CYBER RANGES, THEIR ROLE IN SECURING SMART BUILDINGS

Marian ION [62]
George CĂRUȚAȘU [1,63]

Abstract

IoT devices are already part of our day-to-day life, and their role increases every day. Buildings and all kind of other constructions will be managed by, or with support or IoT/ICS/ICT equipment, that must be protected 24/7/365 as some of them quickly become obsolete. In terms of cybersecurity, this equipment represents potential doors to the safety of buildings, their inhabitants or users, and their personal or confidential data. People, the society and the market need to prepare to manage risks brought by the usage of millions of old, unpatched, unmaintained ICS and ICT devices. Considering the accelerated rhythm of technology adoption, new cybersecurity technologies, such as cyber ranges, already provide the basis for future approaches to intelligent and knowledgeable management of cybersecurity in IoT contexts.

Keywords: ICS, ICT, cybersecurity, smart building, cyber range

1. Introduction

Cybersecurity of modern constructions presents o series of risks encountered, until recently, only in managing aspects of critical infrastructures. These risks are generated by the usage at an increasingly larger scale of measuring and control technologies such as IoT, IIoT or SCADA in most human activities, among which the construction sector stands out as foundation for all other economic sectors. Regardless we are talking about residential constructions, offices, production facilities, bridges, or other physical built infrastructures, they represent the foundation of more than 60% of the entire modern human activities in time spent inside or in the proximity of constructions, as well as considering the volume of activities. According to World Economic Forum [1], "For nearly the entire population of the world, the built environment heavily influences quality of life. In the United States, for instance, people on average spend nearly 90% of their time indoors.". Considering the importance of the construction sector itself, the same source highlights the fact that „The construction industry serves almost all other industries, as all economic value creation occurs within or by means of buildings or other "constructed assets". As an industry, moreover, it accounts for 6% of global GDP. It is also the largest global consumer of raw materials, and constructed objects account for 25-40% of the world's total carbon

[62] Doctoral School, University Politehnica of Timisoara, 2 Piata Victoriei, 300006 Timisoara, Romania, ionmarian@gmail.com
[63] Department of Informatics, Statistics and Mathematics, Romanian-American University, Expozitiei 1B, 012101 Bucharest, Romania, carutasu.george@profesor.rau.ro

emissions.". "The State of European Cities 2016. Cities leading the way to a better future" report of the European Commission [2] also acknowledges the increased trend of urbanizing population within the European Union, observing that the population in urban areas (cities, towns and suburbs) increased from 65% to 72% between 1961 – 2011. This aspect reflects not only in living areas, but also in working and utilities infrastructures, increasing the impact construction sector have.

Improving cybersecurity of built infrastructures represents a major concern for all their administrators. In many implementations modern technologies mix with old, obsolete technologies posing a higher-than-normal risk to both, inhabitants, and users, as well as the infrastructures itself. Technologies not updated present similar risks to owners, administrators, or users of buildings.

Several tools emerged in the last decades facilitating learning and protection when dealing with cybersecurity of buildings, but more are still to be made. The mix between cyber ranges and artificial intelligence is among the best aids market can provide to increase the security of smart buildings and other smart infrastructures.

2. Cybersecurity of smart buildings

The technological advancements of last decades lead to an accelerated introduction of modern measuring and control technologies in management of buildings and other built infrastructures. Smart constructions include complex systems to monitor their technical and functional parameters and report on working conditions, deviations, malfunctions, or other situations of interest, such as utility provisioning, environmental parameters, etc. As buildings are used by humans mostly for living and working, providing appropriate safe conditions required for people is mandatory, considering legal requirements and business considerations. Therefore, interior, and exterior lighting, emergency lighting, air conditioning, air circulation, plants watering, utilities provisioning, control access, etc., are things that can be managed by automatic systems in smart buildings. Smart utility constructions have different requirements focused more on the functional aspects and the proper functioning of their components, but the cybersecurity requirements remain similar.

Considering buildings relevant, a good example is given by Wendzel and others in the paper "Cyber security of smart buildings" [3] defining a smart building as "a building equipped with integrated technology systems like building automation, life safety, telecommunications, user systems, and facility management systems. … The main goal of a smart building is to connect data, people, and systems.". The same authors [3] highlight the following as main sub-systems of a typical smart building:

- Heating, ventilation, and air conditioning (HVAC) systems;
- • Access control systems in a smart building;
- • Lighting control systems;
- • Fire alarm systems;

- Video surveillance systems;
- • Facility management systems.

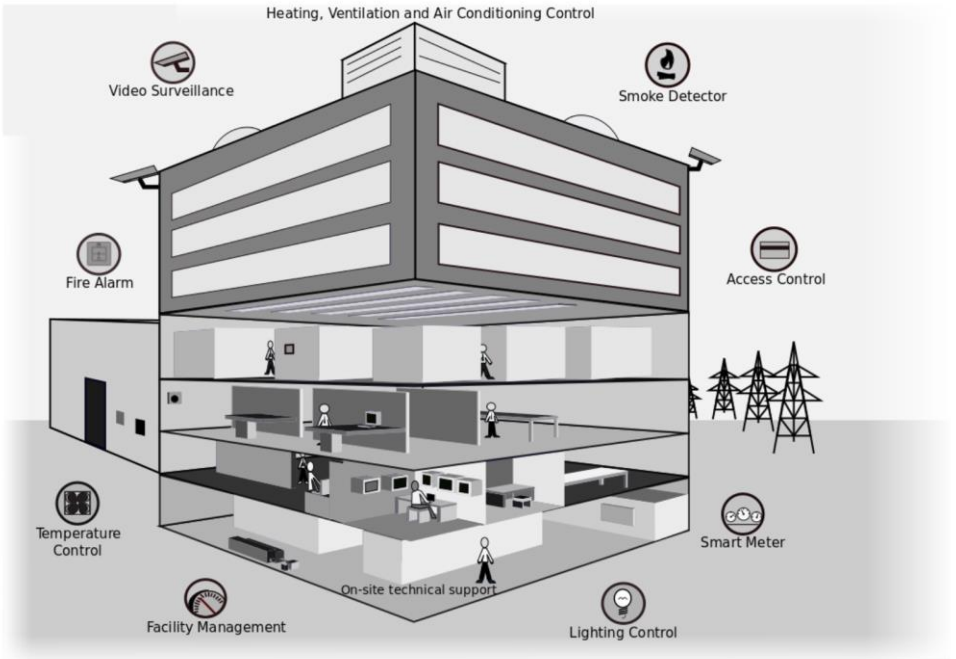

Figure 1.1 Example of a smart building with its components [3]

In addition to the enumeration above, also considering a larger application of technology, we believe it is necessary to extend the architecture of a smart system for buildings and other built constructions with few other sub-systems on functionalities and protection of the infrastructure but not only, such as:

- Utilities provisioning systems – systems dedicated to facilitating and monitor intelligent distribution of utilities to a smart building's interior and dependences. The most common example of such sub-systems are smart metering systems for the necessary utilities, like water, gas, heat, electricity, also represented graphically in the image above. Smart energy generation systems are, as well, good examples of utilities provisioning systems.
- Waste management systems – systems dedicated to automatically monitor, store and report waste deposits generated by inhabitants and users of buildings. A common example are smart waste bins systems capable to compress wastes, rotate bins and report for collection when full.
- Safety control systems – systems monitoring weather, climatic conditions and other relevant parameter, and automatically managing windows, doors, water leakage. Fire detection and control, also represented by the above-mentioned authors, may be considered a component of safety control systems for people and infrastructures. As well, dangerous gas detection, air quality and purification/sterilization, or emergency lights and exits.

- Integrative or interoperability systems – IT&C systems facilitating integration or interoperability between different systems and functionalities of a smart building. Due to technological progress, different types of modern automation systems for buildings management tend to overlap in functional and technological layers (infrastructure management, invoicing, ordering, networking, cybersecurity, etc.), while differences tend to diminish, especially in technological aspects, considering technological convergence, system architecture, TCP/IP based data protocols, etc. These include BMSs (Building Management Systems), FMSs (Facility Management Systems), and other categories of state-of-the-art automation systems handling business and functional processes of a smart building.
- Cybersecurity systems – dedicated systems specially designed and implemented to protect IT&C and smart infrastructures ((I)IoT, SCADA, etc.) from cyber-attacks. These systems include customized firewalls, intrusion detection and intrusion prevention systems, automatic recovery, intelligent traffic analysis, etc.

A different category of smart equipment to be more and more found inside a building is represented by consumers' smart devices, that don't come with the building, but with the inhabitants and users of a building. These devices come in a wide range of categories, varying from smartphones, smartwatches, and other kind of portables to smart appliances, multimedia, gaming, or equipment for elders, ill people, or persons with disabilities. Despite this obvious diversity, much equipment integrate on different technological and functional layers with existing ICT/ICS infrastructure, such as: wired or wireless TCP/IP data network, device management layers, voice command, access control, surveillance systems, data exchange, automatic ordering and/or invoicing software, etc. Moreover, these systems may come to function interdependent with each other. Approaching a gate by a car may activate plate recognition software inside a video surveillance system, opening of the gate and activate certain other sub-systems, such as exterior and interior lighting, garage opening, or interior heating. Similarly, when entering a building face recognition software may recognize a person, deactivate security alarms, and activate lighting, elevator, heating, bring up a ramp for a wheelchair, open TV, etc. Therefore, due to the purpose and wide applicability of IoT systems and equipment, their usage is currently generalizing in all relevant human activities.

As technology evolves and weight of software increases in modern systems, down to field equipment, their associated cybersecurity risks increase as well in both, diversity, and complexity. Until recently, automation infrastructures were independent devices, dedicated systems handling only few aspects usually industry oriented with cybersecurity concerns caused mostly by difficult remote management access to equipment, a reduced rate and level of technological updates: simple predictable architectures, low complexity of equipment, reduced automation functionalities. Still, hardware-based implementation made hacking attempts quite difficult to perform. Current technology is changing, with more and more functions performed at software level instead of hardware, and automatic functionalities of smart constructions are increasingly managed by complex ICT/ICS systems capable to integrate and manage different kind of sensor and actuating equipment. Both, commercially and openly licensed standards and technologies get more and more traction in managing production and data processes in most industries, increasing also technological complexity and diversity in equipment and implementations. Therefore,

while technology develops and spreads, new risks emerged and need to be managed, related to remote access, software bugs, loose implementations, loose interoperability, or loose security. Consequently, we are observing a corresponding increase in cybersecurity attack surface on these kinds of technologies, as well as a considerable increase in volume, diversity, and complexity of cyber-attacks. As well, technological diversification and complexity will deepen the issues encountered in managing smart constructions, facilitating the introduction of new potential cybersecurity breaches or vulnerabilities.

It is important, therefore, to observe the continuous convergence of traditional and modern technologies on conceptual and technological levels, as well as the convergence of ICS and ICT technologies, leading to common technological approaches and a deepening sharing of benefits and risks in initially different scope technologies, such as ICT and ICS.

Considering all above, we believe cybersecurity of ICT and ICS systems already need to be redefined on integrative bases, capable to ensure security on separate layers, and to function integrated. The similarity with the ISO/OSI model and the TCP/IP stack implementation cannot be overlooked, as they are some best examples in terms of standardization on separate layers and integrated functioning.

3. Incident simulation in cyber security

Smart buildings and, generally, smart infrastructures, provide a higher level of comfort for their users, but also may provide a higher degree of risk to personal data and private life. Smart buildings and other smart infrastructures are physical infrastructures whose functionalities were enhanced with help or ICT and ICS technologies. Some of the most representative technologies currently used by people are, considering their categorization, the following:

- ICT equipment: smartphones, computers/laptops, tablets, Wi-Fi routers/Internet access, etc.
- ICS equipment: wearables (smart watches, smart trackers, etc.), smart TVs, content streaming devices, smart energy and lighting appliances, voice control devices, etc.

They are supplemented with other ICS equipment used in smart buildings, such as: different kinds of smart sensors, video monitoring systems, actuators, etc.

All these equipment and countless more have information about us, our habits, our location, our data. And most of them are already connected to Internet using Wi-Fi devices or GSM technologies. With a lifetime of about 5 years or more, while probably being properly secured at purchase time, all these equipment quickly become obsolete in terms of cybersecurity. In two years or less we all end up with daily used technologies that may represent a vulnerability to us, our properties, and our data. Moreover, many Wi-Fi or other Internet-connection devices end up in the same way, with unpatched vulnerabilities and open gates into our properties, infrastructures, and data.

While many appliances and applications are continuously created to help us protect the things we own, little effort was put into education of common IT users, administrators, or managers of smart buildings. Two advanced tools that are getting accessible and handy are represented by infrastructure modelling and simulation software, and cyber ranges.

Modelling and simulation software concentrate on functionalities related to modelling ICT and ICS infrastructures in their virtual representations on computers and simulating their proper functioning. National Instruments LabView, and Schneider's IGSS (Interactive Graphical SCADA System) are representative solutions for modelling and simulation of, mostly, ICS infrastructures. They allow the transposition of industrial control systems and the creation of control software in virtual environments, mostly by mouse, drag-n-drop and right click, requiring limited programming skills for common tasks. They allow working scenarios to be built and run, object libraries to be created and reused, and provide limited functionalities related to ICT systems.

Cyber ranges add a separate layer of cybersecurity and educational functionalities. While both categories share many functions, the present paper concentrates on the more advanced solutions represented by cyber ranges. Cyber ranges provide an augmented experience for users, allowing them to dynamically interact with the simulated infrastructures, re-run scenarios and monitor real time effects following their actions and interactions.

According to NIST, cyber ranges are „interactive, simulated representations of an organization's local network, system, tools, and applications that are connected to a simulated Internet level environment." [4]. In their same material NIST also defines a cyber range as a „Realistic simulation of the internet, systems, applications, and devices in a training environment". NIST definitions reflect the widely accepted positioning of cyber ranges as simulated IT environment and infrastructures, with a substantial role in learning and incident management processes, as it also results from NIST's The Cyber Range: A Guide [5]. The papers lean deeply on roles of cyber ranges but, in our opinion, fail to look further in the future of cybersecurity and this kind of technology.

Moreover, considering the potential impact of cybersecurity tests on ICT/ICS infrastructures there are numerous substantiated arguments for not testing live infrastructures on common bases. Instead, virtualizing ICT and ICS architectures, modelling common behavior of equipment inside data networks and simulating ICT/ICS/cybersecurity incidents have the large benefits of not raising potential risks of damaging live infrastructures, and allow the repeatability of simulations over and over again in controlled, risk-free environments. The similarities with game theories principles cannot be ignored, in this perspective [6]. Also, a large number of games are simulating, for already more than 20 years and in very realistic details, different management situations and scenarios (cities, businesses) [6], transportation technologies (trains, cars, plains) [7], large and very large structures (solar system, galaxies) [8], or behavioral scenarios (cybersecurity, businesses) [9-11].

Technological advancement made augmented simulation the next logic step in learning through gaming, cyber ranges being one of the most relevant examples. In this perspective, cyber ranges are virtual, physical, or augmented representations of ICS and ICT systems in

controlled environments, meant to facilitate testing different cybersecurity incident scenarios and their impact on the respective infrastructures. Most cyber ranges are entirely virtual, in virtualized environments replicating desired scenarios. Still, small scale physical infrastructures, or a mix of real and virtual equipment may be used, considering the needed scenario's requirements. Obviously, virtual cyber ranges provide the most desirable conditions for risk free environments, and repeatability conditions. Virtualized environments and infrastructures may be 1:1, scaled up or scaled down, to a resolution capable to keep results relevant considering the physical infrastructure and, also, the purpose of the tests.

Several very important functionalities need to be provided by cyber ranges when dealing with simulating cybersecurity incidents in virtual environments, such as:

- High degree of fidelity, representing the ability to provide the most accurate replica of the physical systems, from functions and ports to network communication and programmable behaviors.
- High level of standardization, representing the ability to use standardized data structures, data interfaces, or protocols.
- Flexibility, representing the capacity to model different ICT/ICS infrastructures and scenarios without altering main functionalities of the systems.
- Infrastructure's segmentation, representing the ability to segment the simulated ICT/ICS infrastructures by physical and logical criteria, based on scenario's requirements (e.g., networking, sensoring, actuating, server, application, or other layers).
- Reusability, representing the capacity to allow users to reuse virtual items in different architectures and scenarios.

Other relevant functionalities relate to usability, accessibility for disabled people, or multilingualism.

Several cyber range solutions are available at time of writing, with a variable palette of functionalities. Most of them include functionalities, such as: modelling ICT and ICS infrastructures, simulating their functioning and data exchange, preparing, managing, and running incident scenarios, as well as providing the necessary interaction for learning processes. Some examples are: CyberGym's CTTA (Cyber Training and Technologies Arena), Silensec Cyber Range (provided by Silensec), Cyberbit Range (provided by Cyberbit), CASTLE (Cyber Security and Learning Environment provided by the Austrian Institute of Technology), etc. These solutions are only few examples of cyber ranges applied technology and provide commercially the above-mentioned functionalities as services on premises or cloud computing infrastructures.

Thus, due to their functionalities, cyber ranges can facilitate design of smart infrastructures, test their cybersecurity, or educational processes. While currently cyber ranges still represent a niche subject in the ICT and IoT world, being more closely related to professional environments, they are bound to become one of the most important learning tools in cyber security for everyone. Therefore, while still needing specialized knowledge

on cyber security, we appreciate cyber ranges will become more and more accessible for common people, and processes automation will drive the next step in their evolution to smart, integrating, adapting cybersecurity software solution.

4. Conclusions

Autodesk estimates [12] that only in urban areas about 11100 new buildings were built daily in 2018 in the entire world, and approx. 14700 new buildings to be built daily by 2050. This numbers adds to all the existing buildings, leading already to a countless number of constructions. This amount represents, also, the number of physical infrastructures that need to be protected from cybersecurity incidents. People using those buildings and their data need to be protected, as well.

As buildings become more and more accustomed to smart technologies, the need for extended cyber security services raise exponentially. The quantity and quality of knowledge necessary to protect a huge, unknown number of buildings, people and data exceeds the possibility of the market now, and in 2050. The only reasonable solution is to automate current technologies to provide relevant information and knowledge, as well as necessary actions, to ensure automatic responses to cyber incidents, and to automatically protect people and data inside the building.

A potential solution, already at hand for several of the needed functionalities, is represented by cyber ranges. Augmented solutions able to model ICT and ICS infrastructures, simulate functions and behavior and, possibly, protect against cyber incidents and detect unexploited vulnerabilities of obsolete equipment with support from AI technologies, cyber ranges will also provide specialized knowledge for people with administration and protection of respective buildings.

References

[1] Shaping the Future of Construction A Breakthrough in Mindset and Technology, World Economic Forum and The Boston Consulting Group, 2016, https://www3.weforum.org/docs/WEF_Shaping_the_Future_of_Construction_full_report__.pdf, retrieved 2021/08.

[2] The State of European Cities 2016. Cities leading the way to a better future, European Commission, 2016, https://ec.europa.eu/regional_policy/sources/policy/themes/cities-report/state_eu_cities2016_en.pdf, retrieved 2021/08.

[3] Cyber security of smart buildings, S. Wendzel, J. Tonejc, J. Kaur, A. Kobekova; 2016, https://www.researchgate.net/requests/r91879198, retrieved 2021/08.

[4] Cyber range, NIST, 2018, https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf, retrieved 2021/09.

[5] The Cyber range: A guide – Draft, NIST, 2020, https://www.nist.gov/system/files/documents/2020/06/25/The%20Cyber%20Range%20-%20A%20Guide%20%28NIST-NICE%29%20%28Draft%29%20-%20062420_1315.pdf, retrieved 2021/09.

[6] Salman Zulfiqar, Binesh Sarwar, Saira Aziz, Khurram Ejaz Chandia, Muhammad Kaleem Khan, An Analysis of Influence of Business Simulation Games on Business School Students' Attitude and Intention Toward Entrepreneurial Activities, Journal of Educational Computing Research, 2018, https://journals.sagepub.com/doi/full/10.1177/0735633117746746, retrieved 2021/11.

[7] , Ioanna Kourounioti, Shalini Kurapati, Heide Lukosch, Lóránt Tavasszy, Alexander Verbraeck, Simulation Games to Study Transportation Issues and Solutions: Studies on Synchromodality, Transportation Research Record: Journal of the Transportation Research Board, 2018, https://journals.sagepub.com/doi/10.1177/0361198118792334, retrieved 2021/11.

[8] National Institutes of Natural Sciences Japan, Largest virtual universe free for anyone to explore, ScienceDaily, 2021, https://www.sciencedaily.com/releases/2021/09/210910121651.htm, retrieved 2021/11

[9] Max Juraschek, Christoph Herrmann, Sebastian Thiede, Utilizing gaming technology for simulation of urban production, The 24th CIRP Conference on Life Cycle Engineering, 2017, https://www.sciencedirect.com/science/article/pii/S2212827116313932/, retrieved 2021/11.

[10] Benjamin D. ConeMichael F. ThompsonCynthia IrvineCynthia IrvineThuy D. NguyenThuy D. Nguyen, Cyber Security Training and Awareness Through Game Play, Security and Privacy in Dynamic Environments, Proceedings of the IFIP TC-11 21st International Information Security Conference (SEC 2006), 2006, https://www.researchgate.net/publication/220722774_Cyber_Security_Training_and_Awareness_Through_Game_Play, retrieved 2021/11

[11] Merijke Coenraad, Anthony Pellicone, Diane Jass Ketelhut, Michel Cukier, Jan Plane, David Weintrop, Experiencing Cybersecurity One Game at a Time: A Systematic Review of Cybersecurity Digital Games, Simulation & Gaming, 2020, https://journals.sagepub.com/doi/10.1177/1046878120933312, retrieved 2021/11

[12] Autodesk, 13,000 Buildings per day Infographic, 2018, https://cdn.redshift.autodesk.com/2018/08/13000-buildings-per-day-infographic1.pdf, retrieved 2021/11