BÁNKI KÖZLEMÉNYEK
1. ÉVFOLYAM 3. SZÁM

The electronic component for the aim of protecting laboratories

A komplex védelem elektronikai komponense a laborbiztonság érdekében

Tamás Berek
* National University of Public Service / Institute of Military Leadership Training, Faculty of Military Sciences and Officer Training, Budapest, Hungary
berek.tamas@uni-nke.hu

Abstract

The state of our future security can be destroyed, besides many definite factors, by the usage of chemical, biological, radiological and nuclear (CBRN) weapons, devices used for peaceful industrial aims, or the chemical, biological or nuclear components of research that are not 'guarded' properly and can be used for criminal aims. Unofficial access to the radioactive and infectious and poisonous materials and the prevention of their expropriation, their defense is of extreme importance. On the other hand, the special staff of the above-mentioned establishments, in certain occupations, has to face risks posed by chemical, biological, radiological sources. However, these risks can be significantly diminished by a properly worked out defense program. For the reason that the workers at dangerous workplaces and the users of dangerous devices and materials would not be harmed by the everyday working conditions and also that by unlawful appropriation of costly devices or dangerous materials or devices containing dangerous materials and this way, the danger posed by these would not get beyond of the controlled working areas or from the territory of the establishment, so the creation of the physical protection of the mentioned areas and equipment is extremely important. After the accomplishment of the concept of property protection, with the planning of the complex security system, the work on the proper rate establishment of security subsystems needs serious analyzing and evaluation. The author shows that with the inducement of the electronic component of the property protection, what characteristics have to be taken into consideration because of the security risks dangerous materials pose.

***Keywords*:** laboratories, complex security system, integrated physical protection

Összefoglalás

Jövőnk biztonsági környezetének állapotát több más meghatározó tényező mellett a CBRN fegyverek, eszközökön kívül békés célú ipari, vagy kutatási kapacitások nem kellően „őrzött" vegyi, biológiai, vagy nukleáris összetevőinek bűnös szándékú felhasználása is ronthatja. A laboratóriumokban és egyéb létesítményekben található radioaktív, fertőző és méreganyagokhoz való illetéktelen hozzáférésnek és azok eltulajdonításának megakadályozása érdekében azok védelmének biztosítása kiemelt jelentőséggel bír. A fenti intézmények szakállománya bizonyos munkakörökben ugyanakkor ki van téve fizikai-, kémiai-, biológiai- és sugárveszélynek, mely kockázatok jelentősen csökkenthetők megfelelően kidolgozott védelmi program kialakításával. Annak érdekében, hogy a veszélyes munkaterületet, eszközöket, anyagokat használók számára ne jelentsen közvetlen veszélyt a mindennapi munkavégzés, illetve a nagy értékű eszközök és veszélyes anyagok vagy veszélyes anyagokat tartalmazó eszközök eltulajdonításával az általuk hordozott veszély ne kerüljön ki az ellenőrzött munkaterületekről és az intézmény területéről, az érintett területek és berendezések fizikai védelmének körültekintő kiépítése létfontosságú. A vagyonvédelmi koncepció kialakítását követően a komplex biztonsági rendszer tervezésekor komoly elemző és értékelő munkát követel meg a védelmi alrendszerek helyes arányainak kialakítása. A szerző bemutatja, hogy a vagyonvédelmi komplexum elektronikus komponensének kialakításakor milyen sajátosságokat kell figyelembe venni a veszélyes anyagok biztonsági kockázata okán.A szerzők pár mondatban foglalják össze a cikk célját.

***Kulcsszavak*:** laboratóriumok, komplex biztonsági rendszer, fizikai védelem

1 INTRODUCTION

In February, 2008, a common EU CBRN work team was organized as a result of the common EU CBRN special policy, whose aim is to diminish the endangerment of the EU citizens from an unexpected CBRN attack.

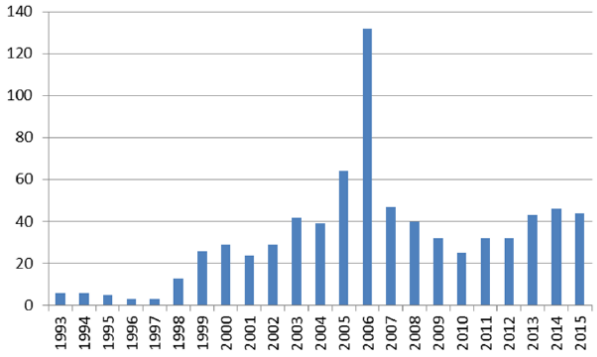
This CBRN work group, taking into consideration the general level of the CBRN endangerment, with the assessment of particular problems, together with other factors, established, with regards to the CBRN prevention that "it is easy to get access to several CBRN materials and turn them into weapons". [1] From the point of view of the risk factors of the CBRN materials that can be mentioned the order mentioned by the work group was ranging primarily from chemical materials, in smaller scale, of biological organisms and radioactive radiation sources.

According to the impact examination, the decision about the development of the EU capacities was made in connection with the fight against CBRN. In prevention, the basic task is to impede any access to legitimately produced or used CBRN materials by any unauthorized persons, including terrorists or other criminals. The first element of

this requirement is to establish authorization and continuous control. The other important element is the control and supervision of CBRN materials. In the publication of 2009 of the European Commonwealth Committee that deals with the strengthening of the chemical, biological, radiological and nuclear security and guaranteeing the proper defense of the CBRN materials and the limitation of the possibilities of their access for inappropriate use. [1]

According to the 2016 report of the International Atomic Energy Agency (IAEA)there were 2889 events reported in connection with radioactive materials between 1993 and 2015, of which 454 events were unauthorized possession and connected crimes, 762 events were proven stealth and 1622 incidents were other illegal activities, in 51 cases the incidents could not be characterized. [2]

The reported thefts and losses included, among others, such radioactive sources as 137-Cs, 241-Am, 90-Sr, 60-Co, 192-Ir which show that the sources are usually portable industrial devices and due to their mobility, they can be easily stolen or lost. It means that it is necessary to improve the efficiency of security regulations and procedures in the future. Thieves are not interested in the possible usage of the radiation source but in the black-market value or the metal mass of the device.



1. figure: Incidents reported to the ITDB involving theft or loss, 1993–2015. [2]
Source: IEAE Incident and Trafficking Database (ITDB)Figure title

There is another worry appearing among specialists in connection with CBRN threats. The significant development of the molecular biology and genetics and the consequent appearance of new laboratories with elevated security levels can be noticed. On the one hand, it makes possible for researchers to research in their own countries such dangerous disease spreaders as SARS crown viruses hemorrhagic fever, the access to which was limited and difficult and on the other hand it carries a risk in other countries where, due to financial problems, it is difficult to take care of the physical protection of dangerous establishments in the long run. Those that show lack of keeping regulations in biological security and biological protection are of potential risk sources. There can be serious abuse by those who are authorized or have access against those who, with the development of certain elements of biological security and defense, the protection elements against of personal abuse should also be developed. Accidents in laboratories or the escape of a dangerous biological materials is not necessarily the result of illegal activities or a sabotage, improper activities in the labs or wrong packaging of dangerous materials and their transportation can also cause the escape of these materials. [3]

2 THE PLANNING CONSIDERATIONS OF THE ESTABLISHMENT OF THE SECURITY SYSTEM

The especially important element of the above-mentioned precautionary measures aimed at the lessening of the security threats is the physical protection of the dangerous materials that can be used for criminal purposes, too. For the formation of the protection of the lab that accordingly to its function needs to operate with different dangerous materials (radioactive, chemical, biological) or needs to detect these materials, certain characteristics need to be taken into consideration.

During the induction and detailing of the endangerment originating from the lab activities and its surroundings, it is important to establish the aim of the protection, the sources of the danger and accordingly, to plan and build the system of protection so that each protectable value and activity is indicated.

For the protection to be continuous and comprehensive, with the buildup of the security system, the separate, independent from each other, autonomous subsystem effectiveness and harmonization as well as the provision of the condition of controlling is necessary. The effectiveness of the physical guarding is provided by mechanical and electric devices together with vitally strong combination of procedures, not to forget about the role of the preventive measures.

A basic document that establishes the order of security provision, it needs to be studied carefully during the defense planning. There is a need for building up a security system where an algorithm that provides supervising conditions for the autonomous operability of the integrated subsystems harmonizes their communication, and at the same time, it provides the possibility for intervention for the supervising personnel within the authority area of the staff of the establishment.

In the interest of the protection system build up, as part of the defense philosophy, risk assessment is necessary. It needs to tackle the question of escaping of the dangerous poisonous radioactive materials into the outer surroundings, as a result of carelessness, criminal aims or even a technical mistake. [4]

The aim of the risk assessment in the given establishment, its operation is the detection, grouping and evaluation of the possible risks in the connection with the activities. During the evaluation the possibility of the risk appearance, their effect as well as avoidance, measures taken to lessen the impact are examined. During the evaluation, the following factors are needed to be considered:

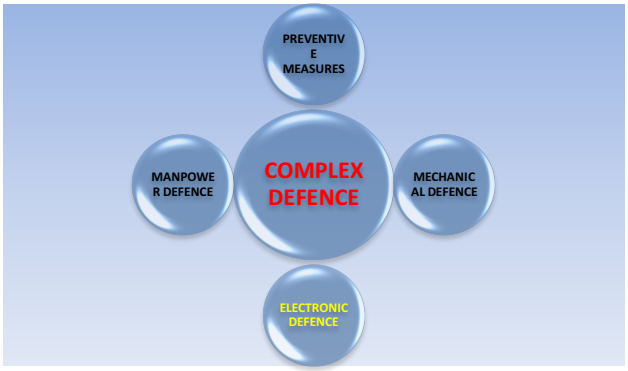
- The surrounding characteristics of the establishment, the criminal statistics of the area
- The architectural, energetic, electronic, IT subsystems
- The operational systems of the establishment, regulations, rules of the authorities
- Basic functions of the establishment, temporary, supplementary functions
- Composition of the personnel and visitors [5]

The size and placement of the lab in its surrounding is of utmost importance and it also needs to be evaluated

previously. During this evaluation, it is necessary to establish the especially important elements of the building that can be an easy target in case of an attack. The examination of the size and placement of the building is important from the point of view of the dangerous areas, places for storing dangerous materials within the building since they are significant for the organization of defense.

It is also important to examine the activities taking place in the establishment. The controlled work areas and work processes brought about within the lab complex, including personnel and the dangerous materials, the protection of the waste collection points is of extreme importance. The same protection applies to areas not considered to be work places and the outer surroundings of the lab.

Materials built into the establishment (technical devices, the use of special building materials, instalment of special technology, etc.), their quality and quantity also defines the establishment of the defense, the security plan of the security service and the acceptance of the future operational regulations. It is not enough to protect the place from the potential criminals, the staff who does the examination of the dangerous materials and the continuous work process also needs to be protected with no less effort. [6]



2. figure: Components of complex property protection
Source: edited by Berek

3 ELABORATION OF THE PROTECTION CONCEPT

The protection concept describes the components, functioning, relationship, methods of operation of the individual elements of the property protection system. It defines the parameters of the necessary mechanical, electronic IT defense subsystems, devices, their interdependency, their functional characteristics, operation, the methods of maintenance. [5]

During planning, it is necessary to indicate those areas where heightened protection is needed due to the presence of sources of danger. Special entrance authorization is necessary. When dangerous areas in labs are protected there is little opportunity to fulfil viral tasks, so it is necessary to increase the rate of the electrical protection equipment and at the same time the strengthening of the inner control is also in the forefront. It is the task of the Lab staff to control the regulations and procedures, to operate and maintain the security systems. It is well-known that the efficiency of the property defense system is determined by the efficiency of the weakest element. In improperly built systems quite often the living component is the weakest link. For the security maintenance of the building, besides the establishing of the responsibility areas, the provision of controllability and as one of its conditions, the formation of the regulation system is very important to prevent breaking the rules or in case of inner sabotage, for the establishment of responsibility and the assurance of its connection to the proper person.

For the lab complex it is necessary to create a building control system when during its operation the need for human intervention comes up in case of mistake correction or in unforeseen exceptional security danger.

According to the above-mentioned the following electronic systems are necessary in the involved establishments:

- Intrusion and attack detention system
- Video surveillance and taping system
- Entrance allowing system
- Electronic fire warning system
- Systems monitoring the presence of dangerous materials

The first three of the above-mentioned elements are mainly components of direct property defense but they also provide protection for activities and people who work in dangerous zones.

3.1 Intrusion detection system

The main aim of the intrusion detection system is the information for the staff about an unauthorized intrusion or its attempt. The properly planned and settled system, with its sensors built directly on the devices of the mechanic protection, informs the staff at the very beginning of the damage of the mechanic protection on the spot by sound and light signs or with distance signs, through the telephone center directly or indirectly. [5]

The planning guidelines pertaining to intrusion systems are introduced in the MSZ EN 50131-1 specification dealing with the “Detection systems, intrusion and attack detection systems. System requirements” The specification ranks the intrusion and attack systems and parts of their elements into the desired level of security. The levels of security are based on the levels of risk which are based on the type of the given establishment, the values found inside and the level of the typically expectable threat. According to the above-mentioned the specification ranks the electronic property protection devices into four security categories. From the low risk 1st stage which deals with the intruder with limited knowledge and having easily accessible manual instruments, to the 4th level security where the intruder is supposedly has high level of special knowledge and special instruments.

For the property protection of labs working with dangerous materials, the intrusion system must be security level 3 or 4.

Level 3. Medium or high-level risk. The intruder or the robber is supposedly well-skilled with intrusion and attack systems. He possesses a large number of instruments, portable electronic devices.

Level 4. High risk. It must be applied when security is the number one priority. The intruder or robber is supposed to be able to plan in detail an intrusion or a robbery. He must have resources and the whole scale of devices including devices capable to substitute the basically important parts of elements of the intrusion and attack system. [7]

The sensors and the special nuclear, biological and chemical detectors, signals coming from meteorological

sensors must be processed by a system that is capable to maintain all of them together and can control the warning and indication units together with the necessary building supervision equipment.

The information provided by the property protection systems inside the buildings, with special attention to the video surveillance and intrusion systems (video images, list of events, address distribution, etc.) and their inappropriate handling can significantly raise the chance of possible theft and can diminish the efficiency of the protection system. Accordingly, the event list of certain centers as well as the stored videos can hide sensitive information from the point of the security of the lab complex, that's why their access must be strictly regulated.

3.2 General requirements concerning access systems

During the planning of the access system of an analytical lab it is necessary to examine, among others, the specifics of the zones of the building, persons with authorization for entrance, the danger sources of the controlled areas in connection with the dangerous materials. It is necessary to define functions expected of the entrance system.

The main function of the entrance system is the inside and outside access to the building as well as regulation of the different levels of movement within the object. Nowadays, besides the determination of the access authorization there is an expected need for the limitation and changeability of the authorization both in time and place. The person following function of the access system is also important since the movements and the presence of the person present in the lab is recorded by the system and it can indicate the number of people and their time spent in the controlled areas. The maintenance function of the "guest card" issued for temporary access is also important from the point of view of the lab.

From the point of view of the lab operator there is an expectation from the access system to have the function of building supervision that makes it possible to switch on and off the ventilation of the airing system as well as the system of cooling automatically depending on the amount of people inside. Nowadays modern software makes it possible that with certain defined outputs connected to the programmed input events the center could be able to perform conditional operations. It can switch on cameras, e.g. at the doors of poison storing, in the case of PLC (Programmable Logic Controller) the air technical equipment can be switched on or off at different times or with event control.

The ability to archive and store events is certainly the highlighted function of the system as well as logging. In the case of a lab, besides the above-mentioned, an important requirement is to monitor the dangerous materials in the lab by a subsystem whose detectors are situated in controlled areas and they can be integrated into the electronic component of a complex property protection system.

Taking into consideration the danger sources of an analytical lab, the access system must be able to operate online. This method of operation provides the installation of several functions important for the security of industrial units and workplaces.

The basic elements of the access system, points installed at the entrance to objects, sites and zones are connected to computer centers through the online systems of the local communication network [5]

This center must be able, even with the operation of several entrance points, to make complicated decisions that need the simultaneous assessment of the number of people present in the controlled zone, their authorization of presence, rights for performing tasks in the lab (the classification of particular persons according to the above-mentioned points), the signals from the detectors of the property monitoring web and other equipment that provides the safe maintenance of the establishment (e.g. airing engines).It is crucial if we need the performance of security decision mechanisms that considers the entire state of the security system of the lab. For example, if in the radiological lab the allowed number of persons, according to the safety regulations is maximum 6, then the entrance for the 7^{th} is not allowed. In this case, of course, it is necessary to support the system with additional elements so as to avoid cheating the system.

The program of the center that provides the online operation of the access system and that also directs the controllers according to the defined authorization, needs to provide the following possibilities:

- In case of being empty, certain zones should be entered only by two persons
- In certain cases, the push bolt of the electronic safety lock needs to be loosened
- In case of zone emptying automatic closure
- Listing of persons inside

Areas where dangerous materials are and there is work with those must be protected by an access system that needs the possession and use of a physical device, such as a proximity smart card. The application of only one identification principle often cannot be considered as a risk rate solution. In the case of especially protected zones the biometric identification or a committee type, including at least two persons, needs to be measured.

It seems that certain biometric based access with personal identification directly to a certain lab zone needs a separate examination since certain specifics of the lab work can exclude certain procedures, for example rubber gloves wearing makes finger printing is impossible. Emergency opening, at the same time, is a basic requirement for each system. The system should make it possible to open the entrance points in case of an extreme event for the sake of escape of the staff inside.

The entrance controls have to have an input that having sensed the warning of the fire system or the disaster warning opens the entrance points automatically. For each entrance point it is necessary to plan a door opening device (panic button) in case of emergency situation. Emergency openers are usually push buttons. In case of danger (or in case of sensing it) by pushing the button the controller, having disrupted the electricity circuit of the electric lock, makes the door possible to open. The emergency buttons should be fitted to the entrance points of the zones protected by entrance terminals, to the labs, next to readers [4]

The access system is an efficient device of protection during work time. With its usage, it is possible to register the identity of those wanting to enter and the time of the entrance.

3.3 CCTV and the electronic article surveillance

During worktime, the protection of the intrusion detection center being in partially sharpened status is supplemented by the CCTV with the help of information

gathering and its storing. The CCTV can provide the lab with significant help in case of possible events. When cameras are set several requirements need to be satisfied. On the one hand, cameras are needed to be placed at points where they can provide assessable recordings according to the aim of application in such way that the recording would show an event important only from the security point of view, or in case of identification, a certain person. When the place of the cameras is created, since the main aim is not deterrence, the site needs to be discreet and at the same time efficiency should not be limited. Offices of the lab, including changing rooms, rooms for cleaning do not need to be monitored by cameras. On the one hand it is not necessary, on the other hand, it disturbs the staff but at the routes of movement, at certain workplaces of the lab (e.g. at the chemical suction booth) a recording of a work procedure can be an important document in case of an accident. The similar surveillance of the poison and isotope storage can be of crucial importance at the identification of the culprit of a robbery or smuggling.

It is natural that The CCTV system cannot hurt the basic rights of the staff, cannot provide information about the research and analytical work. When this efficient element of zone observation is created it is important that the recorded image is fixed according to the data protection rules and the expected image quality and the time synchronization is provided. In case of password access, it is important to place the cameras at an angle where the passwords of the staff cannot be observed or recorded.

From the point of view of security technics, it is important that in the observed dangerous work zones, following an undesirable event, the source of danger is identified and the responsibility is established. The choice of cameras proper for the given aim is influenced by several factors. It is necessary to examine the working environment of the cameras and the resolution of the image coverage. Naturally this specifies the choice of the optics.

When examining the resolution, it can be generally said that high resolution cameras are expensive, so they need to be optimized according to the task. Quite often it is necessary to analyze the information of the image recorded in the lab when procedure detection or identity establishment takes place, so high-resolution cameras are very important in such places. Because of sensitiveness the cameras have to be operated in changeable light circumstances inside, some of them work for 24 hours; consequently, the application of highly sensitive cameras is advisable.

From the point of view of the basic requirements concerning work with radioactive materials the regulation of radiology protection states that “The recording of radioactive materials and their compounds has to be established in a way that accordingly that the types of materials, their quantity, placement, designation and their use can be established and controlled.” To reach this aim RF devices are needed that can be controlled from distance, be resistant to outer impacts (chemical, radiological), can be operated with high level of security, able to perform tasks similar to the functions of the EAS systems. If the need for the above-mentioned security is realized, following the necessary tests, having defined isotopes or samples, the system can immediately warn who and when worked with an isotope as long as the staff the pattern storage, the isotope cupboard and the samples/isotopes are provided with identification devices.

A warning issued by sensors, properly placed in the lab and which monitor the presence of dangerous materials, should also appear in the offices of dispatchers but the neutralization of the intrusion detection system and subsystem monitoring the presence of dangerous materials whose detectors are connected to the warning subsystem, the authorization of measures have to stay within the area of the professional and personal supervision of the lab.

4 CONCLUSION

When a project is created and maintained, where there are materials stored temporarily or operationally, their presence, by itself, is a source of danger. During the planning and inducement of protection in the controlled area, the provision of the highest level of the technical, mechanical, electronic and personal security, is one of the main aspects of the creation of the planned security technology subsystems in accordance with the function of the lab.

To know the type of dangerous materials and storage is vital in order to take appropriate safety measures for prevent an accidental incident. [8]

In an emergency event the controlling system is able to perform several measures simultaneously; its basic task is the prevention of emergency situations, so in case if they happen a vital support of the operation of the system is needed. Monitoring the controlled areas it has to signal immediately so that the operator can intervene immediately. A sensitive part of the complex protection is the information about the technological system and the controlled zones, so the control system needs to ensure that only authorized personnel has access to it. The task of people who work in the establishment is the handling and acknowledgement of warnings, which is a serious responsibility. That is why in the system of control the levels and areas of responsibility have to be precisely defined.

The fact and method of misappropriate unauthorized possession of the dangerous materials and isotopes that are wanted to be used with criminal intentions by those who have authorized access to them cannot be detected and indicated by the intrusion detection system. The proxy card and the access code can be stolen or blackmailed. In such cases the CCTV integrated into the access control system can provide the real identity of the person entering the establishment.

When the protection of the establishments testing dangerous materials is induced, thanks to the proper buildup of the concept of the property protection, the complex security technical system must be able to handle the building supervision and the devices monitoring Dangerous materials together with the elements of property protection system to provide the possibility of operative intervention in a way that together with the expected level of protection, the conditions of work are taken care of without the staff feeling to be threatened.

REFERENCES

[1] A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak a vegyi, biológiai, radiológiai és nukleáris biztonság Európai Unión belüli megerősítéséről – az EU CBRN cselekvési terve {SEC(2009) 790}

[2] IEAE Incident and Trafficking Database (ITDB) a Nemzetközi Atomenergia Ügynökség honlapján http://www-ns.iaea.org/security/itdb.asp (letöltés: 2017. 09.26.)

[3] Berek Tamás - Pellérdi Rezső: ABV (CBRN) kihívásokra adott válaszlépések az EU-ban 2011. Bolyai Szemle XX. évf. 2. szám, ISSN: 1416-1443 http://archiv.uni-nke.hu/downloads/bsz/bszemle2011/2/Berek_Pellerdi.pdf

[4] Berek Tamás: ABV (CBRN) analitikai laboratórium beléptetőrendszere a biztonságos üzemeltetés szolgálatában 2011. Hadmérnök http://www.hadmernok.hu/2011_2_berek.pdf

[5] Utassy Sándor: Komplex villamos rendszerek biztonságtechnikai kérdései, Doktori (PhD) értekezés, 2009.

[6] Berek Tamás - Bodrácska Gyula: Az élőerős őrzés az objektumvédelem építőipari ágazatában , 2010. Hadmérnök, http://www.hadmernok.hu/2010_4_berek_bodracska.php

[7] Móré Attila : MSZ EN 50131-1:2007/A1:2009. Riasztórendszerek. Behatolás- és támadásjelző rendszerek 1. rész: Rendszerkövetelmények in Detektor Plusz, 2010/ 1-2. sz.

[8] Berek Lajos-Solymosi János: Veszélyes anyagok szállításának biztonsága 2015. Bolyai Szemle XXIV évf. 2. szám, ISSN: 1416-1443 https://folyoiratok.uni-nke.hu/document/uni-nke-hu/bolyai-szemle-2015-02.original.pdf