Interdisciplinary Description of Complex Systems 18(3), 337-342, 2020

SECURITY ISSUES OF SMART CITY CONSTRUCTION

Richárd Pető*

Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering
Budapest, Hungary

DOI: 10.7906/indecs.18.3.2
Regular article

Received: 9 March 2020.
Accepted: 25 May 2020.

ABSTRACT

Building and operating a smart city must be based on a solid foundation. A stable foundation can only be built if all the necessary (security) elements are in place, and the connection among the elements is both established and functioning. It must be therefore clarified what security elements (areas of expertise) are required. The purpose of this article is to briefly present the security fields relating to smart city constructions and their interrelationships on the basis of the previous publication. By harmonizing the elements, risks can be reduced to an acceptable level.

KEY WORDS

IT, information, construction, construction yard, security, coordination, risk

CLASSIFICATION

JEL: D21, F52, G38, H11, H12, K00

*Corresponding author, η: Richárd Pető, petorichard.mk@gmail.com; +36 30 935 7667;
Hungary, 1096 Budapest Haller utca 20,

INTRODUCTION

In this article, the information technology (IT) approach to city/building constructions, and the construction of interconnecting systems have been discussed. Their significance is due to the fact that as early as the planning stage, a large amount of data (such as personal data, technical designs, financial documents, etc.) will be collected and managed, and they will be classified as confidential or even secret.

It should be taken into consideration that there are several buildings, objects, or things in which some type of a sensor is installed, and in some way they communicate the state of the systems or even the measured readings to the user. If this information is accessible to an unauthorized person, it can be misused, which will cause damage.

Two important facts can be deduced from the above information. The first is that nowadays it is increasingly difficult to mention anything that is not controlled by electronics or is not networked, which means that nearly everything communicates with the system user. The other fact is that as early as at the planning phase – that is well before any physical work is done on the construction site – significant risks can be expected [1].

EXAMINATION OF CONSTRUCTION PROJECTS

Sensitive information at risk (including later phases of the construction process) may include:

- (Day-to-day) organization plan (nature of workflows, workflow areas, company manpower, expected material deliveries, temporary and permanent storage areas, type and quantity of equipment and materials in warehouses and construction sites);
- construction plan of the structure of buildings;
- network and system blueprints for buildings (electrical network, water and sewage network, gas pipeline network, IT network, security system network, fire alarm network,);
- details of general contractor;
- regulations of the general contractor and those of the operation of the construction site;
- details of subcontracting companies;
- partnership contracts and commitments;
- performance confirmations and payments;
- official approvals;
- events and event logs;
- etc. [2, 3].

Data management may vary significantly from country to country. In the case of China, information gathering is centrally managed. Based on the data collected from different systems, the rights of the population are determined or even limited. When it comes to the European Union, it is the legal harmonization between the EU member states that plays an important role. Its objective is to develop and adopt regulations among the parties, which do not violate each other's rights. In recent years perhaps the best example of this effort has been "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)", referred to briefly as the GDPR. Of the latter, it should be noted that it applies only to personal data, while it is not applicable to company secrets or confidential data [4].

Data and the networks that transfer them are omnipresent, and therefore, inevitable. The question is how these values can be protected. The answer is given through a complex system.

Basically, there are three main categories of data carriers [5, 6]:

- Persons as data carriers: A knowledge-based factor that may be intentionally or accidentally compromised.
- Hard copy (and traditional) media: This type includes various administrative tasks, treatment of documents and its entire process.
- IT-based media: The management of IT systems, including their operation, user management.

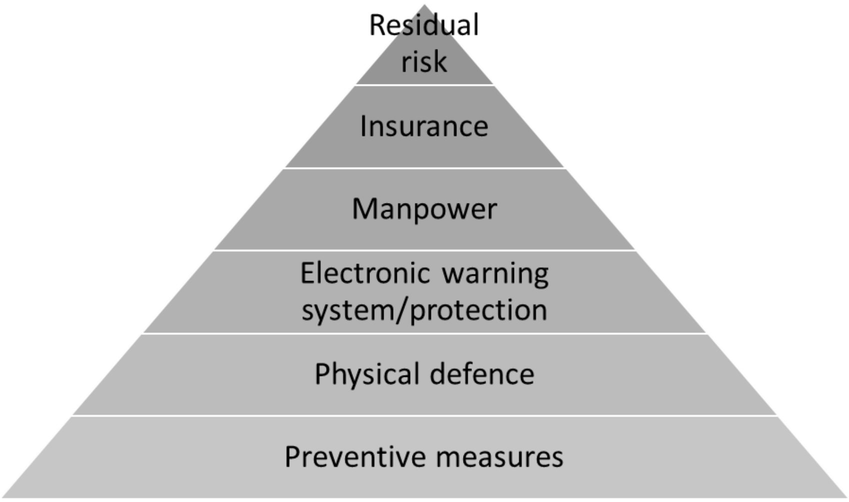

Figure 1. Steps of establishing security/safety (Security Pyramid)[1] [7].

The security pyramid provides a well-structured, general guidance. The security pyramid illustrates the components of protection and how they are built on one another. Each level has its own “mission” [8-12]. Each level can be further divided into sub-levels or components which may be called efficient, in dependence on having met the criteria. The summary of its levels (with reference to building protection):

The lowest level is made up by preventive measures. Basically, this is the fundament of the entire system, which is present anywhere at other levels as well. These measures include the introduction of and compliance with regulations and measures, without which other levels would be ineffective. For example:

- If the front door of a house is not closed, the physical protection built into the door, which is the lock in this case, will not serve its purpose.
- If the intrusion detection system is not armed, it will not signal the intruder.

The level of physical protection[2] consists of physical devices that make it difficult to enter or exit a given facility (e.g. a prison). Applying the previous example:

- If the door of a house is closed, but no built-in lock is available, no protection can be ensured in spite of any intention to protect the building.

The level of electronic signalling systems is responsible for signalling intrusions. The **fun**ction of various different sensors – movement, opening, breaking, vibration, sound etc. – is to signal in cases other than the “normal” (event-free) status. An electronic version of protection is an electronic device which is able to resist an intrusion regardless of its effect.

- The front door of a house has a lock and it is locked. If there is nothing to signal the alteration of normal status – e.g. in the case of a break-in, which is considered as a deviation from a “normal” status, that is the closed position –no protection will be provided.

The level of personnel is responsible for the immediate elimination of perceived adverse acts. This category includes the human force responsible for protection (bodyguards, security personnel, armed security guards, K-9 guards – the police in some respects – and trained (guard)dogs).

- The front door of a house has a lock and it is locked. If the intrusion detection system signals but there is no one to respond to the intrusion alarm, the necessary protection will not be achieved.

In spite of the security measures taken and established, a harmful event may occur in an unpredictable manner (for example, the attacker somehow gains access to the secured object, the fire extinguisher does not put out the fire, or not in the expected way, etc.), which may even be a chain of accidental events. In such cases it is the insurance service that will compensate the injured party.

The top level of the pyramid is represented by the so-called residual risk factors (also known as own risks). This level is always present, but its value or magnitude can be influenced. The more hazards are eliminated / minimized or the closer the probability of their occurrence is to zero, the lower its indicated value is. Since one cannot prepare for everything, this value can never equal zero.

There may also be a model similar to the security pyramid, which for simplicity will now be labelled as “extended security pyramid”.

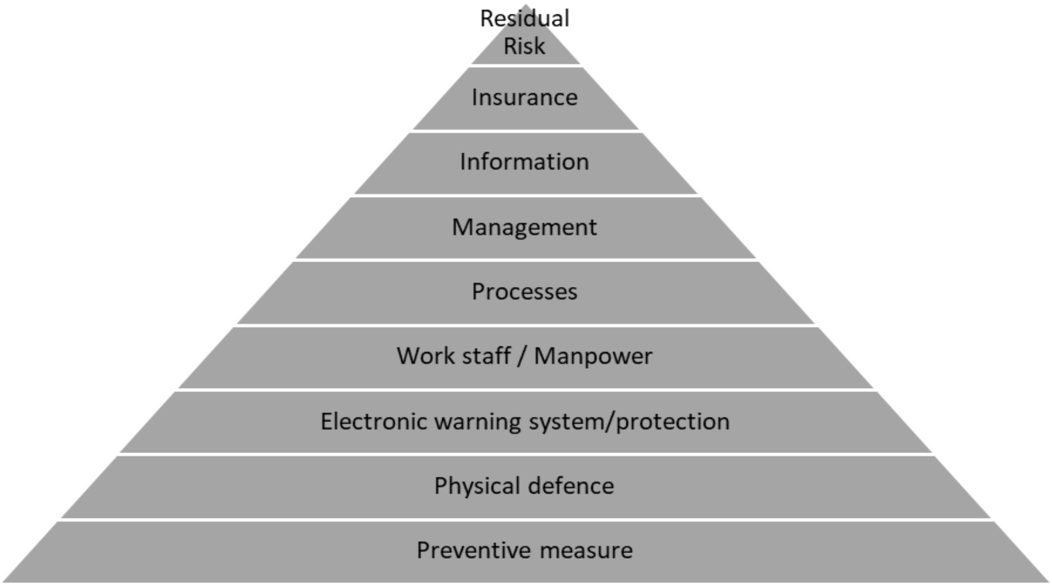

Figure 2. Steps of establishing security/safety (Extended Security Pyramid) [13].

The extended security pyramid has another three levels added:

- processes,
- management,
- information,

and at the level of labour force, the staff also appeares. A significant part of an organization is made up by employees who are not part of the security personnel. Through their involvement and security training, security risks can be reduced. Well-trained staff will initially be passive but later on, they get dynamically involved in security activities. Passive participation means simple compliance with the rules and regulations, while active involvement means noticing vulnerability or attack activities, and taking some action against them (signalling to security, recognising suspicious activities, etc.).

“Information” represents a significant part, as it comprises the basis of the decision-making process at management level. Various processes and their orders of execution are determined on the basis of information. These processes can be considered as the instructions of the organization. The composition of the instructions consists of the relevant legislation and the internal, individual regulations of the organization. These regulations include, for example, the rules of the operation of the organization or organizational unit, the various organizational and production processes, or even the rights and obligations of guarding and security.

For those with no or limited security awareness the extended security pyramid gives a greater insight into how the system of the company works. In contrast, the other security pyramid consisting of fewer levels tends to be based on its main pillars, helping to make the levels more transparent and easier to memorise. Unlisted levels are included in various standards, and partly in legislation, each of which is integrated into different levels.

There are several examples to prove the above statements through asking and answering the following questions:

- Can a deal be concluded between a seller and a buyer if either of them is not aware of the other, or possibly of the product to be sold? Obviously not, because there is a lack of information and of its flow.
- The seller and the buyer can make a decision to sell or buy a product based on the necessary information. At this level (personal) management appears.
- What is the process of sale and purchase? The rules of the process (rules of procedure) are determined by the legislation and the participating parties. This is where the level of process appears.

The security pyramid (including the extended one) formulates levels that can be interpreted and applied as a system in other branches of security technology as well.
Returning to the original question of how values and valuables can be protected, the answer lies in the security pyramid shown above, that is, in the regulation and technology of its elements.

CONCLUSION

In the course of construction work, a large amount of data and information is transferred, most of which is classified as personal or confidential. If these data are not handled with due care, they can be compromised and easily misused. The article briefly summarizes what data could be involved and how it could be carried. Examining the above possibilities, it can be claimed that the key to the problem is the relationship between the security pyramids, the elements of the pyramid and their regulation.

REMARKS

[1] On the basis of other approaches, the structure of a pyramid or its levels would not be possible to interpret. E.g., 1) from an economic aspect, the budget of used solutions may significantly differ depending on the facility to protect, which means that the lowest level of the pyramid would not be made up by preventive measures. 2) in the interpretation of protective solutions, residual risk could not be interpreted. Through insurance, which is optional, it is only the extent of the harmful event that may be decreased, while the residual risk would not be involved in risk reduction. Nevertheless, this approach is applied here, because it can be interpreted as a general thumb rule, as a “technically” structured system.

[2] Mechanical protection may be a more precise term. the two terms are used here as synonyms.

REFERENCES

[1] Utassy, S.: *Komplex villamos rendszerek biztonságtechnikája*. Ph.D. Thesis. Zrínyi Miklós Nemzetvédelmi Egyetem, Bólyai János Katonai Műszaki Kar Katonai Műszaki Doktori Iskola, Budapest, 2009,

[2] Buildingworld: *Organization plan.* http://epitovilag.hu/organizacios-terv, accessed 17th June 2018,

[3] –: *No CXXXIII of 2005 Private security, and the activities of private investigators of the European Union.*
https://mkogy.jogtar.hu/jogszabaly?docid=a0500133.TV, accessed 4th February 2020,

[4] Horváth, Zs.: *Preface to IT security.*
In. *IT Security Engineer; Standard rules of IT security*.
Óbuda University, 2017,

[5] Constructible: *Cybersecurity In Construction: What You Need to Know.*
https://constructible.trimble.com/construction-industry/cybersecurity-in-construction-what-you-need-to-know, accessed 29th July 2019,

[6] MyIT: *3 Biggest Construction Cybersecurity Risks.*
https://www.myitsupport.com/3-biggest-construction-cybersecurity-risks, accessed 29th July 2019,

[7] The Chartered Institute of Building: *The role of security in the construction industry*.
https://www.ciob.org/sites/default/files/The_Role_of_Security_in_the_Construction_Industry.pdf, accessed 29th July 2019,

[8] –: *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, General Data Protection Regulation).*
https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=HU, accessed 11th November 2019,

[9] Berek, L.; Berek, T. and Berek, L.: *Security*.
Óbudai University Donát Bánki faculty of mechanical and safety engineering, Budapest, 2016,

[10] Horváth, Zs.: *Az információbiztonsági irányítási rendszer alapjai.*
https://anzdoc.com/az-informaciobiztonsagi-iranyitasi-rendszer-alapjai.html, accessed 14th December, 2018,

[11] Berek, L.: *Biztonságtechnika, Nemzeti Közszolgálati Egyetem.* In Hungarian.
http://real.mtak.hu/19709/1/biztonsagtechnika.original.pdf, accessed 8th September, 2018,

[12] Pető, R.: *Safety and Security of Constrution sites.*
Óbuda University, Budapest, 2019,

[13] Papp, R.: *Pyramid of Security.*
Óbudai University Donát Bánki faculty of mechanical and safety engineering, Budapest, 2016.