Original article
Dependability, vol. 18 no.4, 2018 DOI: 10.21683/1729-2646-2018-18-4-51-55

Ensuring an efficient transportation infrastructure security system by means of solutions that enable detection of intrusions into protected areas

Natalia A. Kuzmina, *Far Eastern State Transport University, Khabarovsk, Russia*

Natalia A. Kuzmina

Abstract. *Due to the nature of its operations, the transportation industry in itself is a potential source of danger. In case of unlawful aggressive intrusions the danger becomes real and fraught with grave consequences. The statistics of the last 10 to 15 years show that 50 to 70% of accomplished terrorist attacks were associated with transportation. Individual measures cannot ensure transportation security. The problem must be approached comprehensively and systemically. Transportation security greatly contributes to the national security of the Russian Federation. The Federal Law of February 9, 2007 no. 16-FZ On transportation security, for the first time in Russian practice, raised the question of securing the entire transportation industry of the Russian Federation, established the legal foundations of the activities related to the protection of transportation infrastructure and vehicles against acts of unlawful interference, including those of terrorist nature. For the first time, a single systemic approach to anti-terrorist protection is provided for all means of transportation. The transportation industry is quite vulnerable to terrorist attacks. We are talking about vehicles, transportation lines, stations, vehicles carrying dangerous loads. The vulnerability of transportation is due to the possibility of damage to signalling, automation and communication assets, whose protection is complicated due to the scale and extent of Russia's railways. Despite the problems and objective difficulties related to the legislation in the area of transportation security, the workers of the Russian railway industry make their best effort to ensure protection of transportation infrastructure and vehicles against acts of unlawful interference. Promptly reacting to other challenges and threats, they ensure reliable operation of the transportation industry, thus preserving the peace and safety of our citizens. This paper examines matters related to ensuring efficient safety of transportation infrastructure. A significant emphasis is placed on the systems that enable detection of intrusions into protected areas of a facility.*

Keywords: *transportation security, act of unlawful interference, transportation infrastructure facility, security system, facility protection, intruder, sensors, annunciator.*

For citation: *Ensuring an efficient transportation infrastructure safety system by means of solutions that enable detection of intrusions into protected areas. Dependability 2018;4: 51-55. DOI: 10.21683/1729-2646-2018-18-4-51-55*

Despite the measures taken by transportation infrastructure managers and carriers that aim to improve the protection of the transportation industry, the threat of acts of unlawful interference (AUI) remains. Statistics show that, unfortunately, it is not yet possible to completely eliminate the possibility of an act of unlawful interference. In this regard, the priority task is to hinder AUI attempts against transportation infrastructure facilities and vehicles as well as to disrupt the intruders' plans.

This is only possible if the government and the society deliver a consolidated approach to the security issues [1].

The Federal Law no. 16-FZ On transportation security makes it compulsory to protect transportation infrastructure facilities against AUIs [2].

Protection, as a rule, involves the availability of technical means of protection that correspond with the facility's category.

This approach does not include an efficiency assessment of the measures taken and the ability of the whole system to meet real threats. There is no guarantee that in case of an emergency situation the response will be prompt and correct.

What should be an effective security system for the facility and how to protect it? This issue is relevant today for many transportation infrastructure facilities, which face the difficult task of ensuring transportation security.

At the beginning of 2014, the Federal Law no. 15-FZ On Amendments to Certain Legislative Acts of the Russian Federation on Transportation security came into force. With this document the gaps of the Federal Law no. 16-FZ On transportation security issued in 2007 were eliminated. This basic law had an extremely broad interpretation, and did not contain specific requirements to the forces and means of ensuring transportation security, and in some areas only formalized the process [3].

Under a comprehensive approach to ensuring the security of transportation infrastructure facilities, the reasons that enabled a terrorist attack should be considered as symptoms of unsatisfactory operation of such facilities, whose improvement must be the focus of the efforts, application of human and material resources.

According to the theory of the multiplicity of causes of emergency situations proposed by D. Peterson, Professor of University of Colorado (US), it is possible both to predict the possibility and identify the circumstances of their occurrence. Consequently, security, in transportation included, not only can, but should be controlled as any other part of the transportation system. Transportation security should be one of the inherent, daily functions of the chief executive officers and managers in various positions (among such functions could be cost reduction, enabling the required volume of freight and passenger traffic).

When solving problems of ensuring security of transportation infrastructure facilities, systems that allow detecting intrusions into protected areas play a major role. For this purpose different system control panels are used that notify about intrusions into protected areas with an indication of the place and time of violation of the area boundary. These systems ensure data collection from sensors that monitor the area of possible intrusions, detecting the fact of unauthorized entry and transmission of alarm to the system control panel. The system control panels are often integrated with fire warning systems and have practically the same structure.

The area protection system includes centralized control equipment, input control equipment (ICE) or panels (ICP) and control sensors of the protected area. A computer or special control panel that fulfills its function in some systems enables the centralized management of the system. ICE supplies power to loops with the associated sensors in the area, receives and analyzes the messages transmitted by the sensors, generates and transmits the alarm to the centralized control station, controls the warning devices and other security systems. In small facilities the ICE can control all systems without data transmission to the centralized control station.

Various annunciator sensors that differ in type, operating principle and functionality are employed in system control panels to monitor the areas of potential intrusion. Among such sensors are magnetic, vibration, photoelectric, microwave, ultrasonic sensors, loops, glass break sensors, motion sensors.

The most simple, cheap and widely used sensors are *magnetic contact sensors* installed on windows and doors of the protected facilities. These sensors include a magnetically controlled contact (seal switch) installed on the moving part of the window and a permanent magnet installed on the window or door frame.

An example of such sensor is the IO-102-14 (SMK-14, seal switch) compact removable magnetic contact security annunciator used for doors and windows protection (Figure 1, a).

Glass break sensors (Figure 1, b) react to the sound of breaking glass and are designed for the windows of protected facilities. The principle of sensor operation is based on the spectrum analysis of the detected noise and its comparison with the reference sound signals recorded in the sensor memory. The most advanced sensor types sound a warning signal in two cases: glass being hit and sound of breaking glass.

Vibration sensors (Figure 1, c) detect vibrations and shocks associated with attempts to destroy the protected facility. The operation principle of such sensors is based on the piezoelectric effect or electromagnetic induction for conversion of vibration signals into analyzed electric signals.

Photoelectric infrared (beam) sensors (Figure 1, d, e) are used for protection of corridors, flights of stairs, gates and entrances, as well as for the facility perimeter protection.

At the core of sensor operation is a barrier of modulated infrared beams created by special emitters for the purpose of protection of a facility's secured area. When an intruder crosses the barrier's sensitivity zone, an alarm is triggered.

Loops of security alarm systems are bands of aluminum foil glued to components of protected structures (glass, door etc.) and included in the security alarm circuit. If a structure with a band is destroyed, the security alarm circuit is broken and an alarm is triggered.

Motion sensors allow detecting movement in protected areas based on the changes in the intensity of infrared radiation when heat-emitting objects move within the sensor's sensitivity zone. As an object moves, infrared radiation reflects from different segments of the optic system that causes the generation of a number of impulse signals detected by the

a *b* *c* *d* *e*

Figure 1. a) IO-102-14 (SMK-14, seal switch) magnetic contact annunciator; b) IO329-3 Arfa glass break sensor; c) Shorokh-2 (IO-313-5/1) surface vibration security annunciator; d) NR110QS four-beam infrared barrier sensor; e) application scheme of radial sensors

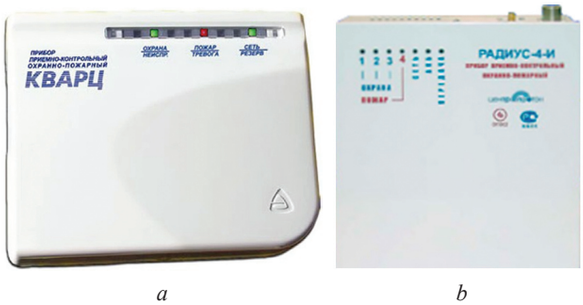
electronic sensor system. To protect against false triggering, today's motion sensors use microprocessors that process detected signals. Two types of infrared passive annunciators of the Foton family are presented as an example of motion sensors in Figure 2.

Along with the above types of annunciators, radio-wave, ultrasonic, micro-wave, capacitance-type sensors can be used in a security alarm system, whose operating principles are based on the analysis of signals reflected from an object or on the changes in the area and capacity of the protected facility. However, these sensors are much less widely used, since they are very sensitive to the environmental changes, type of the protected facility and various destabilizing factors.

Alarm annunciators transmit information to another mandatory structural component of any security system, i.e. ICE or ICP in case of smaller facilities. The function of the ICE is hardware performance verification, collection and analysis of the information received from annunciators, alarm transmission to the security panel, management of light, sound and fire warning signalling, as well as management of other technical equipment and systems of facility protection. The Quartz, Radius, Signal, Rif devices are examples of input control, security and fire equipment.

Quartz (Figure 3, a) is a fairly simple ICE that enables power supply and supervision of one loop with connected security and fire annunciators.

This device also controls emergency voice alarm communication systems and sends warning signals to the central monitoring panel.



a *b*

Figure 3. Input control equipment: a) Quartz; b) Radius-4I

The Radius-4I and Radius-6I input control, security and fire alarm equipment (Figure 3, b) used in the railway industry can be applied both for centralized and autonomous protection of facilities against unauthorized access and fires.

Radius-4I allows monitoring 4 loops; Radius-6I allows monitoring 6 loops with associated security and fire annunciators. After receiving a signal from an annunciator, the device sends a warning signal via communication channels as well as alerts of protected area intrusion or fire by means of light and sound signals. Both devices indicate the loop status using LEDs. The operating temperature range of the device is -10°C to +50°C, which allows it to be used widely in the protection of various facilities.

a *b*

Figure 2. Motion sensors: a) Foton-9 infrared passive alarm sensor; b) Foton-21 electrooptical ceiling-mounted security annunciator

Protection of geographically distributed fixed facilities involves the use of radio communication-based security systems that use a radio channel for transmission of intrusion and fire alerts. Rif String-202 is an example of such systems. This system includes a base station located in the security center, a monitoring panel and a computer, as well as input control equipment with transmitting devices installed in the facilities. One control panel allows controlling up to 600 10 MW transmitting devices (installed in the facility). Depending on the local topography, the system's range of communication varies from 25 to 50 kilometers or more with the help of ultra-narrow band communication channels and noiseless coding. The system uses digital filtering, simultaneous and parallel processing of all signals received via different communication channels from the controlled facilities. The input control equipment transmits each new message over a new frequency randomly selected from 1024 preprogrammed communication frequencies. Equipment operability is verified with each facility transmitter sending a pilot signals to the base station once per minute. Rif String-202 operation does not require authorization documents due to the use of licensed frequencies and low-power transmitters.

For total control of large areas, radio communication-based security systems can also be used that collect data from radio warning sensors installed around the facility area. In this case sensors are installed around the whole territory of the protected facility in such a way as to make sure the distance between them does not exceed the sensor operation radius, which ensures foreign object detection and does not create so-called dead zones. When a person or a foreign object enter a sensor's sensitivity zone, the sensor identifies it as an emergency situation and sends a warning signal to the system control panel via the radio channel.

In many cases, it is sufficient to control the perimeter to ensure security and completely eliminate the possibility of an unauthorized entry into the territory. Such

systems are called perimeter security systems. They are indispensable for facilities taking up large areas, such as airfields, warehouses, transport and logistic hubs, as well as extended facilities, such as railways and motorways, pipe lines etc.

Perimeter security systems allow detecting trespassing of protected areas and sending a warning signal much earlier than an intruder can reach important facilities located around such area. These systems are often structurally related with the physical fence of a protected facility, therefore, their operation directly depends on the physical parameters of the fence, presence of vibrations, materials used, as well as the equipment locations, quality of installation and a number of other factors.

To ensure reliable facility protection, perimeter security systems shall meet specified requirements, such as:

- total control of the whole perimeter of the protected facility and absence of "dead zones"
- high sensitivity of intruder detection
- low probability of false triggering
- dependable operation in terms of electromagnetic interference from active equipment and industrial facilities located nearby
- dependable operation in various climatic conditions.

Currently, beam, radio wave and capacitance-type perimeter security systems are most often used to ensure facilities security. These systems have high efficiency of detection and allow reliable protection of an area. However, beam-based systems, such as infrared barriers can effectively control only straight sections of the perimeter. Radio wave-based systems are sensitive to surface geometry and work poorly if there are trees or bushes in the protected area, which is typical for railways and motorways. Capacitance-type systems require the presence of a physical fence around the facility, since they detect the electric field and capacity changes as the intruder approaches or touches such fence.

Wire and radio wave systems can also be used to protect extended facilities. Such systems consist of two parallel feeders installed along the protected area. One of the feeders serves as a receiving antenna, and the other is a transmitting antenna. If a foreign object gets within the feeder's operating range, field distortion ensues, which modifies the parameters of the received signal that is constantly picked up by the respective equipment.

The radio communication-based security systems under consideration are normally integrated with video surveillance systems, since potential intruders must be identified.

Naturally, all decision-making in a security system relies on humans. They monitor the status of technical assets, receive warning signals, control the response actions. Despite a clear action plan, strict compliance with the transportation safety requirements as regards railway infrastructure and rolling stock, in non-typical situations the natural human factor may come into action due to fatigue, confusion and even negligence. Then, an error or delay in responding to threats can cause loss of human life [4].

Over the last few years, a number of terrorist attacks were carried out in transportation facilities or using vehicles. Both Russian and international statistics are clear. Thus, ensuring the security of transportation infrastructure facilities and vehicles against intentional acts of unlawful interference in the form of terrorist attacks and sabotage has become a pressing problem around the world [5].

In 2017, 670 acts of unlawful interference were registered within the Russian railway system. Among them are cases of terrorist nature, including 68 reports of threats of terrorist attacks. 142 foreign objects were uncovered on tracks. 79 and 269 cases were registered of railway tracks and signalling systems dismantling, respectively.

Also in 2017, 5 cases of explosive substances and 665 cases of unattended suspicious objects were detected in railway facilities. 20 units of firearms, 1292 bullets of various calibers and 49 explosive objects were confiscated [6].

Meanwhile, the experience of the US, Canada and a number of European countries shows that the improvement of transportation security is a major concern not only for the Government. The problem is very urgent and public organizations are actively involved in it. For example, in the US hundreds of private companies and firms managed by non-governmental organizations regularly allocate significant shares of their annual budgets to research and development of solutions in the area of transportation security. The above observations show that both the concern of radical and urgent improvement of transportation security and allocation of financial, organizational and human resources should not be the burden of the Government alone. Additionally, even the best designed transportation security system cannot function effectively without an all-around support of the civil society.

Summarizing, it should be reminded that one of the primary tasks of a transportation infrastructure company or operator is to ensure human security. Security is one of the key conditions for the development of an individual, a society or a Government. This always requires people to be competent as regards the threats and methods of protection.

Application of physical protection assets in combination with organizational measures and actions of transportation security units is the primary factor of detection and response to acts of unlawful interference against property, freight and individuals in railway facilities.

An efficient security management system is like a good soldier who is responsible for the accurate and timely execution of assigned duties and tasks both in peace and war time. It also creates a comprehensive vision of the situation and minimizes the probability of a mistake [7].

References

[1]. Starovoytov AS. Zashchishchennost obiektov transporta neobkhodimo podderzhivat [Security of transportation facilities must be maintained]. Transportnaya i tekhnologicheskaya bezopasnost 2017;2:100-101 [in Russian].

[2]. Federal Law of 09.02.2007 no. 16-FZ On transportation security [in Russian].

[3]. Federal Law of 03.02.2014 no. 15-FZ On amendments to a number of legislative acts of the Russian Federation concerning transportation security [in Russian].

[4]. Order of the Government of the Russian Federation of 26.04.2017 no. 495 On the approval of transportation security requirements, including the requirements for antiterrorist security of facilities (territories) subject to security levels for various categories of transportation infrastructure facilities and railway vehicles [in Russian].

[5]. Kuzmina N, Odudenko T. Ensuring transportation security in the transport infrastructure and means of railway transport facilities. In: Proceedings of the XV International Academic Congress Fundamental and Applied Studies in the Modern World. Oxford (United Kingdom): Oxford University Press»; 2016.

[6]. <www.roszeldor.ru.>

[7]. Protsess evoliutsii ne ostanovit [The evolutionary process is unstoppable]. Transportnaya i tekhnologicheskaya bezopasnost 2017;2:34 [in Russian].

About the author

Natalia A. Kuzmina, Candidate of Pedagogy, Associate Professor of the Department of Transportation Management and Transportation Security, Far Eastern State Transport University, Khabarovsk, Russia, e-mail: kuzminaprepodavatel@mail.ru

Received on 10.01.2018