Learning Proposal for Cybersecurity for Industrial Control Systems Based on Problems and Established by a 4.0 Didactic Advanced-Manufacturing-Plant

Bruno Santos Junqueira[1*], Marvim Vinicius Souza de Souza[1], Victor Bittencourt Lima[1], Wallace Souza Faria de Jesus Gonçalves[2], Herman Augusto Lepikson[2]

[1]Center of Competence in Advanced Manufacturing, SENAI CIMATEC; [2]Automation Department, SENAI CIMATEC; Salvador, Bahia, Brazil

Researches data indicate that the search for cybersecurity professionals to protect industrial control systems (ICS) in Brazil is increasing, mainly because of the rise in cyber-attacks directed at the industry. However, we observed a deficiency of professionals with the required competence in ICS cybersecurity, which involves technology-information fields (IT) and operational technology (OT). On the other hand, there is a lack of educational institutions with the right strategies for training professionals who master the technologies for ICS protection. This paper presents a strategy through procedures to address this lack by evaluating scenarios of practices for the development of competencies in ICS cybersecurity through the problem-based learning (PBL) methodology. The scenarios combine theory and practice involved in solving ICS cybersecurity problems, using PBL with the support of SENAI CIMATEC's 4.0 Advanced Manufacturing Plant (AMP).

Keywords: Cybersecurity. Industry. Scenarios. Practices. Problem-Based.

Abbreviations: PLC: Programmable Logic Controller; IDS: Intrusion Detection System; IPS: Instrusion Prevention System.

Introduction

Cybersecurity has been gaining prominence in managerial and governmental agendas. Industry 4.0 is an inevitable tendency. It comprises a type of industrialization where intelligent machines, storage systems, and production facilities are integrated end-to-end, by cyber-physical systems (CPS) capable of autonomously exchanging information, triggering actions, and controlling themselves independently [1]. All this integration is supported by nine enabling technologies: Internet of Things (IoT) and Industrial IoT (IIoT); cybersecurity; extended reality; big data analytics; autonomous robots; additive manufacturing; simulation and digital twins; systems integration; and cloud computing. In the era of Industry 4.0, where working machines are connected to the network and with each other using smart devices and operating in the cloud, the scale and variety of cyber-attacks have grown exponentially [2].

Within Industry 4.0, the emergence of cyber risks marks the presence of CPS in industrial environments, where vulnerabilities and threats can critically impact business models and lead to a loss of competitiveness. A study carried out by Tüv [3] states that 61% of manufacturing industries struggle in mitigating cyber risks, and only 34 % of all cyberattacks in the operational environment are detected. These data refer to all harmful attacks, including attacks coming from information technology (IT) systems, as some of them may result in intruders attacking the operational technology (OT) systems present in the operating network through the corporate network [3].

Cyber risks deman that cybersecurity strategies shall be integrated with organizational initiatives, information, and communication technologies, aiming to ensure the security of data, knowledge, and performance of the production value chain. Consequently, research and education in the cybersecurity area of Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems have attracted the interest of several institutions around the world through the

Received on 12 December 2021; revised 10 February 2022.
Address for correspondence: Bruno Santos Junqueira. Av. Orlando Gomes, 1845 - Piatã, Salvador - BA- Brazil. Zipcode: 41650-010. E-mail: brunosjunq@gmail.com.

high industrial demand for cybersecurity training for such systems in recent years [4].

In Brazil, seeking to achieve the Industry 4.0 model, industries prioritize the pillars of Systems Integration, Data Analysis, and IoT [5]. However, according to ISC2 [6] there is still a growing demand for qualified professionals with knowledge related to ICS cybersecurity. But regular, traditional courses are not well fitted to cope with some learning needed for this specialization, considering that hands-on practice is essential to deal with the nuances posed by the diverse cyber-attack specificities in ICS. The best fit for this purpose is active-based learning techniques, in which problem-based learning (PBL) has the advantage of bringing the necessary practice to the specific student problem. The creation of scenarios and routines enabled by PBL allows the insertion of students in situations involving cybersecurity problems associated with ICS in procedures. In PBL, students work together to analyze and solve problems and communicate, evaluate, and integrate information from diverse sources [7]. However, to be an efficient method, it should have an environment for hands-on practices that represents an industrial plant. In this context, SENAI CIMATEC, to contribute to industrial-technological advancement, was the first institution to integrate ICS cybersecurity in Brazil into its Advanced Manufacturing Plant (AMP). So, this research proposes scenarios of practices through learning based on current problems, which will be solved in AMP by adding ICS cybersecurity competence.

Materials and Methods

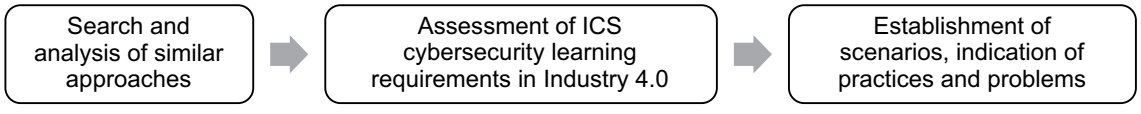
We used a method based on three steps to develop the ICS cybersecurity training scenarios considering Industry 4.0 environments (Figure 1).

Basic documental research and analysis of similar approaches were carried out to check the scenarios and practices already developed. After that, we assessed the learning requirements linked to cybersecurity technologies applied in Industry 4.0. Finally, we established the scenarios and indicated the practices and problems based on research related to cybersecurity in Industry 4.0.

Search and Analysis of Similar Approaches

Laboratories for security experiments and cybersecurity training exist in various manifestations. The traditional approach is a dedicated computer lab for IT security training [8]. In this kind of lab, a two teams approach, like red and blue, is followed, where a group of people is authorized and organized to emulate attacks or exploitation capabilities. There is also a high industry demand for cybersecurity training for ICS and SCADA systems. However, many existing research centers are limited by the lack of testbeds or models capable of representing actual instantiations of ICS applications and an inability to observe an entire SCADA system. The reasons are usually high costs and limited space for such laboratories [4]. The lack of ICS cybersecurity training strategies in educational institutions in Brazil is also associated with these reasons. Another is the lack of competent professionals to give a specific discipline to this topic. We chose PBL based on risks and benefits. As a benefit, we have a student-centered approach, which collaborates to greater understanding, interdisciplinarity, and the development of necessary lifelong skills. In contrast, as risks, creating suitable problem scenarios can be

Figure 1. The method used for scenario development.



difficult, and PBL may require more study time, taking away time from other subjects, developing anxiety because learning certainly will be messier, needing one instructor, or more, to guide the students. PBL has already been used to improve the efficiency of cybersecurity education, helping students to develop a wide range of skills in technical aspects, teamwork, making judgments, and developing as lifelong learners [9]. In contrast to traditional learning, in PBL a scenario-based problem is presented to a student, who must seek what they need to learn to solve practical problems that would likely appear during their professional life [10] (Figure 2).

Assessment of ICS Cybersecurity Learning Requirements in Industry 4.0

For the AMP to be used as a cybersecurity laboratory in the context of Industry 4.0, it is necessary to verify which technologies should be addressed in the scenarios. The general security requirements for ICS can be divided into three categories: network protection, authentication and authorization, and secure communication [11]. Based on these requirements, we raised specific conditions for the protection of ICS in Industry 4.0 using ICS cybersecurity standards.

With the adoption of Industry 4.0 technologies, the Industry 3.0 pyramid model became obsolete. So, the interdependence between hierarchical levels of communication is no longer a crucial factor, and the connectivity between the factory floor (field level) and the systems present at corporative levels gets relevant. Thus, a pillar model is consolidated, where systems at the field level and their industrial assets are constantly interacting as CPS to improve the performance of processes (Figure 3) [12].

As a consequence of this interaction, in addition to the industrial floor or field assets, data is stored in systems of the corporate level such as Enterprise Resource Planning (ERP), Plant Information Management (PIMS), and Manufacturing Execution (MES) that are also critical and must be protected.

Establishment of Scenarios, Indication of Practices, and Problems

We analyzed data from research and problems related to cybersecurity in Industry 4.0 to establish the scenarios and indicate practices and problems. ICS cybersecurity problems can be divided into three classes: people, process, and technology [13]. The technology problems are linked to the safety of the control and network components of an ICS [11]. Moreover, the top three industrial threats are phishing and social engineering, ransomware, and DNS-based DoS attacks. Besides, 57 % of the experts say that renewable and cutting-edge technologies present in Industry 4.0 are increasing the risks of cyber-attacks [3].

In addition to surveys data on cybersecurity problems, to create the scenarios it is necessary to take into account a classification referring to the needs of the labor market in the area of ICS cybersecurity. IT cybersecurity can be divided into seven categories, 33 specialty areas, and 52 work roles [14]. We didn't find a similar classification for the OT context, so it was used as a reference. Also, to address the problems involving knowledge in

Figure 2. Traditional learning x problem-based learning [10].

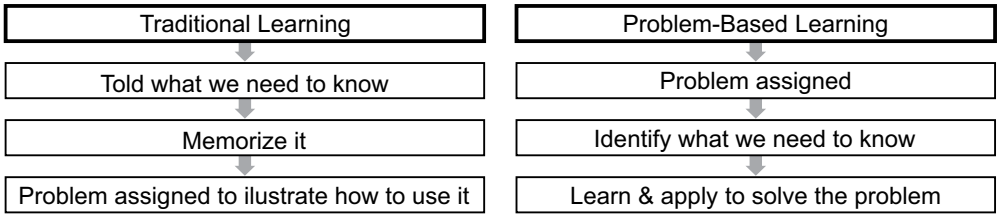
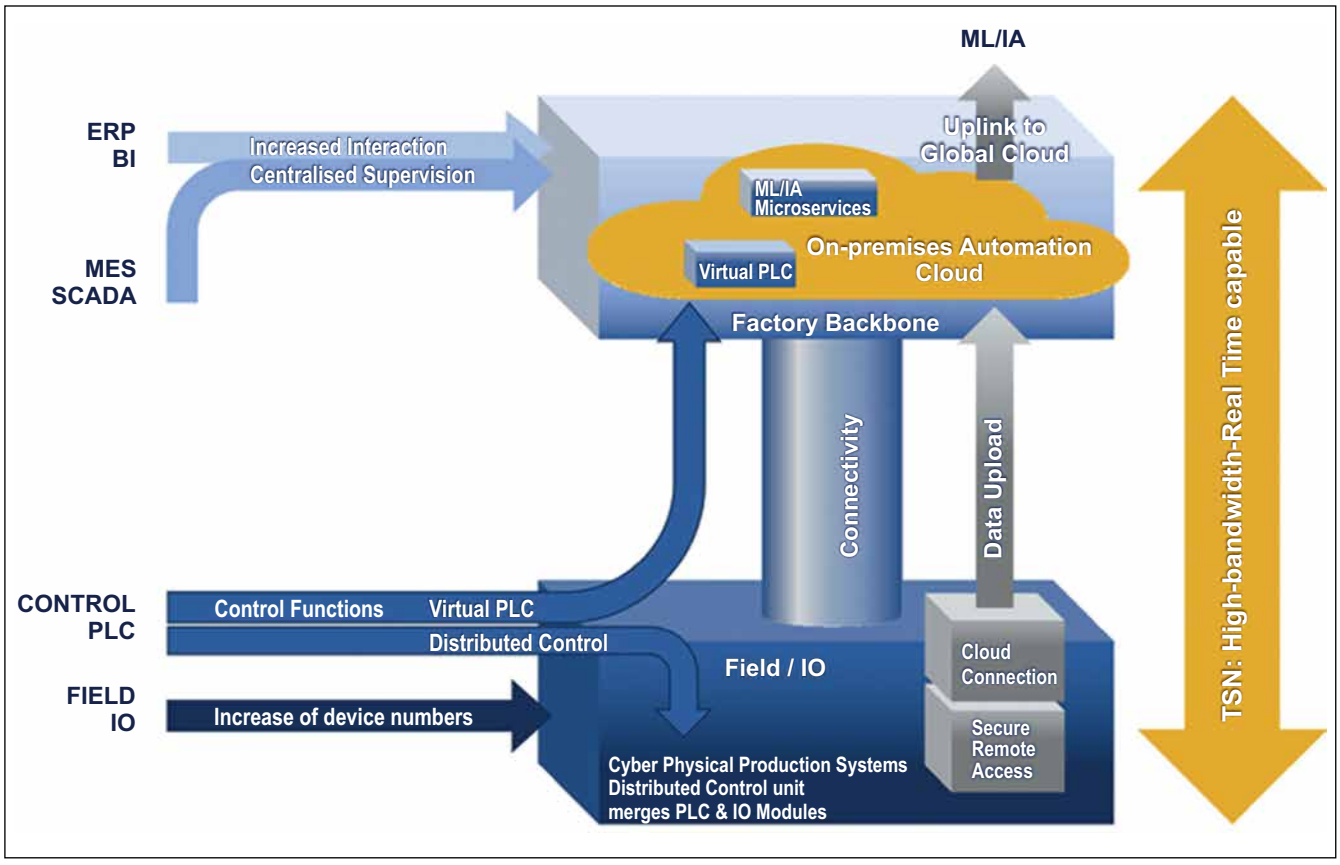


Figure 3. Pillar model of Industry 4.0 automation [12].



ICS needed for the labor market, the results of a survey carried out by Filkins and colleagues [15] were taken into account, which pointed out that process and technology practices can be more useful to people's development.

Results and Discussion

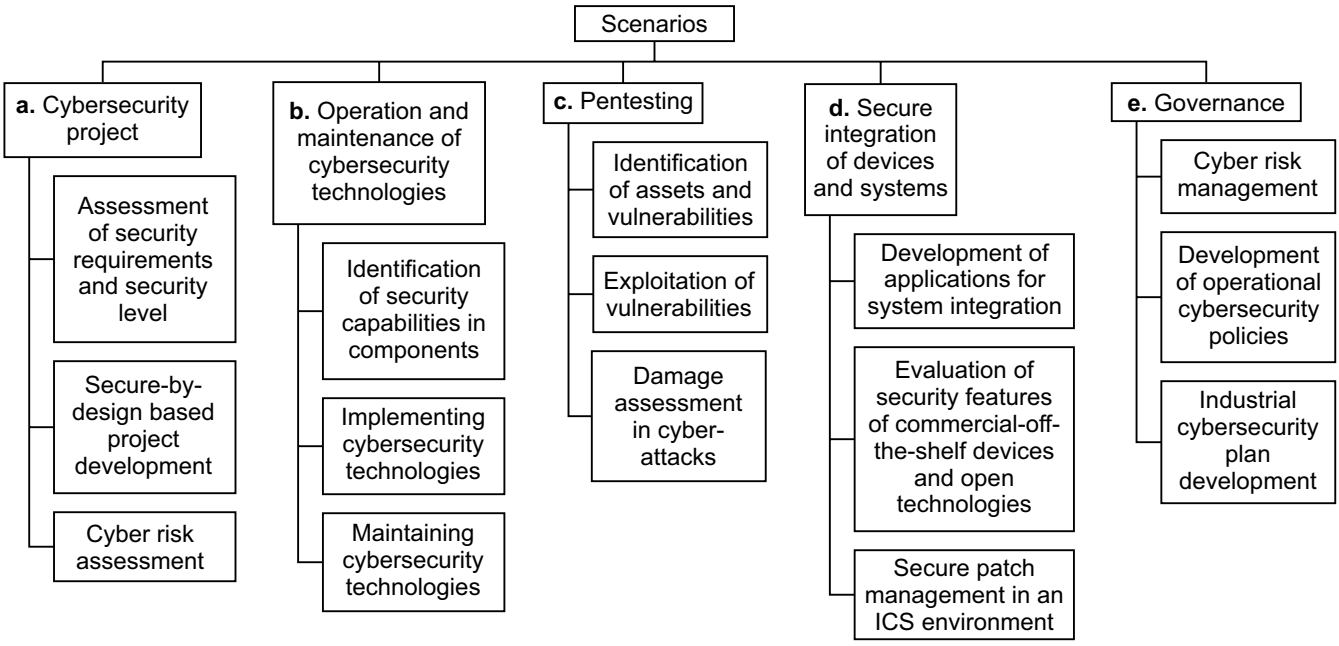
The scenarios were assembled and practices and problems were indicated through the proposed method. The resources needed to carry out the practices and solve the problems through PBL were raised. And, we discussed the method of evaluating the performance of students participating in the practices.

Scenarios, Practices, and Problems

At the end of the research and similar analysis, the scenarios are needed to (Figure 4): a. develop or securely provision industrial cybersecurity projects from scratch [14,16], b. operate and maintain ICS cybersecurity technologies [14,16] and c. gather information about security breaches in ICS to see what damage is possible in the event of an attack, which is a common practice in IT cybersecurity known as pentesting (vulnerability testing), enabling to see how to protect and defend the infrastructure [14,17].

For Industry 4.0, data analysis and integration between the floor or field and management systems are currently done through software solutions provided by third-party vendors or commercial-off-the-shelf device integrations [13]. It can cause several problems brought by the lack of security integrated into some solutions. It reveals the need for two additional scenarios: d. secure integration of devices and systems, because of the need to collect and operate data and devices in industry 4.0; and e. governance, which aims to address the need for IT and OT alignment to oversee and govern security

Figure 4. Proposed scenarios and practices.



breaches, which according to 63 % of security experts, is one of the reasons for the increase of risk [3,14].

In addition, the use of parts of the IEC 62443 [18] or other standards families, can assist in the development of problems associated with the practices. So, already existing requirements and recommendations to ensure ICS cybersecurity can be followed by students.

Application at SENAI CIMATEC AMP

SENAI CIMATEC's AMP integrates several Industry 4.0 technologies, being an environment prepared to receive professionals of all technical levels. The manufacturing process present in this plant consists of manufacturing 25 and 40 mm pneumatic cylinder bases, where the raw material is turned, milled, and later sent to modular process stations [19]. In the context of this process, each scenario and practice will be applied, seeking to solve problems in specific parts of the AMP.

First, in scenario a., an insecure topology configuration implemented in the AMP can serve as a basis for a new secure topology by inserting cybersecurity technologies into the previous one. In the case of scenario b., technologies already implemented can be re-implemented or updated, leading students to seek the necessary information to carry out this process. In scenario c., students can use the computers in the lab to connect to a virtualized network or even the network with the lab devices to gain practical experience in industrial network pentesting. In scenario d., practices can be done where commercial-off-the-shelf devices and open technologies must be evaluated and tested to verify their safety. And finally, in scenario e., students can split into multidisciplinary teams to use a risk analysis methodology to assess possible cyber risks involving the AMP.

Resources

To enable PBL and evaluate students' performance in solving problems related to the indicated practices, some resources will be necessary, such as standards, documentation, ICS components, and Industry 4.0 technologies.

For scenario a. it is important to have access to standards that include ICS protection technology requirements and recommendations. These standards serve as a basis for evaluating the insecure network topology models, provided by

the tutor, including the corporate and industrial networks. In addition, network topology and diagram design software required appropriate symbology for ICS.

For scenario b., in addition to having the control components and networks of an ICS, such as PLC, IDS, IPS, and firewalls, it is vital to have access to manuals and other documentation of cybersecurity technologies to be implemented or maintained for the protection of ICS. A vulnerable network must be set up, and the topology design must be provided to situate the student in the arrangement of the network elements.

In the scenario, c. computers need to connect to a deliberately vulnerable industrial network to assess the ability to identify assets and vulnerabilities. Computers must have virtualization software to configure the components of an ICS for pentesting, segregated from the academic network. In this way, it will be possible to assemble a vulnerable network, with ICS purposely vulnerable, to challenge students to find vulnerabilities and point out possible damages.

Scenario d. requires IIoT devices and access to code development software compatible with the practice's programming language. It can be useful to access standards used for patch management in ICS and documentation of protocols and programming languages used for the ICS integration or maintenance solutions. At last, manuals or other documentation of commercial-off-the-shelf devices and open technologies to industrial systems integration can be necessary.

Scenario e. requires access to the standard designed to carry out the cyber risk analysis of industrial processes and the documentation or standard of the defined risk analysis methodology detailing the process for performing the risk analysis. Moreover, a framework to indicate mitigations for each type of cyber-attack will be useful.

Student Performance Evaluation

The evaluation manner of problems resolution defined in each practice can consist of assessing documentation, exams, or presentations exposing what was developed to successfully solve the problem assigned in the scenario.

Conclusion

We stated that the scenarios proposed for problem-based learning, involving ICS, can be achieved based on the method proposed in this study. The method, starting from the investigation through the research of similar approaches that addressed scenarios, practices, and problems involving the learning of ICS protection technologies, enabled the analysis of information and evaluation of cybersecurity learning requirements in Industry 4.0, which brought a broad vision for future training at SENAI CIMATEC's AMP through 5 possible scenarios and 15 educational practices for PBL on ICS cybersecurity. It is crucial to clarify that the scenarios and practices set out in this study are not the first to be proposed at SENAI CIMATEC, nor the only ones possible, since ICS cybersecurity had already been carried out in the institution.

Due to paper submission limitations, the scenarios and practices proposed in this work are only those that proved to be the most important during the stages of research, analysis, and requirements evaluation. Therefore, the study established scenarios that can be used in the AMP in the future. On top of that, a collection of statistical data through satisfaction surveys submitted to the students engaged in the practices proposed here can validate the learning capacity that the scenarios and practices made possible, as well as the degree of importance of the experiences that students obtained performing the practices involved in each scenario.

References

1. Kagermann H, Wahlster W, Helbig J. Securing the future of German manufacturing industry. Recommendations for implementing the strategic initiative Industrie 4.0. Final report of the Industrie 4.0 Working Group. Acatech 2013:5-78.

2. Mahoney TC, Davis J. Cybersecurity for Manufacturers: securing the digitized and connected factory. 2017.
3. Tüv R, Ponemon Institute. The 2020 Study on the State of Industrial Security, 2020. Disponível em: https://go.tuv.com/otsurvey-2020?wt_mc=Advertising.Personalselling.no- interface.CW20_I07_FSCS.button.&cpid=CW20_I07_FSCS_PS. Acesso em: 6 de ago. 2021.
4. Sitnikova E, Foo E, Vaughn RB. IFIP AICT 406. The power of hands-on exercises in SCADA cyber security education. In IFIP AICT 2013;6(8).
5. Ribeiro MS et al. A Indústria 4.0 e a computação no Brasil. 2019.
6. ISC2. Cybersecurity Professionals Stand Up to a Pandemic, (ISC)2 Cybersecurity Workforce Study, 2020. Disponível em: https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.as. Acesso em: 6 de ago. 2021.
7. Duch BJ, Groh SE, Allen DE. The power of problem-based learning: a practical "how to" for teaching undergraduate courses in any discipline. Stylus Publishing, LLC, 2001.
8. Willems C, Meinel C. Online assessment for hands-on cyber security training in a virtual lab. In: Proceedings of the 2012 IEEE Global Engineering Education Conference (EDUCON). IEEE 2012:1-10.
9. Figueroa A, Santiago et al. A RFID-based IoT cybersecurity lab in telecommunications engineering. In: 2018 XIII Technologies Applied to Electronics Teaching Conference (TAEE). IEEE 2018:1-8.
10. Kurt S. Problem-based learning (PBL) in educational technology. 2020;January 8. Disponível em: https://educationaltechnology.net/problem-based-learning-pbl/. Acesso em: 9 de ago. 2021.
11. Drias Z, Serhrouchni A, Vogel O. Analysis of cyber security for industrial control systems. In: 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC). IEEE 2015:1-8.
12. Futura-Automation. System-On-Chip-Engineering-Pillar. Disponível em: https://futura-automation.com/2019/07/05/the-accumulating-case-for-deterministic-control/system-on-chip-engineering-pillar-sb/. Acesso em: 11 de ago. 2021.
13. Daniel AUP, Hongmei HE, Tiwari A. Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. Journal of Cyber Security Technology 2017;1(1):32-74.
14. Newhouse W et al. National initiative for cybersecurity education (NICE) cybersecurity workforce framework. NIST special publication 2017;800:181.
15. Filkins B, Wylie D, Dely S. 2019 state of OT/ICS cybersecurity survey. SANS™ Institute, 2019. Disponível em: https://www.forescout.com/resources/2019-sans-state-of-ot-ics-cybersecurity-survey/. Acesso em: Acesso em: 11 de ago. 2021.
16. Stouffer K et al. Guide to industrial control systems (ICS) security. NIST special publication 2011;800(82)16.
17. DUGGAN, David et al. Penetration testing of industrial control systems. Sandia national laboratories, p. 7, 2005.
18. Futura-Automation. Understanding IEC 62443. Disponível em: https://www.iec.ch/blog/understanding-iec-62443/. Acesso em: 12 de ago. 2021.
19. Bittencourt V et al. Proposta de reformulação para aplicação de tecnologias da indústria 4.0 em uma planta de manufatura avançada. VI SAPCT, 2021.