmental phase of designs. Unlike traditional hazard control methods that respond to incidents during construction projects, PtD takes a proactive position by addressing potential risks during the design phase. This methodology immediately eliminates potential health and safety hazards, reducing workers' dependence on personal protective equipment, which is considered the least effective measure in the hazard control hierarchy.

Similar methodologies to control hazards were applied in different countries. For example, the UK government periodically revised the legislation, with the iteration of the Construction Design and Management Regulations [48], intensifying the focus on the responsibilities of principal designers to prevent injuries and fatalities throughout the project's design phase. The Work Health and Safety Act [38] includes provisions for employers, designers, and other parties' construction projects in Australia. This law prioritizes safety in all stages of the construction process. In Singapore, it is known as the Design for Safety (DfS) [49] regulation, which was introduced by the government's initiative in the Workplace Safety and Health Council [50]. This enables the Singapore government to accept construction projects executed with a strong emphasis on security.

3.3.4. Privacy Regulations

There are many data privacy regulations worldwide, but the most well-known one that inspired many of these regulations is the General Data Protection Regulation (GDPR) [51]. GDPR is a comprehensive data protection and privacy regulation in the EU. It was adopted on 25 May 2018, and it changed the previous Data Protection Directive, introducing adequate changes in the procedures for collecting, processing, storage, and exchange of personal data within the EU. In addition, the Digital Fairness Act was proposed and it is expected to be introduced in 2026, addressing deceptive online practices, contracts, influencer marketing, and personalization in digital services.

The California Consumer Privacy Act (CCPA) [52] is exclusively for Californian individuals and businesses in the US. This is the primary data privacy regulation at the state level in the United States. Drawing from GDPR, it has served as a blueprint for equal data privacy rules applied by other states. Effective from July 2020, the CCPA will empower consumers to manage various institutions' use of their personal information.

3.3.5. Safety and Security Standards

There are several organizations' writing standards related to safety and security. The most important are the Institute of Electrical and Electronics Engineers (IEEE) [53], the International Electrotechnical Commission (IEC) [54], the International Organization for Standardization (ISO) [55], the American National Standards Institute (ANSI) [56], the

National Institute of Standards and Technology (NIST) [57], Underwriters Laboratories (UL) [58], the European Committee for Standardization (CEN) [59], the European Committee for Electrotechnical Standardization (CENELEC) [60], the Internet Engineering Task Force (IETF) [61], the International Society of Automation (ISA) [62], and the American Society of Mechanical Engineers (ASME) [63], among others. Table A2 provide an overview of the most essential safety and security standards. We identify three main sectors: occupational health and safety standards, information technology, and product/industrial (See Appendix A).

3.4. Security in Remote Laboratories and OLMS

The security of remote laboratories is focused on two main areas: data security and instrument security. Most OLMSs are designed primarily for educational purposes, but they collect and store student personal data and login credentials. Data stored in the system database must be secured to prevent unauthorized use of the instruments. Because the students can manipulate the laboratory instruments remotely without supervision, the laboratory station's instruments can be at significant risk of being damaged. For this reason, instrument security is one of the most critical security aspects of the OLMS. There are three different levels of instrument security in remote laboratories:

- Inflexible or static sharing: An instrument in a remote laboratory has some possible user input areas; a unique combination of these inputs related to specific functions is required in each laboratory experiment. In this situation, the security level must be controlled by the number of functions related to the inputs and restricting some instrumentation uses.
- Flexible or partial sharing: In this scenario, any input is connected with the corresponding function, and several combinations of this function can perform a range of values in a laboratory experiment activity. Here, the level of security is given by the number of functions allowed to the users over the instrumentation. Given that the user has more control over the instrumentation, it increases the risk of invalid inputs; for that reason, a stricter validation scheme is needed.
- Complete or total sharing: In this case, each input must be attached to an available function over the network with the capability of turning on/off the instruments, giving the user complete control over the remote laboratory instrumentation. The user controls the instrumentation, so strict and strong scheme validation is needed [64].

3.4.1. Classification of Security Attacks in OLMS

Security attacks in remote laboratories can be classified into three primary categories: network-based, access-based, and device-based attacks.

- Network-based attacks target the infrastructure that enables communication between users and remote laboratories, aiming to interrupt data flow or block users from accessing and controlling experiments. Typical network-based attacks, such as denial-of-service (DoS) and distributed denial-of-service (DDoS), can cause system outages, while more sophisticated threats, like man-in-the-middle (MITM) attacks, put at risk data integrity and confidentiality, compromising sensitive information [65–68] .
- Access-based attacks involve unauthorized attempts to gain entry or privileges within the OLMS by exploiting weaknesses in authentication or authorization processes. These attacks can target some components, including hardware, software, and communication channels, exploit vulnerabilities in devices or networks to gain control, manipulate or hijack experiments, or cause serious harm to the integrity of OLMSs. Some examples include attempts to connect using protocols like RDP, WMI, and

FTP, or exploiting vulnerabilities to gain unauthorized control over experiments in remote labs [67,68].

- Device-based attacks target physical devices to undermine their functionality, security, or integrity. These attacks may involve tampering with the hardware, exploiting weaknesses in the device's software or firmware, or causing damage through manipulation or environmental influences. Examples include physical damage, hardware compromise, and attacks exploiting vulnerabilities in remote laboratory devices [67,68].

Table A3 includes an overview of security attacks classification (See Appendix A).

3.4.2. Impact of Security Attacks in OLMS

The potential damage caused by a security attack on OLMSs is proportional to the complexity of the remote laboratories. Remote laboratories with simple setups are less at risk of severe damage, though server failures could disrupt their operation. Basic security measures are enough to address these issues. On the other hand, when dealing with more advanced remote laboratories integrating complex hardware and software, vulnerabilities increase. A malicious user gaining control of the system could send harmful commands, disrupt experiments, damage equipment, or even trigger dangerous situations like flooding or fires. This risk is even higher in scientific remote labs that rely on expensive, highly specialized instruments. A security attack in these cases could lead to severe financial losses alongside the potential dangers mentioned earlier. Because of this, different remote environments require specific security measures to prevent attacks and protect the integrity of the experiments and the system's safety [67].

3.5. Safety and Security Issues and Solutions Proposed

Several researchers have considered safety and security in the last decades. For example, Maiti et al. [69] explored safety concerns in remote laboratories where several users implement and share experiments within collaborative systems. They identified different factors for system reliability: the architecture and main elements of the rigs, along with the characteristics of the network and the roles of users and developers. In addition, to address hardware/software failures, Casini M. et al. [70] proposed a method that involves deploying a bootable live CD on the server side of the remote laboratory to reduce downtime caused by hardware or software failures and to improve the system's overall reliability. Kozík et al. [17] recommended robust authentication mechanisms, mainly for access control. They also pointed out the need for firewall protection and Intrusion Detection Systems (IDSs) to safeguard against unauthorized access and misuse. Marangé et al. [71] introduced a dual validation filter approach to enhance operator and equipment safety that employs a "system validation filter" to check results before sending them out to the plant and a "functional validation filter" to ensure that function usage aligns with the selected autonomy mode, effectively reducing violations of safety constraints. Security against malicious attacks in remote laboratories has been analyzed by Gerža et al. [65], who examined software and hardware risks and recommended best practices to mitigate them. Chellaiah et al. [72] introduced an alternative authentication method using an image-based password system, leveraging a sequence of cartoon images for secure login. Similarly, Krbeček et al. [67] focused on user registration, authentication via a username–password system, and emphasizing secure data storage within a Learning Management System (LMS). In addition, Krbeček et al. [73] propose a two-layered communication framework that ensures data reliability through the TCP/IP protocol and created a specialized data communication and diagnostic interface designed for individual remote experiments within the RLMS (Remote Laboratory Management System).

Sáenz et al. [74] developed a client–server configuration to enable remote connectivity with hardware devices. The client receives a JavaScript application using this approach while the server executes Java processes. A similar approach was implemented by Herrera et al. [75], who utilized Easy Java Simulation (EJS) to create the interconnection between the real hardware with user interfaces for controlling electrical machines. Their system maintains security by controlling load voltage and frequency in isolated mode, while also supplying active and reactive power to the network. Another security strategy for remote laboratories was introduced by Border [76] who proposed access to the RLES (Remote Laboratories Emulation System) which facilitates lab access and scheduling via read-only virtual server libraries, which can be copied, stored, and deployed. Li et al. [77] introduced a system where students virtualized environments on their desktop systems, guest operating instances alongside other software on a single physical device. On the network security front, Richter et al. [78] devised a virtual machine-based approach, segmenting network access via two virtual network cards, one managing internal system access and another handling external connections. This design prevents malicious software from infiltrating the broader university network.

Furthermore, Pálka et al. [79] proposed a remote laboratory architecture integrating multiple security zones to regulate user access based on resource privileges. Their model enhances resilience against attacks by balancing control measures with heightened user awareness and robust data protection mechanisms anchored in information assets. This layered approach to security offers a holistic strategy for mitigating risks in remote laboratory environments. Another approach is proposed by Uckelmann et al. [34], who applied the VDI/VDE 2182 guidelines to assessing safety and security in federated laboratories. Additionally, Sanchez-Viloria et al. [80] implemented the MQTT IoT protocol to ensure Smart Adaptive Remote Laboratory (SARL) security. Finally, Werner et al. [81] proposed using blockchain technology for secure access control. Also, Fabini et al. [82] proposed SecTULab, a secure remote laboratory access solution integrated with Moodle. It prioritizes security and privacy and supports group-based lab access using Moodle's features implementing e2e secured access. In addition, Pedraza et al. [83] present BridgeServer, a real-time web server that provides secure access to remote labs by utilizing locally stored credentials. It features secure file downloads, session time management, and automated access control through API validation, which is integrated with a booking system. Alternatively, Al-Maqousi et al. [84] introduce a multilayered security model for remote cyber training laboratories that ensures authentication, monitoring, integrity, encryption, and access control at multiple tiers. This multilayered model incorporates tried-and-true and new methods like multifactor authentication, VPNs, attribute-based access control, and anomaly detection. Moreover, Al-Zoubi [85] incorporated a blockchain-based cyber-physical lab on the Ethereum platform where an Interplanetary Files System (IPFS), and IoT devices programmed in LabVIEW are presented. It uses smart contracts to store and share lab data in a manner that is decentralized and secure. A private blockchain network guarantees confidentiality and protects against attacks. It also ensures students' privacy and the integrity of the learning process, protecting confidentiality, data integrity, availability, and authorization. In addition, Walchatwar et al. [68] presented a comprehensive security analysis of the hardware, communication interfaces, and platform of the IoT-based remote labs (RLabs). The approach focuses on the security aspects, such as a vulnerability assessment using industry-standard tools and executing four targeted attacks to exploit identified weaknesses, such as remote physical hardware manipulation, denial-of-service, man-in-the-middle attacks, and dictionary attacks. Moreover, mitigation strategies are proposed to improve confidentiality, integrity, and availability (CIA), aiming to provide secure platforms for practical learning experiences in science and engineering education.

Ensuring laboratory safety and security prevents malfunctioning incidents and intentional damage. Educational institutions like universities and schools must be particularly cautious about safety and security concerns, as remote labs in these settings are highly susceptible to potential risks. Each educational institution must have safety and security rules for physical and virtual laboratories. Some universities require that the students take safety and security training before using a laboratory [34].

Table A4 include an overview of the research addressing safety and security and remote laboratories (see Appendix A).

4. Results

An exhaustive analysis of the existing literature on safety and security solutions for OLMSs and remote laboratories revealed seven key areas of focus: general security concerns, security frameworks, access control and authentication, threats and vulnerabilities, integrity and monitoring, communication security, and safety. In Table 2, we use these seven focus areas to re-classify the papers we found that suggest the solutions. However, despite these solutions, several critical gaps emerged. For example, the technical complexity inherent in developing secure OLMSs presents a significant barrier when specialized skills and resources are required. It could increase the risk of security vulnerabilities due to the demand for specialized skills. Simplifying this process would broaden developer participation and enhance overall security. While standard technologies are often employed, a lack of standardized architecture creates heterogeneity and prevents scalability and widespread adoption, particularly for educational purposes. Even though research benefits from diverse systems, standardized OLMSs would make education easier. In addition, we identify a lack of security patterns specialized for remote laboratories. The development of security patterns would offer numerous benefits, for example, providing developers with ready-to-use security strategies and simplifying the creation of secure OLMSs. These security patterns would support the creation of consistent reference architectures and frameworks, leading to uniform security best practices in all implementations. Integrating a "security by design" philosophy, informed by these patterns, would significantly reduce vulnerabilities and improve the overall security posture of online laboratories.

Table 2. Safety and security solutions.

General Security Concerns	Security Frameworks	Access Control and Authentication	Threat and Vulnerabilities	Integrity and Monitoring	Communication Security	Safety
Saenz J. et al. [74]	Maiti A. et al. [69]	Pedraza B. et al. [83]	Walchatwar et al. [68]	Al-Zoubi, A. et al. [85]	Sanchez-Viloria J.A. et al. [80]	Casini, M. et al. [70]
Uckelmann D. et al. [34]	Li P. et al. [77]	Werner E. et al. [81]	Gerza, M. et al. [65]		Krbecek, M. et al. [73]	Kozik T. et al. [17]
Border C. et al. [76]	Richter Th. et al. [78]	Fabini J. et al. [82]	Krbecek M. et al. [67]		Palka L. et al. [79]	Maiti A. et al. [69]
	Chellaiah P. et al. [72]					Marange P. et al. [71]

5. Conclusions and Future Work

Several educational institutions incorporate an OLMS to provide an interactive learning system that allows students to control professional engineering equipment and acquire practical, real-life experience via online remote laboratories with 24/7 access. However, implementing these online remote laboratories entails specific safety and security risks that must be foreseen before implementation. In addition, these implementations must comply with international or federal standards and regulations and the University's specific laboratory use rules.

This paper presented a literature review of safety and security for these OLMSs, and discussed privacy and security standards and regulations developed by different

nations and standards development organizations. This analysis resulted in a taxonomy, and categorizations of security attacks and proposed solutions that will facilitate the development of design patterns and architectures needed to attain security by design in remote laboratories.

The SARL research group actively participates in multiple IEEE standard development working groups and incorporates emerging standards into the SARL platform to remain current and align with latest developments in e-learning. By adopting and implementing safety and security standards, SARL can build a strong framework to safeguard user data, prevent unauthorized access, maintain the integrity and confidentiality of information exchanged during remote online laboratory sessions, and ensure to constrain parameters for the safe operation of laboratory stations. The next step is the documentation of best practices in the form of UML models organized in secure design patterns for OLMS platforms and their remote laboratories that can be combined to form a cohesive, secure architecture.

In January 2025, the IEEE Learning Technology Standards Committee [86] approved the creation of a new Total Learning Architecture (TLA) [87] Study Group. This group aims to lay the foundation to develop technical specifications, standards, and policy guidance for integrating current and emerging learning technologies into an integrated, interoperable learning services environment. This capability will enable personalized, data-driven, and technology-enabled lifelong learning across academia, industry, and government agencies.

Funding: This research received no external funding.

Data Availability Statement: Not applicable

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

Appendix A

Table A1. Safety and security regulations.

Aspects	Directive 89/391	OSHA	HSG65	WHS
Scope	EU's general occupational safety and health principles.	U.S. federal agency overseeing workplace safety and health.	UK guidance for managing health and safety.	Australian model for workplace health and safety.
Focus	General safety framework.	US federal agency overseeing.	UK guidance for managing health.	Integrated approach to workplace health and safety.
Key Concepts	Employer and employee responsibilities, risk assessment, and preventive measures.	Employer responsibilities, standards, training, and inspections.	Plan–Do–Check–Act model, leadership, and risk management.	Duty of care, consultation, cooperation, and risk assessment.
Enforcement	Implemented by EU member states' laws and regulations.	Enforced by OSHA through inspections, citations, and fines.	Guidance rather than regulation based on risk management.	Regulated and enforced by Australian authorities.
Reporting	Involves risk assessment and reporting of hazards and measures.	Reporting requirements for workplace incidents, injuries, and illnesses.	Emphasizes reporting incidents, near-misses, and lessons learned.	Requires reporting of certain incidents and hazards.
Documentation	May require documentation of risk assessments and preventive measures.	Requires documentation of safety policies, training, incidents, and more.	Encourages documentation of risk assessments and safety measures.	Requires records of incidents, training, and assessments.
Participation	Requires worker involvement in safety and health matters.	Emphasizes worker rights, reporting, and involvement.	Encourages employee involvement in safety management.	Involves worker consultation and representation.

Table A1. *Cont.*

Aspects	Directive 89/391	OSHA	HSG65	WHS
Improvements	Promotes a cycle of planning, acting, and evaluating for improvement.	Encourages continuous improvement in workplace safety.	Promotes a cycle of planning, acting, and evaluating for improvement.	Emphasizes ongoing improvement in health and safety.

Data from [36–39].

Table A2. Safety and security standards.

Standard/Initiative	Sector	Remarks
IT-Grundschutz [88]	IT	The IT-Grundschutz methodology, developed by Germany's Federal Office for Information Security (BSI), offers a systematic framework for identifying and implementing cybersecurity measures across organizations. It is designed to align with the international standard for information security management systems [89] .
HSG 65 (UK) [38]	Occupational health and safety	British guidelines mainly targeting executives, proprietors, and supervisors, especially those responsible for establishing or supervising their organization's health and safety protocols. This guidance can also benefit employees, their representatives, professionals, and educators specializing in health and safety practices.
ISA/IEC 62443 [90]	IT	This standard was developed by the International Society of Automation (ISA) and the International Electrotechnical Commission (IEC), outlines a framework for securing Industrial Automation and Control Systems (IACSs). It offers a systematic approach to safeguarding industrial networks, systems, and components against cyber threats.
ISO 45001 [91]	Occupational health and safety	Facilitates the creation of secure and wellness-oriented work environments, prevent potential hazards, promoting the ongoing enhancement of processes, and diminishing risks persistently. Replaces the OHSAS 18001 standard.
ISO/IEC 27000 [89]	IT	The ISO 27000 family is a series of international standards that provide guidelines and best practices for information security management.
ISO/IEC 15408 [92]	IT	This standard is intended to be utilized as the fundamental basis for appraising the security attributes of IT products.
Information Security Forum (UK) [93]	IT	Designed for experts in risk management, information security management, and security practitioners, SOGP assists organizations by enhancing agility in capitalizing on new opportunities while effectively handling linked risks and swiftly addressing ever-changing threats to prevent costly incidents, operational disruptions, and harm to reputation. Recognizing and fulfilling regulatory and compliance mandates.
NERC 1300 [94]	IT	This standard requires organizations to recognize and safeguard essential cyber assets linked to the dependable functioning of the bulk electric system.
NIST SP 800-53 [95]	IT	NIST 800-53, developed by the National Institute of Standards and Technology, is a cybersecurity standard and compliance framework. It establishes standards, controls, and assessments to address various risk factors, cost considerations, and organizational capabilities.
VDI/VDE 2182 (Germany) [96]	IT	This standard outlines the implementation of precise measures to ensure the IT security of automated machinery and industrial facilities. It encompasses considerations regarding the automation devices, systems, and applications employed in automation processes.
ISO 31000 [97]	IT	Risk management guidelines provide principles, the framework, and the process for effectively handling risks. It applies to organizations of all sizes across various sectors and industries.

Table A2. *Cont.*

Standard/Initiative	Sector	Remarks
IEEE Cybersecurity Initiative [98]	IT	The IEEE Cybersecurity Initiative (CYBSI) was introduced through collaboration between the IEEE Computer Society and the IEEE Future Directions Committee in 2014. The objective is establishing a primary online platform for security and privacy experts, enhancing students' and educators' understanding of cybersecurity, and enhancing the design and execution of security and privacy measures by professionals. The CYBSI offers a collection of standards and initiatives designed to tackle fundamental components of the cybersecurity framework.
ETSI EN 303 645 [99]	IT	It is an international standard designed for consumer IoT devices. This standard establishes a foundational level of security to shield IoT devices from prevalent cyber threats, as well as from extensive and orchestrated malicious activities like distributed denial-of-service (DDoS) attacks and unauthorized surveillance of individuals' private lives.
FIPS 140 [100]	IT	Developed by the NIST, FIPS 140 outlines the security criteria to be met by cryptographic modules, offering four tiers to include diverse potential uses and settings. It aims to ensure the security of the cryptographic module's design and execution, such as specification, interfaces, authentication, state model, physical security, operational conditions, key management, electromagnetic compatibility, self-tests, design reliability, and countermeasures against various attacks.
ACSC Essential Eight [101]	IT	The ACSC Essential Eight refers to a set of cybersecurity strategies outlined by the Australian Cyber Security Centre (ACSC). It outlines the security criteria to be met by cryptographic modules, offering four tiers to include diverse potential uses and settings. It aims to ensure the security of the cryptographic module's design and execution, such as specification, interfaces, authentication, state model, physical security, operational conditions, key management, electromagnetic compatibility, self-tests, design reliability, and countermeasures against various attacks.
IEC 61508-1:2010 [102]	Product	IEC 61508-1:2010 is a component of the IEC 61508 series, an international standard dedicated to securing the functional safety of electrical, electronic, and programmable electronic systems.
ANSI Z10 [103]	Occupational health and safety	Occupational safety and health management systems aid organizations in recognizing and mitigating safety and health hazards. This process involves diminishing the likelihood of incidents, adhering to regulations, and executing interventions to lower risk levels.
IEC 61511 [104]	Industrial	This is a technical guideline that outlines methodologies for engineering systems designed to safeguard industrial processes by employing instrumentation. These systems, known as Safety Instrumented Systems, are integral for ensuring process safety.
UL 2900 [105]	Product	UL 2900 is a set of cybersecurity standards developed by Underwriters Laboratories (UL) to assess the security capabilities of network-connected products.

Source: adapted and expanded from [34].

Table A3. Security attacks classification.

Category	Attack Type	Target	Effect	Methods
Network-Based	Denial-of-service (DoS) and distributed denial-of-service (DDoS)	OLMS servers and networks	Prevents legitimate users from accessing services, causing downtime	CMP flood (Ping of Death): overloads servers with oversized ping packets (can be DoS or DDoS) SYN flood: floods system with incomplete TCP connection requests UDP flood: xonsumes network resources with excessive UDP packets HTTP flood: overwhelms web interfaces with fake requests, crashing the system
	Spoofing, altered, and replayed routing attacks	Communication between IoT devices and remote labs	Attackers inject false routing data to manipulate information flow	Fake error messages, routing loops, or unauthorized redirection
	Man-in-the-middle (MITM) attacks	Communication between remote lab users and servers	Intercepted credentials or altered experimental data	Attackers impersonate legitimate servers to deceive users

Table A3. *Cont.*

Category	Attack Type	Target	Effect	Methods
Access-Based	Unauthorized remote access (RDP, FTP, and SSH exploits)	Remote laboratory servers with public IPs	Attackers gain full control over OLMS	RDP exploit: an attacker can use brute-force methods to guess credentials and gain remote access to the system; once in, they can manipulate experiments or data FTP exploit: attackers can exploit vulnerable FTP services by downloading, uploading, or modifying sensitive files on the server SSH exploit: attackers can exploit SSH vulnerabilities to gain unauthorized access, control remote systems, or steal sensitive data
	Fake identity attacks	Remote authentication systems	Attackers impersonate users to execute malicious commands	Credential theft via phishing, social engineering, or database breaches
Device-Based	Physical tampering and power supply manipulation	Sensors, actuators, and lab hardware	Device malfunction, data manipulation, or permanent damage	Overloading circuits, altering firmware, or triggering power surges
	Device property exploits (low-end vs. high-end devices)	Low-end: limited processing power (easier to exploit)	Low-end: vulnerable to simple exploits	Exploiting security weaknesses based on device capabilities
		High-end: more secure but susceptible to advanced threats	High-end: Targeted with malware injection	

Data from [65–68].

Table A4. Overview of the research addressing safety and security and remote laboratories.

Author/Year	Issue	Solution
Al-Maqousi., 2024 [84]	Security	Introduced a multilayered security model for remote cyber training laboratories, incorporating innovative techniques like multifactor authentication, VPNs, attribute-based access control, and anomaly detection, ensuring robust authentication, monitoring, integrity, encryption, and access control across multiple tiers.
Al-Zoubi A. et al., 2023 [85]	Security	Implemented a secure, decentralized cyber-physical lab using blockchain, IPFS, and IoT devices, leveraging smart contracts for data storage and sharing, and a private blockchain network to ensure confidentiality, integrity, availability, and authorized access, thus protecting student privacy and the learning process.
Border C. et al., 2007 [76]	Security	Access to the RLES (Remote Laboratories Emulation System) was facilitated through read-only virtual server libraries, which are capable of being copied, stored, and deployed.
Casini M. et al., 2007 [70]	Safety	Proposed a technique involving the deployment of a bootable live CD on the server side of the remote laboratory to minimize downtime due to hardware or software failures and to enhance the system's reliability.
Chellaiah P. et al., 2017 [72]	Security	Implemented an image-based password system using a narrative framework that offers a unique approach to enhance both security and user experience on digital platforms.
Fabini J. et al., 2021 [82]	Security	Developed SecTULab, a Moodle-integrated secure remote lab access system, emphasizing privacy and group-based access through end-to-end encryption.
Gerza M. et al., 2014 [65]	Security	Examined the security aspects of remote laboratories against malicious attacks and analyzed the potential risks.
Herrera M.R. S et al., 2013 [75]	Security	Employed EJS (Easy Java Simulation), which permits interaction between the laboratory station and the control panel that monitors operations.
Kozik T. et al. 2012 [17]	Safety	Recommended using an authentication mechanism, firewall, and IDS (Intrusion Detection System).

Table A4. *Cont.*

Author/Year	Issue	Solution
Krbecek M. et al., 2013 [67]	Security	Proposed the creation of automatic logs, the use of a registration-and-reservation system, and the use of Uninterruptible Power Supply in case of a power blackout.
Krbecek M. et al., 2015 [73]	Security	Describes the security measures employed in the TCP/IP protocol and the development of a dedicated data communication and diagnostic interface for individual remote experiments within the RLMS (Remote Laboratory Management System).
Li P. et al., 2008 [77]	Security	Introduced a decentralized virtual lab approach for a distance education course on intrusion detection, utilizing virtualization technology to run multiple virtual machines with diverse operating systems on students' computers.
Maiti A. et al., 2015 [69]	Safety	Described the features and components of distributed Peer-to-Peer Remote Access Laboratories (P2P RAL).
Marange P. et al., 2007 [71]	Safety	To ensure the safety of the remote laboratories, a validation filter approach was used, based on the logical constraints and a modification of the difficulty level of automation.
Palka L. et al., 2016 [79]	Security	Described a series of recommendations and procedures to secure data storage in the data warehouse scheme for the needs of remote laboratories. As a solution, an architecture with a dynamic multitiered trust model is deployed to ensure the security defining the level of access for users.
Pedraza B. et al., 2024 [83]	Security	Incorporated a BridgeServer, which is a real-time web server that ensures secure access to remote labs using locally stored credentials. It includes secure file downloads, session time management, and automated access control through API validation integrated with a booking system.
Richter Th. et al., 2012 [78]	Security	Utilized two separate virtual machines, one used to manage server access and the other to control external access to the virtual machine.
Saenz J. et al., 2016 [74]	Security	Proposed a framework for reusing their VRLs through a Java model running on a server and a JavaScript GUI on the client side.
Sanchez-Viloria J.A. et al., 2021 [80]	Security	Implemented the MQTT protocol (IoT Protocol) to SARL to ensure security.
Uckelmann D. et al., 2021 [34]	Security/Safety	Applied the VDI/VDE 2182 guidelines for assessing safety and security in federated laboratories.
Walchatwar N. et al., 2024 [68]	Security	Analyzed the security of IoT-based remote labs by conducting vulnerability assessments and targeted attacks, followed by proposing mitigation strategies to enhance confidentiality, integrity, and availability for secure educational platforms.
Werner E. et al., 2021 [81]	Security	Proposed the use of blockchain technology to ensure security and access control in remote laboratories.

Source: adapted and expanded from [34].

References

1. Larbaoui, Y. Security, Control and Management of Smart Remote Laboratory for Remote Experiments in Electricity and Electronics. *Int. J. Adv. Trends Comput. Sci. Eng.* **2020**, *9*, 4068–4076. [CrossRef]
2. Pena-Molina, A.E.; Larrondo-Petrie, M.M.; Zapata-Rivera, L.F. The Need for E-Learning Standards for Online Laboratory Management Systems. In Proceedings of the 2022 IEEE Learning with MOOCs (LWMOOCS2022), Antigua Guatemala, Guatemala, 29–30 September 2022; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA , 2022; pp. 240–245. [CrossRef]
3. Latin American and Caribbean Consortium of Engineering Institutions (LACCEI). Available online: https://laccei.org (accessed on 23 January 2025).
4. Organization of American States (OAS). Available online: https://www.oas.org/en/ (accessed on 23 January 2025).
5. SARL. Available online: http://www.labinawindow.com/ (accessed on 23 January 2025).

6. Larrondo-Petrie, M.M.; Zapata-Rivera, L.F.; Aranzazu-Suescun, C.; Sanchez-Viloria, J.A.; Pena-Molina, A.E.; Santana, K.S. Addressing the Need for Online Engineering Labs for Developing Countries. In Proceedings of the 2021 World Engineering Education Forum/Global Engineering Deans Council (IFEES/GEDC), Madrid, Spain, 15–18 November 2021; IEEE: Piscataway, NJ, USA, 2021. [CrossRef]
7. *IEEE 1876–2019*; Standard for Networked Smart Learning for Online Laboratories. IEEE: Piscataway, NJ, USA, 2019. Available online: https://standards.ieee.org/ieee/1876/5482/ (accessed on 23 January 2025).
8. *IEEE P2834*; Standard for Secure and Trusted Learning Systems. IEEE: Piscataway, NJ, USA, 2023. Available online: https://sagroups.ieee.org/2834/ (accessed on 25 January 2025).
9. *P7004.1*; Recommended Practices for Virtual Classroom Security, Privacy, and Data Governance. IEEE: Piscataway, NJ, USA, 2023. Available online: https://standards.ieee.org/ieee/7004.1/10285/ (accessed on 29 January 2025).
10. *P2881*; Standard for Learning Metadata. IEEE: Piscataway, NJ, USA, 2023. Available online: https://standards.ieee.org/ieee/2881/10248/ (accessed on 30 January 2025).
11. ISO/IEC 2700x Information Security Standards Geneva, Switzerland. 2023. Available online: https://www.audit-academy.be/en/glossary/iso-2700x-information-security-standards (accessed on 30 January 2025).
12. Aburdene, M.F.; Mastascusa, E.J.; Massengale, R. A Proposal for a Remotely Shared Control Systems Laboratory. In Proceedings of the Frontiers in Education Twenty-First Annual Conference, Engineering Education in a New World Order, West Lafayette, IN, USA, 21–24 September 1991; IEEE: Piscataway, NJ, USA, 1991; pp. 589–592. [CrossRef]
13. Machotka, J.; Nafalski, A.; Nedić, Z. The History of Developments of Remote Experiments. In Proceedings of the 2nd World Conference on Technology and Engineering Education, Ljubljana, Slovenia, 5–8 September 2011. Available online: http://www.wiete.com.au/conferences/2wctee/papers/17-12-Machotka-J.pdf (accessed on 30 January 2025).
14. Ramirez, D.; Ramirez, M.S.; Marrero, T.R. Novel Use of a Remote Laboratory for Active Learning in Class. *Chem. Eng. Educ.* **2016**, *50*, 1–8 .
15. Andini, N.F.; Dewi, P.M.; Marida, T.A.C.; Wibawa, A.P.; Nafalski, A. A Decade of Evolution of Virtual and Remote Laboratories. *Bull. Soc. Inform. Theory Appl.* **2023**, *7*, 63–73. [CrossRef]
16. Zapata-Rivera, L.F. Models and Implementations of Online Laboratories; A Definition of a Standard Architecture to Integrate Distributed Remote Experiments. Ph.D. Thesis, Florida Atlantic University, Boca Raton, FL, USA, 2019.
17. Kozik, T.; Simon, M. Preparing and Managing the Remote Experiment in Education. In Proceedings of the 2012 15th International Conference on Interactive Collaborative Learning (ICL), Villach, Austria, 26–28 September 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 1–4. [CrossRef]
18. U.S. Department of Defense (DOD). Available online: https://www.defense.gov (accessed on 13 January 2025).
19. Office of the Director of National Intelligence (NCSC). National Cyber Security Center. Available online: https://www.dni.gov/index.php/ncsc-home (accessed on 13 January 2025).
20. *DOD 5200.28-STD*; Trusted Computer System Evaluation Criteria. US Department of Defense: Washington, DC, USA, 1985.
21. Brewer, D.F.C. Applying Security Techniques to Achieve Safety. In Proceedings of the 3rd Safety-Critical Systems Symposium (SSS'93), Bristol, UK, 30 August–3 September 1993; pp. 246–256.
22. Common Criteria International Standard. Common Criteria Portal. Available online: https://commoncriteriaportal.org (accessed on 30 January 2025).
23. Communications-Electronics Security Group (CESG). Available online: https://www.gov.uk/government/organisations/cesg (accessed on 30 January 2025).
24. Department of Trade and Industry (DTI). Available online: https://www.dti.gov.ph (accessed on 30 January 2025).
25. Commercial Computer Security Centre (CCSC). Available online: https://www.cyber.gc.ca/en (accessed on 1 January 2025).
26. Commission of European Communities. Available online: https://sdgs.un.org/statements/commission-european-community-14908 (accessed on 1 January 2025).
27. Information Technology Security Evaluation Criteria (ITSEC). ITSEC Wikipedia. Available online: https://en.wikipedia.org/wiki/ITSEC (accessed on 1 January 2025).
28. US Computer Security Act. Available online: https://www.govinfo.gov/app/details/BILLS-114s1990is (accessed on 1 January 2025).
29. US National Institute for Standards and Technology (NIST). Available online: https://www.nist.gov/ (accessed on 1 January 2025).
30. National Computer Security Center (NCSC). Available online: https://www.dni.gov/ncsc (accessed on 1 January 2025).
31. Anderson, T. *Safe and Secure Computer Systems*; Blackwell Scientific Publications: London, UK, 1989.
32. Jonsson, E.; Olovsson, T. On the Integration of Security and Dependability in Computer Systems. In Proceedings of the IASTED International Conference on Reliability, Quality Control and Risk Assessment, Washington, DC, USA, 4–6 November 1992; pp. 93–97.
33. Pietre-Cambacedes, L.; Bouissou, M. Cross-Fertilization Between Safety and Security Engineering. *Reliab. Eng. Syst. Saf.* **2013**, *110*, 110–126. [CrossRef]

34. Uckelmann, D.; Mezzogori, D.; Exposito, G.; Neroni, M.; Reverberi, D.; Ustenko, M. Safety and Security in Federated Remote Labs—A Requirement Analysis. In *Cross Reality and Data Science in Engineering, REV 2020, Advances in Intelligent Systems and Computing*; Springer: Cham, Switzerland, 2020; Volume 1231. [CrossRef]
35. Yang, S.; Sang, N.; Xiong, G. Safety Testing of Safety-Critical Software Based on Critical Mission Duration. In Proceedings of the 10th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC'04), Washington, DC, USA, 3–5 March 2004; pp. 97–102.
36. Directive 89/391. ISA. 2023. Available online: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards (accessed on 12 January 2025).
37. OSHA. 2023. Available online: https://www.osha.gov (accessed on 12 January 2025).
38. HSG65. 2023. Available online: https://www.hse.gov.uk/pubns/books/hsg65.htm (accessed on 12 January 2025).
39. Safe Work Australia. 2023. Available online: https://www.safeworkaustralia.gov.au (accessed on 12 January 2025).
40. US Consumer Product Safety Act (CPSA). 2023. Available online: https://www.cpsc.gov/s3fs-public/pdfs/blk-media-cpsa.pdf (accessed on 12 January 2025).
41. National Commission on Product Safety (NCPS). 2023. Available online: https://www.usa.gov/agencies/consumer-product-safety-commission (accessed on 12 January 2025).
42. Canada Consumer Product Safety Act. 2023. Available online: https://www.canada.ca/en/health-canada/services/consumer-productsafety/reports-publications/industry-professionals/canada-consumer-product-safety-act-guide.html (accessed on 12 January 2025).
43. UK Consumer Protection Act. 2023. Available online: https://iclg.com/practice-areas/consumer-protection-laws-and-regulations (accessed on 12 January 2025).
44. General Product Safety Regulation (GPSR). 2024. Available online: https://trade.ec.europa.eu/access-to-markets/en/news/eus-general-product-safety-regulation-gpsr-new-era-consumer-protection (accessed on 10 January 2025).
45. Australian Consumer Law (ACL). 2023. Available online: https://consumer.gov.au (accessed on 12 January 2025).
46. Australian Competition and Consumer Commission (ACCC). 2023. Available online: https://www.accc.gov.au (accessed on 12 January 2025).
47. Prevention Through Design (PtD). 2023. Available online: https://www.cdc.gov/niosh/docs/2011-121/pdfs/2011-121.pdf (accessed on 12 January 2025).
48. Construction Design and Management Regulations. 2023. Available online: https://www.hse.gov.uk/construction/cdm/2015/index.htm (accessed on 12 January 2025).
49. Design for Safety (DfS). 2023. Available online: https://www.tal.sg/wshc/topics/design-for-safety/about-design-for-safety (accessed on 12 January 2025).
50. Workplace Safety and Health Council (WSHC). 2023. Available online: https://www.tal.sg/wshc (accessed on 12 January 2025).
51. General Data Protection Regulation (GDPR). 2023. Available online: https://gdpr-info.eu (accessed on 12 January 2025).
52. California Consumer Privacy Act (CCPA). 2023. Available online: https://oag.ca.gov/privacy/ccpa (accessed on 12 January 2025).
53. IEEE. 2023. Available online: https://www.ieee.org (accessed on 12 January 2025).
54. International Electrotechnical Commission (IEC). 2023. Available online: https://www.iso.org/about-us.html (accessed on 12 January 2025).
55. International Organization for Standardization (ISO). 2023. Available online: https://ansi.org (accessed on 12 January 2025).
56. American National Standards Institute (ANSI). 2023. Available online: https://www.ansi.org/ (accessed on 12 January 2025).
57. National Institute of Standards and Technology (NIST). 2023. Available online: https://csrc.nist.gov/news/2023 (accessed on 12 January 2025).
58. Underwriters Laboratories (UL). 2023. Available online: https://www.ul.com (accessed on 12 January 2025).
59. European Committee for Standardization (CEN). 2023. Available online: https://www.cencenelec.eu/european-standardization/european-standards/ (accessed on 12 January 2025).
60. European Committee for Electrotechnical Standardization (CENELEC). 2023. Available online: https://www.cencenelec.eu/european-standardization/cen-and-cenelec/ (accessed on 12 January 2025).
61. Internet Engineering Task Force (IETF). 2023. Available online: https://www.ietf.org (accessed on 12 January 2025).
62. International Society of Automation (ISA). 2023. Available online: https://www.isa.org (accessed on 12 January 2025).
63. American Society of Mechanical Engineers (ASME). 2023. Available online: https://www.asme.org (accessed on 12 January 2025).
64. Maiti, A.; Tripathy, B. Remote Laboratories: Design of Experiments and Their Web Implementation. *Educ. Technol. Soc.* **2013**, *16*, 220–233.
65. Gerza, M.; Schauer, F.; Jasek, R. Security of ISES Measureserver® Module for Remote Experiments Against Malign Attacks. *Int. J. Online Eng.* **2014**, *10*, 4–10. [CrossRef]

66. Nawir, M.; Amir, A.; Yaakob, N.; Lynn, O.B. Internet of Things (IoT): Taxonomy of security attacks. In Proceedings of the 3rd International Conference on Electronic Design (ICED), Phuket, Thailand, 11–12 August 2016; pp. 321–326. [CrossRef]
67. Krbeček, M.; Schauer, F.; Jasek, R. Security Aspects of Remote e-Laboratories. *Int. J. Online Eng.* **2013**, *9*, 34–39. [CrossRef]
68. Walchatwar, N.; Gureja, A.; Ihita,G.V.; Ojha, A.; Chaudhari, S. Security Analysis of IoT-based Remote Labs. In Proceedings of the 11th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, Austria, 19–21 August 2024; pp. 39–46. [CrossRef]
69. Maiti, A.; Kist, A.; Maxwell, A.D. Design and Operational Reliability of a Peer-to-Peer Distributed Remote Access Laboratory. In Proceedings of the 2015 12th International Conference on Remote Engineering and Virtual Instrumentation, Bangkok, Thailand, 25–27 February 2015.
70. Casini, M.; Prattichizzo, D.; Vicino, A. Operating Remote Laboratories through a Bootable Device. *IEEE Trans. Ind. Electron.* **2007**, *54*, 3134–3140. [CrossRef]
71. Marangé, P.; Gellot, F.; Riera, B. Control Validation of DES Systems: Application to Remote Laboratories. In Proceedings of the 2nd International Conference on Digital Information Management, Lyon, France, 28–31 October 2007.
72. Chellaiah, P.; Nair, B.; Achuthan, K.; Diwakar, S. Using Theme-Based Narrative Construct of Images as Passwords: Implementation and Assessment of Remembered Sequences. *Int. J. Online Eng.* **2017**, *13*, 77–93. [CrossRef]
73. Krbeček, M.; Schauer, F. Communication and Diagnostic Interfaces in Remote Laboratory Management Systems. *Int. J. Online Eng.* **2015**, *11*, 43–49. [CrossRef]
74. Sáenz, J.; Esquembre, F.; Garcia, F.J.; de la Torre, L.; Dormido, S. A New Model for a Remote Connection with Hardware Devices Using Javascript. *IFAC-PapersOnLine* **2016**, *49*, 133–137. [CrossRef]
75. Herrera, M.S.; Márquez, J.A.; Borrero, A.M.; Sánchez, M.M. Testing Bench for Remote Practical Training in Electric Machines. *IFAC Proc. Vol.* **2013**, *46*, 357–362. [CrossRef]
76. Border, C. The Development and Deployment of a Multi-User, Remote Access Virtualization System for Networking, Security, and System Administration Classes. In Proceedings of the 38th SIGCSE Technical Symposium on Computer Science Education, Covington, KY, USA, 7–11 March 2007; ACM: New York, NY, USA, 2007; pp. 576–580. [CrossRef]
77. Li, P.; Mohammed, T. Integration of Virtualization Technology into Network Security Laboratory. In Proceedings of the 38th Annual Frontiers in Education Conference, Saratoga Springs, NY, USA, 22–25 October 2008; p. S2A.
78. Richter, T.; Watson, R.; Kassavetis, S.; Kraft, M.; Grube, P.; Boehringer, D.; Logothetidis, S. The WebLabs of the University of Cambridge: A Study of Securing Remote Instrumentation. In Proceedings of the 9th International Conference on Remote England Virtual Instrumentation (REV), Bilbao, Spain, 4–6 July 2012.
79. Pálka, L.; Schauer, F. Safety of Communication and Neural Networks for Security Enhancement in Data Warehouse for Remote Laboratories and Laboratory Management System. In Proceedings of the 6th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Dallas-Fortworth, TX, USA, 13–15 July 2015.
80. Sanchez-Viloria, J.A.; Zapata-Rivera, L.F.; Aranzazu-Suescun, C.; Molina-Pena, A.E.; Larrondo-Petrie, M.M. Online Laboratory Communication Using MQTT IoT Standard. In Proceedings of the 2021 World Engineering Education Forum/Global Engineering Deans Council, WEEF/GEDC 2021, Madrid, Spain, 15–18 November 2021. [CrossRef]
81. Werner, E.; Matias, J.C.; Berejuck, M.D.; Saliah-Hassane, H. Evaluation of Blockchain Techniques to Ensure Secure Access on Remote FPGA Laboratories. In Proceedings of the 9th International Symposium on Digital Forensics and Security, ISDFS 2021, Elazig, Turkey, 28–29 June 2021; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2021. [CrossRef]
82. Fabini, J.; Hartl, A.; Meghdouri, F.; Breitenfellner, C.; Zseby, T. SecTULab: A Moodle-Integrated Secure Remote Access Architecture for Cyber Security Laboratories. In Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES'21), Vienna, Austria, 17–20 August 2021; Association for Computing Machinery: New York, NY, USA, 2021; p. 148. [CrossRef]
83. Pedraza, B.; Villazón, A.; Ormachea, O. Enhancing Accessibility for Real-Time Remote Laboratories: A Web-Based Solution with Automated Validation and Access Control. In *Smart Technologies for a Sustainable Future*; Auer, M.E., Langmann, R., May, D., Roos, K., Eds.; STE 2024. Lecture Notes in Networks and Systems; Springer: Cham, Switzerland, 2024; Volume 1028. [CrossRef]
84. Al-Maqousi, A. Enhancing Security in Remote Laboratory Environments: A Layered Approach. In Proceedings of the 6th International Conference on Statistics: Theory and Applications (ICSTA'24), Barcelona, Spain, 19–21 August 2024. [CrossRef]
85. Al-Zoubi, A.; Aldmour, M.; Sedky, M.; Aldmour, R. Blockchain Utilization in Cyber-Physical Laboratories for Engineering Education 4.0. In Proceedings of the Open Science in Engineering, REV 2023, Thessaloniki, Greece, 1–3 March 2023; Lecture Notes in Networks and Systems; Auer, M.E., Langmann, R., Tsiatsos, T., Eds.; Springer: Cham, Switzerland, 2023; Volume 763. [CrossRef]
86. IEEE Learning Technology Standards Committee (IEEE LTSC). Available online: https://sagroups.ieee.org/ltsc/ (accessed on 12 February 2025).
87. Total Learning Architecture (TLA). Available online: https://adlnet.gov/projects/tla/ (accessed on 12 February 2025).

88. IT-Grundschutz. Available online: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html (accessed on 8 January 2025).
89. ISO/IEC 27000 Family. Available online: https://www.iso.org/standard/iso-iec-27000-family (accessed on 11 January 2025).
90. *ISA/IEC 62443 Series of Standards*; The World's Only Consensus-Based Automation and Control Systems Cybersecurity Standards. International Auditing and Assurance Standards Board (IAASB): New York, NY, USA, 2025 . Available online: https://www.isa.org/standards-and-publications/isa-standards/isa-iec62443-series-of-standards (accessed on 8 January 2025).
91. *ISO 45001:2018*; Occupational Health and Safety Management Systems—Requirements with Guidance for Use. ISO: Geneva, Switzerland, 2018. Available online: https://www.iso.org/iso-45001-occupational-health-and-safety.html (accessed on 11 January 2025).
92. *ISO/IEC 15408-1:2022*; Information Security, Cybersecurity, and Privacy Protection. ISO: Geneva, Switzerland, 2022. Available online: https://www.iso.org/standard/72891.html (accessed on 11 January 2025).
93. The ISF Is a Leading Authority on Information Security and Risk Management. Available online: https://www.securityforum.org (accessed on 11 January 2025).
94. NERC 1300: Cyber Security Standard. Available online: https://www.nerc.com/pa/Stand/Pages/default.aspx (accessed on 11 January 2025).
95. *NIST SP 800-53 Rev. 5*; Security and Privacy Controls for Information Systems and Organizations. NIST: Gaithersburg, MD, USA, 2025. Available online: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final (accessed on 11 January 2025).
96. *VDI/VDE 2182*; IT-Security for Industrial Automation—General Model. Available online: https://www.vdi.de/richtlinien/details/vdivde-2182-blatt-1-it-security-for-industrial-automation-general-model (accessed on 11 January 2025).
97. *ISO 31000:2018*; Risk Management. ISO: Geneva, Switzerland, 2018. Available online: https://www.iso.org/iso-31000-risk-management.html (accessed on 11 January 2025).
98. IEEE Cybersecurity Initiative. Available online: https://cybersecurity.ieee.org (accessed on 11 January 2025).
99. *ETSI EN 303 645*; Cyber Security for Consumer Internet of Things: Baseline Requirements. ETSI: Sophia Antipolis, France, 2025. Available online: https://www.etsi.org (accessed on 11 January 2025).
100. FIPS 140 Security Requirements for Cryptographic Modules. Available online: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf (accessed on 11 January 2025).
101. ACSC Essential Eight. Available online: https://Cyber.gov.au (accessed on 12 January 2025).
102. *IEC 61508:2010 CMV*; Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems—Parts 1 to 7. IEC: Columbus, OH, USA, 2025. Available online: https://webstore.iec.ch/publication/22273 (accessed on 12 January 2025).
103. *ANSI Z10 Standards*; Occupational Safety and health Management Systems Help Organizations to Continuously Identify and Eliminate Safety and Health Risks, Reduce Incident Potential, Comply with Regulations and Implement Risk-Reducing Interventions. American Society of Safety Professionals: Park Ridge, IL, USA, 2025. Available online: https://www.assp.org/standards/standards-topics/osh-management-z10 (accessed on 12 January 2025).
104. *IEC 61511*; Functional Safety—Safety Instrumented Systems for the Process Industry Sector—Part 1: Framework, Definitions, System, Hardware and Application Programming Requirements. IEC: Columbus, OH, USA, 2025. Available online: https://webstore.iec.ch/publication/24241 (accessed on 12 January 2025).
105. *UL 2900*; Your Destination for Trusted Safety Standards. UL Standards & Engagement: Evanston, IL, USA, 2025. Available online: https://www.shopulstandards.com (accessed on 12 January 2025).

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.