CYBER-SECURITY IN THE NEW ERA OF INTEGRATED OPERATIONAL – INFORMATIONAL TECHNOLOGY SYSTEMS

Vlad Daniel Savin
Bucharest University of Economic Studies, Bucharest, Romania
vlad.savin@ager.ro

Abstract

Digital Revolution has forced previously isolated networks of critical infrastructures to become more digitally integrated. Recent cyber-attacks, including Stuxnet and Wiper, have exposed a new set of cybersecurity vulnerabilities in this field. This new environment has forced previously isolated networks of critical infrastructures like utilities or power plants to become more digitally integrated. This paper offers a view into the most efficient current defense solutions. It also offers a glimpse into the need for the further development of new protection mechanisms developed on the emerging new technologies. The risks posed by the integration of Information Technology solutions with Operational Technology systems have been a key topic also at the latest World Economic Forum conference, where cyber-attacks of critical infrastructures were discussed in the context of the most significant risks for the upcoming decade. The findings of this paper are applicable to other industries. The paper aims to highlight that by initially understanding the vulnerabilities of the IT components and by taking the right cybersecurity preventive measures, critical infrastructure can be protected against these kinds of threats. The research framework behind this paper was directed towards analysing the cyber risks associated with the convergence between the Information Technology solutions with the Operational Technology systems of critical infrastructure.

Keywords: Cybersecurity; industrial control systems; cyber challenges; malware; intrusion detection systems.

DOI: https://doi.org/10.24818/beman/2021.11.1-05

1. THE INTEGRATION OF OPERATIONAL TECHNOLOGY WITH IT – A STRUCTURAL CHANGE

The society and economy of the Fourth Industrial Revolution is one that is dependent and relies on computer systems and Information Technology solutions. Thus, as our reliance on IT systems increases so cyber-attacks become more potentially harmful. As more operations move into the digital world, cybersecurity becomes a priority for companies during this period of unprecedented change. Normally, the systems behind critical infrastructures have run in isolation from the outside networks. The digital revolution has transformed and upgraded the nature of Industrial Control Systems from an isolated type to a more open network (Ahmadian et al., 2020). This upgrade has facilitated new capabilities (remote access and control to the ICS infrastructures) but also brought new cyber vulnerabilities to the system. Recent high-profile cyber-attacks on nuclear facilities have raised concerns about cybersecurity vulnerabilities. In comparison with conventional cyber-attacks, which mainly bring reputational and economic losses, successful attacks on ICSs can lead to fatal and disastrous results like the explosion of nuclear reactors.

Thus, the successful attacks on ICS can lead to severe disruptions in industrial output and safety of the society and hence the imperious need to defence in depth these critical infrastructures. Cyber-attacks on major targets are not new. In 1997, a leading anti-virus company discovered two vulnerabilities for ICS (ICS, 2019). 20 years later, the same company detailed a number of almost 200 known vulnerabilities for the ICSs. As ICSs become more exposed to the world of the internet, the ICS operators must understand that the nature of the vulnerabilities and threats they are exposed to increases and enlarges too, and they have to diligently improve the defence mechanisms of the ICSs (Baykara & Das, 2018).

As the industrial infrastructures converge with the digital world and expand their capabilities to meet the ever-increasing stakeholders' pressures, their protection mechanisms need to be in tune with its new architecture. (Obodoeze et al., 2018). The challenge is that with the introduction of automated control and management, ICS security inherits the vulnerability challenges of remotely accessible systems.

Major data breaches and cyber-attacks on high-profile critical infrastructures like Stuxnet and the attack on the Ukraine power grid raised the awareness of the cybersecurity importance for these industrial environments. Stuxnet infiltrated the Iranian nuclear plant most probably through a USB and then spread it within the entire network (Langner, 2011). The malware broke down the entire ICS infrastructure. The attack caused substantial physical damages to the reactors' centrifuges that delayed the Iranian nuclear program for a couple of years and brought huge economic losses to Iran. Stuxnet was different from any other previous virus. It escaped the IT world and affected the OT operations controlled by newly deployed IT systems. A couple of years later, in 2015, another major cyber-attack compromised the ICS systems of the Ukrainian energy companies (Hasan et al., 2018). The attack resulted in the energy supply being temporarily cut off for 6 hours in Ukraine. This is considered to be the first successful cyber-attack on the energy grid and also the first-of-its-kind that disrupted the safety, security, and reliability of power supply from a national power grid. Both high-profile cyber-attacks raised the awareness of the importance of cybersecurity within critical infrastructures.

Cyber vulnerabilities are growing as the Operational Technology systems of the critical infrastructures become progressively more reliant and integrated with Information Technology systems. The spiral use of commercially developed software within the ICSs, due to economic constraints and resources, further escalates the cyber threats and vulnerabilities faced (Constantin, 2020).

The United Nations' initiatives on climate and sustainability may call for even more integration between energy systems to facilitate the use of more renewables and hydrogen. Setting up more digital connections between different networks requires securing these connections and to identify vulnerabilities and potential threats before attacks happen. These digital connections will require that the Operational Technology fully integrate and communicate with the Information Technology networks to deliver the efficiency and automation needed (Hasan et al., 2018).

Although Operational Technology networks were developed to be secured and isolated – using their own communication protocols, Information Technology systems are a lot more accessible to cyber threats. The process of integrating the OT with IT means not only the creation of more connectivity - it needs to address also the threats brought in by the IT system by adopting new security tools and procedures (Savin & Serban, 2019). The challenge is a new one – OT was designed to address an operational situation, it did not need sophisticated protection systems thus being an isolated type. IT brings a new dimension to these operational systems – an opportunity to make systems more efficient and new threats to its safe operations – in the form of cyberattacks.

The need for on-time communication channels to supervise and conduct remote-control between previously isolated systems, coupled with the emergence of automation systems, and, at the same time, the larger number of companies adopting this ICS remote control solutions – all these increases the possible attack vectors and diversify the channels for hackers to achieve their plans.

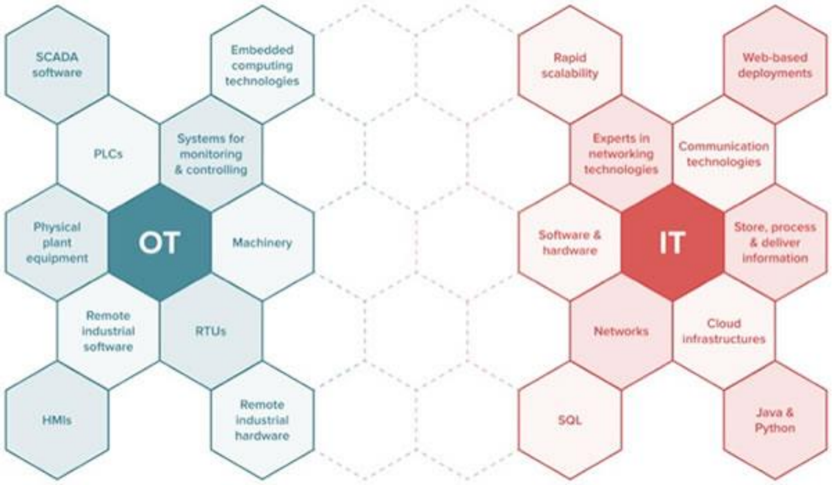
SCADA software
Embedded computing technologies
PLCs
Systems for monitoring & controlling
Physical plant equipment
OT
Machinery
Remote industrial software
RTUs
HMIs
Remote industrial hardware
Rapid scalability
Web-based deployments
Experts in networking technologies
Communication technologies
Software & hardware
IT
Store, process & deliver information
Networks
Cloud infrastructures
SQL
Java & Python

FIGURE 1. THREAT EMPHASIS IN IT VS OT INDUSTRIAL ENVIRONMENTS

Source: I-SCOOP. EU, 2021.

Figure 1 details the different approaches the IT and OT experts have upon securing their systems. The cybersecurity concerns of IT teams are oriented towards defence tools that keep the confidentiality, integrity, and availability of the information within their system. While OT security experts are concerned about protecting human lives and the safety and efficiency of the physical operations. These different priorities tend to lead to conflicting security policies between the IT and OT security teams. These contrasting procedures and actions lead to different approaches in securing the operations of the systems (Araghi & Shams, 2012).

2. ICS COMPONENTS TARGETED BY THE CYBER-ATTACKS

The framework conducted for the research of this paper analysed several cybersecurity studies on critical infrastructures aiming to understand the current as well as the developing cybersecurity threats and vulnerabilities used by attackers (Bompard et al., 2013), (Choo, 2011), (Hasan et al., 2018). The elements of the ICS targeted by cyber-attacks are the hardware, software, and network components. For each category, the most common vulnerabilities' exploitations have been described and remedies have been suggested to tackle them.

3. HARDWARE VULNERABILITIES AND DEFENCE MECHANISMS

The hardware components are the physical parts of the industrial network. Through exploitation of the hardware vulnerabilities, attackers can make use of known weaknesses to control the system (Brodsky & Radvanovsky, 2016). In comparison with software-level attacks where updates or detection tools for malware search to identify attacks, the majority of the hardware-based cyberattacks are susceptible to escape such detections. Taking advantage of these deficiencies, hardware-based attacks are on the rise (Potlapally, 2011).

Most common types of Hardware vulnerabilities:

Hardware Trojans

Trojans for hardware equipment are the most common hardware malware. A hardware Trojan maliciously modifies the logic behind the electronic circuits to alter the planned process of the system. They have a variety of troublesome effects. A hardware Trojan might change when triggered, an electronic circuit to provide remote unauthorised permission or to accept commands that otherwise should be rejected. Another type of Trojan might attach the chip's buffets and hence consume more power than normal. In a more serious scenario, Trojans might prevent operations of a resource. A Denial-of-Service Trojan could affect the target module to exhaust its scarce resources. It could also physically affect the device's settings, including ignoring commands from other peripherals or simply destroying the components (Nicholson et al., 2012).

Illegitimate Hardware Copies

Illegitimate copies of hardware are another main source of malicious exploitation since they can contain Trojans. The pressures of the current economic context to reduce costs have increased the trend for companies to purchase untrusted hardware from cheaper sources. The current economic model forces outsourcing and buying tampered-off equipment from untrusted factories in low-cost countries.

Hardware-Enabled Security Tools

Different mechanisms have been developed to defend against attacks on hardware equipment.

Tamper-resistant hardware: Hardware equipment that is tamper-resistant has become critical due to its position within the networks as an entry point to the network's security.

Trusted Computing Base: Another development has been the Trusted Computing Base (TCB), which is considered as the set of hardware components that are valuable to the security of the whole network. Rigorous checks are done to audit these devices to ensure the security of the TCB and thus of the entire network. These safety mechanisms are in place to divert the attackers from getting the critical design elements of the industrial systems.

4. SOFTWARE VULNERABILITIES AND DEFENCE MECHANISMS

Program errors create software vulnerabilities. A software fault is a common indication used to define a deficiency in a computer program. Cyberattacks usually use software imperfections such as design flows, missing data encryption, SQL injection, buffer overflows, issues with libraries, and other types of bugs to control the systems in unintended ways from the original design, thus obtaining unauthorised access to data, compromising it or causing Denial of Service (DoS). The majority of cyberattacks continue to use system bugs and design flows – making these the key vulnerabilities in information security. Programming errors can open the door for attackers even in front of Firewalls, Intrusion Detection Systems (IDS), or other defence protocols (Carcano et al., 2011). Thus, it is imperative to prevent, detect and react to software imperfections. In this section, the paper aims to address the main software vulnerabilities within the ICS infrastructures.

Most common types of Software vulnerabilities:

Buffer Overflow

Software exploitation happens when the software is abused. The majority of cyberattacks target software vulnerabilities by taking advantage of snags in memory, user validation, and access privileges (Howard, 2009). The attack on memory safety is executed by modifying the contents of memory. One of the common ways of achieving this is by buffer overflow. The attack on buffer overflow happens when a program stores more information in a buffer than it was built to hold. Since the buffer is programmed to keep a certain amount of data, the extra information can overflow and corrupt by overwriting valid data in other adjacent buffers.

Data Validation

The process of input validation refers to the process of data flowing in a certain way. Misleading data validation can drive data to corrupt SQL databases. SQL injection is one of the most common attacks in a website's database. An attacker inserts SQL commands to alter the database (Bompard et al., 2013). The attacker exploits a defect knowing that the output is reliant on the successful application of other successive events.

Software-Enabled Security Tools

The primary objective for all the software defence programs is to develop solutions and to create a safe software environment. Engineers look and discover the common errors that lead to software threats and vulnerabilities and try to establish a better-secured software code.

IDS and anti-malware

IDS and antivirus software are the most common tools for detecting software attacks (Coates et al., 2010). IDS detect exploits or interactive attackers while antivirus scanners detect malware based on known malware signatures. Antivirus scanners are the most popular defence mechanisms.

Type-safe programming languages

Secure design and development is a technique that verifies that the program is defect-free. Testing software errors is a tool developed to uncover flaws in programming languages. The testing software module was designed to check and ensure that the application performs as expected, meets the security requirements, and does not contain errors or bugs. The testing process consists of trying to identify defects, which are considered variances between the actual and the expected results. A type-safe language program also prevents memory management errors. Reducing programming errors aims to limit the privileges a program has while running. The mechanism follows the principle of least privilege - an old design principle. The main idea is to offer the program only the rights needed to operate. By limiting these privileges, the possible damages are restricted in case of an attack (Davis et al., 2006).

Sandboxing

Another emerging cyber defence tool is sandboxing, which executes and verifies the code in a restricted virtual environment, limiting the initial access to the operating system, before granting the access of the code to be executed on the physical system.

5. NETWORK AND PROTOCOL VULNERABILITIES AND DEFENCE TOOLS

When the network protocols were developed, they were designed to support entirely different environments, which were much smaller in scale. Given the complexity and large dimensions of today's industrial networks, they do not properly work and support all the traffic generated within these environments. The weaknesses of the protocols become more evident when the operators and users have narrow knowledge of the architecture of the networks. Examples of this limited knowledge include insufficient encryption schemes, patches not applied in time, and lack of properly configured security filters and policies.

Most common types of Network and Protocols vulnerabilities

Cyber-attacks commonly happen by manipulating the limitations of the following network protocols: Internet Protocol (IP), Transmission Control Protocol (TCP), and Domain Name System (DNS).

IP and IPSec

The Internet Protocol is the main protocol on which the traffic within the network happens. It offers the main data needed for packets to route between computers and routers. However, the IP was not built to check the authenticity and privacy of the data transmitted. This embedded lack of security permitted the packets to be hijacked or changed while they were routing over unknown networks. To solve this gap, another protocol was developed, IPSec, which provides secured and encrypted IP traffic. This protocol has been used for the establishment of the VPN, which forms a secure route between a computer from outside and a trusted network.

TCP

The TCP protocol transmits packets in a reliable way and directs the order in which the packets are transmitted, being a core protocol. As with the IP, the development of the TCP was not included security mechanism, so the lines are susceptible to malware injections or for the connections to be broken or hijacked.

DNS

The DNS protocol uses human-readable host names and translates them into IP addresses. The DNS replies are not authenticated – hence a hacker can send DNS messages to imitate an Internet server. The DNS servers have been one of the common targets of the Denial-of-Service attacks creating important interruptions on the internet.

Network and Protocol Security Solutions:

Cryptography

Cryptography is the most common system to protect information. It aims to offer confidentiality, message integrity, and authentication in an unsecured network. It is a principal tool to safeguard the information sent between users by encoding data so only users with the right keys can decrypt the information.

Skilled attackers use refined techniques to camouflage traffic loads to look more like genuine traffic. Furthermore, big data flowing on networks requires new analysis algorithms to analyse the uncertainty of information attached. This has led to the creation of a new domain of research, where network security experts collaborate with the design community to elaborate better ways for visualizing the traffic to understand the breaches. The resulting data is then analysed by network experts.

Firewalls and IDS

Typical network defence tools include Firewalls and Intrusion Detection Systems (IDS). The Firewall is the most common tool to protect the systems within the internal network from external attacks. The way it works is by analysing the data packets and determining whether they should be allowed, based on the rules set by the network administrator.

Firewalls can be placed in many layers in the network infrastructure. Network layer firewalls filter traffic at the edge of the network and block packets unless they match certain rules defined by the network administrator.

The proxy server is similar to a Firewall by responding to the input packets and blocking depending on the policies set by the administrator. Both layering tools, firewall, and proxies make it more difficult to manipulate the internal system.

The emergence of new technology increased the capability of the attackers to create more advanced cyber malware. The intrusion detection systems (IDS) analyse any suspicious activity over the network.

These detection systems are extremely valuable in that they detect attacks in the early stages and then can protect further the system from subsequent attacks. In addition, these systems help detect any sign of suspicious activity generated by a user, application, or malware. The system analyses the normal traffic by examining the pattern and reporting abnormal traffic. Such detections are either anomaly-based or signature-based. In the signature-based analysis, the system detects the malicious packets based on their signatures as they route. However, signature-based IDS have been considered ineffective as the sophistication of malware has developed – and hence, advanced anomaly-based IDSs have been designed.

In an anomaly-based signature analysis, the system has no expertise of how the malicious packets look but analysis the changes in the behavior of the system, thus alerting immediately when detecting suspicious software behavior. These systems learn with the help of Artificial Intelligence and Machine Learning technology what is supposed to be normal and legit traffic for an extended period. Still, more holistic approaches to better protect networks are needed, instead of focusing only on configuring specific assets such as Firewalls or IDS. Best practices identified by network-forensic studies include understanding the traffic attack patterns and locating the hackers (Ayodeji et al., 2020).

6. EMERGING CYBERSECURITY TECHNOLOGIES

Artificial Intelligence and Machine Learning

Artificial Intelligence and Machine Learning have both recently seen huge development. It is generally agreed that contemporary effective cybersecurity positions and policies cannot be implemented without depending steadily on AI and ML.   These emerging technologies as with the IT systems brought into the OT networks, apart from the benefits in terms of automating jobs, faster data analysis, and decisions, also bring cyber threats (Raban & Hauptman, 2018). Security experts will be able to use the AI capabilities to address the ICS components' vulnerabilities and to detect threats before being exploited by attackers.

Furthermore, AI capabilities can further secure industrial networks against advanced malware attacks. At the same time, hackers can exploit the IT vulnerabilities with the help of the AI tools deployed to detect breakthroughs in the industrial networks.

7. CONCLUSION

The digitalization of the world economy, coupled with the growing penetration of smart machines and industrial systems, has led to operating systems being increasingly exposed to cyberattacks. Of all types of businesses, critical infrastructures face some of the most critical challenges – a successful cyber-attack has the power to bring not only multiple businesses down but entire regions. As industrial control systems (ICSs) expand their roles and outreach to respond to fresh demands from stakeholders, protection tools need to adapt, in their compatibility, to this new type of operational architecture. Yet challenges exist and are varied, ranging from legacy equipment safety regulations - that may prohibit any modifications being made to equipment - to compliance regulations that require sensitive data to be made available to third parties. Still, for critical infrastructure companies, even such significant challenges are overshadowed by the complex risks that malicious attacks pose.

As cybersecurity vulnerabilities and threats expand for critical infrastructures, the industry's resilience to defending against such threats also needs to further develop. Different techniques and tools exist to remedy vulnerabilities in software, hardware, and networks; however, the consensus is that the best technique is the one that protects everything from inside out. The overwhelming majority of companies protect their perimeters to guard their networks from any outside possible attack.

This research paper has focused on the cyber vulnerabilities that have the power to impact the safety operations of the ICSs. It listed and described the main software, hardware, network, and protocol vulnerabilities, as well as existing solutions to address these.

The results provide administrators in charge of the ICS cybersecurity an insight into the key elements that need protection and the means to achieve such protection for the successful deployment of a security strategy.

However, whilst the paper discusses threats and existing solutions, a significant challenge is that cyber threats are constantly evolving, so ICS administrators must also take continuous measures to secure their assets. Further research is needed to identify threats before they emerge and hence keep a step ahead of possible attackers to best protect and fully integrate OT and IT systems within more digitalized and ultimately more customer-responsive infrastructures. And finally, emerging technologies, as they face their own new, unique cyber threats, will need fresh defensive mechanisms – for which research and investments will be needed.

7.1 Future direction

The potential course of cybersecurity lessons from research results is that organisations must evaluate and focus on how they function and secure their assets and records. The fundamental concern is that the highest priority for many organisations is to gather and not safeguard records. The lack of end-to-end security and the neglected encryption of stored data in many situations is only one aspect exacerbating the issue and its effect on consumers.

The research directs the integration of IT-OT this means that OT managers should do their utmost to understand the IT climate. The research advises that organisations align the IT and the enterprise with the evolving OT system requirements, practices, resources, procedures, and employees. In addition to IT/OT integration, coordination is the way to tackle organisational shifts. Alignment of IT/OT starts with the awareness of what each entity is doing and how they vary. When looking to progress into the industrial revolution as the market leaders, an advanced cybersecurity approach that involves the full safety lifecycle, starting from the factory floor to the business is crucial.

Cybercriminals are continuously looking for fresh vulnerabilities and advanced techniques to cheat and destroy institutions and organizations in this era of digital change and globalization. Despite this, organizations should be conscious not just of the ever-increasing uncertainty, but also of risks to cybersecurity.

Acknowledgments

I would like to express my gratitude to Professor Nadia Ciocoiu from Bucharest University of Economic Studies for the valuable support and guidance provided.

REFERENCES

Ahmadian, M. M., Shajari, M., & Shafiee, M. A. (2020). Industrial control system security taxonomic framework with application to a comprehensive incidents survey. *International Journal of Critical Infrastructure Protection*, 29, 100356. https://doi.org/10.1016/j.ijcip.2020.100356

Araghi, S., & Akbar Shams-Baboli, A. (2012). Improving Security in SCADA Systems. EEE, 2(3): 158–163. https://doi.org/10.5923/j.eee.20120203.09

Ayodeji, A., Liu, Y., Chao, N., & Yang, L. (2020). A new perspective towards the development of robust data-driven intrusion detection for industrial control systems. *Nuclear Engineering and Technology*. https://doi.org/10.1016/j.net.2020.05.012

Baykara, M., & Das, R. (2018). A novel honeypot based security approach for real-time intrusion detection and prevention systems. *Journal of Information Security and Applications*, 41: 103–116. https://doi.org/10.1016/j.jisa.2018.06.004

Bompard, E., Huang, T., Wu, Y., & Cremenescu, M. (2013). Classification and trend analysis of threats origins to the security of power systems. *International Journal of Electrical Power & Energy Systems*,50: 50–64. https://doi.org/10.1016/j.ijepes.2013.02.008

Brodsky, J., & Radvanovsky, R. (2016). The future of SCADA and control systems security. 371–374. https://doi.org/10.1201/b19545-29

Carcano, A., Coletta, A., Guglielmi, M., Masera, M., Nai Fovino, I., & Trombetta, A. (2011). A Multidimensional Critical State Analysis for Detecting Intrusions in SCADA Systems. IEEE Trans. *Ind. Inf.*, 7(2): 179-186. https://doi.org/10.1109/tii.2010.2099234

Coates, G. M., Hopkinson, K. M., Graham, S. R., & Kurkowski, S. H. (2010). A Trust System Architecture for SCADA Network Security. IEEE Trans. *Power Delivery*, 25(1): 158–169. https://doi.org/10.1109/tpwrd.2009.2034830

Constantin, L. (2020). 32 Hardware And Firmware Vulnerabilities: A Guide To The Threats. CSO Online. https://www.csoonline.com/article/3410046/31-hardware-and-firmware-vulnerabilities-a-guide-to-the-threats.html

Choo, K.-K. R. (2011). The Cyber Threat Landscape: Challenges and Future Research Directions. SSRN Journal. https://doi.org/10.2139/ssrn.2339821

Davis, C. M., Tate, J. E., Okhravi, H., Grier, C., Overbye, T. J., & Nicol, D. (2006). SCADA Cyber Security Testbed Development. https://doi.org/10.1109/naps.2006.359615

Hasan, S., Ghafouri, A., Dubey, A., Karsai, G., & Koutsoukos, X. (2018). Vulnerability analysis of power systems based on cyber-attack and defense models. https://doi.org/10.1109/isgt.2018.8403337

Savin, V. D., & Serban, C. (2019). Cybersecurity Vulnerabilities And Threats Of Scada Systems In Critical Infrastructures. In *Proceedings of the INTERNATIONAL MANAGEMENT CONFERENCE* (Vol. 13, No. 1, pp. 234-237). Faculty of Management, Academy of Economic Studies, Bucharest, Romania.

Howard, M. (2009). *24 Deadly Sins of Software Security*. McGraw Hill Professional.

i-SCOOP. 2021. *IT and OT convergence - two worlds converging in Industrial IoT*. [online] Available at: <https://www.i-scoop.eu/internet-of-things-guide/industrial-internet-things-it-ot/> [Accessed 23 February 2021].

ICS, K., 2019. Threat Landscape For Industrial Automation Systems, H1 2019 | Kaspersky ICS CERT [WWW Document]. Kaspersky. URL https://ics-cert.kaspersky.com/reports/2019/09/30/threat-landscape-for-industrial-automation-systems-h1-2019/ (accessed 7.31.20).

Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. IEEE Secur. *Privacy Mag.*, 9(3): 49–51. https://doi.org/10.1109/msp.2011.67

Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of Cyber-Warfare. Computers & Security, 31(4): 418–436. https://doi.org/10.1016/j.cose.2012.02.009

Obodoeze, F. C., Obiokafor, I. N., & Asogwa, T. C. (2018). SCADA for National Critical Infrastructures: *Review of the Security Threats, Vulnerabilities and Countermeasures*. IJTSRD, 2(2): 974–982. https://doi.org/10.31142/ijtsrd9556

Potlapally, N. (2011). Hardware security in practice: Challenges and opportunities. https://doi.org/10.1109/hst.2011.5955003

Raban, Y., & Hauptman, A. (2018). Foresight of cyber security threat drivers and affecting technologies. FS, 20(4): 353–363. https://doi.org/10.1108/fs-02-2018-0020