Guideline to Safety and Security in Federated Remote Labs

https://doi.org/10.3991/ijoe.v17i04.18937

Dieter Uckelmann (✉)
HFT Stuttgart, Stuttgart, Germany
dieter.uckelmann@hft-stuttgart.de

Davide Mezzogori, Giovanni Esposito, Mattia Neroni,
Davide Reverberi, Maria Ustenko
University of Parma, Parma, Italy

Jannicke Baalsrud-Hauge
Bremen Institute for Production and Logistics (BIBA),
Bremen, Germany

Abstract—The interest of the educational community in the laboratory- (lab) based education has grown steadily. As remote labs have started to be a reliable alternative to traditional hands-on labs, security and safety issues are becoming increasingly important, as their interconnected nature raises new and challenging issues. The complexity increases when multiple institutions are involved in a federated lab infrastructure. This paper provides a guideline for assessing safety and security in federated labs following the VDI/VDE 2182 guideline and verifies the concept based on remote labs in three different academic institutions.

Keywords—Safety, Security, Remote Labs, Federated Labs

1 Introduction and Context

Recently remote and virtual labs have started to be a reliable alternative to traditional hands-on laboratories. Corresponding lab-networks allow to share costs, provide efficient control of user access to the experiment environment, and may improve the availability of lab-infrastructures [1]. Safety and security in real labs are important issues to avoid both malfunctioning behaviors and intentionally caused harm. This is especially true for remote labs since they are highly connected systems [2]. Remote labs in public institutions such as universities and schools are extremely vulnerable to security issues [3]. Federated remote labs including multiple independent institutions and network structures are yet increasing the security risks involved.

In literature, there has been little focus on safety except e.g. chemistry and biology labs. Although Scopus lists more than 2,000 works on remote and networked labs, few of them discuss safety and security issues in detail. A structured approach to access

safety and security for federated remote labs is missing [4]. Furthermore, most researchers focus either just on safety or security, and they lack work approaching both issues simultaneously. While safety and security are required, the specific requirements of university labs should be considered [4]:

1. The need for a simple solution approach on safety and security, as universities have to deal with a limited number of human recourses for operational tasks.
2. The need to look jointly at safety and security, to reduce effort and address the interplay of both topics influencing each other.
3. The need for a flexible and iterative approach, as university labs are constantly changing, especially in educational topics related to new technologies.

Federated remote infrastructures share similar problems as connected Industry 4.0 environments. Both rely on IT-connected physical worlds which are more vulnerable to cyber-espionage [5]. Consequently, remote access is among the Top10 threats for industrial control systems [6]. There is an increased risk due to digitally increased attack surfaces [7]. While offline labs require physical presence to attack the system, remote labs can be attacked worldwide. Therefore, security issues in the "virtual world" can cause harm in the "physical world". It is eminent, that safety and security for remote labs need to be tackled in a joint approach.

Federated lab-structures with multiple involved independent institutions, regulations, and national or regional laws increase the complexity. Therefore, this paper provides a common guideline for networked lab-infrastructures in general and more specifically for participating labs in DigiLab4U – a research project funded by the German Federal Ministry of Education and Research. The guideline is based on VDI/VDE 2182 "IT-security for industrial automation". The usefulness is shown, based on applying the guideline to three labs in Germany and Italy. The findings and corresponding improvements of the guideline will help further participants in the DigiLab4U network to tackle their security and safety issues when opening their lab-infrastructure to the lab network. The case study can also serve for other federated lab networks on how to set up the infrastructure fitting multiple safety and security criteria.

We have performed literature research on scientific papers related to safety for remote labs and on legal requirements. In the next section, we provide a literature overview on safety and security in remote labs. In section 3 we identify further requirements for remote labs. Based on prior research, we have identified and evaluated different solution approaches and selected VDI/VDE 2182 as a basic guideline [4]. This paper continues this work and verifies the theoretical approach by prototypically applying VDI/VDE 2182 in three different labs currently involved in the DigiLab4U network, described in section/chapter 4. However, this must be seen as an iterative approach that needs to address future changes and additions to the federated lab network. Therefore, we focus on aspects of iterative improvements in section 5.

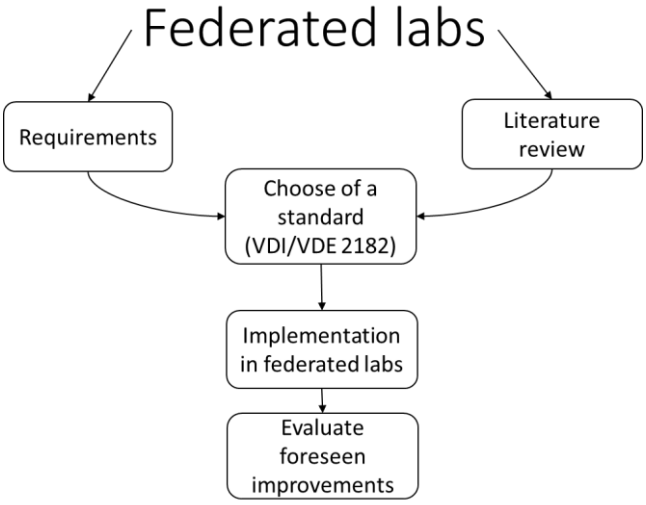

Fig. 1. Methodology map.

2 Literature Review on Safety and Security in Remote Labs

With the aim of performing a review of the existing material on safety and security concerns in remote-labs literature, Scopus was used, as it is one of the largest abstracts and citation database of peer-reviewed literature. The database was queried by using the string (TITLE-ABS-KEY ("remote lab*")) AND (safety OR security). The string complies with the Scopus rules: (i) combinatory rules of AND and OR operators, and (ii) use of asterisk "*" in order to cut the suffix of the word "laboratory" and then consider all its possible declination. Furthermore, the tool is not case sensitive. The query string, as set, gathered 244 documents. The titles and abstracts have been reviewed to only select the papers which are strictly focused on safety and security issues. For instance, thirty-three documents, retrieved out of the full list, propose a holistic description of the developed and implemented solution, and however they do not really discuss safety and security issues in-depth.

Twenty-three papers of interest were detected. By focusing on just the papers in English language available on the web, the final list becomes fifteen papers. Four of them relate to "safety", eleven relate to "security". In the followings, what these papers deal with is reported, distinguishing by the focus (i.e. safety or security).

2.1 Safety

In the researched literature *safety* and *functional safety* are most often used synonymously. According to VDI/VDE 2182 functional safety refers to *"protection against threats to persons and the environment that arise from incorrect functioning of equipment".* The problem of safety in remote laboratories is well discussed by Maiti, Kist &

Maxwell [8]. Their work relates to laboratories where multiple users develop experiments and share them as parts of collaborative systems (i.e. Peer-to-Peer Remote Access Lab). The items on which the reliability of the whole system depends are (i) components and design of experimental rigs, and (ii) network and users (developers) characteristics. Casini, Prattichizzo & Vicino [9] identified the reduction of time to fix software/hardware failure as a key need and solved the issue utilizing a bootable (live) device (CD) on the server-side. Kozík T., Šimon M. [10] suggested implementing a suitable authentication mechanism as the first step to achieve access control. Furthermore, since the remote laboratory is connected to the Internet, it is necessary to protect it by a firewall and by an Intrusion Detection System (IDS), which role is to identify an abuse unauthorized or improper use of a computer system, thus also addressing security issues. Marangé, Gellot & Riera [11] as well as Maiti, Kist & Maxwell [8] proposed an approach using two validation filters to guarantee the safety of the operators and the equipment. It is based on the definition of logical constraints which should in no case should be violated. One filter called "system validation filter" validates outputs before sending them to the plant. The second filter called "functional validation filter" validates the use of the functions regarding the autonomy mode selected. This filter reduces the use of safety constraints which could be violated in the system validation filter.

2.2 Security

In the researched literature security and IT-security are most often used synonymously. According to VDI/VDE 2182 IT-security addresses *"protection against unauthorised access to data and services, in which various aspects of the target of inspection to be protected are described in greater detail by means of security objectives".* Gerža, Schauer & Jašek [12] focused on the security of remote labs against malign attacks. The authors analyze the general and specific software and hardware risks and provide the necessary behavior and practices to implement for preventing them. According to these authors, we have identified three main concerns over security in retrieved papers: (i) users' authentication and authorization (ii) access to and (iii) communication with the server. Ocaya [13] proposed a simplified authentication of permitted clients built-into the server, through alphanumeric username and password (issued at registration and periodically changeable). Chellaiah et al. [14] suggested securing the users' authentication through narrative constructs using a sequence of cartoon images to generate an image-based password system. Krbeček & Schauer [15] also proposed to assure the security of the system employing users' registration and reservation through username-and-password access-system, however, they focused on securing the storage of data into the Learning Management System (LMS) [16]. The solution provided is twofold. Outside communication is based on the TCP/IP protocol, which assures the reliability of data transmission. The inner communication between the experiment and Remote Laboratory Management System (RLMS) *"ensures the transmission of the measured data and preserves them for later use",* using Java language to provide communication and diagnostic services. The use of Java application and tools for security issues concerning the communication between equipment and server has had a widespread development in recent years since the most security applications in virtual and remote labs

(VRLs) are developed with high-level programming tools using Java [17]. Unfortunately, smart devices usually do not run Java. For this reason, Sáenz et al. [17] proposed a structure that allows a remote connection with hardware devices by using a client-server configuration that serves to the client a JavaScript application; leaving the server a task of running the Java part of the virtual and remote lab. A similar solution was deployed in Herrera et al. [18]. They made use of a software solution to provide the security of machinery within their remote bench for testing electrical machine based on Easy Java Simulation (EJS) to connect the real hardware to the user interface for controlling (i) the load voltage and frequency when the machine is connected to the load in an islanded way, and (ii) the active and reactive power injected to the net when the machine is directly connected. To pledge the security of the network of both the single institution and the federated labs (i.e. the universities), the main approach seems to be the use of virtual machines. Border [19] presented the Remote Laboratory Emulation Systems (RLES) solution for accessing and scheduling the labs based on *"read-only libraries of virtual servers that can easily be copied, stored and deployed"*. Li & Mohammed [20] installed the virtual machines on students' personal computers with the guest operating systems and their applications run concurrently on a single physical machine. Richter et al. [21] assured the security of the network by using virtual machines on the users' side, while at the server-side they split the virtual machine into two virtual network cards, the former managing the access to the system from the server itself, and the latter managing the host system making it possible to reach the virtual machine from the outside: *"this small virtual network is otherwise unconnected to the rest of the university system and any potentially malicious programs could not be passed to any other machine on the university campus"*. To provide security to users of the WebLab the authors [1] proposed [22] to use nonintrusive applications. By using those the user can harmlessly utilize any tool, as the application does not allow to read the data from any file at hard disk that the user does not purposely select. Outside communication is based on HTTP protocol that does not need permission on the firewalls.

Finally, a solution summarizing several concepts analyzed employing a remote-lab architecture seems to be the one proposed by Pálka & Schauer [23]. The authors divided the infrastructure into multiple security zones that provide different levels of protection based on whether a user should be granted access to specific resources. Furthermore, to increase flexibility and the ability to recover from a successful attack authors proposed a balanced control and an increased focus on user awareness as well as data protection anchored in the information assets.

3 Requirements for Federated Remote Labs

3.1 Organizational needs for lab-networks

Federated remote lab environments deal with different regional, national, and organizational requirements. To find a common guideline simplicity and flexibility are necessary. Derived from the need for simplicity, we also identify a need to look at safety and security issues jointly. The three needs are described in more detail in the following.

The need for simplicity: Operating university labs is labor-intensive and expensive. Any extra burden, including additional activities for safety and security implied by making labs remotely accessible, will negatively impact the acceptance to integrate labs to a lab network. The need for simplicity is one reason why the VDI/VDE 2182 guideline has been chosen.

The need to look jointly at safety and security: The need on integrating safety and security has been mentioned in the literature, as "safety and security can negatively influence each other, analyzing their interplay in an efficient manner means reducing the effort that needs to be invested in achieving a safe and secure system" [2]. VDI/VDE 2182 is looking at both topics jointly, thus decreasing the overall necessary effort for labs.

The need for a flexible and iterative approach: As university labs are constantly being updated and enhanced through ongoing research, lecturers, researchers, and lab-operators require certain flexibility. Current research approaches "*…lack evaluation of their support for efficient system update handling.*" [2] Iterative safety and security measures need to address the whole lifecycle of the remote labs including development, testing, maintenance, and operation. VDI/VDE 2182 is based on the iterative Deming Cycle – PDCA (Plan, Do, Check, Act) and thus offers the needed flexibility.

3.2 Legal safety requirements

Even though many aspects are regulated in EU directives or national laws, in many cases each country or region has in addition to these more inter-regional regulations, different requirements and procedures on safety. Legal requirements may need to be respected regarding "product safety" (e.g. Produktsicherheitsgesetz in Germany [24]) and "occupational safety and health" (e.g. Directive 89/391 in Europe, Arbeitsschutzgesetz [25] in Germany, D.Lgs. 81/08 "Testo unico sulla salute e sicurezza sul lavoro" in Italy). Further specific laws, for example on chemicals or electromagnetic fields, may apply in certain lab scenarios. In remote labs, the product users (e.g. students of another university) are usually not at risk, as they access the infrastructure through an Internet-connection. However, if physical components are used by the students (e.g. processor-boards connected to the federated lab infrastructure) the requirements concerning product safety may apply. The European Directive 89/391 defines minimum requirements, which have been implemented in national laws [4]. The European Directive 89/391 is based on a list of general principles:

- Avoiding risks
- Evaluating the risks
- Adapting the work to the individual
- Combating the risks at source
- Adapting the technical progress
- Replacing the dangerous by the non- or the less dangerous
- Developing a coherent overall prevention policy
- Prioritizing collective measures (over individual protective measures)
- Giving appropriate instructions to the workers

Directive 89/391 defines not only the principles but also the obligations and actions for employers and workers in every situation.

3.3 Privacy / GDPR requirements

The federated lab infrastructure in DigiLab4U will collect data about students and experiments, create a Learning Analytics (LA) system. As such, being initially designed and developed in European universities, the system must comply with the GDPR 2016/679. As in remote labs, the risk of data breaches must be considered both: for proper countermeasures, and for promptly notifying users. As stated in [26], data protection should be provided by design and as a default. Moreover, the definition and design of the network and software infrastructure should consider such issues as centralized or decentralized data collection and storage systems. The issues are relevant both from economic and practical points of view. For example, if processed data is sent back to each lab, it would certainly require greater technical and economical efforts than having only a centralized solution. On the other hand, a centralized solution will impose significant costs for managing a federated network.

3.4 Existing organizational requirements and procedures in local labs

While working in a lab, several safety issues can arise. Safe and reliable systems should prevent harm to lab assistants, students, machines, as well as protect user data. These goals are common for each institution; however, different universities can have their norms on security and safety. As an example, students at the University of Parma are required to take a Moodle-course, while students at HFT Stuttgart must attend a face-to-face class session at the beginning of their studies.

Current safety practices at HFT Stuttgart (Faculty C): To achieve a 100% training rate, new students at HFT Stuttgart do not get their account data for the university network before they have attended the basic safety instruction course. In a lab-scenario, where students from the University of Parma access remote labs at HFT Stuttgart, occurs the need to have a "common denominator" to let the students conduct experiments easily and safely.

Current safety practices for the RFID lab at the University of Parma (based on an interview with the corresponding lab manager): The access to the lab is forbidden to students without supervision by official full-time staff (i.e. professors, teaching assistants, etc.). The main source of risk is a conveyor and other handling equipment. No harmful substances are present in the lab. If an experiment requires the usage of any special equipment for which the students have never been trained before, such training will be provided by a professor in charge. To operate the lab in a safe manner not more than 7 students are allowed to stay in a lab at the same time. Students are considered equally to employees, as stated by Italian laws D.M. 363/98 and D.Lgs.81/08. It is stated that "*students of university courses, PhD students, postgraduates, trainees, scholarship holders, and similar subjects are equal to employees if they attend educational, research or service laboratories where machinery, equipment and work equipment, in*

general, are used, and chemical, physical and biological agents are present..". According to Article 37 of D.Lgs 81/08, the employer must provide training for all the employees. Students of Parma University must pass a Moodle-based course, which is comprised of three modules. The first two modules are mandatory for each student, regardless of which particular course is attended, the third one is only required for those students who are involved in any laboratory activity in their courses. The first module consists of a generic training, related to situations of risk, possible damage, and injuries, as well as follow-up measures and procedures to prevent and protect against any risk. The second module is associated with low-risk activities (e.g. manual handling of loads, work-related stress, and organizational wellness, etc.), and the last module provides medium risk (e.g. dangerous substances) tasks. Students access the safety course using the university access credentials and attend the lessons in order. Lessons are administered through audio and videos, which must be fully watched in the given order. After that, the platform unlocks a multiple-choice test, which the student must successfully pass, to unlock the next module. Once all tests are positively passed, the system produces a certificate attesting the training.

Current safety at BIBA Lab: BIBA is obliged to follow the safety and security guidelines of the University of Bremen. This implies a yearly safety and security training for all staff members including assistants. The University has a person responsible for this and besides, BIBA has its own safety and security manager, who carries out the training of each new staff member at the beginning.

In addition, there are specific guidelines for the BIBAgamingLab that are based on a risk analysis carried out in 2015 based on different ISO guidelines and regularly updated every February. The lab provides limited access for employees and thus there are restricted working hours. Even trained personnel are only allowed to be alone in the lab if they have announced this to the researchers outside the lab. Outside standard working hours for BIBA, any work requires that 3 persons are available and that it is approved by the head of the BIBAgamingLab. Student or other visitors are not allowed to be unsupervised in the lab.

BIBA personnel who do not have access on a regular basis to the lab are allowed to carry out work if it is requested beforehand and are aware of the gamingLab guidelines.

Most of the work carried out in the lab is related to computer games. Thus, there are guidelines in-line with the GDPR with comprised ethical consideration (for more information see[1]). These guidelines cover all the aspects related to ethical issues, data management, and privacy, which the Lab mostly deals with, including the specific requirements. The guidelines are to be well known to all employees involved in relevant activities. Furthermore, since many of the games we offer, can be accessed online of externals, these guidelines also need to be followed by those and consent hereto is required before (if we store data) as well as a document that it corresponds to national legislation.

[1] https://zenodo.org/record/1256626#.Xcsu71dKg2w; https://beaconing.eu/wp-content/uploads/deliverables/D1.8.pdf; https://beaconing.eu/wp-content/uploads/deliverables/D1.9.pdf

4 Applying VDI/VDE 2182 for Federated Labs

VDI/VDE 2182 on "IT-security for industrial automation" combines safety and security-related topics. Multiple actors (manufacturers, operators, integrators) are distinguished, and individual guidelines are provided. We have adjusted the VDI/VDE 2182 to match the requirements for federated remote labs. We have focused on lab managers, as they will be in charge of implementing corresponding safety and security measures Fig 1.

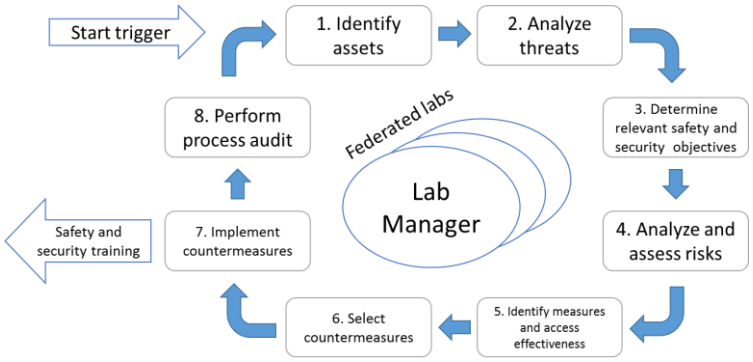

Fig. 2. Adjusted VDI/VDE2182 process model for safety and security in federated remote labs.

We consider a starting trigger to initiate the iterative approach. The starting trigger may be a change in the laboratory equipment, new configurations, or research projects, or other (e.g. time-based) triggers throughout the lifecycle of the lab. The most important trigger for DigiLab4U will be new labs entering the network. The concept of safety and security will be implemented into DigiLab4U training, not only for lab managers but also for students. The safety and security content may be *"just another element in the teaching process"* [27]. Especially in curricula addressing industrial automation and Industry 4.0 related topics, basic knowledge about safety and security is crucial.

4.1 Step 1: Identify assets

Based on VDI/VDE 2182 [28] we define a lab asset as all *tangible and intangible components of labs, lab devices, and lab networks, which may come under threat through direct or remote operations and which are worthy of protection*.

We have identified some typical different assets at the labs in Parma, at HFT Stuttgart and at BIBA to test the proposed model-based VDI/VDE 2182. We must consider that these labs are currently used hands-on and are still not fully remotely accessible. However, remote operation and implementation of these labs to DigiLab4U require some basic understanding of the relevant safety and security issues upfront.

Figure 2 provides an overview of the operating environment following VDI/VDE 2182 Part 3.3 [29].

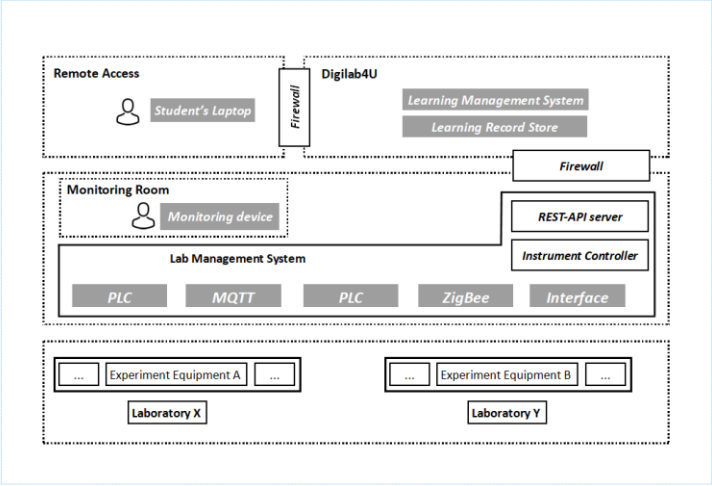

Fig. 3. Adjusted DigiLab4U structure from VDI/VDE2182 overview of the operating environment.

4.2 Step 2: Analyze threats

VDI/VDE 2182 Part 3.3 [29] suggests a four-phased approach to analyze threats. In phase 1, threats are analyzed based on internal and external experience, as well as threat catalogues. The Federal Office for Information Security in Germany (BSI) for example lists the ten most important threats and corresponding countermeasures for industrial control systems [30]. Moreover, the threats must consider machines and people's points of view, being both considered as assets of the system. Indeed, some threats may be classified with a low level of damage from a machine's point of view, while from the worker's perspective the level of damage is significant or serious. For the description of causes in phase 2, we identified the following types of theoretical failures for university labs: (1) software failures, (2) configuration failures (can be checked through verification and validation), (3) hardware failures (mechanical or electrical hardware), (4) human failures (in contrast to configuration failures that these failures can only be eliminated through education and training), (5) attacks and sabotage, and (6) disruptions from the environment (e.g. earthquakes, fires). Disruption from the environment in a very severe case has recently been seen in the Corona crisis, which has affected universities around the globe. This crisis shows that remote access to university labs is not only related to convenience and economic aspects. In phase 3, a detailed vulnerability analysis is performed. Usually, multiple technical and organization people are involved. Table 1 lists examples of identified threats in the DigiLab4U network.

Table 1. Extended threat matrix – Examples (based on [29])

Lab	Asset	Threat	Cause	Example	Vulnerability	Direct consequence
Parma	Conveyor	Control Components Connected to the Internet	Attack (5)	Loss of control of conveyor	Unsecure authentication procedures	People may be hurt during maintenance activities
Stuttgart	Robot	Configuration failure	Human failure (4)	No validation and verification of the code	People may be hurt; a robot may be damaged	People may be hurt; a robot may be damaged
Stuttgart	Robot	Technical malfunction	Hardware failure (3)	Defect sensor	No backup for a single source of failure	People may be hurt; a robot may be damaged
Stuttgart	Database server	Intrusion via remote access	Sabotage (5)	Unsatisfied student/employee	Unsecure authentication procedures	Unauthorized people access data
Future iterations on labs, lab/asset extensions, threats, causes …						

Iterations can be added to the list as they occur (see starting trigger). The direct consequences (see Tab. 1)*"are identified by evaluating what can happen to the plant, the persons, and the organization"* [29]. A catalog of clustered direct consequences can be developed over time and can be shared between different labs.

4.3 Step 3: Determine relevant security and safety objectives

The key system characteristics of the trustworthiness of an IIoT system are safety, security, privacy, resilience, and reliability [31]. VDI/VDE 2182 Part 3.3 [29] as well as the IIoT Security Framework (IISF, [32]) also mentions availability, confidentiality, and integrity as objectives.

The European Union, with Directive 89/391/EEC, contemplates that for the safety and security in an industrial plant, the relevant objectives are defined by an employer with the assistance of an expert worker. Nonetheless, the workers are incited to find new objectives and risks inside the organization, this is a part of the continuous improvement process. Such an approach reveals the possibility to identify the largest number of objectives, evaluate and classify them.

In a scenario where multiple laboratories are involved, a collaboration with lab owners and operators should be encouraged as they are the most qualified people operating in the labs. Additionally, students' collaboration should be increased to receive continuous feedback on safety and security, leading to a continuous improvement process as promoted by the European Union and in VDI/VDE 2182.

4.4 Step 4: Analyze and assess risks

An individual lab manager can define a risk matrix to be used for a specific location and corresponding legal and organizational requirements. If within a network of federated labs standardized risk matrix is used, cross-lab comparisons are simplified. We

suggest the lab risk matrix as shown in Table 2 (based on [29]). As can be seen, the risks in this matrix reflect the impact or damage and the probability of occurrence.

Table 2. Lab risk matrix (based on [29])

Impact examples	Impact	4x4 Matrix Rating			
Serious harm of people	Serious	Medium	Medium	High	Vital
Minor harm of people, serious economic or reputation loss	Significant	Small	Medium	Medium	High
Interruption of operation (weeks, month)	Small	Very small	Small	Medium	Medium
Interruption of operation (hours, days)	Neglectable	Very small	Very small	Small	Medium
		Nearly impossible	Unlikely	Possible	Very likely

Damage

Probability of occurence

4.5 Step 1-4: Extended risk analysis with relevant threats

Table 3 shows an overview of applying the model for five sample lab use-cases based on the first four steps. This table can be used to distinguish critical and non-critical use-cases and to focus on countermeasures more than on the most relevant risks. Values that are reported in Table 2 are used for rating individual threats in Table 3. The impact and probability of occurrence of risks are evaluated and rated from ‘very small’ to ‘vital’.

Table 3. Step 1-4 of the assessment of lab-components, threats, and objectives in DigiLab4U (excerpt, based on [28])

Lab		Parma	Bremen	Stuttgart	Stuttgart	Stuttgart
Lab assets		Conveyor	Remote service	Robot	Robot	Database server
Threat		Control Components Connected to the Internet	Data manipulation	Configuration failure	Technical malfunction	Intrusion via remote access
Cause		Attack	Attack	Human failure	Hardware failure	Sabotage
Example		Loss of control of conveyor	Hacker attacks the remote service connection	Wrong programming, unexperienced user	Defect sensor	Unsatisfied student/employee
Vulnerability		Unsecure authentication procedures	Security measures of the DigiLab4U network	No validation and verification of the code	No backup for a single source of failure	Unsecure authentication procedures
Direct consequence		People may be hurt during maintenance activities	Unauthorized functions in the Bremen network	People may be hurt; a robot may be damaged	People may be hurt; a robot may be damaged	Unauthorized people access data
Objectives	Availability	X	X		X	
	Confidentiality	X	X	X		X
	Integrity		X			X
Identified extent of damage		Serious	Small	Serious	Serious	Significant
Identified probability of occurrence		Unlikely	Very likely	Possible	Nearly impossible	Unlikely
Identified risk		Medium	Medium	High	Very small	Medium
Acceptable extent of damage		No	Yes	No	No	No
Acceptable probability of occurrence		No	No	No	Yes	No
Acceptable risk		No	No	No	Yes	No
Risk reduction necessary		Yes	Yes	Yes	No	Yes
Time of intervention/Priority		Before the next lecture	Immediately	Before the next lecture	Before the next lecture	Immediately

4.6 Step 5: Identify measures and access effectiveness

In step 5, a lab manager lists the possible measures and evaluates their effectiveness. Based on [29] and the provided examples in this paper a corresponding list includes:

- Automatic surveillance of the lab premises: it is planned to install webcams in labs, however in this particular case privacy agreements have to be considered. In the case of securing the area of a robot at HFT, two laser scanners triggering warning and stop commands in real-time will be used.
- Access control system for lab rooms: it is necessary to make sure there is nobody in the room when an experiment is performed, e.g. in the Parma lab it is planned

to construct a protective frame around a belt conveyor, to avoid any harm to lab operator.
- Restrictions on functional features for remote access: it is planned to be implemented for both labs: (i) with RFID chamber HFT doesn't allow all the functionality, but only limited functions; (ii) in Parma the velocity of belt conveyor configuration will be not available from remote, as it can cause damage to lab operator, products and belt conveyor itself.

The lab alliance as such may provide common support and guidance such as:

- Confidentiality agreements with lab service users: certain agreements for the users will be provided.
- Minimum safety and security policies for lab managers and administrators, which may be exceeded by local regulations and laws.
- Standard framework solution for lab-network separation, in the sense that the labs are secured in themselves - several levels of access: 1) access to the central network; 2) access to the individual labs.
- Safety and security lecture courses and self-study material.
- Logging mechanisms: it does not help to prevent problems however it helps to identify failures afterward and improve them.

The evaluation of the effectiveness needs to address the following criteria:

- Achievement of the necessary risk reduction to an acceptable risk level for each identified threat.
- Compliance with the university lab safety and IT security policies.
- Simplicity and flexibility in day-to-day operations (according to the identified needs, see introduction).

4.7 Step 6: Select countermeasures

To better impact the identified and evaluated from step 1 to step 4 risks, following levels of intervention are suggested: (i) elimination of the risk factor, (ii) modification and inhibition of the causes, (iii) automatically detection of malfunctions, and (iv) limitation of the damage. The first three levels can be classified as a prevention of the damage, they act directly on the probability of occurrence, while the last one acts on minimizing, limiting, and eliminating damage and its consequences (also with the use of personal protective equipment).

The selection of the countermeasures should be based on economical, technical, organizational, and educational criteria, and the following factors are to be considered:

- Low influence on existing operation (e.g. speed, space requirements).
- Easy integration and adaptability to changing environments.
- Eexpenditure for procurement, installation, customization, and integration in existing lab infrastructures.
- Expenditure on user training and maintenance.
- Innovative approaches serving as a lab in itself.
- Existing installations and experiences.

In order to secure the robot-operation for an RFID-measurement cabinet at HFT Stuttgart, a standard security fence would have been the easiest option. Alternatively, we could have chosen to buy a cobot with integrated safety features. This would have been a flexible, but slow and costly solution. Therefore, we have chosen a safety laser scanner-based solution instead to allow easy access to the robot and the measurement cabinet, while still offering full robot speed in operation at reasonable cost. If people are entering a defined range, the scanner triggers different signals, first slowing down the robot and finally stopping it, if people enter a proximity range. We collected three different competitive offers and have chosen the cheapest offering for economic reasons. As there has not been any experience with such systems at HFT Stuttgart, the installation will be done by the manufacturer of the safety system. This safety laser installation itself will serve as a show-case for students in a lecture on industrial sensors in the future.

4.8 Step 7: Implement countermeasures

While severe risk may require immediate actions, the usual implementation of countermeasures will be embedded in *"the project schedule"* [29], which in the case of universities is often linked to lecture periods. Changes to the infrastructures of learning labs should be implemented during the off-lecture periods to enable stable lab operation during lecture periods. Testing and validation of implemented countermeasures are necessary. As an example, the safety-system for the robot at HFT Stuttgart will be installed, tested and validated by the manufacturer of the safety-equipment. The installation will be accompanied by the lab technician and the software developers working on the remote access to the robot and the measurement cabinet.

To extend from individual installations to a wider lab network, an organizational concept is required, which identifies measures for normal operation on the one hand and emergencies on the other (tab. 4). To have a faster and more precise method to react at issues and failures, roles, and responsibilities should be identified and assigned [29].

Table 4. Roles and responsibilities

	Examples (Normal operation)	Examples (Emergency operation)	Actions
Role	Lab manager, lecturer, central safety and security staff, IT operations, lecturer (responsible to follow safety and security guidelines in lectures)	Lab manager, lecturer, students, central safety and security staff, IT operations, first aid	All must be informed about people assigned to safety and security roles
Responsibility	(Remote) administration, monitoring (incl. log files), service hardware, service software (e.g. backup, updates), safety and security and safety process design and standardization (incl. backup concept, escalation path), documentation, training material, audits, emergency plans	Error analysis and classification, alerting, initiate emergency measures (e.g. service hardware, service software, first aid), feedback loop to normal operation roles	People/roles must be informed about their corresponding responsibilities and must be trained to be capable of fulfilling them

The following table shows a list of main roles and responsibilities in three labs and their institutions. Besides, there are further specialists responsible for example for hazardous material, radiation, medical officers, and technical facility managers which must be consulted in special cases. Some public institutions are responsible to control legal compliance with safety and security issues.

Table 5. Main roles and responsibilities in the labs

Area of Responsibility	Institution	Role (example: RFID-lab HFT Stuttgart)
General responsibility	University	All staff in leading positions, including deans, professors, lecturers, and lab managers
Initial training for students	University	Dean of faculty (faculty level)
General training material	University	(e.g. in the Learning Management System)
Emergency plans	University	Health and safety officer
IT security concepts	University	Chief Information Security Officer (university level)
IT security lab	Lab	Lab manager, IT
Administration	Lab	Lab technician, IT
Monitoring	Lab	Lecturer, lab technician, appointed safety inspectors
Hardware service	Lab	Lab technician
Software service	Lab	Lab technician
First aid	University	Trained voluntary staff listed for each building
Alerting	University	All via central telephone line
Escalation	University	Health and safety officer
Safety audits	External	Safety consultants, dean of faculty
Documentation	University	Health and safety officer
Initiate emergency measures	University	Health and safety officer
Error analysis and classification	University	Health and safety officer, appointed safety inspectors
Feedback loop to normal operation	University	Health and safety officer, appointed safety inspectors
Documentation	University	Health and safety officer
Guidelines for safety and security	Federated lab network platform	Centralized
Access logging	Federated lab network platform	Centralized

Monitoring of attacks to the network	Federated lab network platform	Centralized
Network related countermeasures	Federated lab network platform	Community
Exchange of safety and security experiences	Federated lab network platform	Community
Exchange of safety and security training material	Federated lab network platform	Community

Organizational countermeasures include safety and security training. As introduced in paragraph 4, a training program has already been implemented at the University of Parma. This training must be followed by each worker and student at the university, and it is organized accordingly with the different faculties and the different risks to which students are subjected. Indeed, the training in Parma is divided into three different levels of risks: low, medium, and high. The students and workers must achieve different levels of training depending on the faculty that they are attending.

Within a network of federated remote labs, a key question remains which responsibilities should be centralized. In the case of DigiLab4U – a research project – no staff for standard operation is funded. Safety and security roles and responsibilities need to be handled by each involved university. However, within the project guidelines and guidelines can be formulated, and logging and monitoring concerning network access and attack can be provided. Extra network benefits can be generated by the community itself through sharing experiences, successful countermeasures, and training material within the network. This exchange should be supported by the lab network platform.

4.9 Step 8: Perform process audits

Even though the safety and security of machinery in laboratories must be guaranteed in university labs, external audits are useful to prove compliance to regulations and to identify potential threats based on the experience of the auditors. Initial audits after installation may be offered by the manufacturers of the corresponding safety systems. For securing the robot environment at HFT Stuttgart, the initial audit covers:

- Recording technical data concerning the device and the application.
- Determination of the occupational safety at the relevant danger area of the machine.
- Functional test of the equipment used.
- Verification of the safeguarding of the hazardous area.
- Check of the integration into the control system according to manufacturer's specifications.
- Preparation of a test report.
- Inspection sticker if the test is passed.
- Establishing the online connection to the device.
- Reading the device configuration.
- Creating a PDF file as an attachment to the inspection report.

Regular audits have a motivating effect on all involved staff to monitor and improve safety in labs. At HFT Stuttgart, labs are externally audited once a year, while at BIBA every two years. Audit results are documented. However, in between audit checks, there may have been changes in the setup or the environment. A manual authorization step by the responsible lab-manager may be required. Further means for checking the current safety and security status and automatic authorization right before the start of the lab-experiment need to be further researched.

However, these audits show two shortcomings concerning federated lab networks. Firstly, the network-related safety and security threats are not in the focus of these audits. In DigiLab4U this will be addressed through specific audits as part of the project. Secondly, an academic value audit is missing. Academic auditing is necessary, as it shows where we stand and what we are looking for. The University of Parma for example has audits on teaching quality and quality of processes by the Italian ministry every 10 years. However, since lab-work at a course is currently considered an add-on but not the core of the lecture, the academic quality of the labs is not directly audited. In a federated lab network, lab quality can be ensured through a peer-review process, though.

5 Iterative Improvements

The guidelines herein presented must consider an approach that enables an iterative and continuous improvement of the overall described procedure. Indeed, given that a federated lab has a nature of an everchanging environment, the safety and security guidelines must comprehend a procedure that enables the infrastructure to be responsive and resilient to changes, with the minimum effort and in the shortest period. To achieve such a degree of adaptivity, the guideline implements an iterative procedure based on event triggers. Indeed, federated remote labs can experience a wide range of changes which could require a revision of the safety and security policies. According to VDI/VDE 2182 Part 3.3 [29] we can distinguish different triggers to start the iteration process.

Firstly, a "newly added (security) component or (security) measure can affect the target of inspection and may, therefore, make it necessary to rerun the risk analysis cycle." As an example, the introduction of more technologically advanced countermeasures, possibly considered a new state of the art, must nonetheless be considered as a trigger for the reevaluation of the analysis, as the interactions between all (security) components in a lab, and in a network of labs, must be taken into account. Concerning the interaction with an overall system, modifications or updates of existing components can be considered as eligible triggers for iterative improvement, as such intervention could potentially alter the way countermeasures act. Regarding the modifications/updates or addition of new (security) components, a high degree of attention must be given to changes in the software infrastructure which enables the communication in the remote lab network. Indeed, each software update must be audited and thoroughly tested beforehand, as well as the compatibility certified. Moreover, software updates could

bring new functionalities, and those can bring to a consideration of new safety and security countermeasures. The addition of new laboratories to the federated network should not be considered as a trigger for iterative improvements but should be handled and considered in the design of the network architecture. However, if the addition of a new lab requires an adaptation and modification of the designed procedure (i.e. a new communication protocol is introduced), such architecture alteration must provoke a new risk evaluation. Moreover, the addition or modification of lab equipment also requires a new risk assessment and countermeasures evaluation.

Secondly, regular audits may be specified in a corresponding safety and security policy. For universities, updates and regular inspections can ideally be performed between the lecture terms. Periodical questionnaires by each partner in the lab network can help to collect feedback and ideas for enhancing the security and safety protocols. In such a way, pro-active crowdsourced feedback can anticipate and more easily adapt to the evolution of the overall network approach.

Thirdly, in case of security-, safety-, security- or privacy-relevant events, ad-hoc actions may be required. New countermeasures are needed to comply with newly discovered threats or weaknesses in infrastructure and architecture.

Fourthly, if the threat situation has changed, e.g. because of organizational changes, a new iteration of the safety and security concept may be necessary.

Fifthly, the safety and security policy may change. This includes (i) the safety and security guidelines represented by changes in the institution's policies, (ii) laws and regulations adaptations, and (iii) modification in the organizational hierarchy, in both federated network and each one of the partners.

6 Conclusion and Outlook

Providing safety and security in a federated lab network infrastructure is a complex task. Based on a literature review and the analysis of requirements for federated university lab networks related to safety and security, we have chosen, followed, and adjusted the VDI/VDE 2182 guideline for implementing an iterative safety and security strategy. We have provided examples from three labs that are participating in the DigiLab4U project. The remote lab scenarios in these labs are currently further enhanced and integrated into the lab infrastructure. Further, yet unknown labs, will be integrated. Those will be able to use the guideline for their risk assessment. Corresponding countermeasures must be investigated and implemented to ensure a safe and secure operation towards the end of the funding period. Therefore, the provided guideline will be further improved, based on the findings in the upcoming implementation phase.

7 Acknowledgement

The project on which this paper is based was funded by the Federal Ministry of Education and Research (BMBF), Germany under the funding code 16DHB2112. The responsibility for the content of this publication lies with the authors.

8 References

[1] M. Tawfik, E. Sancristobal, S. Ros, R. Hernandez, A. Robles and e. al., "Middleware solutions for service-oriented remote laboratories: A review," in Proceedings of IEEE Global Engineering Education Conference (EDUCON), IEEE, 2014, pp. 74-82. https://doi.org/10.1109/educon.2014.6826155

[2] E. Lisova, I. Šljivo and A. Čaušević, "Safety and Security Co-Analyses: A Systematic Literature Review," IEEE Systems Journal, vol. 13, no. 3, pp. 2189-2200, 2018. https://doi.org/10.1109/jsyst.2018.2881017

[3] P. Orduña, L. Rodriguez-Gil, J. Garcia-Zubia, I. Angulo, U. Hernandez and E. Azcuenaga, "Increasing the value of remote laboratory federations through an open sharing platform: LabsLand," in Online Engineering & Internet of Things: Lecture Notes in Networks and Systems, vol 22., M. E. Auer and D. G. Zutin, Eds., Cham, Springer, 2018, pp. 859-873. https://doi.org/10.1007/978-3-319-64352-6_80

[4] D. Uckelmann, D. Mezzogori, G. Esposito, M. Neroni, D. Reverberi, Ustenko and Maria, "Safety and Security in Federated Remote Labs – A Requirement Analysis," in Proceedings of the 16th International Conference on Remote Engineering and Virtual Instrumentation REV 2020, Athens, USA, 2020. https://doi.org/10.1007/978-3-030-52575-0_2

[5] T. Pereira, L. Barreto and A. Amaral, "Network and information security challenges within Industry 4.0 paradigm.," in Procedia Manufacturing, Science Direct, 2017, pp. 1253-1260. https://doi.org/10.1016/j.promfg.2017.09.047

[6] G. Federal Office for Information Security, "Allianz für Cybersicherheit," 06 06 2019. [Online]. Available:https://www.allianz-fuer-cybersicheheit.de/ACS/DE/_/downloads/BSI-CS_005E.pdf?__blob=publicationFile&v=7. [Accessed 02 09 2019].

[7] Industrial Internet Consortium, "Key Safety Challenges for the IIoT: An Industrial Internet Consortium Technical White Paper," 01 12 2017. [Online]. Available: https://www.iiconsortium.org/pdf/Key_Safety_Challenges_for_the_IIoT.pdf. [Accessed 02 09 2019].

[8] A. Maiti, A. A. Kist and A. D. Maxwell, "Design and operational reliability of a Peer-to-Peer distributed remote access laboratory," in Proceedings of 2015 12th International Conference on Remote Engineering and Virtual Instrumentation, 2015. https://doi.org/10.1109/rev.2015.7087270

[9] M. Casini, D. Prattichizzo and A. Vicino, "Operating remote laboratories through a bootable device," IEEE Transactions on Industrial Electronics, vol. 54, no. 6, pp. 3134-3140, 2007. https://doi.org/10.1109/tie.2007.907026

[10] T. Kozík and M. Šimon, "Preparing and managing the remote experiment in education," in 2012 15th International Conference on Interactive Collaborative Learning (ICL). https://doi.org/10.1109/icl.2012.6402077

[11] P. Marangé, F. Gellot and B. Riera, "Control validation of DES systems: Application to remote laboratories.," in 2nd International Conference on Digital Information Management, 2007. https://doi.org/10.1109/icdim.2007.4444318

[12] M. Gerža, F. Schauer and R. Jašek, "Security of ISES measureserver® module for remote experiments against malign attacks," International Journal of Online Engineering, vol. 10, no. 3, pp. 4-10, 2014. https://doi.org/10.3991/ijoe.v10i3.3132

[13] R. O. Ocaya, "A framework for collaborative remote experimentation for a physical laboratory using a low-cost embedded web server," Journal of Network and Computer Applications, vol. 34, no. 4, pp. 1408-1415, 2011. https://doi.org/10.1016/j.jnca.2011.03.024

[14] P. Chellaiah, B. Nair, K. Achuthan and S. Diwakar, "Using Theme-based Narrative Construct of Images as Passwords: Implementation and Assessment of Remembered Sequences," International Journal of Online Engineering (iJOE), vol. 13, no. 11, pp. 77-93, 2017.
[15] M. S. F. &. J. R. Krbeček, "Security aspects of remote e-laboratories," International Journal of Online Engineering, vol. 9, no. 3, pp. 34-39, 2013.
[16] M. Krbeček and F. Schauer, "Communication and diagnostic interfaces in remote laboratory management systems," International Journal of Online Engineering, vol. 11, no. 5, pp. 43-49, 2015. https://doi.org/10.3991/ijoe.v11i5.4926
[17] J. Sáenz, F. Esquembre, F. J. Garcia, L. de la Torre and S. Dormido, "A new model for a remote connection with hardware devices using javascript.," IFAC-PapersOnLine, vol. 49, no. 6, pp. 133-137, 2016. https://doi.org/10.1016/j.ifacol.2016.07.166
[18] M. S. Herrera, J. A. Märquez, A. M. Borrero and M. M. Sänchez, "Testing Bench for Remote Practical Training in Electric Machines.," IFAC Proceedings Volumes, vol. 46, no. 17, pp. 357-362, 2013. https://doi.org/10.3182/20130828-3-uk-2039.00076
[19] C. Border, "The development and deployment of a multi-user, remote access virtualization system for networking, security, and system administration classes," ACM SIGCSE Bulletin, vol. 39, no. 1, pp. 576-580, 2007. https://doi.org/10.1145/1227504.1227501
[20] P. &. M. T. Li, "Integration of virtualization technology into network security laboratory," in 38th Annual Frontiers in Education Conference, S2A, 2008. https://doi.org/10.1109/fie.2008.4720550
[21] T. Richter, R. Watson, S. Kassavetis, M. Kraft, P. Grube, D. Boehringer and S. Logothetidis, "The WebLabs of the University of Cambridge: A study of securing remote instrumentation," in 9th International Conference on Remote Engiand Virtual Instrumentation (REV), 2012. https://doi.org/10.1109/rev.2012.6293099
[22] L. Pálka and F. Schauer, "Safety of communication and neural networks for security enhancement in data warehouse for remote laboratories and Laboratory Management System," in 6th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2015. https://doi.org/10.1109/icccnt.2015.7395191
[23] Federal Ministry of Justice and Consumer Protectionand the Federal Office of Justice, "Act on making products available on the market (Product Safety Act)," 12 2019. [Online]. Available:http://www.gesetze-im-internet.de/englisch_prodsg/englisch_prodsg.pdf. [Accessed 29 08 2019].
[24] Federal Ministry of Labour and Social Affairs, "Act on the Implementation of Measures of Occupational Safety and Health to Encourage Improvements in the Safety and Health Protection of Workers at Work (Arbeitsschutzgesetz, ArbSchG)," 12 2014. [Online]. Available.https://www.bmas.de/SharedDocs/Downloads/DE/PDF-Gesetze/arbschg-en.pdf?__blob=publicationFile&v=3. [Accessed 29 08 2019].
[25] T. Hoel and W. Chen, "Implications of the European data protection regula-tions for learning analytics design," in International Workshop on Learning Analytics and Educational Data Mining (LAEDM 2016), Kanazawa, Japan, 2016.
[26] A. B. González Rogado, A. M. Vivar Quintana and L. Lavandero Mayo, "Evaluation of the Use of Technology to Improve Safety in the Teaching Laboratory," IEEE Revista Iberoamericana de Tecnologias del Aprendizaje, vol. 12, no. 1, pp. 17-23, 2017. https://doi.org/10.1109/rita.2017.2655179
[27] VDI/VDE, "VDI/VDE 2182, Part 3.1: IT-security for industrial automation: Example of use of the general model for manufacturers in process automation, Process control system of an LDPE plant," VDI/VDE, 2013. https://doi.org/10.1007/978-3-642-95653-9

[28] VDI/VDE, "VDI/VDE 2182, Part 3.3: IT-security for industrial automation, Example of use of the general model for plant managers in process industry, LDPE-plant," VDE/VDI, 2016. https://doi.org/10.1007/978-3-642-95653-9

[29] Federal Office for Information Security (BSI), "Industrial Control System Security: Top 10 threats and Countermeasures 2019," 06 06 2019. [Online]. Available: https://www.bsi.bund.de/ACS/DE/_/downloads/BSICS_005E.html;jsessionid=900659989FEBC152C66269CE59D9C94D.2_cid351#download=1. [Accessed 02 09 2019].

[30] Industrial Internet Consortium, "The Business Viewpoint of Securing the Industrial Internet: Executive Overview," 08 09 2016. [Online]. Available: https://www.iiconsortium.org/pdf/IIC-Security-WP.pdf. [Accessed 02 09 2019].

[31] Industrial Internet Consortium, "Industrial Internet of Things, Volume G4: Security Framework," 26 09 2016. [Online]. Available: https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf. [Accessed 03 09 2019].

[32] R. Heradio, L. de la Torre, D. Galan, F. J. Cabrerizo, H.-V. E. and S. Dormido, "Virtual and remote labs in education: A bibliometric analysis," vol. 98, pp. 14-38, 2016. https://doi.org/10.1016/j.compedu.2016.03.010

[33] K. Henke, T. Vietzke, H.-D. Wuttke and S. Ostendorff, "Safety in Interactive Hybrid Online Labs," International Journal of Online Engineering (iJOE), vol. 11, no. 3, pp. 56-61, 2015. https://doi.org/10.3991/ijoe.v11i3.4557

[34] Federal Office for Information Security (BSI), "LARS ICS: Ein Werkzeug für den leichtgewichtigen Einstieg in industrielle Cyber-Security," 11 07 2018. [Online]. Available: https://www.allianz-fuer-cybersicheheit.de/ACS/DE/_/downloads/180711_LARS_ICS_Light_and_Right.html. [Accessed 04 09 2019].

[35] S. Kort and E. Rudina, "The Security for Safety Problem in Cyberphysical Systems," MILS@ HiPEAC, 2016.

[36] F. Reichenbach, J. Endresen, M. M. R. Chowdhury, Rossebø and Judith, "A pragmatic approach on combined safety and security risk analysis," in IEEE 23rd International Symposium on Software Reliability Engineering Workshops, 2012. https://doi.org/10.1109/issrew.2012.98

[37] H. Flatt, S. Schriegel, J. Jasperneite, H. Trsek and A. H., "Analysis of the Cyber-Security of industry 4.0 technologies based on RAMI 4.0 and identification of requirements.," in IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA), IEEE, 2016, pp. 1-4. https://doi.org/10.1109/etfa.2016.7733634

9 Authors

Dieter Uckelmann studied Mechanical Engineering at TU Braunschweig and received his doctorate at the University of Bremen in the Faculty of Production Engineering. Between 2005 and 2012 he has established and managed the LogDynamics Lab at the University of Bremen. Since 2012 he is a professor for Information Logistics at Hochschule für Technik (HFT) Stuttgart. Additionally, since 2017 he is a visiting professor at the University of Parma, where he co-supervises two PhD candidates. He has been a visiting researcher at the University of Cambridge (UK, 2009) and University of Parma (Italy, 2016). The focus of his research work is in the field of the Internet of Things, Industry 4.0, and Smart Buildings, the value of information, as well as on lab-based research and education. Since 2018, he coordinates the project DigiLab4U and

works in other research projects on Smart Public Buildings and industrial sensor/augmented rality applications. Furthermore, he is co-editor of the "International Journal of RF-Technologies: Research and Applications". Prior to his academic career, he has been working in different management positions for several IT companies. Email: dieter.uckelmann@hft-stuttgart.de

Davide Mezzogori has received his Ph.D. in Industrial Engineering at the University of Parma. He is now a research fellow at the University of Parma at the Department of Engineering and Architecture. He is co-author of 6 international scientific publications. He has published articles on the application of Machine Learning and Deep Learning algorithms to Industrial problems, such as demand forecast in the fashion industry, the application of neural networks to WLC systems, as well as articles on optimization algorithms (i.e. metaheuristics) applied to engineering operations management, such as scheduling problems and warehouse allocation problems. He is involved in the OPEN DIGILAB4U international project, particularly the development of a serious game for supply chain and operation management education.

Giovanni Esposito is a PhD student in Industrial Engineering at the University of Parma (Italy). His research interests comprehend RFID application for supply chain management and supply chain modelling towards Industry 4.0. He also visited the Stuttgart University of Applied Sciences (Germany), currently, he acts as a local manager for the University of Parma on the DigiLab4U project (http://digilab4u.com/). His ORCID iD is https://orcid.org/0000-0001-5150-0855.

Mattia Neroni was born in November 1993 in Reggio Emilia (Italy). He studied at scientific high school and piano conservatory at the same time. He achieved a bachelor's degree and then a master's degree both in Management Engineering and both at the University of Parma. During his studies, he spent a year abroad for a job in London (UK). Currently, he is in the final year of PhD student at the Department of Engineering and Architecture at the University of Parma. His PhD is focused on the development and validation of algorithms for performance improvement in logistics, and his research interest mainly consists of Data Science, Operational Research, and Operations Management. He is currently co-author of 5 scientific publications and other 6 publications under revision. In the last year, he has been also research guest for 3 years in a technical University in Stuttgart (Germany), namely the Hochschule fur Technik, and invited speaker in a major conference (i.e. Moscow International Logistic Forum 2020).

From the industrial point of view, he is the designer and developer of several algorithms for performance improvement in automated storage systems, a couple of algorithms for empty space optimization in automated storage systems, a web application for production tasks scheduling, a web application for working hours control, the design of an assembly line according to lean principles, and many other industrial solutions in pre-implementation control. His ORCID-ID is: http://orcid.org/0000-0002-4507-4789.

Davide Reverberi was born in 1992 in Parma (Italy). He completed his higher study as an accountant, and he received his Bachelor's and master's degrees in management engineering at the University of Parma. During his university studies, he worked in an industry for tomatoes transformation as a person in charge of inbound logistics. He is now a research fellow at the University of Parma at the Department of Engineering and Architecture. Since May 2019 he is involved in the Open Digital Laboratory for You

(DigiLab4U). During this period, he followed four different workshops on technical and educational topics in laboratories. He is currently co-author of two international scientific publications, and one other publication under revision.

Maria Ustenko was born in 1994 in Moscow (Russia). She received her master's degree in nanotechnologies and circuitry at the Peoples Friendship University of Russia in Moscow in 2018. During her studies, she spent a term abroad, and after graduation worked as a Jr. engineer in a leading Chinese telecommunication company. Since 2019 she is a research fellow at the University of Parma (Italy) at the Department of Engineering and Architecture. She is currently a co-author of 3 scientific publications and another one is under the revision.

Jannicke Baalsrud Hauge is head of the BIBA GamingLAB and works as a senior researcher at Bremer Institut für Produktion und Logistik (BIBA) Bremen, Germany. Furthermore, she is associate professor for production logistics and program director for the master programs on sustainable production developments (2y program) and on applied logistics (1y program) at KTH, Sweden. From 2001 to 2003 she worked as a research scientist at the University of Bremen, with her main responsibility being the functional architecture of an e-commerce software. 2003 she joined BIBA, where she is responsible for the BIBA Gaming LAB as well as coordination of the BIBA contribution in several national and international projects in the field of Serious Gaming as well as ICT in production and supply chain networks and CPS. Besides supervising BSc, Master and PhD students, she is teaching SG application development, re-engineering, decision making and supply chain risk management. Her main topics are on development of SG and simulation applications, development of GBL concepts, requirements engineering (IT solutions for logistics, CPS and SG), process analysis and business modelling. Jannicke is member of several boards and has authored 250+ papers.

Article submitted 2020-09-29. Resubmitted 2020-12-04. Final acceptance 2020-12-07. Final version published as submitted by the authors.