Magyar Rendészet 2020/2. 169–181. DOI: 10.32577/mr.2020.2.9

Design Principles of a Physical Protection System for Data Centres (Essential Requirements for the Security Staff in the Physical Protection System)

Tamás HORVÁTH[1]

The best practices and knowledge of different guidelines would be absolutely useful for professionals in the field of security technology. It is essential for the design and implementation of the data centres which are not really common facilities due to security reasons. Their location, proper activities, even the circumstances of their operation, all this should not be public knowledge. The design and implementation of the data centres depend on their security risk level. This may be fairly known for professionals, but a summary of the essential requirements would be useful for all people involved. In my practice, our company has got a chance to make a complex security plan for a Data Centre, so I would like to present the architectural and security aspects which may be important in the given case. Since a certain level of security is required in a given case, and different levels belong to different physical protection systems (PPS), I have created a facility security matrix to serve as a guideline and to help to decide what kind of PPS should be installed in different cases.

Keywords: *practical guide, data centre, security risk, Physical Protection System, protection in depth, security in depth, controlled zone, protected zone, facility security matrix*

Introduction – General aspects

There are no general standards for designing and implementing physical protection systems of data centres, but the professionals have not been left without certain guidelines, since the best practices for those who are interested in security market are widely available in the international technical literature.[2]

Looking for the facts how to design a physical protection system for data centres, we realise immediately that dealing with security systems alone is not enough, we should

[1] Dr. HORVÁTH Tamás, tanársegéd, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Magánbiztonsági és Önkormányzati Rendészeti Tanszék
Tamás HORVÁTH, PhD, lecturer, University of Public Service, Faculty of Law Enforcement, Department of Private Security and Local Governmental Law Enforcement
https://orcid.org/0000-0001-5273-9980, horvathtam@uni-nke.hu

[2] Forrás: www.sans.org/reading-room/whitepapers/awareness/data-centre-physical-security-checklist- (2020. 04. 08.)

also face some architectural requirements.

Summarising all the most important requirements which can be found in different guidelines, practice methodology and design of PPS[3] of data centres, I would like to present what we are capable of concerning design in case of an assignment to do so.

Due to the limitations of my study, there was no chance to focus on the complete security systems of facilities, so I had decided to deal with the classic security systems, while the BCM/DRP and the fire protection systems were out of my interest this time.

Principles of implementation of physical protection systems

I had best start with a general overview of PPSs, emphasising their most important elements. For a proper security system, it is always useful to have a well-detailed structure of elements.

There is no regular process to decide what level of security risks have to be managed. There is only one method which may help to decide what type of physical security system could be implemented in the facility in question. If we had a simple but specified risk analysis which could be used in the security field, it would not only be effective but practical as well for all people involved.

Based on my experiences I could initiate a rather simple but suitable way to make the proper classification in industrial facilities. By way of a certain risk analysis matrix one could classify the facilities based on two features:

1. Embeddedness of the facility into society (If there were some operation problems, how many people would be affected?);
2. What kinds of technology and property data have they, and what level of protection is needed?

Details of Table 1 to be read:
Facility impact on surroundings

1. If the business continuity (BC) of Institute/company is damaged, activity of them is being jammed or stopped, which affects around a few hundred people.
2. If the business continuity (BC) of Institute/company is damaged, activity of them is being jammed or stopped, which affects around a few hundred people and can cause local troubles for citizens. The local government's intervention may be needed. (E.g. local water supply.)
3. If the business continuity (BC) of Institute/company is damaged, activity of them is being jammed or stopped, which affects around a few thousand people and can cause local troubles for citizens. The local government's intervention may be needed. (E.g. reserve power plants have to be launched.)

[3] PPS: Physical Protection System in abbreviation.

Table 1: Facility matrix. Source: compiled by the author

FACILITY MATRIX			Facility impact on surroundings (social embeddedness)				
			If the business continuity (BC) of institute/company is damaged, activity of them is being jammed or stopped, which affects around a few hundred people.	If the business continuity (BC) of institute/company is damaged, activity of them is being jammed or stopped, which affects around a few hundred people and can cause local troubles for citizens. The local government's intervention may be needed. (E.g. local water supply.)	If the business continuity (BC) of institute/company is damaged, activity of them is being jammed or stopped, which affects around a few hundred people and can cause local troubles for citizens. The local government's intervention may be needed. (E.g. reserve power plants have to be launched.)	If the business continuity (BC) of institute/company is damaged, activity of them is being jammed or stopped, which affects around a few hundred people and can cause local troubles for citizens. The local government's intervention is needed. (E.g. water supply for an entire city.)	Embeddedness of the institute/company is given regionally. The quantity of their employees could reach a few thousand people. If their bussiness activity were stopped it could cause trouble for the entire country. (E.g. data centres; nuclear power plant.)
			1	2	3	4	5
Technology and property data to be protected	Institute/company does not apply technology which has to be protected and they don't work with data which has to be protected.	1	1	2	3	4	5
	Institute/company does partially apply technology which has to be protected and its damage could cause troubles only for them. They don't work with data which has to be protected.	2	2	4	6	8	10
	Institute/company does apply technology which has to be protected and its damage could cause troubles locally. They do work with data which has to be protected and if it were published it could make trouble locally.	3	3	6	9	12	15
	Institute/company does apply technology which has to be protected and its damage could cause troubles regionally. They do work with data which has to be protected and if it were published it could make trouble regionally.	4	4	8	12	16	20
	Institute/company does apply technology which has to be protected and its damage could cause troubles governmentally. They do work with data which has to be protected and if it were published it could make trouble governmentally. (For example: national energy supply or NATO/EU/National classified data.)	5	5	10	15	20	25

4. If the business continuity (BC) of Institute/company is damaged, activity of them is being jammed or stopped, which affects around a few thousand people and causes local troubles for citizens. The local government's/governments' intervention is needed. (E.g. water supply for an entire city.)
5. Embeddedness of the institute/company is given regionally. The quantity of their employees could reach a few thousand people. If their business activity were stopped it can cause trouble for the entire country. (E.g. data centres; nuclear power plant.)

Technology and property data to be protected

1. Institute/company does not apply technology which has to be protected and they do not work with data which have to be protected.

2. Institute/company does partially apply technology which has to be protected and its damage could cause troubles just for them. They do not work with data which have to be protected.
3. Institute/company does apply technology which has to be protected and its damage could cause troubles locally. They do work with data which have to be protected and if it were published it could make trouble locally.
4. Institute/company does apply technology which has to be protected and its damage could cause troubles regionally. They do work with data which have to be protected and if it were published it could make trouble regionally.
5. Institute/company does apply technology which has to be protected and its damage could cause troubles governmentally. They do work with data which has to be protected and if it were published it could make trouble governmentally. (For example: national energy supply or NATO/EU/National classified data.)

Table 2: Classification of the level of security risks. Source: compiled by the author

Security risk level	Abbreviation	Value of risk	Marks
Low level security risk facility	**LLSRF**	1-2	
Medium level security risk facility	**MLSRF**	3-4	
High level security risk facility	**HLSRF**	5-12	
Extended level security risk facility	**ELSRF**	13-25	

Before having decided on the security risk level, we had to organise a meeting discussing what type of technology would be used and what kinds of data would be operated in our Data Centre in question. (Remark: all required information might be protected so it is not a surprise if we had to make a special privacy statement.)

Preparing for our design process we had set a technical meeting for our partners. Its primary function was to obtain the essential security information about the Data Centre. During the technical meeting we obtained the following information:

1. Servers will be operated by the administration and several governmental companies which deal with financial and commercial businesses.
2. Servers would be installed by different commercial and industrial companies as a recovery or secondary sites.
3. The applied technology must be protected by physical security system evidently controlled by the administration.
4. Data owned by the administration would be classified as national protected data which require high security level.
5. The administration would provide a document of requirements called Design Basis Threat (DBT)

After the technical meeting the security risk level could be seriously considered. After the calculation, we can see that the Data Centre in question reached the highest classification level, the Extended Security Risk Facility level, which means that a complex security system has to be designed.

Table 3: Definition of Data Centre security coefficient. Source: compiled by the author

TWO FACTORS for Data Centre	Value
Technology and property data to be protected	5
Facility impact on surroundings (social embeddeness)	5
Facility cofficient	25

As the next step, a security risk analysis should be conducted. The best choice would be if we put together – extending the administration's DBT – a 'Risk Cloud' where we can collect all the security risks related to the facility in question. In my practice the most successful process was when we used four security risk groups in our 'Risk Cloud' as follows:

1. Security risks caused by the operation of the facility itself
2. Security risks caused by technical difficulties
3. Security risks caused by criminal conditions of the surroundings
4. Security risks caused by human activities in the facility itself

These four groups of risk has to be enough for an analysis satisfactory for the design and the evaluation process for the physical security system. Unfortunately, there is not enough room for presenting the security risk analysis, taken into consideration that it is not in my focus at all, but I hope the topic in question provides opportunities for provoking new thoughts. Let us return to the practical guide.

Architectural aspects

Before making any decision on the design of a PPS of a data centre, one should deal with an important question: how to build up the facility itself architecturally, taking into account physical security requirements? This question should be solved first, because later, when the building is structurally ready, it could not be modified easily.

The physical security of the facility may be endangered by any kinds of signs expressing the proper activities of the company. For that reason, the function of the firm should not be advertised on the building, including any relevant logos or pictograms.

1. Windows of server's rooms should not face any offices or public area. If the structure of the building should make windows necessary for any reasons, the standard glasses has to be changed to bullet proof ones.
2. The facility's parking places should be placed minimum 18 m (60 feet) from the façade of the building to mitigate the damages of an explosion's effect and the first-degree direct accidents.
3. During the architectural process the experts should take into account the roof stability against any kinds of drone attacks.
4. Green area[4] of the facility should be regularly tended allowing the correct operation of the physical protection system. The property structure has to support the security operation through the removal of all the physical objects secure enough for intruders to hide – not only on the site, but in a minimum 10 m wide zone next to the fence.
5. On both sides of the property's border fence, 3 m wide paths should be left clean for patrols and for the proper operation of security technology and surveillance system.
6. The border fence should be minimum 2.5 m high and equipped with NATO barbed wire.
7. The track of incoming roads should be built by using special barriers which can slow down the approaching vehicles' speed to 40 km/h. If the special track could not be built for any architectural reason, road blockers have to be implemented on lanes, 10 m away from the vehicle gate, which should be remotely driven.
8. Central Alarm System (CAS) should be installed next to the personal entrance of the server building, in a room which is proper for the reception office with surveillance monitors in the back. (Concerning the monitors' screens, a special requirement should be taken into consideration, namely, no one can be out of sight.)
9. Security Guards (SG) and Respond Force (RF) should have an armoury, a rest room and locker room as well as a load/unload place.
10. Close to the reception area a room for personal checking should be provided.
11. Next to the reception area a room called registration office should be placed for producing access cards, including the ability to take personal pictures, to print access cards and to register biometric data.
12. Next to the personal entrance a waiting area should be built where the visitors and partners without access rights can wait for a few minutes. In this waiting room a special cupboard with locks should be placed for keeping certain devices which are prohibited to enter with into the building after the turnstile.
13. Any entrance of the facility should be blocked generally, including the personal gates. Next to the vehicle gate the facility should provide a few parking places for temporary waiting and security check.

[4] Green area is where the grass and the trees, bushes can be found in the complete area of the property.

Building up the Security System

The complete physical protection system design should be constructed by the principle of protection and security in depth.

Protection in depth

Protection in depth implementation is one of the most important aspects of the physical protection system due to the increased effectiveness of the detection and the neutralisation of intruders. With the theory of the protection in depth having been applied, here you can find the solution in case of the property in question.

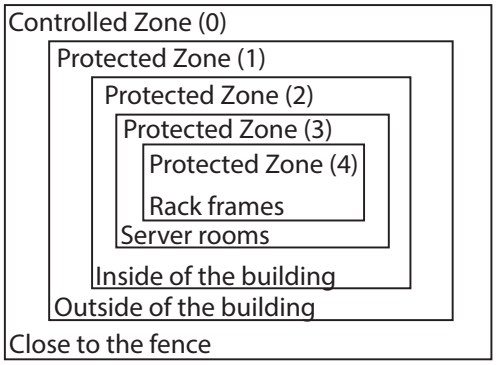

Figure 1: Protection in depth applied in the Data Centre. Source: compiled by the author

Security in depth

The protection in depth is about the structure of the physical protection system. The security in depth based on the PPS is about the effectiveness of the physical security combined with today's IT/ITC security.

$P_{(effectiveness)} = P_{(interruption)} \times P_{(neutralisation)}$
$P_{(security\ in\ depth)} = P_{(effectiveness)}1 \times P_{(effectiveness)}2 \times P_{(effectiveness)}3 \times P_{(effectiveness)}4$
$P_{(zone\ effectiveness)} = f_{(P(detection)}; P_{(delay)}; P_{(response))}$

$P_{(effectiveness)}$ = Probability of effectiveness
$P_{(interruption)}$ =Probability of interruption (e.g. of a saboteur activity)
$P_{(neutralisation)}$ = Probability of the neutralisation (e.g. saboteur has been arrested or shot)
$P_{(security\ in\ depth)}$ = Probability of security in depth
$P_{(zone\ effectiveness)}$= Probability of zone effectiveness depends on $P_{(detection)}$; and $P_{(delay)}$; and $P_{(response)}$
$P_{(detection)}$ = signal probability of a sensor
$P_{(delay)}$ = delay probability of a mechanical structure
$P_{(response)}$ = probability of success of respond force

Analysing the formulas, it is easy to realise that probability (P) of effectiveness in any zone depends on the probability of detection, delay[5], and response[6].[7] However, according to some scholars, "Security in Depth refers to a holistic approach to the protection of assets where based on the threats which pose a risk across an entire organisation or facility different layers and levels of security controls are implemented to ensure access to a protected asset is restricted to those with legitimate access rights. Thus it is argued that Security in Depth can be represented by the formula…"[8]

P(effectiveness) means the probability of effectiveness depends on multiplication of probability of neutralisation[9] and the probability of interruption.[10]

P(security in depth) can be calculated by multiplication of each probabilities of efficiency.

As for the zones of the facility in question, there are one (1) controlled and four (4) protected zones.

I. Controlled zone – out of property, outside the fence – Zone (0)

The controlled zone means a fairly large zone which is close to the fence of the property. That is the most important zone in the detection of intrusion in time, while it can also provide for the required path of patrols.

II. Protected zones in the facility

1. Perimeter protection zone (1)
2. Building protection zone (2)
3. Server protection zone (3)
4. Rack frame zone (4)

At the design process of the PPS, the following requirements should be taken into consideration:

1. Violent penetration without permission has to be prevented through the application of a wide range of special equipment (for example, bollards, barriers, barbed wire, etc.).
2. A complex regulation of entry policy has to be carried out and all of the owner's partners and visitors have to get familiar with this, even if the classified circumstances were operated. The complex regulation means that the operation of the staff and the vehicle entrances have to be regulated in a detailed way.

[5] Delay: delay provided by mechanical structures.
[6] Response: activity of responding force.
[7] Adams et al. (2005) 226–229.
[8] Cool–Corkill–Woodward (2012) 33.
[9] Probability of neutralisation: success of respond force.
[10] Probability of interruption: probability of interruption of saboteur activity.

3. Trespassing to the controlled zone should be prevented not only with technical devices but special configuration of the entry system, too. (For instance, anti-pass back, direction control, attendant requirement etc.)
4. Visitors can be let in only if they were accepted by someone from the staff, otherwise, they have to be accompanied all over the property by guards.
5. All movements in the facility have to be controlled by surveillance system. During the design it should be taken into consideration that all sorts of movements of people and vehicles must completely be covered by cameras. A great advantage of a carefully implemented CCTV system[11] is that it can be activated by the sensors of the alarm system. It can easily be assessed which can provide the shortest reaction time on the part of the Response Force.
6. On the other hand, the surveillance system may have a video analytics system focused on difference areas of the protected zones, which is an extremely useful support for guards in the monitor room.
7. Regarding the status of doors and windows, each one of the property must be controlled by the intrusion alarm system monitored in the control room.

Physical Protection System to be implemented

Data centre security staff

The security staff should perform a host of duties on a daily basis:

- monitoring the intrusion security alarm systems;
- dispatch mobile security officers to emergencies;
- monitoring to prevent unauthorised access, such as tailgating;
- assist all individuals who have authorised access to enter the Data Centre;
- controlling access to the Data Centre by confirming identity;
- issue and retrieve access badges;
- respond to telephone and radio communications.

An essential requirement is the acceptance of the complete integrated physical protection system (IPPS), which is to be based on security guards. In Hungary, similarly to other foreign countries, we have special regulation for that.

There are two different types of security officers in base:

1. security guards by Act CXXXIII of 2005 on the rules of personal and property protection and private investigation;[12]
2. armed security guards[13] by Act CLIX of 1997 on armed security guard, nature conservation and field guard.

[11] CCTV system: Close Circuit Television system.
[12] Standard security guard with self-defence equipment.
[13] Specialised security guards having right to use offensive weapons.

Depending on the types of protected data, in data centres the armed security guards may be the best but certainly not the cheapest solution. Speaking about their tasks, their duties could be followed easily:

"Armed security guards, therefore, should be trained in other methods of diffusing potential problems, preventing or stopping violence, or preventing or stopping crimes from being committed, for whatever charge they are hired to protect. Ultimately, though, armed guards must be proficient with firearms and their weapons in case they are ever called upon to use them during their duties. Armed security officers are private security guards that are hired to protect an area, a person or persons from potential attack, hostilities or criminal activities.

An armed security guard could be hired or employed but it is important that regulation in case must be kept, as usual."[14]

It is absolutely recommended that the radio communication system had special features like the transmission of GPS positions and man down.[15]

Another requirement is a security guard inspection system, by way of which one can see the accurate position of guards patrolling around the property. (An IP based radio communication system with special features is highly recommended.)

Controlled zone (Zone N0)

The controlled zone is the basic element of the zone systems, because this is the area where the security check is on low level. As the name of the zone says, the area in question is only under control and not protected; the difference is pretty high.

1. The controlled zone is to be installed outside, next to the fence. It should be installed at the property border, in at least 10 m width, with all the vegetation in this sector trimmed and cut, providing a proper sight for PPS. The sector in question should be an area sensible for video analytics of thermal cameras (such as virtual fence) and suitable for security patrols, too.
2. For people and vehicles which arrive to the facility, a video entry phone system should be installed, because all the gates must be closed all the time. (Remark: there are no visitors or partners who arrive by chance. All the people coming to the Data Centre [DC] must be reported previously. Those who have swiped the access cards with authorisation can enter; they use the readers of the access system under the security guard check.)

[14] Fast Guard Security Service (s. a.).

[15] Man down feature means that when the user in trouble falls to the ground due to some kinds of accident or illness the radio sends an emergency sign transmitting its accurate location, which can be seen on the screen of dispatch program.

Protected zones

The protected zones can represent the entire physical protection system of a data centre. The requirements which can be found here are general. The results of security risks assessment of any protected buildings would be similar at all facilities where the protected zones are essential. This is the most important part of the PPS of data centres. The protected areas must be well considered and implemented.

Next, I am going to present the most important specifications of the protected zones which can satisfy requirements of professionals and the official regulations as well.

Perimeter protection zone (Zone N1)

1. The perimeter protection zone should be controlled by a complex security system with complex intrusion alarm, CCTV system and swipe access systems, in addition to Security Guards and Respond Force services.
2. Perimeter protection includes virtual fence with thermal cameras extended with video analytics.
3. Supporting the virtual fence, a few speed dome cameras must be installed, which are alarm assessment devices with the required zoom lenses.
4. Nowadays the PPS must be prepared for drone activities, therefore, Pan/Tilt/Zoom cameras have to be installed so that flying objects in the area over the horizon can be controlled.
5. The zone to be controlled has to be created next to the fence, but inside; it should be installed at the property border, in at least 3 m width, with all the vegetation in this sector trimmed and cut, providing the proper sight for PPS. The sector in question should be an area sensible for video analytics of thermal cameras (such as virtual fence) and suitable for security patrols, too.
6. In the 3 m wide sector inside, next to the fence, a cover protection must be implemented by IR or micro-wave barriers.
7. Against violent intruders approaching by vehicles, bollards and road blockers must be implemented. It is essential that the track lane of the approaching route is designed in a way that the speed of vehicles over 3.5 tons (trucks and lorries) cannot reach 40 km/h, due to the blocking capability of bollards or road blockers.
8. The entry side of the vehicle gates have to be equipped with chasses scanner and plate recognition system.
9. For the people and vehicle checks, security guards should be equipped with portable explosion scanner (“electric nose”).

Building protection zone (Zone N2)

1. At the personal entrance of the building, two tripod turnstiles should be installed, where a personal control should be made by Security Guards.
2. The front of the reception area facing the waiting area should be built from bullet proof wall and glass, which means that audio device has to be installed on glass table for speaking through.
3. Different sectors of the building should be approached through tripod turnstiles with card readers and PIN code keyboards. (Two-step authentication method.)
4. Beyond the two-step authentication (possession and knowledge-based access) card readers should be used for individual office accesses.
5. All access points must be controlled by the surveillance system. Depending on the field of view (FOV) and the lighting conditions, 2 MP cameras are supposed to be enough.
6. Visitors should give visitor cards which should be enough for access through the full-height turnstile, but with the configuration of attending card method. (Remark: attending card method means that the visitor card should be joined to another employee's card, after which the visitor can move in the inside of the building together with his/her attendant.)
7. All the people who want to enter the building have to go through a Multi-Zone Metal Detector.

Server rooms (Zone N3)

1. In the server rooms, which is a highly protected area, the use of a biometric authentication method is recommended, together with the use of access cards and the two-step authentication.
2. All access points have to be controlled by the surveillance system. Depending on the field of view (FOV) and the lighting conditions, 2 MP cameras are supposed to be enough. In my opinion, the ideal duration of archiving time would be 30 days, but it depends on the local policy and regulation.
3. Unauthorised access attempts must be immediately sent to the monitor room as a warning message.

Rack frames (Zone N4)

1. Each mechanical locks of rack frames should be changed to specialised electronic driven locks integrated into the access system.
2. Mechanical locks of the side and back doors of rack frames should be sealed, because the security level of the locks is not enough for the required policy.

Conclusion

The 'Best Practices' may be absolutely useful for all people concerned, not just for professionals but the respective partners, too. It is very important that every partner in the foreseen cooperation should speak about the same technical and security problems, knowing that the budgets of security systems may be very expensive if we do not know what we want. An optimised security budget should be supported by a security risk analysis which has to be made before the design process starts.

BIBLIOGRAPHY

Cool, Michael – Corkill, Jeff – Woodward, Andrew (2012): *Defense in depth, protection in depth and security in depth: a comparative analysis towards a common usage language*. Perth, Edith Cowan University, Security Research Institute. DOI: https://doi.org/10.4225/75/57a034ccac5cd

Adams, D. G. – Snell, M. K. – Green, M. W. – Pritchard, D. A. (2005): Between detection and neutralization. In: *Proceedings 39th Annual 2005 International Carnahan Conference on Security Technology*. Las Palmas, 2005. DOI: https://doi.org/10.1109/ccst.2005.1594846

Fast Guard Security Service (s. a.): *What is an armed security officer?* https://fastguardservice.com/what-is-an-armed-security-officer/ (Downloaded: 23. 01. 2020).

Recomended literature

Scalet, S. D.: 19 ways to build physical security into your data center. *CSO*. www.csoonline.com/article/2112402/physical-security/physical-security-19-ways-to-build-physical-security-into-a-data-centre.html (Downloaded: 13.04.2017)

Effective Data Centre Physical Security Best Practices for SAS 70 Compliance. http://www.bing.com/search?q=Effective+Data+Centre+Physical+Security+Best+Practices+for+SAS+70+Compliance&src=IE-SearchBox&FORM=IESR02 (Downloaded: 13.04.2017)