# LEARNING PROPOSAL FOR CYBERSECURITY FOR INDUSTRIAL CONTROL SYSTEMS BASED ON PROBLEMS AND ESTABLISHED BY A 4.0 DIDACTIC ADVANCED-MANUFACTURING-PLANT

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

*[a] Center of Competence in Advanced Manufacturing, SENAI CIMATEC, Brazil*
*[b] Automation Department, SENAI CIMATEC, Brazil*
*[c] brunosjunq@gmail.com*

**Abstract:** Researches data indicates that the search for cybersecurity professionals to protect industrial control systems (ICS) in Brazil is increasing, as a result of the rise in cyber-attacks directed at the industry. However, there is a deficiency of professionals with the required competence in ICS cybersecurity, which involves the areas of information (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 required for the protection of ICS. This paper seeks to present a strategy to address this lack through the evaluation of indicative scenarios of practices for the development of competencies in ICS cybersecurity through the active problem-based learning (PBL) methodology. The proposed scenarios combine the theory and practice involved in solving ICS cybersecurity problems, through the use of PBL with the support of SENAI CIMATEC's 4.0 Advanced Manufacturing Plant (AMP).

**Keywords:** Cybersecurity; Industry; Scenarios; Practices; Problem-based.

# PROPOSTA PARA APRENDIZAGEM DE CIBERSEGURANÇA DE SISTEMAS DE CONTROLE INDUSTRIAL BASEADA EM PROBLEMAS E APOIADA POR UMA PLANTA DIDÁTICA DE MANUFATURA AVANÇADA 4.0

**Resumo:** Dados de pesquisas indicam que a busca por profissionais de cibersegurança para proteger sistemas de controle industriais (ICS) no Brasil tem aumentado, principalmente em decorrência do aumento de ataques cibernéticos dirigidos à indústria. Entretanto, observa-se que há uma grande deficiência de profissionais com a competência em cibersegurança de ICS, que envolve as áreas de tecnologia da informação (IT) e de operação (OT), indicando uma carência de estratégias por parte das instituições de ensino para a formação de profissionais que dominem as tecnologias necessárias para a proteção de ICS. Este trabalho busca apresentar uma estratégia para lidar com esta carência a partir da avaliação de cenários indicativos de práticas para o desenvolvimento de competências em cibersegurança de ICS por meio da metodologia ativa de aprendizado baseada em problemas (PBL). Os cenários propostos combinam a teoria e a prática envolvida na resolução de problemas de cibersegurança de ICS, por meio do uso de PBL com o apoio da Planta de Manufatura Avançada 4.0 (AMP) do SENAI CIMATEC.

**Palavras-chave:** Cibersegurança; Indústria; Cenários; Práticas; Problemas.

ISSN: 2357-7592

## 1. INTRODUCTION

Cybersecurity has been gaining prominence in managerial and governmental agendas. Industry 4.0 is a real and 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 9 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 into 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 presence of CPS in industrial environments is marked by the emergence of cyber risks, where vulnerabilities and threats can critically impact business models and lead to a loss of competitiveness. A study carried out by [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 refers 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 operational network through the corporate network [3].

Cyber risks demand that cybersecurity strategies shall be integrated with organizational initiatives and information and communication technologies, aiming to ensure the security of data, information and performance of the production value chain. Consequently, it is observed that in recent years 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 high industrial demand on cybersecurity training for such systems [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 [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 the kind of learning needed for this specialization, considering that hands on practice is essential to deal with the nuances posed by the diverse cyber-attacks specificities in ICS. Active-based learning techniques are best-fitted for this purpose and, among these, problem-based learning (PBL) has the advantage of bringing the necessary practice in the specific student problem. The creation of scenarios and practices enabled by PBL allow the insertion of students in situations involving cybersecurity problems associated with ICS in real scenarios.

In PBL, students are asked to work together to analyze and resolve problems, and to communicate, evaluate, and integrate information from diverse sources [7]. However, for this methodology to be efficient, it is necessary an environment for hands-on practices that represents an industrial plant. In this context, SENAI CIMATEC, in order to contribute to industrial technological advancement, was the first institution to integrate ICS cybersecurity in Brazil into its Advanced Manufacturing Plant (AMP). In view of this, this research proposes scenarios for the realization of practices through learning based on real problems, which will be solved in the AMP as a way to add ICS cybersecurity competence.

ISSN: 2357-7592

## 2. METHODOLOGY

In order to develop the ICS cybersecurity training scenarios considering also Industry 4.0 environments, a methodology based on three steps was followed, as shown in Figure 1.

Figure 1. Methodology used for scenario development

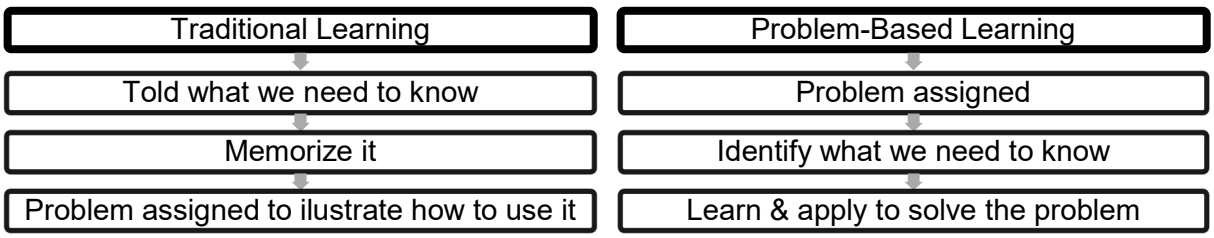

A basic documental research and analysis of similar approaches was carried out for the verification of scenarios and practices already developed. After that, learning requirements linked to cybersecurity technologies applied in Industry 4.0 were assessed. Finally, the scenarios were established and practices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

### 2.1. 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 in cybersecurity training for ICS and SCADA systems. However, many existing research centres 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 reason is the lack of a specific discipline for this topic, caused due to the scarcity of professionals with the required competences to minister this discipline.

The decision of choosing PBL instead of other methodology is based on the analysis of benefits and risks related to it. As benefits 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 difficult and PBL may require more study time, taking away time from other subjects and also creating anxiety, because learning certainly will be messier, needing one instructor, or more, to constantly guide the students. PBL has already been used to improve the efficiency of cybersecurity education and to help students develop the wide range of skills needed to be a cybersecurity professional, including technical aspects, team work, making judgments and developing as lifelong learners [9]. As can be seen in Figure 2, 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 will likely be faced during their professional life [10].

Figure 2. Traditional Learning x Problem-Based Learning [10]

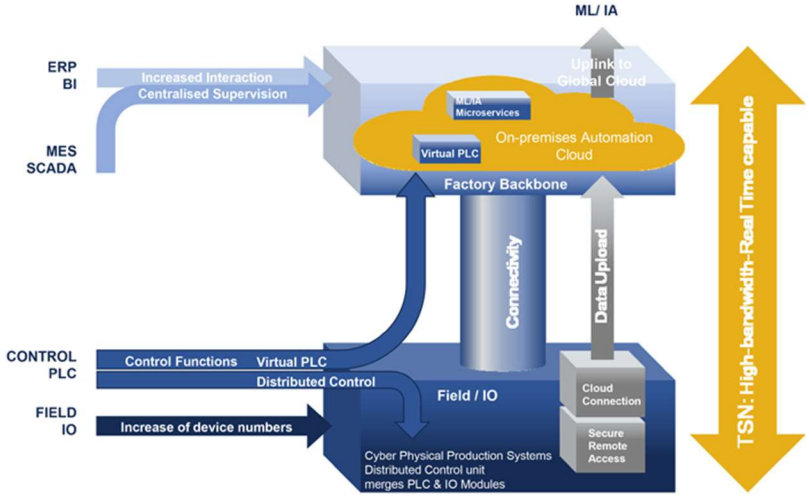


## 2.2. Assessment of ICS cybersecurity learning requirements in Industry 4.0

In order 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 general requirements, it is possible to raise specific requirements for the protection of ICS in Industry 4.0 using ICS cybersecurity standards as a basis.

It is important to note that, as Industry 4.0 technologies are adopted, the Industry 3.0 pyramid model becomes obsolete. As a consequence, the interdependence between hierarchical levels of communication is no longer a characteristic factor and the connectivity between the factory floor (field level) and the systems present in corporative levels gets relevance. Thus, a pillar model is consolidated, as shown in Figure 3 [12], where systems at the field level and its industrial assets are constantly interacting, as CPS to improve the performance of processes.

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




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

## 2.3. Establishment of scenarios, indication of practices and problems

To establish the scenarios and indicate practices and problems, data from researches and problems related to cybersecurity in Industry 4.0 were analyzed. 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 7 categories, 33 specialty areas and 52 work roles [14]. As a similar classification was not found for the

OT context, it was used as a reference. Also, to address the problems involving knowledge in ICS needed for the labor market, the results of a survey carried out by [15] were taken into account, which pointed that process and technology practices can be more useful to people development.

## 3. RESULTS AND DISCUSSION

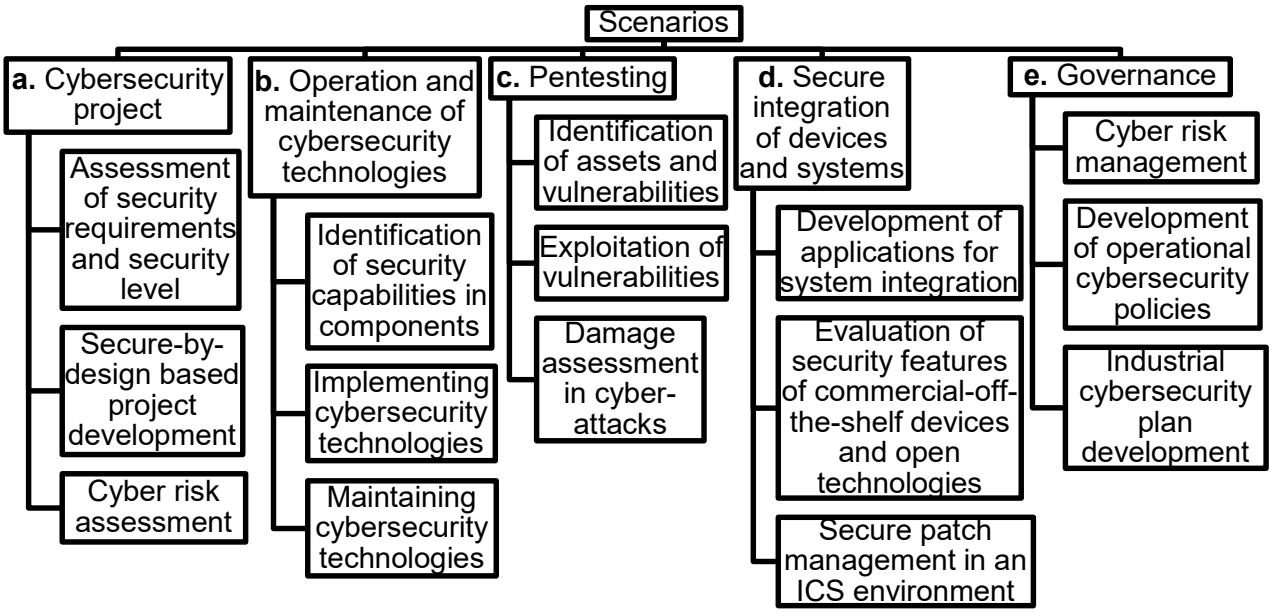
Through the proposed methodology, scenarios were assembled and practices and problems were indicated. Next, the resources needed to carry out the practices and solve the problems through PBL were raised. At last, a discussion was made about the method of evaluating the performance of students participating in the practices.

### 3.1. Scenarios, practices and problems

At the end of the research and similar analysis, it was observed that 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].

In the context of Industry 4.0, data analysis and integration between the floor or field and management systems is generally done through software solutions provided by third-party vendors or commercial-off-the-shelf device integrations [13]. This can cause several problems brought by the lack of security integrated to some solutions. This reveals the need of two additional scenarios: **d.** secure integration of devices and systems, which is justified by the necessity 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 breaches, which according to 63 % of security experts, is one of the reasons for the increase of risk [3,14].

Figure 4. Proposed Scenarios and Practices




In addition to the above considerations, the use of parts of the IEC 62443 [18] or other families of standards, is appreciated to assist in the development of problems

associated with the practices. In this way, already existing requirements and recommendations to ensure ICS cybersecurity can be followed by students.

### 3.2. Application in 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 MPA.

First, in scenario **a.** an insecure topology configuration implemented in the AMP can serve as a basis for the development of 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 in order 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.

### 3.3. Resources

In order to enable PBL and the evaluation of students performance in solving problems related to the indicated practices, some important resources will be necessary, such as standards, documentations, ICS components and Industry 4.0 technologies.

For the scenario **a.** it is important to have access to standards that include ICS protection technology requirements and recommendations. These standards will serve as a basis for the evaluation of insecure network topology models, provided by the tutor, which must include the corporate and industrial network. In addition, network topology and diagram design software with appropriate symbology for ICS is required.

For the scenario **b.**, in addition to having the control components and networks of an ICS, such as PLC, IDS, IPS and firewalls, it is important 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, in order to situate the student about the arrangement of the network elements.

In scenario **c.** computers need to connect to a deliberately vulnerable industrial network in order 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, in order to challenge students to find vulnerabilities and point out possible damages.

The scenario **d.** requires IIoT devices and access to code development software compatible with the practice's programming language. Having access to standards used for patch management in ICS and documentations of protocols and programming languages used for the ICS integration or maintenance solutions can be useful. 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.

### 3.4. Student performance evaluation

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

## 4. CONCLUSION

Based on the methodology proposed in this study, it is possible to state that the proposed construction of scenarios for problem-based learning involving ICS can be achieved. The methodology, 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 important 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 made it possible to establish scenarios that in the future can be used in the AMP. As a suggestion for future investigations, a detailing of the practices can be made. 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.

## 5. 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, pp. 5-78, 2013.

[2] MAHONEY, Thomas C.; DAVIS, Jim. **Cybersecurity for Manufacturers: Securing the Digitized and Connected Factory**. 2017.

[3] TÜV Rheinland, 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, R. B. (2013). IFIP AICT 406, **The Power of Hands-On Exercises in SCADA Cyber Security Education**. In IFIP AICT (Vol. 6, Issue 8).

[5] RIBEIRO, Matheus dos Santos et al. **A Indústria 4.0 e a computação no Brasil**. 2019.

[6] (ISC)², **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, Barbara J.; GROH, Susan E.; ALLEN, Deborah E., **The power of problem-based learning: a practical "how to" for teaching undergraduate courses in any discipline**. Stylus Publishing, LLC., 2001.

[8] WILLEMS, Christian; MEINEL, **Christoph. 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. p. 1-10.

[9] FIGUEROA, Santiago et al. **A RFID-based IoT Cybersecurity Lab in Telecommunications Engineering**. In: 2018 XIII Technologies Applied to Electronics Teaching Conference (TAEE). IEEE, 2018. p. 1-8.

[10] Kurt, S. **Problem-Based Learning (PBL)**, in *Educational Technology*, January 8, 2020. Disponível em: https://educationaltechnology.net/problem-based-learning-pbl/. Acesso em: 9 de ago. 2021.

[11] DRIAS, Zakarya; SERHROUCHNI, Ahmed; VOGEL, Olivier. 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. p. 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] ANI, Uchenna P. Daniel; HE, Hongmei; TIWARI, Ashutosh. **Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective**. Journal of Cyber Security Technology, v. 1, n. 1, p. 32-74, 2017.

[14] NEWHOUSE, William et al. National initiative for cybersecurity education (NICE) cybersecurity workforce framework. **NIST special publication**, v. 800, n. 2017, p. 181, 2017.

[15] FILKINS, Barbara; WYLIE, Doug; DELY, **Sans 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, Keith et al. **Guide to industrial control systems (ICS) security**. NIST special publication, v. 800, n. 82, p. 16-16, 2011.

[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, Victor et al. **PROPOSTA DE REFORMULAÇÃO PARA APLICAÇÃO DE TECNOLOGIAS DA INDÚSTRIA 4.0 EM UMA PLANTA DE MANUFATURA AVANÇADA**. VI SAPCT, 2021.