The Importance of SCADA Systems Educational Programs in Higher Education from a Cybersecurity Perspective

Tiberiu Ion[1]
[1)] *National Defense University "Carol I", Bucharest, Romania.*
E-mail: ion.tiberiu@unap.ro

Please cite this paper as:
Ion, T., 2021. The Importance of SCADA Systems Educational Programs in Higher Education from a Cybersecurity Perspective. In: R. Pamfilie, V. Dinu, L. Tăchiciu, D. Plești, C. Vasiliu eds. 2021. *7th BASIQ International Conference on New Trends in Sustainable Business and Consumption.* Foggia, Italy, 3-5 June 2021. Bucharest: ASE, pp. 835-843
DOI: 10.24818/BASIQ/2021/07/105

Abstract

Nowadays manufacturing organizations are rapidly transforming to smart factories, in the context of a new stage of industry development known as Industry 4.0. While this new phase in the production and manufacturing sector is booming, associated technologies promise multiple benefits and opportunities across all major market sectors. From the Internet of Things to cloud-based design systems, implementing virtual technologies in the manufacturing area, not to mention critical industries, represents a great challenge in terms of cybersecurity and data privacy issues.

In order to avoid major roadblocks in adopting Industry 4.0 technologies, SCADA systems had been developed and represent a hybrid system that focuses on traditional cybersecurity issues, plus Industry 4.0 own unique security and privacy challenges in terms of a more digitalized industrial sector. Taking into consideration the success that SCADA technologies have in digitalizing manufacturing industries as well as critical sectors like energetic production, transportation or healthcare, implementing and monitoring such a system, especially when interfaced with internet communication technologies, calls for special trained human resources.

In this regard, the present paper provides an overview on the importance of SCADA systems within Industry 4.0, while highlighting different university specialization approaches. Modern cybersecurity curricula must be updated in order to sustain a deeper specialization that is required for understanding and developing SCADA systems, mainly by creating laboratories where students as future specialist can make test, develop new solutions and understand different technologies linked to different manufacturing sectors. Thus, the current paper provides a comparative presentation of different approaches that universities can apply in order to develop SCADA research laboratories, by incorporating efficient virtual techniques and technologies and build a more realistic and attractive learning platform, in terms of cost efficiency for student and engineering education.

Keywords

SCADA, cyber security, critical infrastructures, university programs
DOI: 10.24818/BASIQ/2021/07/105

Introduction

Cybersecurity represents today one of the most debated subjects within multiple domains or sectors, mostly because of its multidisciplinary approach and digitalization, that brings together manifold resources like "tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets" (ENISA, 2015).

Taking into consideration that cybersecurity resides in the core of each sector, being influenced by the specific resources, input and output of the sector and being driven by specialized cybersecurity professionals, different stakeholders ask: What should they do to better enhance cybersecurity in relation to their industry's needs, taking into consideration that most sectors are hybrid sectors – using both cyber systems and physical systems?

This question represents a challenge from the perspective of cybersecurity in assuring the three general security objectives of (i) confidentiality, (ii) integrity, and (iii) availability (also known as the CIA triad in the information security industry) (Weber and Studer, 2016) in the context of a shortage of about three million cybersecurity professionals globally (Kam et al, 2020).

In this context, the present paper presents the concept of SCADA (Supervisory Control And Data Acquisition) technology and its importance in automating some of the most important industries for any country. Currently, SCADA technologies are used to manage specific data belonging to the energy sector, hydrological sector or other fields that define critical resources for a nation. The need to implement this technology as a stand-alone discipline in university educational programs is determined by the growing demand to digitize critical industries, in the context of ensuring high and permanent cyber protection.

These main issues are addressed in the two sections of the current article, highlighting the main aspects that have influenced the evolution of SCADA technology, as well as the importance for future specialists to enhance the knowledge on how to use and apply SCADA systems in a correct, practical and safe way.

In the context of technological evolution, the digitization and robotization of industries towards the fourth industrial revolution (Industry 4.0) will lead to a rapid increase in the use of SCADA systems (monitoring, control and data acquisition systems) (Research and Markets, 2021). In addition, the increasing use of information technology specific solutions that characterize Industry 4.0, such as IoT (Internet of Things) devices, cloud computing and artificial intelligence, is evidence of the use of SCADA systems in an adapted and rethought way, so they can be efficient and in scope to technological progress.

Lack of expertise in the information security field, as well as insufficient awareness of the complexity and imminent impact of cyber threats, most common met in the government environment or different specialists, represents a major barrier in adopting specific security measures for Industry 4.0. Usually, the specialists involved in the implementation of new solutions at a government level have only security knowledge in the field of IT (Information Technology) or only in the field of OT (Operational Technology), while Industry 4.0 and the concept of Smart Manufacturing requires extensive expertise, with applicability in multiple fields. For example, a specialist in this field must additionally have knowledge on network security and embedded systems, which operate in a converged system. The solution of this problem can be achieved only by promoting cyber education in the university environment in order to train specialists in the field and promoting joint exercises and partnerships between academia and companies that manage/use such systems.

The efficiency of SCADA technologies in the fourth industrial revolution

A transformative event known as the Fourth Industrial Revolution/Industry 4.0 is taking place in multiple major market sectors, which use industrial systems connected to Internet communication technologies. Its origins lie at the core of Germany's efforts to sustain its leadership in innovation and manufacturing (UNIDO, 2018). The progress made has led to the creation of intelligent factories and production organizations that operate more efficiently and with a more efficient control and management of production processes, data and machines.

Until this point, the global industry has experienced three evolutionary revolutions, modern society being now witness for the beginning of the fourth one. From an evolutionary point of view, all four revolutions had a major contribution to modern progress, from industrial engineering and electricity to automatization and information technology. A schematic progressive presentation of the four revolutions can be found in Figure no. 1.

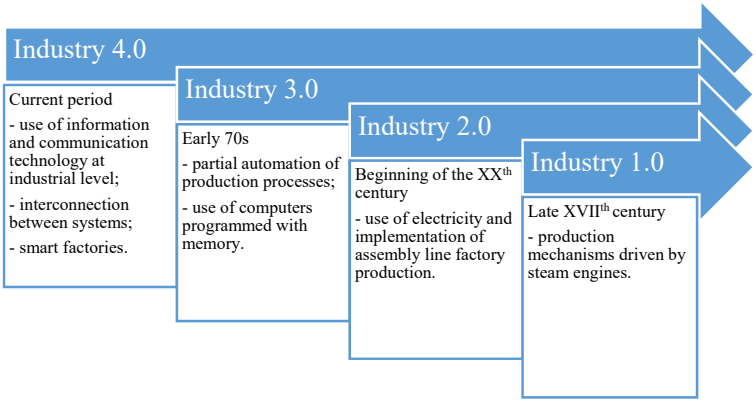

Figure no. 1. The four industrial revolutions
Source: own research

Automatization and data collection began to emerge by the third Industrial Revolution. Back then, classic technologies from Industry 3.0 propagated the collected data through several devices arranged hierarchically on multiple levels (layers), starting from different industrial sensors to Programmable Logic Controllers (PLC), Distributed Control Systems (DCS), Human-Machine Interface (HMI) and finally evolving to SCADA systems.

Industries have long relied on proprietary technologies, using communication protocols and master computers from the same vendor (Ujvarosi, 2016), to monitor equipment and production, in a closed system, but with their migration to Industry 4.0 they become interconnected, and even more, the use of advanced machine learning algorithms for the automation of industrial processes is becoming more common. In addition, the use of cloud computing technology is becoming more and more attractive, because of the efficiency that a whole system can manage data, by reducing the layers between gathering information from field devices (actuators, sensors), to the top where information is processed (Application Layer). Implementing SCADA solutions that learn, adapt, and potentially act autonomously rather than simply execute predefined instructions is the new way enterprises are heading to (Rajeswar, 2019).

The IoT technology is a key element in Industry 4.0, conceived under the German federal government's High-Tech Strategy focusing on information and communication technology to improve manufacturing (Lydon, 2018). It represents a convergence of industrial equipment with advanced computing and ubiquitous communication technologies, for example the use of IP (Internet Protocol).

Multiple researches on the advantages of IoT allowed the introduction of these technologies in industrial applications and business processes, leading to the new concept of IIoT or Industrial IoT. With the emergence of Industrial IoT, SCADA systems will be enhanced by the use of IoT technologies. Thus, IoT will extend SCADA and its value chain to make industrial business more predictable, cost reduced and more profitable (Rajeswar, 2019). OT's or traditional hardware and software systems usually used in industrial environments were not designed to work within the Internet network, but now with the development of IIoT, the need of emergent requirements for industrial applications has risen. In this sense, Industrial Control Systems (ICS) as PLC's, DCS's and HMI's have evolved to extend IIoT systems.

With the growing complexity of connected devices used in industrial companies, the need for data aggregation, data exchanging and the need of system interoperability has substantially increased. SCADA systems have been great for monitoring and controlling manufacturing processes, but with the help of IoT devices more data from any industrial process can be gathered and, by applying predictive analytics, a more manageable data system can be established. IoT equipment can provide quality information at capacities that never been achieved before and therefor, by analysing and using this kind of information, enterprises can improve the ability to predict future events.

The increasing use of big data and predictive analytics will mean a new challenge to many enterprises and many have understood this, according to a research done by Oracle and Intel, 60% of businesses see an integrated Cloud Platform as the route to unlocking the potential of disruptive technologies at the heart of Industry 4.0, such as robotics or artificial intelligence (Oracle, 2016). In this context, cloud technologies provide companies the computing power they need, that results in shorter innovation cycles and increased operational efficiency.

Usually, cloud computing provides three types of services: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). But when it comes to Industry 4.0, a new type of cloud service emerges. Cloud manufacturing is a new manufacturing model developed from the concept of Manufacturing as a Service (MaaS) (Wei, et al, 2020). Thus, many manufacturing companies adopt Cloud Manufacturing as a business model to enable production resources virtualization. This modern production concept uses technologies such as IIoT, Cyber-Physical Systems (CPS), Manufacturing Data Management, Cloud computing and makes them all available over Internet.

However, existing Internet connected technologies are affected by cybersecurity and data privacy issues, which pose major challenges and barriers to the widespread adoption of Industry 4.0 technologies (Thames and Schaefer, 2017). Therefore, as SCADA systems adopt IT solutions by being designed using network protocols and operating systems (OS), they start to resemble IT systems. This integration provides less isolation for IIoT devices or ICS from the outside world.

While cybersecurity solutions have been implemented to deal with security challenges in typical IT systems, special solutions must be designed for SCADA environment and, most important, for IIoT devices that operate critical cloud applications. In this regard, a well-known cybersecurity strategy to avoid cloud computing vulnerabilities is represented by edge computing. By applying this computing topology, data storage is closer to the devices where it's being gathered, rather than relying on the Internet to transfer them on the servers where the cloud is operating, creating advantages that, besides security reasons, contribute to achieving low latency by reducing the physical distance that data must travel for processing and analysis.

Research in cybersecurity for SCADA systems is challenging. These systems have critical requirements of high availability, use specialized computing devices, software and protocols and, by applying Industry 4.0 technologies, it gets more difficult to operate these systems in a secure manner. Thus, the need of specialized training programs, to perform effective applied research with real world equipment is imperial for SCADA specialists to train.

Research methods

Based on the importance of SCADA technologies in both economic and social development of certain markets and sectors, the purpose of the study is to explore the main resources that future SCADA and cybersecurity specialists can access in order to gain knowledge and develop certain skills that are essential for the digitalization of critical sectors. Having higher education as the starting point of the specialised learning process and taking into consideration the physical and financial means that universities must own in order to make the learning process more productive, different types of SCADA laboratories from different universities and companies (for example University Politehnica of Bucharest) were subjected to field research (both physically and virtually) in order to identify an efficient cost-resource solution.

The used method is considered appropriate, as the researched field does not always behave like a homogeneous community, as different universities or companies have access to different resources and design different laboratories (small vs medium vs large; physical vs virtual; modular vs static etc.).

For a better approach, starting June 2020, these aspects were addressed within the project "Center of Excellence for CyberSecurity and Critical Infrastructure Resilience (SafePIC)". The project's main outcome, that is estimated to be delivered by July 2023, will be the establishment, development and operationalization of a center of excellence in cybersecurity of critical infrastructures for preventing, analysing, monitoring and responding to cybersecurity incidents.

Cybersecurity and SCADA in higher education programs: analysis and proposals

Taking into consideration the multiple benefits that SCADA systems can bring to any organization, business, industry or governmental sector (like 24/7 maintenance, proactive monitorization of any network, remote interaction from any place and more) there is a growing need of specialized human resources that can activate in this domain. The most important segment of the SCADA technology is the software development phase, as specialists involved in this phase must relate on multiple knowledge domains, both from the industry sector and cybersecurity sector.

In this regard, the traditional cybersecurity specialization that multiple universities tend to introduce in the IT curricula, must be analysed from the perspective of its final destination. More exactly, the industry or business and government environments need more specialists in cybersecurity, but each sector's particularities will have a big influence on how cybersecurity should be perceived and must be implemented in order to be more efficient to the sector in scope.

This represents the main difference between a cybersecurity specialist that works for a car producing line in a big company, like Ford or Volkswagen and another cyber-specialist having same position but within a hydroelectric company. Both specialists will have the same perception on cybersecurity and its main outcome, but the technology used in this scope or the way in which various IT solutions will be implemented will be diametrically opposed.

Having these differences in mind, cybersecurity academic curricula should be designed in order to help future specialists train in specific domains and acquire certain expertise specific to that domain. This performance can be achieved by providing students and universities access to the latest SCADA software and technologies (Schneider Electric, 2012). Taking into consideration that big tech companies invest a big percent of their budget in developing SCADA technologies that result in intellectual property or company secrets, accessing this kind of information involves costs for universities that lead to higher nominal fees that future specialists must assume. On the other hand, some universities are implementing low-cost SCADA systems, equipping experimental laboratories with the necessary hardware and using an innovative approach which combines low-cost NI data acquisition PCI cards and inexpensive analog and digital sensors and output devices (Otieno, 2007).

Despite the chosen approach, universities that promote cybersecurity programs must have a clear list of sectors that refer to critical infrastructures. This list can vary from a country to another, but there are some main sectors that are common from a nation to another. These generally include agriculture, healthcare, nuclear reactor, transportation, energy sector, civil and chemical engineering, water plants and research (Geeta and Kolin, 2021). All these domains are illustrated in the figure below:

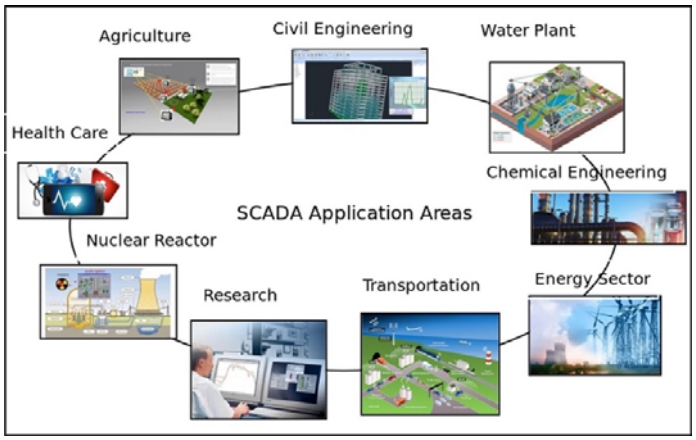

Figure no. 2. SCADA critical infrastructures appliance
Source: Geeta and Kolin, 2021

Suitable academic programs on cybersecurity for these types of complex systems are essential. In order to fulfil this purpose, physical, remote or virtual laboratories are excellent support tools that help

students as future specialists to consolidate their theoretical knowledge through experiments with real industrial equipment used in these sectors. These dedicated research and development SCADA cybersecurity laboratories must be capable of providing students real hands-on experience by operating latest SCADA software and hardware equipment, tailored to the specific situations and requirements of organizations. In order for the research to be carried out, the attack scenarios need to be reproduced in a controlled environment, so that the student can understand the behaviour of the threat and also be able to experiment different solutions on how to stop it. A model based on cybersecurity techniques needs to be applied in a university SCADA system laboratory that must include:

- vulnerability analysis;
- National Institute of Standards and Technology-Risk Management Framework (NIST-RMF) standardization and best practices;
- using teams as a cybersecurity assessment technique;
- ICS vendor equipment analysis and system monitoring;
- SIEM testing and implementations;
- configuration and deployment of tools for situational awareness such as event monitoring, intrusion detection system, intrusion prevention system, system logs etc;
- insider threat mitigation program;
- detect and prevent man-in-the-middle, ransomware and other well known and documented cyber attacks.

In order to help the academic and research sector, different European governmental authorities have increased their involvement in the cybersecurity of ICS by establishing a global framework for developing protection activities for these systems (DelCanto et all, 2015). Moreover, European organizations such as Information Sharing and Analysis Center (ISACs), Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and National Institute of Standards and Technology (NIST) are continuously introducing security guidelines, rules and regulations, and standards for the security of ICS (ECSO, 2018). In this sense, universities cand easily adopt a standardize approach of their curricula in this domain.

To facilitate active learning, a real SCADA laboratory with physical hardware sensors, actuators, dedicated communications linked to servers (physical and virtual) and fully equipped for research, is one possible way to achieve well trained students in cybersecurity. However, each ICS used in production has different hardware sets and configuration for its SCADA system: some SCADA architectures are fully centralized, while other are distributed with a hierarchical structure. Modern SCADA systems tend to move towards fully automatic closed loop system, while traditional systems usually need human intervention to operate. Big data analytics and merging IIoT devices also play an important part in SCADA systems: as data is gathered from sensors, the system's state is estimated, and various analytics are displayed for operators to take actions. The obvious reasons where physical labs have an advantage over remote and virtual labs is represented by the interaction between students and real equipment that can also involve collaborative work. This ideal learning solution comes with high costs for the university in acquiring all the device needed to make more test scenarios available and the disadvantages of scheduling effort and location restrictions.

A modern efficient time scheduling effort solution to solve physical boundaries is to remotely share controlled access to SCADA laboratories. Remote laboratories are best alternatives to working in a real laboratory because, if properly designed, they can offer the same advantages as a real laboratory and also the flexibility in choosing the time and place for performing test scenarios. In this case, one single important aspect must be taken into consideration, respectively the access throughout internet. To manage in a secure manner users' access from the Internet to the SCADA laboratory, a web server and a proxy server are used. These servers operate in a demilitarized zone (DMZ), which restricts the incoming connections to provide additional security (DelCanto, et al., 2015).

In this case, the web server will provide a friendly web interface for the users and allow them to perform specific tasks within the cybersecurity SCADA laboratory and, depending on the privileges the students have, they can perform practical tasks using physical equipment available in this environment. So, students can interact from anywhere with a physical laboratory through a computer with Internet connection. The proxy server will be used for network address translation (NAT), net filtering,

connection tracking logs and other specific security measures. This server will bridge the web application that user interact with the local network that the SCADA laboratory servers will operate.

The most cost-efficient solution for a cybersecurity SCADA laboratory is to use specialize software to fully virtualize SCADA equipment. Virtual laboratories can be quickly reconfigured to model and simulate different SCADA systems relevant to a specific production industry or critical infrastructure system and simulated. This virtual laboratory simulates learning environments that allow students to explore concepts and theories online without using expensive physical SCADA equipment. By using this software for virtualization, creates an alternative access to SCADA technologies, but the lack of real data from physical devices and that the student will use only idealized data for analysis represents the main disadvantage of this type of laboratory. The issue of implementing virtual laboratories is usually determined by the informatics tools that are available in each institution or simply limited to some technology or technique in order to show its efficacy (Rodriguez, et al., 2016).

But the ideal solution for building a cybersecurity SCADA laboratory that provides all the necessary learning resources is to combine all three types of laboratories: physical, remote and virtual. In this case, the main resource will be the physical laboratory, equipped with all the necessary hardware and upgraded with specialized software, in order for teachers and students to be able to virtualize more complex scenarios that are used in the production industry. The final facility of this hybrid laboratory would be to make all of these resources available remotely. But in this scenario, the hardware and software architecture make it the most difficult to realize, from a cost and a complexity perspective.

So, virtual and remote SCADA laboratories have a significant advantage over physical laboratories because they can provide flexible access to their users at a lower cost, which is very important for universities and future students. In this context, teachers must adapt and understand the importance of a well-designed virtual laboratory that can offer the pedagogical advantage of a more complex presentation of the concepts in the study field of concern.

Conclusions

One of the main objectives of Industry 4.0 is represented by the digitalization of industries and multiple sectors, while the Internet of Things is increasingly used to facilitate communications and data transfer. Whereas some service sectors can easily adapt to this new approach, the manufacturing sector and the critical industries like energetic, transportation, healthcare or different research facilities (like nuclear research) are sensitive to such changes which can raise a number of issues and threats.

In this context, SCADA technologies were developed in order to efficient digitalize such industries and create centralize system that can monitor and manage important systems as a whole. Thus, adopting new security approaches is not easy as cyber-physical security risk in manufacturing processes has risen and without specialists that cand monitor a SCADA system, its implementation can represent a cybersecurity threat for the organization. Therefore, in order to excel in SCADA technologies, specialists must have multiple areas of competence, starting with IT and cybersecurity knowledge and deepening the specialization with a series of knowledge specific to the field of activity (energy, medicine, various types of production etc.).

Universities must take into consideration that the process of training students in this field is a difficult one, especially in terms of the resources needed to put theoretical elements into practice and to be able to test different threats specific to different fields and sectors, mainly equipped laboratories. Thus, for the academic sector this objective represents a difficult challenge taking into consideration the costs that it involves. Therefore, different approaches regarding the resources that universities can use in this scope highlighted different solutions:

- learning efficient solutions that involve complex testing laboratories (with physical and virtual elements);
- cost efficient solutions that involve virtual laboratories.

Despite the chosen solution, teachers must opt for a multidisciplinary approach that combines cross-industry presentations and offers a more complex description of the concepts in the study field. Nevertheless, cybersecurity will continue to represent a growing discipline within multiple universities'

curricula, but without a specific direction in studying this concept, a permanent gap will exist between the learn techniques and applying security knowledge in manufacturing specific fields (e.g. oil extraction process, car production lines) or critical industries or services (e.g. hospital monitoring, nuclear research).

Acknowledgement

This paper was elaborated within the project "Center of Excellence for Cyber Security and Critical Infrastructure Resilience (SafePIC)" contract no. 270/23.06.2020, ID 120436, funded through the Competitiveness Operational Program 2014-2020, priority axis 1, Action 1.2.1: Stimulating the demand of enterprises for innovation through RDI projects carried out by enterprises individually or in partnership with R&D institutes and universities, in order to innovate processes and products in economic sectors with growth potential.

References

DelCanto, C.J., Prada MA., Fuertes, J.J., Alonso, S. and Domínguez, M., 2015. Remote Laboratory for Cybersecurity of Industrial Control Systems. *IFAC-PapersOnLine*, 48(29), pp.13-18.

Geeta, Y. and Kolin, P., 2021. Architecture and Security of SCADA Systems: A Review. *International Journal of Critical Infrastructure Protection*, 34, Article number: 100433.

Kam H.J., Menard, P., Ormond, D. and Crossler, R.E., 2020. Cultivating cybersecurity learning: An integration of self-determination and flow. *Computers & Security*, 96, Article number: 101875.

Lydon, B., 2018. How do you define IoT and Industry 4.0 as it relates to industrial manufacturing? *International Society of Automation – InTech.* May/June [online] Available at: <[online] Available at: <https://www.isa.org/intech-home/2018/may-june/features/how-do-you-define-iot-and-industry-4-0> [Accessed 04 April 2021].

Oracle, 2016. Cloud: *Opening up the Road to Industry 4.0.* [pdf] Available at: <https://www.oracle.com/webfolder/s/delivery_production/docs/FY16h1/doc30/reportIaas.pdf> [Accessed 07 April 2021].

Otieno, A., 2007. Development of SCADA Experimental Systems through Student Projects to Enhance the Automation Curriculum in a Manufacturing Engineering Technology Program. *American Society for Engineering Education*, 12, pp.1-11.

Rajeswar, K., 2019. Industry 4.0 wave - Relevance of SCADA in an IOT world and journey towards a true digital enterprise. *IEEE India Info*, 14(3), pp.78-88.

Research and Markets, 2021. *SCADA Market with COVID-19 Impact by Offering (Hardware, Software, Services), Component (Programmable Logic Controller, Remote Terminal Unit, Human? Machine Interface, Communication System), End User, and Region - Global Forecast to 2026*, [online] Available at: <https://www.researchandmarkets.com/reports/5306259/scada-market-with-covid-19-impact-by-offering> [Accessed 27 March 2021].

Rodríguez, F., Guzmán, J.L., Castilla, M., Sánchez-Molina, J.A. and Berenguel, M., 2016. A proposal for teaching SCADA systems using Virtual Industrial Plants in Engineering Education. *IFAC-PapersOnLine*, 49(6), pp.138-143.

Schneider Electric, 2012. *Develop your own courseware to enrich SCADA education at institutions of higher learning. Academic Program*, [online] Available at: <https://download.schneider-electric.com/files?p_enDocType=Brochure&p_File_Id=682844284&p_File_Name=SCADA-Academic-Program-Brochure-2012.pdf&p_Reference=DIA6ED1090813EN> [Accessed 12 April 2021].

Schaefer, D. and Thames, L. eds., 2017. *Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing*. 1st ed. 2017 ed. Springer Series in Advanced Manufacturing. Cham: Springer International Publishing : Imprint: Springer.

The European Union Agency for Network and Information Security (ENISA), 2015. *Definition of Cybersecurity. Gaps and overlaps in standardisation*, [online] Available at:

<https://www.enisa.europa. eu/publications/ definition-of-cybersecurity> [Accessed 12 March 2021].

Ujvarosi, A., 2016. Evolution Of Scada Systems. *Bulletin of the Transilvania University of Braşov*, 9(58), pp.63-68.

United Nations Industrial Development Organization (UNIDO), 2018. *What can policymakers learn from Germany's Industrie 4.0 development strategy?* [online] Available at: <https://www.unido.org/api/ opentext/documents/download/11712839/unido-file-11712839> [Accessed 01 April 2021].

Weber, R.H. and Studer, E., 2016. Cybersecurity in the Internet of Things: Legal aspects. *Computer law & security review,* 32(5), pp.715–728.

Wei, W., Zhou, F., Liang, PF., 2020. Product platform architecture for cloud manufacturing. *Advances in Manufacturing*, 8, pp.331–343.