Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 7, July 2021 : 7579 - 7588

Research Article

Digital transformation, cybersecurity challenges and countermeasures.

Nabil Cherkaoui [1], Youssef El Hassani [1], Rachid Chakib[2], Ghazaly Salifou Labo[3], Tiefolo Camara[3]

[1]ENCG Fez, LAREMEF Laboratory, Sidi Mohamed Ben Abdellah University, Morocco
[2]LIMIE Laboratory, ISGA Rabat, Morocco
[3]LIMIE Laboratory, ISGA Casablanca, Morocco

Abstract

Digital transformation is currently one of the major global concerns. Indeed, this trend will allow companies to benefit from considerable productivity thanks to the dematerialization of resources to the cloud and the adoption of new technologies such as AI, Big Data, IoT. In this context, attacks linked to digitization are multiplying and becoming more and more sophisticated. One of the critical sectors requiring urgent digital transformation is industry, without this transformation, companies lose their competitiveness. Considering this need, cyber-attacks aimed at industrial networks have become increasingly developed. The IEC 62433 standard provides a global framework to support digital transformation by guaranteeing increased security. This paper consists of describing this standard, enumerating the cyberattacks threatening digital transformation and thus proposing solutions for increased security.

Keywords: Digitalization, digital transformation, cybersecurity, cyberattacks, IEC 62433.

I- Introduction

Digitization is today an essential lever for the modernization of the administration as well as for the improvement of production [1]. This digital transformation is based on emerging technologies such as artificial intelligence (AI), Big data, cloud computing and the Internet of Things [2]. In the face of globalization, information is now processed automatically, computers nowadays are used practically in all industries. Whether in the medical field, bioinformatics, automation, home automation, robotics, telecommunications, image processing, management or even in the industrial environment.

Today, thanks to the evolution of information technologies, the world is experiencing an exponential evolution in the fields of information collection, processing and storage. Information systems in several areas have been the scene of a number of malicious acts, cyber-attacks, information theft, alteration and even espionage. In Florida, a cyberattack on drinking water resulted in the chemical composition of the city's waters being manipulated. The cybercriminal increased the rate of caustic soda, immediately brought back to level by employees and most recently, in May 2021, a pipeline attack in which the company paid a

ransom of $ 4.4 million in order not to interrupt its operations. The consequences are still disastrous for companies.

It is in this context that cybersecurity is about protecting computers, servers, mobile devices, electronic systems, networks and data against malicious attacks. Cybersecurity field include several categories: Network security, Application security, Information security, End-user training, Operational security and risk management.

At the industrial level, there are Cyber-physical systems (CPS) [3] which constitute the structure which links (Industrial Internet of things) the IIoT [4] and play an increasingly important role in industrial processes and in the control of production (smart factory). They consist of objects connected to each other or through the Internet to form a simple network system. Sensors allow systems to acquire and process data. This data is then made available to the various services connected to the network which use these actuators to directly impact the measurements taken in the real world. This leads to the merging of the physical world and virtual space in the Internet of Things.

Thus, the industrial information system is a complex system, that is to say a set made up of a large number of interacting entities whose integration makes it possible to complete a common mission. Ensuring security will first come down to an audit for a more detailed knowledge of the information system and also to define a common language, to clarify and harmonize practices, hence the importance of developing standards which by definition is a set of characteristics, rules, metrics and / or conventions applicable to activities.
Software-defined network (SDN) is a paradigm that allow an easy management of equipment and the centralization of control [5][6][7]
Standards prevent the multiplication of interpretations and ensure the interoperability of networks and systems. The rest of the paper is organized as follows, in section 2 we will present the related works. In section 3 we will provide an overview on the IEC 62433 standard. In section 4 we will present cybersecurity in the industrial environment. In section 5 we will present the attacks in the industrial environment. In section 6 we will present countermeasures and we will conclude in section 7.

II- Related works

The digital transformation has aroused interest, whether it is from actors in the industrial world or in the field of scientific research. Indeed, several works have been published proposing models of digital transformation in various structures, for example universities, companies, factories, administrations. GregoryVial [8] conducted a review explaining the concepts of digital transformation, through this research the author highlighted all the challenges that can slow down this transformation. Gordon Fletcher and Marie Griffiths [9] have shown the inability of VUCA in supporting companies towards digital transformation, especially in the era of the COVID-19 pandemic. The authors went on to show that digitization allows companies to be more flexible, competitive and resilient to change. Subodh Mendhurwar & Rajhans Mishra [10] studied the architecture of the digital transformation of a company where IoT and social technologies are essential. The authors discussed a set of vulnerabilities and limitations that this architecture can have threatening business activities. Imanol Mugarza et al. [11] carried out a study concerning the IEC 62433 standard, as the latter reinforces the security of the architectures as well as the processes of its implementation. Three different stakeholders are defined in this study, the asset owner, the service provider and the product provider. the authors have shown the importance of coordination between these three elements for increased security.

III- Overview IEC 62433

By publishing in 2007 the first specific benchmarks for industrial cybersecurity, ISA Committee 99 well anticipated the need, which is now recognized, to ensure solid protection of critical infrastructures. The recent attacks (Stuxnet, Duqu, Shamoon, Gauss, Flame ...) attest to this. The work of ISA99 is now carried out in harmony with that of the IEC and there is now more talk of IEC62443 than of ISA - 99.

The two sets of standards are merged thus going beyond what was possible for ISA - 84, IEC 61508 and its derived standards. Cybersecurity and functional safety are now the two major security concerns aimed at achieving a safe situation in E / E / PE (Electrical, Electronic, Programmable Electronic) systems. Cybersecurity is a complex subject and the ISA / IEC repository has several components, like the ISO2700x standards or the US NIST800 - xx standards (which are not prescriptive).

The IEC 62443 standard is a set of recommendations, it is not binding on manufacturers or their critical infrastructures. This flexibility allows the standard to adapt to the contexts and specificities of critical installations. "The IEC 62443 standard is a real benchmark for cybersecurity in industrial facilities, since it serves as a common basis. It can be used partially, as needed, or be supplemented by another business standard.
The IEC 62443 standard carries with it a project to harmonize best cyber practices in this fragmented market which is used to operating in a closed system. This standard makes it possible to evolve towards more interoperability and this, with an international scope ".
Until then there was on the one hand the security of information systems (ISO 27000), and on the other hand industrial security (operational safety and functional safety with IEC 61508 and industry standards). The IEC 62443 standard now serves as a link between these two environments which, in fact, are increasingly converging. It constitutes a virtuous circle in the service of cybersecurity risk management for industrial facilities as a whole. But this crossroads between OT and IT is still proving complex. "The IT universe is very focused on confidentiality and integrity: if an attack is suspected, we will immediately have this tendency to disconnect the system. On the other hand, a factory needs to produce without interruption and has to face both human and environmental risks, "says Fabien Miquet, Product and Solution Security Officer at Siemens.

The IEC 62443 standard is made up of several documents - for informed audiences - grouped into four parts.
● "General 62443-1": this first section groups together documents intended for general concepts, terminology and methods. In particular, it defines a glossary;
● "Policies & procedures 62443-2": this second section specifies organizational measures, and is aimed at operators and maintainers of automation solutions. It also contains recommendations in the context of corrections and updates of system components, respecting the specificities of critical industrial infrastructures (IEC-62443-2-3);
● "System 62443-3": this third section is dedicated to the operational safety means of ICS (Industrial Control Systems), or rather IACS (Industrial Automation and Control Systems) - not to be confused with SCADA, since the standard defines its own definition of instrumentation and control infrastructures. It provides a current assessment of the various cybersecurity tools, describes the method and means for structuring their architecture into zones and conduits and provides an overview of techniques for protecting against cyber attacks. It thus proposes the segmentation of IACS by zones according to the criticality levels of the equipment (62443-3-2), while recalling that these zones will then be able to communicate with each

other - whether by USB key, network cable or even VPN link. . Certainly the most interesting part since it presents the elements of an in-depth cyber defense;

● "Component 62443-4": finally, this fourth section is intended for equipment manufacturers of instrumentation and control solutions: PLCs, supervision elements, engineering stations and other switching equipment. This part describes on the one hand the safety requirements for this equipment and presents the best practices for product development.

IV- Cyber security in the industrial environment

Cyber-security of industrial facilities, cyber-physical systems and more generally IIoT systems is a very topical issue. To understand the threat context affecting industrial control systems (ICS), it is helpful to understand the difference between information technology (IT) and operational technology (OT).

IT covers systems and technologies, including software, communications systems, hardware and services, to process and manage data, thus constituting an information system. As for operational technology (OT), it covers all the systems and processes used to detect or bring about a change in the event of anomalies in devices, processes and physical events in a factory.

So we can conclude that IT is for data processing and OT for physical process management and control.

An ICS encompasses different types of control systems, including supervision and data acquisition systems (SCADA), distributed control systems (DCS) or programmable logic controllers (PLC). It is designed to monitor and control the operation of machines, tools and associated devices.

Cybercrime has grown exponentially in recent years, with many computer information processing (IT) systems under attack which can spread rapidly and can have detrimental impacts on industry. The evolution of industrial facilities (OT), which today are interconnected through a network, makes them a prime target for cybercriminals. Objects connected to each other and accessible from the Internet further increase this usable attack surface. OT systems are vulnerable to all forms of threats, but the most common are ransomware attacks.

The latest IBM Security annual report notes an intensification of cyber attacks in 2021. Manufacturers linked to the fight against covid have experienced a doubling of cyber attacks.

In the next section we will see some attacks, their consequences, the attack vectors and the security proposal deployed.

V- Attacks in the industrial environment

a) IT insider

A technician steals passwords from other technicians, logs in to equipment controlling the physical process using the stolen passwords, and issues shutdown instructions for parts of the physical process, automatically triggering a partial shutdown From the factory. A disgruntled IT insider views remote access credentials entered by an ICS support technician visiting a remote office. The disgruntled initiate then uses the credentials to log on to the same remote ICS engineering workstation that the technician logged on to. The initiate displays screens more or less at random and presses the buttons that seem likely to cause the most damage or confusion. These actions trigger a partial shutdown of the factory.

Sophistication: unsophisticated

Result. More serious physical consequences may be possible, depending on the initiate and the details of the industrial process. It would be best to technically revise the factory settings.

b) Ransomware

Common ransomware: Accidental downloading of malware that will exploit known vulnerabilities and not patched encrypts the workstation and spreads
The ransomware targets: Attacker with good computer knowledge with phishing and malicious attachments takes the network using a RAT, sows ransomware, demands ransom and if the payment system fails to activate it. here, the RAT infects the factory and undergoes an emergency shutdown damaging the equipment

Zero-Day Ransomware: Zero-day vulnerabilities in operating systems, applications and firewall sandboxes, created by autonomous ransomware attack groups that spread and exploit the vulnerabilities.

Sophistication: the first not so much while the second uses toolkits and malware developers
Consequence: production stoppage until the system is restored depending on the time required or replacement of important equipment.

Ransomware example: DoppelPaymer, Egregor, Netwalker, RagnarLocker, Ryuk, Sodinokibi, WastedLocker

c) Ukrainian attack

Ukrainian attack: large hacktivist class attack groups steal passwords by phishing, creation of new account with escalation of privilege, knowledge of IHL ICS operation, erasure of hard disks, equipment firmware or even system equipment control and unscheduled shutdowns

Sophisticated Ukrainian attack: a more sophisticated group will use the techniques of the Ukrainian attack and is more sophisticated with regard to cyberattack tools and technical details of power systems, to the above attack scenario is added th two-factor authentication, access the protection relay and reconfigure them. High voltage transformers have been destroyed due to the redirection of the energy flow

Sophistication: This is a summary of the attack techniques used in the 2016 attack on a number of electricity distribution companies in Ukraine. The attackers had good knowledge of cyber systems, but limited knowledge of power distribution processes and control systems.

Consequence: In the case of the attacks on Ukraine, electricity was cut to more than 200,000 people, for up to 8 hours. More generally, unplanned shutdowns are a consequence of this class of attack, and possibly unchecked emergency shutdowns with the potential for property damage that accompanies such shutdowns. The consequences of this attack are more serious ranging to damage to equipment

d) **CELL-phone WIFI**

Attackers use social media, social engineering and phishing attacks to impersonate target organization insiders and extract passwords from WIFI networks. Many of these password-protected networks are part of industrial control systems for critical infrastructure. Attackers connect to these networks using compromised cell phones and scan remote networks until they find computer components vulnerable to

simple denial of service attacks, such as wiping hard drives or SYN flooding. Attackers jeopardize plant operations by triggering an unscheduled shutdown, disconnect from WIFI networks, and start again a few days later. Variation: Install malware on the laptops of office workers who work within range of ICS WIFI networks.
Sophistication: This attack currently requires a degree of cyber sophistication, as the toolkits for this type of hidden WIFI hacking from cellphones currently do not exist on the open Internet and therefore attackers have to write this malware themselves .
Consequences: Repeated factory shutdowns from a source difficult to identify. Staff should eventually determine that the source of the attack is a WIFI network and shut down all WIFI in the factory, or at least change all passwords.

e) Hijacked Two-Factor

Sophisticated attackers seek to compromise operations at an industrial site protected by best security practices. So, they write custom RAT malware to evade antivirus systems and target support technicians at the industrial site using social media searches and targeted phishing emails. Technicians activate malware attachments and allow administrative privileges for the malware because they believe the malware is a video codec or other seemingly legitimate technology. Rather than activating the RAT at the industrial site, where the site's sophisticated intrusion detection systems could detect its operation, attackers wait for the victim technician to be on their home network but must remotely connect to the industrial site. The technician activates their VPN and logs in using two-factor authentication. At this point, the malware activates, moving the Remote Desktop window to an invisible extension on the laptop screen and showing the technician a helpful error message like "Remote Desktop has stopped working." to respond. Click here to try to correct the problem. The malware provides attackers with remote control of the Remote Desktop invisible window. The technician starts another Remote Desktop session on the industrial site, without worrying about the interruption. This way, sophisticated attackers have access to industrial operations as long as the technician's laptop and VPN are on. The only clue of the problem that the ICS IDS sees is that the technician has logged in twice. Attackers end up learning enough about the system to malfunction the physical process enough to severely damage equipment or cause environmental disaster through the release of toxic products.

Sophistication: Currently, this requires a high level of cyber sophistication, as neither of these two factors - the vanquished remote access toolkit is available for free download over the open Internet. To cause a serious physical consequence, in a limited number of remote access sessions, probably also requires a high degree of technical sophistication.

Impact: Any attacker willing to invest sophisticated, custom malware in this type of attack is very likely to persist in the attack until significant adverse results are obtained.

f) IIoT Pivot

Hacktivists annoyed by an industrial site's environmental practices learn from the popular press that the site is starting to use new IoT devices from a particular vendor. Attackers scan the media for other users of the same components, on smaller and possibly less well-defended sites. The hacktivists target these sites with phishing emails and take control over the computer networks and ICS of the less well-defended sites using

the IIoT. Hacktivists gain access to the vendor's IIoT equipment at the sites and find that the operating system for these devices is an older version of Linux, with many known vulnerabilities. The attackers seize one of the IIoT devices. After examining the software installed on the device, they conclude that the device communicates over the internet with a database in the cloud from a well-known database provider. The attackers proceed by downloading Metasploit on the IIoT device and attacking the connection to the cloud database with the most recently released exploit for that database provider. They find out that the cloud provider has not yet applied a security update for this vulnerability and they take over the database servers in the cloud provider. In their study of the relational database and the software on compromised peripheral devices, hacktivists learn that the database has the means to order devices to execute arbitrary commands. This is a "helper feature" that allows the central cloud site to update the software, reconfigure the device, and manage the complexity of the rapidly evolving code base of that edge device. Hacktivists use this feature to send standard attack commands and tools and other software to devices on those ICS networks that hacktivists see as irresponsible targets for the environment. Inside these networks, attackers use these remote control tools and facilities to look around for a period of time and eventually wipe out hard drives or cause other damage they can, triggering shutdowns. unforeseen. In short, hacktivists attacked a heavily defended cloud service client. , from a badly defended customer to a badly defended cloud.

Sophistication: These attackers are of moderate cyber sophistication. They can download and use public attack tools that can exploit known vulnerabilities, they can launch social engineering and phishing attacks, and they can exploit permissions with stolen credentials. Hacktivists generally have a very limited degree of technical sophistication.
Consequences: unplanned shutdowns, loss of production and possible damage to equipment.

g) Stuxnet

Sophisticated attackers target a specific and strongly defended industrial site. They first compromise a somewhat less well-defended service provider, exfiltrate details of how the heavily protected site is designed and protected. Adversaries develop custom, stand-alone malware to target this site and physically damage site equipment. The stand-alone malware exploits zero-day vulnerabilities. Service providers transport malware to the site on removable media. Antivirus scanners are blind to custom malware that exploits day zero. Consequences: The Natanz uranium enrichment site targeted by Stuxnet would have suffered several months of reduced or no production of enriched uranium, due to the interference of the Stuxnet worm in the production process. The site is also estimated to have suffered premature aging and destruction of 1,000 to 2,000 uranium gas centrifuge units. More generally, this class of attack can bypass all physical safety and protection equipment, and can result in loss of life, public safety hazards, and costly property damage. Components of the process and control system, and bypass the equipment protection and safety systems with an attack. The attack also requires a high degree of cyber sophistication, to encode this new attack into custom malware that is undetectable by specific cybersecurity technologies deployed at the target site.

VI- Countermeasure

The ICS network engineering team proposes to implement a number of practices discussed in the recently released government best practice documentation: one-way security gateways, one-way CloudConnect, strict removable media controls, and security testing on the ICS test bench:

• Cascade Security Solutions' one-way security gateways are combinations of hardware and software. The hardware is physically capable of transmitting information in only one direction. The software replicates servers and emulates devices, typically ICS networks to external networks, such as corporate networks and the Internet. External users and applications interact with the replicas as if they were the original servers. Because the gateway hardware is physically capable of transmitting information in only one direction, a gateway deployment allows clients on the destination side of the gateway to monitor the ICS servers through the replicas of the gateway, without any physical ability to control, compromise or in any way influence sensitive information.

• CloudConnect One-Way Waterfall systems use one-way gateway technology to connect ICS networks directly to computer-based cloud services and the Internet. CloudConnect systems collect data from industrial networks, including from industrial Internet of Things (IIoT) edge devices, translate the data into cloud-compatible formats, and push the data to cloud service providers via encrypted, reliable and Internet-compatible transport. For example, CloudConnect systems often send raw data packets and other security monitoring data to central IDS and cloud-based security monitoring centers.
• Strict removable media controls mean that the ability of ICS equipment to mount, read, and write to removable media such as USB drives and DVDs is disabled. Any attempt to use these media on an ICS asset results in security alerts and a reminder from the security team that the offending user has just violated site security rules. An ICS file server is replicated by one-way gateways to the computer network, so removable media are not needed for routine ad hoc file transfer tasks from the ICS network to the computer network. All files that need to enter the ICS network are written to removable media, scanned by eight different anti-virus engines on a stand-alone cleaning workstation, and copied to new known working media. This media is then transferred to a second ICS workstation which makes the new files available on the ICS file server.

Reliably defeating an attack means preventing the physical consequences of the attack essentially every time this class of attack is launched. For example :

• Antivirus (AV) systems do not fight common malware reliably because attacks are launched before antivirus signatures are available for attacks. If common malware reaches a vulnerable system between the time the malware is launched and the time AV signatures are applied, the system is compromised, even if an AV system is deployed.

• Security updates do not reliably neutralize exploits of known vulnerabilities because it takes time for a vendor to create and end users to install the updates. The systems are vulnerable in this time frame. Additionally, sometimes security updates are wrong and, when wrong, fail to effectively address the known vulnerability that drives them.

• Intrusion Detection Systems (IDS) and security monitoring systems are measures of detection, not prevention. Since no set of preventative measures is ever perfect, cybersecurity best practice documents generally all recommend detection and monitoring systems - to understand what activity is normal on a network, to detect how as reliable as possible abnormal activity and to trigger response actions suspicious activity is detected. IDS and surveillance systems, as important as they are, fail to reliably defeat attacks. Indeed, intrusion detection and incident response take time. Meanwhile, compromised equipment is

exploited either manually by a remote attacker or automatically by stand-alone malware, which may be enough to cause the consequences we seek to avoid. In contrast, here are examples of security measures that reliably neutralize a specific class of attack:

• Password theft phishing attack - Two-factor authentication based on RSA-style password dongles reliably defeats remote password phishing attempts. One could postulate an attack that physically steals the password dongle, but it would no longer be a "phishing" attack. A remote attacker only capable of spoofing emails and producing similar websites is not able to defeat this type of two-factor protection system.

• Encryption key scraping software - Trusted Platform Modules (TPMs) reliably thwart attempts to search compromised equipment's memory and persistent storage to steal encryption keys. The TPM hardware is designed so that the encryption keys never leave the hardware modules or appear in the memory of the computer running the TPM. More sophisticated attacks, such as physically dismantling hardware modules from stolen computers, could successfully recover these encryption keys. However, such attacks are no longer the indicated attack, that is, software that searches for keys in the memory and hard disk of a machine.

• Internet-controlled malware - One-way security gateways reliably neutralize Internet-controlled malware. Gateways are physically capable of sending information in only one direction - from an ICS network to a computer / corporate / Internet network, with no ability to resend information. In one-way protected networks, no control signal is physically capable of being sent from the Internet to malware on a compromised ICS network. “Defeat reliably” is a high standard. Achieving this standard is usually only possible by describing a particular attack, or the attacker's abilities, very precisely.

VII- Conclusion

An industry must be operational during production, a component malfunction or an unexpected event that could interfere with the smooth running of the company's activities is a major factor to take into account. Added to that are the external threats, the cyber attacks that the factory is expected to face. To help these companies prevent and defend themselves against these eventualities, the international standard IEC 62443 was born and offers these companies a series of recommendations and guidelines to follow for the integrity and the smooth running of the company's activities.

References

[1] Kerroum, K., Khiat, A., Bahnasse, A., & Aoula, E. S. (2020). The proposal of an agile model for the digital transformation of the University Hassan II of Casablanca 4.0. Procedia computer science, 175, 403-410.

[2] Issaoui, Y., Khiat, A., Bahnasse, A., & Ouajji, H. (2019). Smart logistics: Study of the application of blockchain technology. Procedia Computer Science, 160, 266-271.

[3]Mendhurwar, S., & Mishra, R. (2021). Integration of social and IoT technologies: architectural framework for digital transformation and cyber security challenges. Enterprise Information Systems, 15(4), 565-584.

[4] Rafik, M., Bahnasse, A., Khiat, A., Bouattane, O., & Ouajji, H. (2019). Towards a smart energy sharing in micro smart grid adopting SDN approach. Procedia Computer Science, 151, 717-724.

[5] Bahnasse, A., Louhab, F. E., Oulahyane, H. A., Talea, M., & Bakali, A. (2018). Novel SDN architecture for smart MPLS traffic engineering-DiffServ aware management. Future Generation Computer Systems, 87, 115-126.

[6] Bahnasse, A., Talea, M., Badri, A., Louhab, F. E., & Laafar, S. (2020). Smart hybrid SDN approach for MPLS VPN management on digital environment. Telecommunication Systems, 73(2), 155-169.
[7] Bahnasse, A., Louhab, F. E., Khiat, A., Badri, A., Talea, M., & Pandey, B. (2020). Smart Hybrid SDN Approach for MPLS VPN Management and Adaptive Multipath Optimal Routing. Wireless Personal Communications, 114(2), 1107-1131.
[8] Vial, G. (2019). Understanding digital transformation: A review and a research agenda. The journal of strategic information systems, 28(2), 118-144.
[9] Fletcher, G., & Griffiths, M. (2020). Digital transformation during a lockdown. International Journal of Information Management, 55, 102185.
[10] Mendhurwar, S., & Mishra, R. (2021). Integration of social and IoT technologies: architectural framework for digital transformation and cyber security challenges. Enterprise Information Systems, 15(4), 565-584.
[11] Mugarza, I., Flores, J. L., & Montero, J. L. (2020). Security Issues and Software Updates Management in the Industrial Internet of Things (IIoT) Era. Sensors, 20(24), 7160.