sustainability

MDPI

Article

Designing of Intelligent Video-Surveillance Systems in Road Tunnels Using Software Tools

Tomáš Loveček, Martin Boroš, Katarína Mäkká * and Ladislav Mariš

Faculty of Security Engineering, University of Zilina, Univerzitná 1, 010 26 Žilina, Slovakia
* Correspondence: katarina.makka@fbi.uniza.sk

Abstract: Video Surveillance Systems (VSSs) are integral parts of road tunnels. Currently, they perform a number of functions, such as ensuring the protection of tunnel technologies, monitoring tunnel operation, or recognising license plates. If VSSs are to be designed to protect the tunnel and its technologies from unauthorised intentional human activity, it is necessary to ensure that they are designed in such a way as to meet the essential functionality requirement of the physical protection system (PPS). In this case, the VSS, as one of the alarm systems, should perform the function of early intrusion detection. The verification of the functionality of the PPS is possible using a software tool to model and simulate various intrusion scenarios. This article provides an example of the use of the SATANO software evaluation tool. The VSS enables multiple applications, such as monitoring, detection, knowledge, and identification. In this paper, the defined current standardised requirements for the design of VSSs in tunnels are considered from the point of view of their possible use for intelligent video analysis, enabling the recognition of various risk situations (e.g., faults or accidents of vehicles). Using the software tool, IP Video Design Tool, the requirements for the design of cameras in tunnels are assessed and adapted from the perspective of the use of intelligent video analysis. In the event that there is a requirement to use the VSS during emergency situations (e.g., fire), it is necessary to assess the operating conditions and period of time through which the VSS would operate in a given tunnel. This article presents the results of the simulation of the spread of a fire in a tunnel and its impact on the operation of the VSS.

Keywords: video surveillance system; tunnel; model and simulation; designing; software tool

Citation: Loveček, T.; Boroš, M.; Mäkká, K.; Mariš, L. Designing of Intelligent Video-Surveillance Systems in Road Tunnels Using Software Tools. *Sustainability* **2023**, *15*, 5702. https://doi.org/10.3390/su15075702

Academic Editors: Tomáš Tichý and Rastislav Pirník

Received: 13 February 2023
Revised: 8 March 2023
Accepted: 18 March 2023
Published: 24 March 2023

1. Introduction

The requirements for the protection of assets against the intentional actions of unauthorised persons in order to damage, destroy or steal a protected tangible or intangible property located in the object and owned or managed by a natural or legal person are determined primarily by generally binding legal regulations and the technical and national requirements of insurance companies or other third parties, such as parent companies or strategic customers.

The Slovak Republic, with an area of 49,035 km^2, currently has a total of 36 motorways and expressway tunnels in operation, under construction, or in the construction-planning process [1]. In 2011, the Ministry of Transport, Construction and Regional Development of the Slovak Republic, Section of Road Transport, Roads and Investment Projects, processed a document containing the requirements for risk analysis in tunnels (TP 02/11) [2]. The subject of TP 02/11 is the creation of a uniform methodology for the analysis of safety risks in road tunnels in accordance with the Regulation of the Government of the Slovak Republic No. 344/2006 Coll., on the minimum safety requirements for tunnels in the road network [3].

The methodology for risk analysis, according to TP0 2/11, concerns threats related to failures and accidents (collisions) as initiating events. From these triggering events, scenarios are then generated by combining different types of accident (accidents involving

a single vehicle, accidents in one-way traffic involving two or more vehicles moving in the same direction, etc.) and their possible consequences (e.g., fire as a consequence of a breakdown, fire as a consequence of an accident, dangerous goods catching fire, and the release of hazardous substances). The scenarios in the TP 02/11 methodology were developed using the Event Tree Analysis (ETA) method.

The assumed branches of the Event Tree give rise to 36 generic damage scenarios with different combinations of mechanical events, fire events, and/or dangerous-goods events, with different levels of vehicle involvement. There are a number of possible causes of initiating events that result in vehicle(s) crashes in road tunnels. According to their basic division, these can be intentional and unintentional. Currently, the likelihood that the cause of an incident is an unauthorised person deliberately acting to damage, destroy, or steal road-tunnel equipment increasing. These initiating events have many possible causes, including hacking attacks on the tunnel's central control system or a physical attack by a booby-trapped explosive system placed in the tunnel tube or in the vehicle itself passing through the tunnel.. In order to investigate these events, it is advisable to use the Fault Tree Analysis (FTA) method.

Where there are requirements for the protection of an object, there is often a need to take certain security or protective measures, which should be arranged in such a way as to ensure the protection of the property of the owner or operator of the object (e.g., a road tunnel).

In the case of road tunnels, in addition to the above-mentioned technical regulation, TP 2/2011, there is no other national or European generally binding legislation defining the requirements for the tunnel's physical protection system (PPS) against the intentional damage to or destruction or theft of road-tunnel equipment by unauthorised persons [2]. In terms of the significance of a road tunnel, it can be part of a national or European transport infrastructure. In this case, the requirements for its protection are defined by Act No. 45/2011 Coll., on Critical Infrastructure [4], which describes a system of security measures designed to protect an element of critical infrastructure, combining mechanical barriers, technical security devices, the security features of information systems, physical protection, and organisational and control measures. The national law is a transposition of the European Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [5]. Even if the tunnel in question is an element of national or European critical infrastructure, there is no methodological guidance specifying how the PPS is to be designed to ensure it provides a certain minimum required level of protection.

Based on [4], the operator of critical infrastructure must set the range of protective measures to protect the critical infrastructure element (CIE) based on the assessment of the threat of disruption to or the destruction of the CIE. The operator must process a security plan that includes the risk evaluation of the threat of disruption to or destruction of individual facilities of the element, their weak points (vulnerabilities), and the estimated consequences of their disruption or destruction for the functionality, integrity and continuity of the element's activity.

Furthermore, according to [5], risk analysis means a consideration of relevant threat scenarios in order to assess the vulnerability to and the potential impact of disruption to or the destruction of critical infrastructure.

International norms and generally binding legal regulations do not further specify how the threat of disruption to or destruction of individual CIE facilities should be processed. One option is to use a software tool for the evaluation of the PPS (e.g., SAVI, SAPE, SATANO).

In the Slovak Republic, there is methodological guidance for constructions falling within the energy and industrial sector; the Ministry of Economy of the Slovak Republic (MH SR) issued methodological guideline no. 29014/2014-1000-53190 MH SR, on security measures for the protection of critical infrastructure elements in the energy and industry sectors [6].

In general, the requirement of the national and European generally binding legislation is to create a PPS that, as an expedient way of arranging security measures, makes it possible to prevent an unauthorised person from achieving their objective, which may be, for example, the theft, damage or destruction of a protected object of interest. The PPS can be understood as a system implemented by technical and regime security measures, which can be divided into alarm systems, mechanical barriers, security services, and regime measures [7,8].

Mechanical barriers serve to deter, slow down, or stop an unauthorised person or intruder, while alarm systems serve to detect the intruder and, trigger an alarm. Security services are integral parts of the PPS; they ensure timely intervention and the detention of the intruder. The mode protection ensures the proper functioning of these security measures [9].

Currently, some of the above-mentioned PPS elements are implemented in real conditions in road tunnels in Slovakia. Video Surveillance Systems (VSSs) are the most frequently implemented [10]. The purpose of these devices is, in most cases, to monitor the situation in road tunnels. They are also used to detect intruders or, subsequently, to identify them. For example, the Branisko tunnel uses 71 fixed cameras with remote parameterisation to monitor situations in the tunnel and in transverse connections. There are two rotating cameras located in front of the tunnel portals. In certain cases, other alarm systems, such as Intrusion and Hold-Up Alarm Systems (I&HAS), Electronic Access Control Systems (EACS), or Alarm Transmission Systems (ATS) with a link to Monitoring and Alarm Receiving Centres [11–15] are implemented in tunnels. The requirements for these systems are defined by technical standards and depend on the degree of risk, the type of offender envisaged, or the nature of the object. In the case of VSS space security, standard EN 62676-1-1 defines four levels of security (Table 1), depending on the type of object and/or the size of the risk [11].

Table 1. Security levels of VSS [11].

Degree of Security	Degree of Security	Requirements	Object Type
Level 1	Low risk	The VSS has no intrusion protection and monitoring of basic functions is not required.	Small storage areas (<400 m^2) for products of low attractiveness (vegetables or newspapers). Companies whose activities do not indicate an impact on values (life, health, property) or confidential information (e.g., a sugar factory).
Level 2	Low-to-medium risk	The VSS system has simple intrusion protection and no monitoring of basic functions is required.	Large storage facilities (>400 m^2) for products of low attractiveness. Companies whose activities do not indicate an impact on values or confidential information (e.g., medical laboratories, paper mills, feedstocks, etc.).
Level 3	Medium-to-high risk	The VSS system has medium intrusion protection and is required.	Large storage facilities (>400 m^2) for products of medium attractiveness (e.g., shopping centers). Companies whose activities may affect values but not confidential information (e.g., public buildings, ports, airports, banks, etc.).
Level 4	High risk	The VSS system has high intrusion protection and monitoring of basic functions is required.	Storage space of products of high attractiveness (e.g., jewels, regulated drugs). Companies whose activities may affect values and confidential information (e.g., mobile phone points of sale, military laboratories, government buildings, etc.).

According to EN 62676-4, a threat assessment and risk analysis should be carried out prior to the design of a VSS [16]. Threats to premises should be identified and their likelihood and impact should be assessed subsequently. A risk assessment should be carried out and the VSS should be designed to mitigate these risks. All risk-related processes should be carried out in accordance with ISO 31 000:2018 [17], which defines the basic general principles for risk management.

Although the requirements for the parameters and the functionalities of alarm systems are defined by individual technical standards, the question remains over how to design an entire PPS to meet certain minimum requirements for its effective application. Since no general binding regulation or technical standard specifies comprehensive requirements for the protection of road tunnels, it is necessary to base tunnel-protection systems on a minimum level of functionality.

To model a PPS, it is necessary to create one for each and every particular road tunnel. First of all, it is necessary to select which elements, devices, or spaces are potential targets for intruders. Subsequently, it is necessary to determine the dislocation and parameters of existing or proposed protection elements on which the values of the input parameters will be based (e.g., the breakthrough resistances of mechanical barriers, probabilities and detection locations, the reaction times of the intervention unit, or intruder-movement times). Based on obtaining all the necessary data for the input parameters and map documents, it is possible to create a model of the road-tunnel-protection system and then conduct and evaluate possible simulations of attack scenarios.

2. Materials and Methods

In the case of setting a minimum level of protection, a quantitative approach based on the basic principle of functionality is used, according to which it is necessary to use so many elements of protection that the intruder is eliminated by the intervention unit before their objective is achieved [10]. To create possible attack scenarios and analyse the vulnerability of a given object, it is possible to use one of the existing software tools. Three software tools are standard components of PPS-assessment approaches in this area:

- SAVI (Systematic Analysis of Vulnerability to Intrusion);
- SAPE (Systematic Analysis of Physical Protection Effectiveness);
- SATANO (Security Assessment Of Terrorist Attack In A Network Of Objects).

The comparison of these three tools was elaborated via a set of criteria reflecting the defined conditions [18]. The SAVI software tool (1987) is the first in this area, and many other tools used in practice implement its principles. In assessments by PPS SAVI, a deterministic algorithm and simple methods of ASD display are used. The SAPE software tool (2009) expands the SAVI principles with a new 2D model of the protected area, also using the heuristic algorithm of the calculation. As a brand-new tool for PPS assessment, SATANO (2016) enables the simulation of the attack-vector modification, e.g., the representation of an entity with the specific characteristics of detection, deceleration, or elimination.

The SATANO (Security Assessment of Terrorist Attack in a Network of Objects) software tool, developed at the University of Žilina, in Žilina, is a simulation tool that allows users to quantitatively assess the level of PPS on various 2D-map documents (Figure 1). The software tool was created as one of the outputs of the CI-PAC project: Critical Infrastructure Protection Against Chemical Attack (HO-ME/2013/CIPS/AG/4000005073).

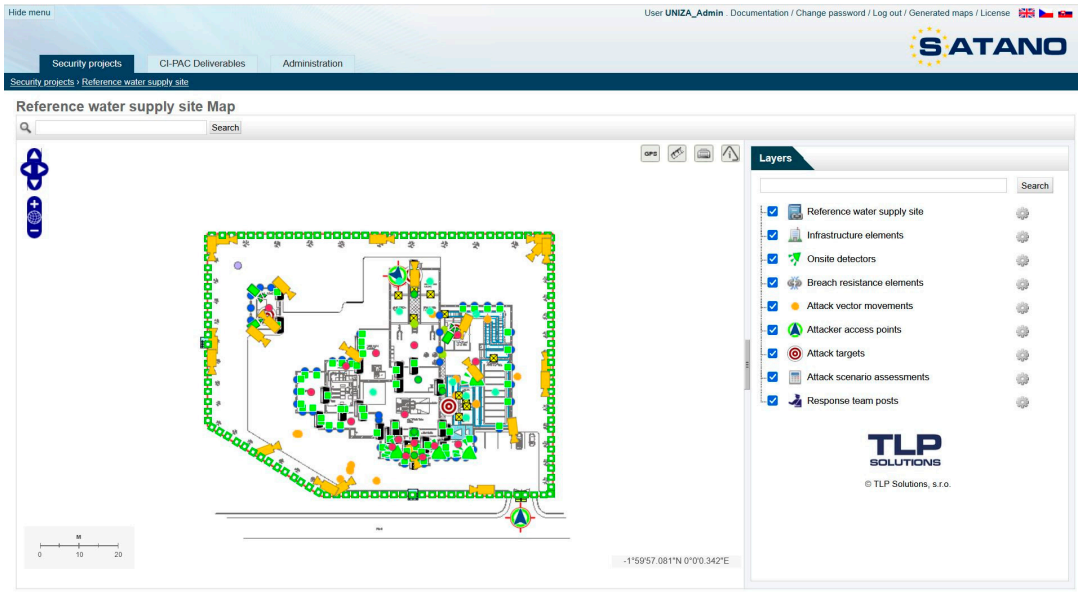


Figure 1. GUI software tool, SATANO: Security Assessment of Terrorist Attack in a Network of Objects.

The SATANO SW tool is based on the basic premise of system functionality, i.e., that it is necessary to use so many security measures that the intruder is detected and intercepted by the intervention unit before reaching their objective, which is considered to be damage to or destruction of the protected object of interest. The tool excludes any random influences that may interfere with intrusion into a protected area. The intruder is presumed to have all the necessary information on the protected object of interest (decided on the basis of certainty) and to know the shortest path to the protected object of interest, which is determined by the total time taken to breakthrough all barriers, including the times required for the transfer. This total time is calculated from the first point at which the intruder is detected by the alarm system (e.g., VSS).

In Annex No. 2 of Government Regulation No. 344/2006 Coll., one of the measures described is that in all tunnels with a control centre, video surveillance systems and a system capable of automatically reporting a traffic failure (such as stationary vehicles) or a fire are installed [3]. The requirements for the design, implementation, operation, and maintenance of camera surveillance, the automatic traffic-incident detection (AID) system, and the automatic recognition system are defined in the methodological guideline TKP 40, defining the technical and qualitative conditions (TKP). In the case of tunnels, camera surveillance is part of tunnels' safety equipment and is always connected to the central control system. Specifically, IP cameras are divided into [18]:

- security cameras in tunnels;
- cameras designed to monitor traffic in tunnels;
- cameras designed to recognise vehicle-registration numbers;
- mini-dome or bullet cameras, installed in the escape corridors of tunnels.

The cameras designed to monitor traffic in tunnels are fixed in tunnel tubes and bays. Their main purpose is to monitor and evaluate the fluidity of traffic, or to monitor certain installations of technological equipment in tunnels. These cameras are always equipped with software for AIDs.

The surveillance cameras in tunnels are fixed or PTZ cameras, which are specifically installed in tunnel tubes, in escape and connection corridors, in technology rooms, and in other service areas of tunnels, such as boarding areas, entrances to areas with objects of interest, etc. Their main purpose is to monitor the movement of persons in escape and connecting corridors with a focus on the safe escape of persons from tunnel pipes, the

protection of premises with technological equipment, etc. These cameras are not equipped with or connected to the AID module. The AID system allows lane tracking and evaluation at the same time [19] in situations involving or requiring:

- stationary vehicles;
- driving in the opposite direction;
- sudden drops in speed;
- traffic-density monitoring for normal, dense, slow, congested, and stopping-and-moving traffic;
- smoke in the tunnel;
- pedestrians;
- a dropped object on the road (e.g., lost cargo, etc.).

For the functionality of the AID system, the standard [19] defines the minimum values of technical parameters such as the type of sensor, coding, minimum resolution, light sensitivity, number of frames per second, signal-to-noise ratio, backlight compensation, automatic white balance adjustment, AGC function, video-image detection, etc.

The cameras in tunnel tubes need to be positioned in such a way that the entire tunnel tube is covered by the camera footage, so that the camera footage includes all the entrances to escape corridors, bays, SOS cabinets, pavements, and access points to other technological equipment, without restricting the view of the passing cross-section. To this end, the design of the deployment of cameras is undertaken at the design stage, but only after all the other technological facilities are deployed.

When deploying cameras for traffic evaluation in a tunnel, each camera is must have the subsequent camera in its frame, with an overlap of at least 15 m to 20 m. A maximum distance of 80 m between cameras is required (for a straight tunnel pipe). For arches, each camera must see the following camera with a sufficient overlap, of at least 15 m to 20 m, over the entire width of the tunnel tube (Figure 2).

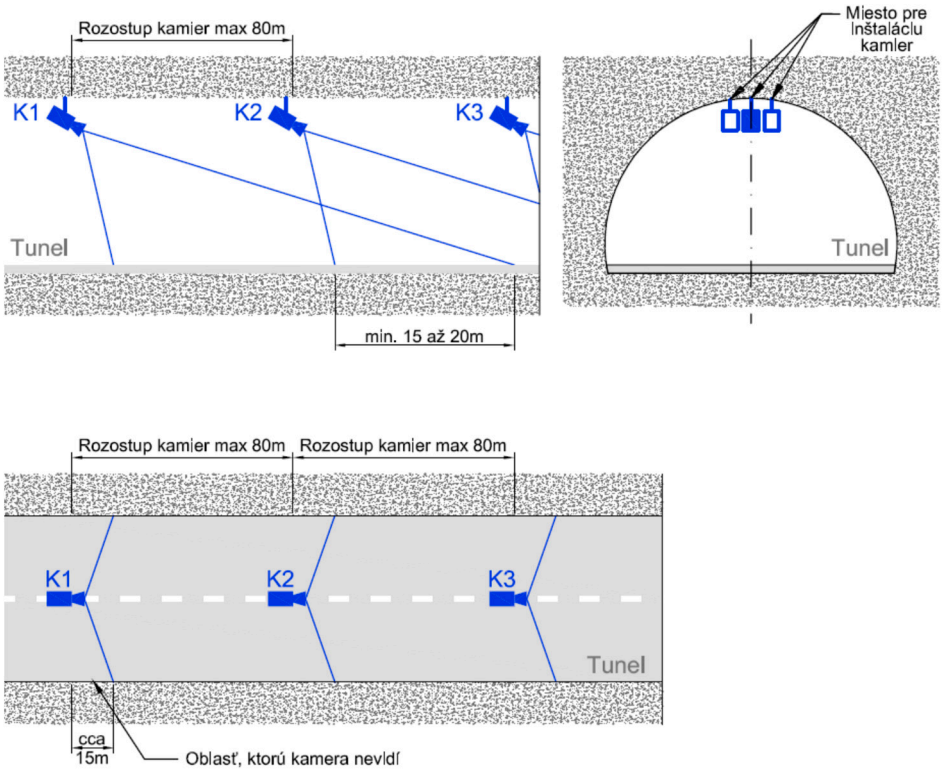


Figure 2. Installation of cameras in tunnel tube for traffic monitoring (TKP 40). Legend: Rozostup kamier max. 80 m, spacing of cameras, max. 80 m; Miesto pre inštaláciu kamier, place for camera installation; Oblasť, ktorú kamera nevidí, area that the camera does not monitor.

Figure 2 shows that the maximum distance between the two cameras is 80 m. However, it is not clear from the TKP 40 what the image quality will be at this distance. The image quality and/or application requirements of the camera system are defined by NOR EN 62676-4(16) (see Table 2).

Table 2. The VSS system applications, adapted according to [16].

Application (Purpose) of the VSS System	Specification
Detection	The details of the image must be sufficient to enable the observer to determine with sufficient certainty whether or not a person is present. The target must occupy at least 10% of the height of the image (or more than 40 mm of the captured scene per pixel, i.e., 25 px/m).
Observation	The details of the image must be sufficient to allow the observer to recognise the characteristic features of the individual, such as the peculiarity of their clothing, and also to observe activities in the surroundings. The target must occupy at least 50% of the height of the image (or more than 16 mm of the captured scene per pixel, i.e., 62.5 px/m).
Recognition	The details of the image must be sufficient to enable the observer to determine with a high degree of certainty that the same person they have seen before is on the screen. The target must occupy at least 25% of the height of the image (or more than 8 mm of the scene being shot per pixel, 125 px/m).
Identification	The details of the image must be sufficient to enable the observer to identify the individual beyond all doubt. The target must occupy at least 100% of the height of the image (or more than 4 mm of the captured scene per pixel, i.e., 250 px/m).
Investigation	The details of the image must be sufficient for a judicial investigation. The target must occupy at least 400% of the height of the image (or more than 1 mm of the scene being shot per pixel, i.e., 1000 px/m).

According to TKP 40, the operating temperatures of cameras should be in the range of −30 °C to +55 °C, and the cameras should be equipped with IP 66 enclosures [19]. This requirement corresponds approximately to environment class III, according to EN 50130-5 and STN EN 62676-1-1 [11,20], which describes an outdoor environment protected from the direct influence of weather (e.g., rain, sun, etc.). The camera was tested at temperatures of −25 °C and +55 °C, at a relative humidity of 93%. At the same time, it must resist falling water droplets and the effects of sulfur dioxide.

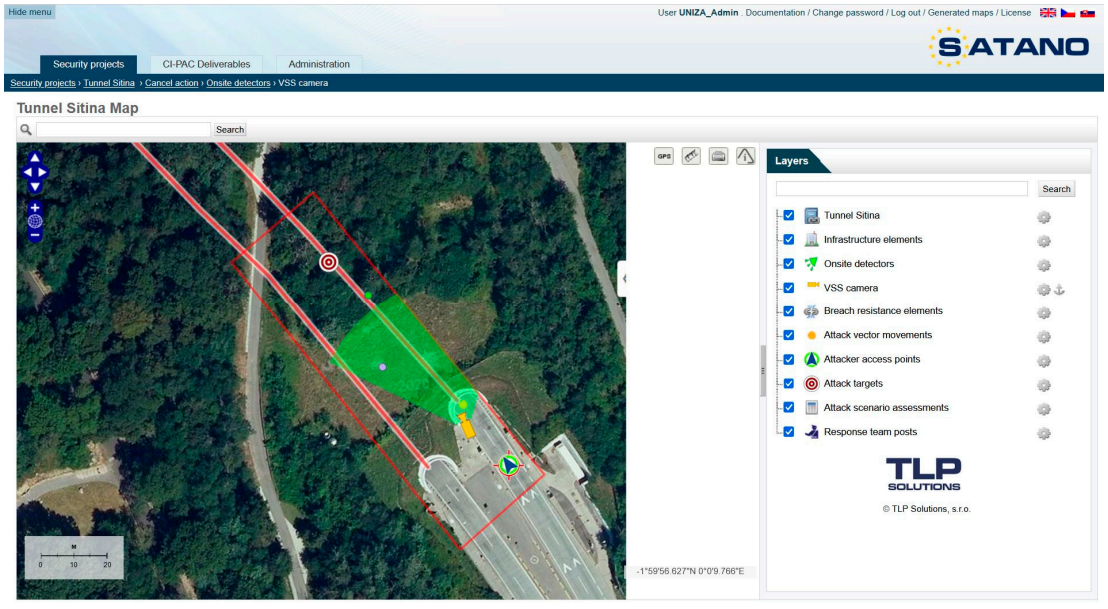
Temperature fluctuations can cause problems not only for the human body but also for parts of electronic systems. Undoubtedly, these systems also include transport VSSs, which have to withstand extensive temperature changes throughout the year. In winter, the temperatures in some of the locations in which cameras are installed can reach as low as −20 °C. By contrast, in the summer period, under the influence of sunlight, the ambient temperature of a camera can be +35 °C and above. Different tunnel situations can cause situations in which VSSs are exposed to even greater temperature extremes (e.g., in tunnel fires). However, temperature is not the only influencing factor in the proper functioning of VSSs. The immediate surroundings of the camera are also of great importance. In the event that the camera is in a dusty environment, this dust can unpleasantly affect the proper functioning of the entire system.

3. Results

The overall minimum level of tunnel protection could be given by the minimum values of the output variables of the quantitative models, confirming the functionality of the entire protection system. The most frequently cited output variables of quantitative models include (Figure 1):

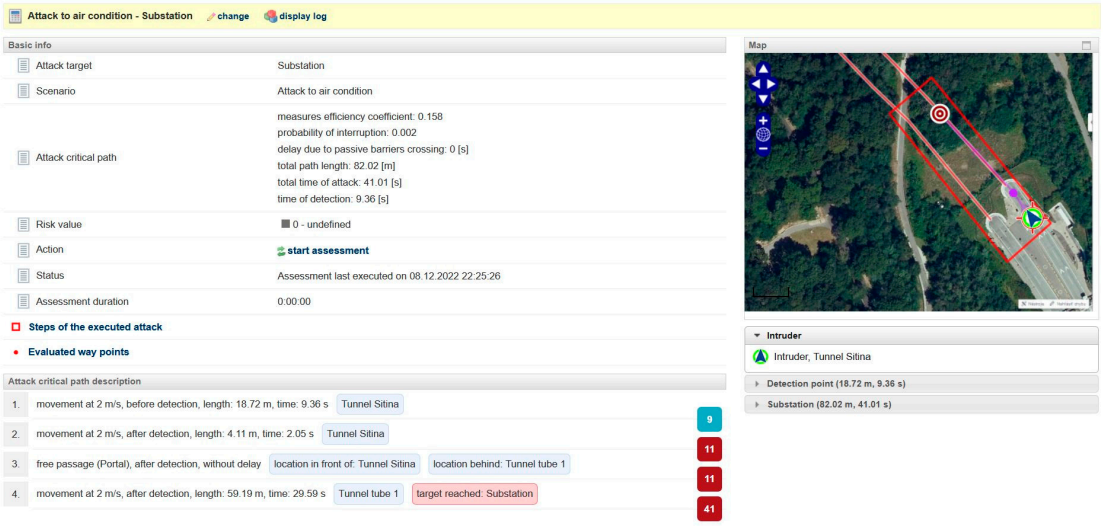
- the coefficient of the effectiveness of the protective measures [7,8];
- the likelihood of eliminating the intruder;
- the cumulative probability of intruder detection.

The established minimum output values (e.g., the probability of eliminating an intruder must be greater than 0.95) indicate how many mechanical barriers with associated breakthrough resistance are to be implemented at the specified response time of the intervention unit. Furthermore, the minimum values of the output parameters indicate the probability of detecting an intruder by each element of the alarm system. Figure 3 creates a model of a scenario involving unauthorised intrusion into the Sitina tunnel, followed by a simulation with the SATANO software tool. In this scenario, the intruder intended to pass through the tunnel's entrance portal to the air-conditioning substation located in the central part of the tunnel; the intruder was detected by a security camera located at the entrance to the tunnel portal. The evaluation of the breach, as well as of the intervention itself, was carried out by the security services' intervention unit. The results of the simulation show that if the time taken by the security services unit had been at least 600 s, it would not have been able to intervene against the intruder in time. The total time that an intruder would need from their detection by the VSS camera at the tunnel-entrance portal would be only 41 s, at an assumed average movement speed of 2 m/s. It follows from the above that it is necessary either to ensure the more timely detection of intruders or to increase the passive resistance of the air-conditioning substation.



(**a**)

Figure 3. *Cont.*



(**b**)

Figure 3. (**a**) PPS tunnel model using the SATANO SW tool, (**b**) results of the simulation of the scenario of the intruder attack on the Sitina tunnel substation.

From the point of view of the design of the VSS, it is important to determine the purpose of this alarm system, which may include, for example, monitoring, detection, and identification. According to TKP 40, only IP cameras with a CCD or CMOS sensing element (chip) with high resolution, i.e., 1080 p or higher, and with H.264 compression or better [18] can be used in IP-camera surveillance. From the point of view of light sensitivity, the requirement at 30 IRE for light conditions is 0.1 (colour) or 0.01 (B&W) lux. At the same time, camera functions, such as day and night vision, noise reduction (S/N) (>50 dB), wide dynamic range (>60 dB), or backlight compensation, are required.

Figure 4 shows a model for capturing a camera in tunnels simulated using the IP Video Design Tool. The camera's parameters, such as height, tilt, resolution, and camera-sensor size, were specified according to regulations [19].

Figure 4 shows that cameras in the range of 15 to 80 m (standardised according to TKP 40) are only capable of motion detection (up to 46% of the scene being shot), which meets the standard to EN 62676-4 [16], according to which only the presence of a person or object can be detected. In the case of the requirement to implement smart solutions (e.g., Intelligent Video Analytics), through which it would be possible to automatically recognise not only the presence of persons in a given space, but also their non-standard behaviour, the scene captured should not fall below the level of observation (more than 16 mm of the captured scene per pixel, i.e., 62.5 px/m) or recognition (more than 8 mm of the captured scene per pixel, 125 px/m). By modelling the ability of the camera to sense non-standard behaviour in the tunnel, using the IP Video Design Tool software tool, it is possible to conclude that the maximum distance between two cameras should therefore be reduced to at least 50 m (it is currently up to 80 m, in accordance with TKP 40), or the minimum camera resolution should be increased (e.g., a camera with a minimum resolution of 5 Mpx).

As mentioned above, extreme temperatures can have an impact on smart technologies installed in tunnels (e.g., VSS). These transport VSSs must withstand extensive temperature changes during the year, which are caused by the natural environment or by emergency situations (e.g., car fires). As part of the project, SMART TUNNEL: Telematic support for emergencies in the traffic tunnel (APVV-17-0014), transport VSS were tested against extreme temperature changes. Extremely high and low temperatures were created using the VÖTSCH VCL 7010 climate chamber, which can create temperatures in a range from −70 °C to +180 °C. According to EN 50130-5, the lowest temperature considered is −25 °C [20], which is sufficient for the local conditions of Slovakia. From the point of view of the load on the cameras in the tunnels, it is relevant to monitor the exposure of the

cameras to high temperatures. The limit value was the temperature at which the camera stopped working properly or completely.

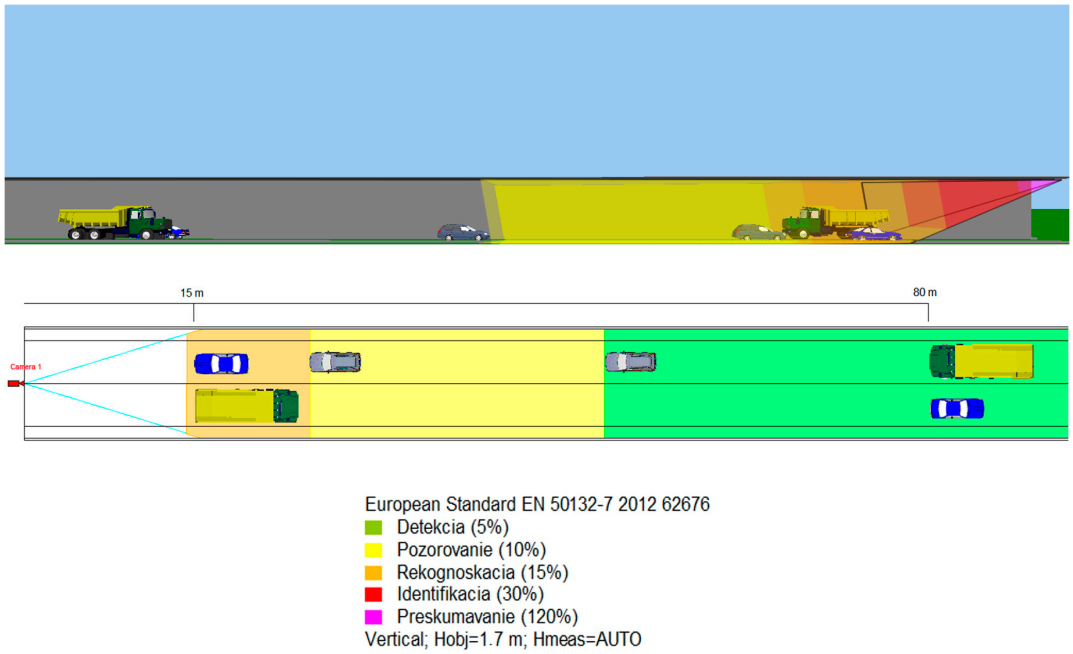


Figure 4. Evaluation of tunnel-camera shooting according to TKP 40 requirements. Legend: Detekcia, detection (5%); Pozorovanie, observation (10%); Rekognoskácia, reconnaissance (15%); Identifikácia, identification (30%); and Preskúmavanie, investigation (120%).

The subject of the test in the climate chamber was a selected camera system from the company, DYNACOLOR. The camera is of environment class 3, which means that its recommended operating temperature range from −10 °C to +50 °C, at a humidity level below 90%. To evaluate the image quality, the CCTV Test Chart was placed in the field of view of the camera at a distance of 2 m. The temperature was gradually raised to the level of +180 °C. The temperature of +152 °C (Figure 5) was the temperature ceiling for the tested camera, which means that the camera stopped fully communicating and sending data to the output-imaging control at this temperature. This measurement showed that the temperature specified by the manufacturer may not always be the limit temperature.

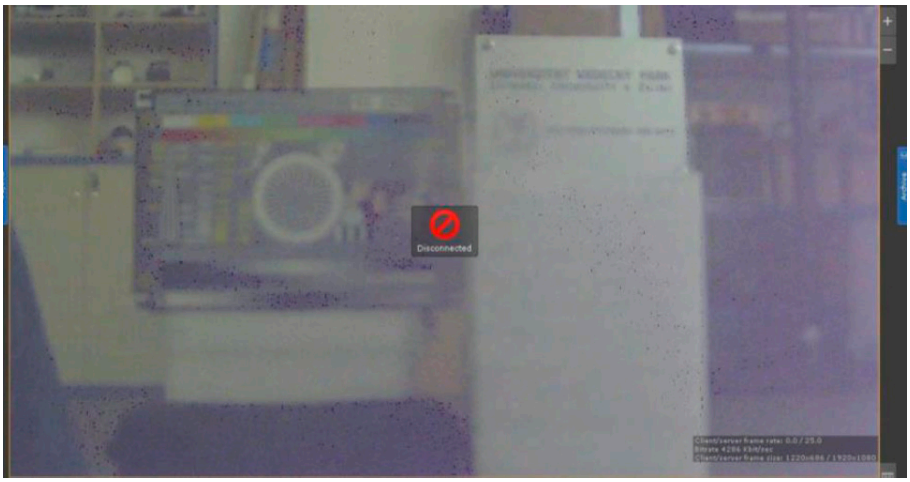


Figure 5. Camera image at +152 °C [21].

Further investigations revealed whether this caused irreversible damage to the camera. The last measurement was taken from a temperature of 152 °C to a temperature of −70 °C, which was the lowest temperature created in the climate chamber. The image of the camera was partially restored at 30 °C. A further investigation was carried out to determine whether there was irreversible damage to the camera. The last measurement was taken from a temperature of 152 °C to a temperature of −70 °C, which was the lowest temperature created in the climate chamber. The image of the camera was restored at a temperature of 30 °C, at which point the camera began to communicate again. However, there was partial permanent damage to the camera. Subsequently, the signal from the camera was lost at a temperature of −65.5 °C.

Another research task was to determine whether the above-mentioned critical value above 150 °C could be reached in tunnels in the event of a fire, which is the most likely emergency scenario in tunnels. A simulation was carried out using the software program, Fire Dynamics Simulator, and the subsequent images were displayed in Smokeview. As part of the simulation, all the parameters of the TKP 40 detected and projected so far were observed [18], in particular the camera pitch, with a maximum length of 80 m. For this reason, a 129-m-long tunnel pipe with a usable area of 38.34 m^2 was used for simulation purposes, and the simulation took place in the direction of the wind. The aim of the simulation was to determine the time t, the value of which indicates at what point in time, in selected types of fire, a critical temperature occurs that threatens the functionality of the camera. The simulation was carried out while maintaining two basic conditions, namely with and without automatic extinguishing equipment (AEE). Within the source of burning, three variants were considered, namely a passenger car (5 MW), a van (15 MW), and a truck (30 MW). The time results of the simulations are shown in Table 3. The expression of the time required for the formation of critical temperature with and without the use of AEE was made in order to improve safety in road tunnels. According to TP 13/2015, the spaces in tunnel tubes and emergency bays may be equipped with AEE; if necessary, this may be undertaken as a result of a tunnel-safety-risk analysis [22]. The AEE with water mist was chosen because of its good results in many European countries. This type of system is installed in tunnels under the River Tyne, in Newcastle.

Table 3. Time taken to reach a critical temperature of 150 °C at selected distances.

Distance from Fire (in Wind Direction) (m)	5 MW		15 MW		30 MW	
	AEE for Water Mist		AEE for Water Mist		AEE for Water Mist	
	No (s)	Yes (s)	No (s)	Yes (s)	No (s)	Yes (s)
20	85.5	-	54.9	615.6	37.8	81
40	93.6	-	64.8	-	45	85.5
60	174.6	-	72	-	53.1	98.1
71	408.6	-	78.3	-	60.3	103.5

The data in Table 3 show that a critical value of 150 °C was measured at certain outputs and distances. This fact also depends on the used AEE, thanks to which, directly above the fire, a critical temperature arose only for a few seconds, which did not mean damage to the camera. Figure 6 shows the temperature patterns for 5 MW.

As mentioned above, using AEE, a critical value was measured only at a certain point (90.9 s), but only for a very short time (0.3 s), directly above the source of burning. A view of the simulation at 90.9 s is shown in Figure 7.

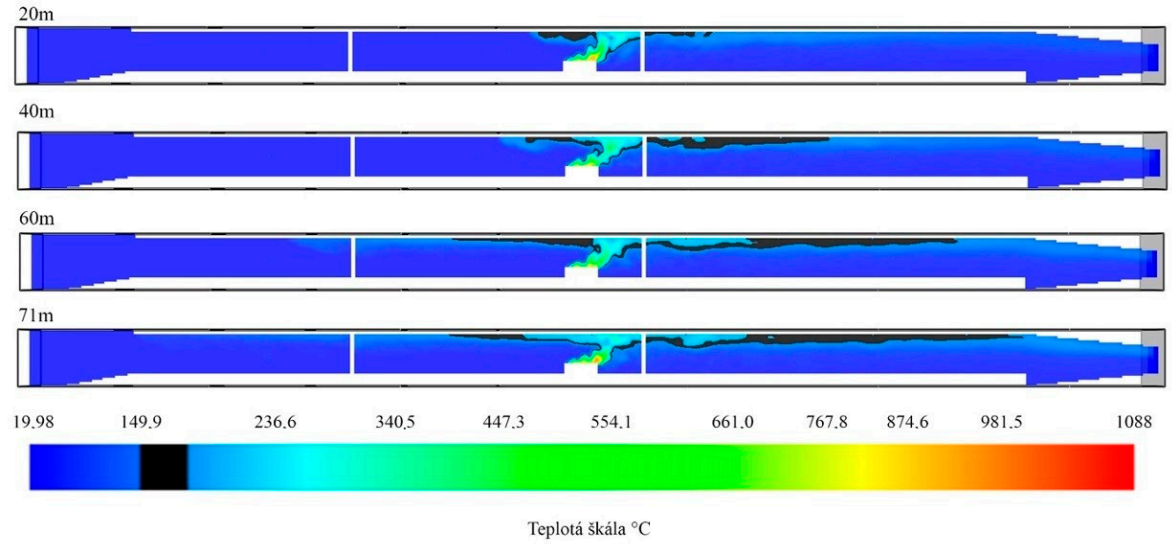


Figure 6. Illustration of the critical temperature (black colour) at a heat source of 5 MW at selected distances without the use of AEE in the tunnel.

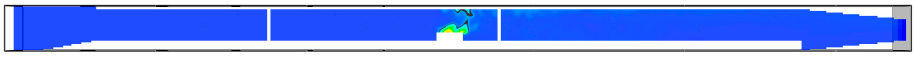


Figure 7. Illustration of the critical temperature (black colour) at a 5 MW heat source using AEE at 90.9 s.

According to Table 3, with a heat source of 15 MW, similar results were achieved. With the AEE used, a critical temperature of 615.6 s was reached for a short time, but only at a distance of 20 m. The results obtained are shown in Figures 8 and 9.

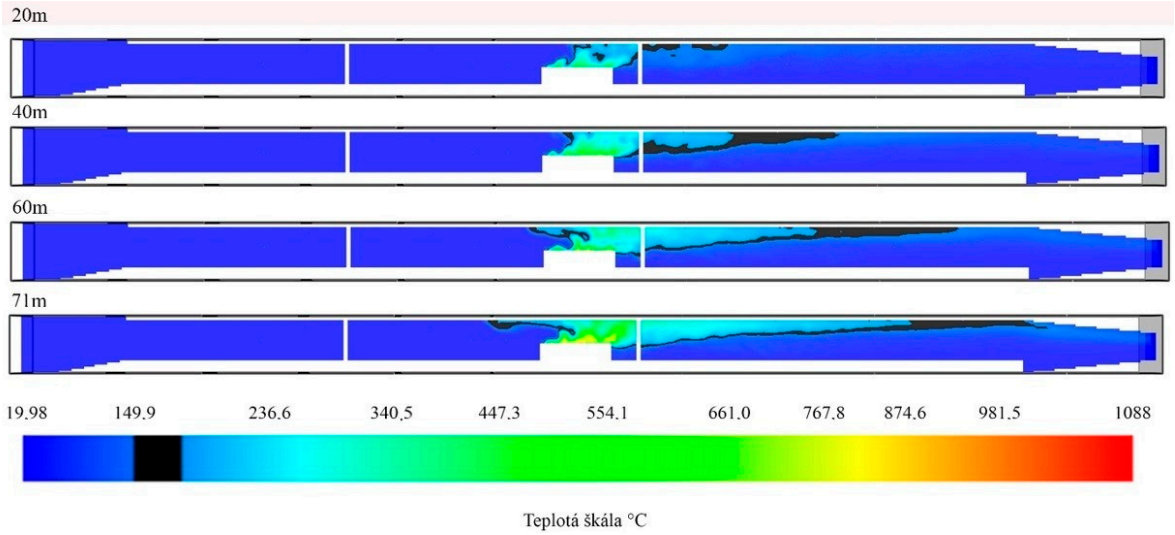


Figure 8. Illustration of the critical temperature (black colour) at a 15 MW heat source at selected distances without the use of AEE in the tunnel.

Figure 9. Illustration of the critical temperature (black colour) at a 15 MW heat source using an AEE at 615.6 s.

The only option in which the critical temperature was recorded even when the AEE was used was a heat source of 30 MW, which corresponded to the burning of the truck. The results of the simulations are shown in Figures 10 and 11.

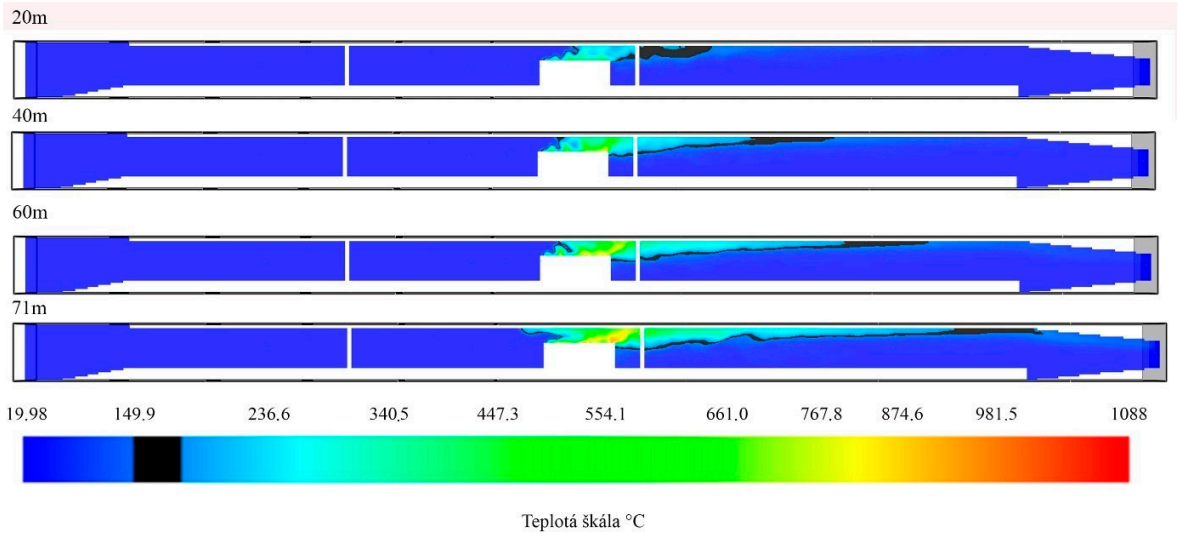


Figure 10. Illustration of the critical temperature (black colour) at a heat source of 30 MW at distances taken without the use of AEE in the tunnel.

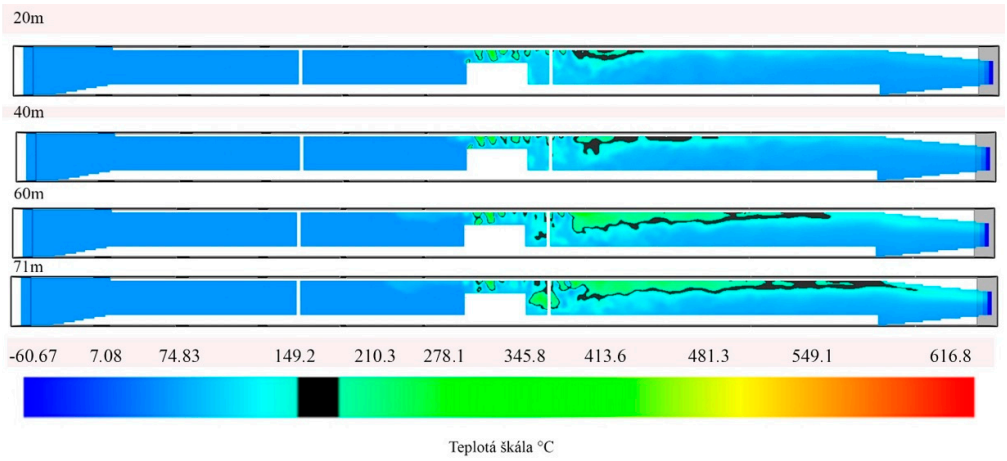


Figure 11. Llustration of the critical temperature (black colour) at a heat source of 30 MW at distances taken using AEE in the tunnel.

The above measurements under laboratory conditions created the starting conditions for testing the cameras in real road-tunnel conditions. A critical temperature of 150 °C was established, which had a fatal effect on the operation of the camera. Subsequently, using the software tool, Fire Dynamics Simulator, we determined the selected distances (20, 40, 60, and 71 m) at which the critical temperature of 150 °C in the immediate vicinity of the camera would be reached. A significant finding was that when using AEE with water mist in tunnels, this time was significantly increased or eliminated altogether. Based on the above, it can be concluded that, in addition to having a direct impact on fire safety in road tunnels, AEE also has an impact on the operational capacity of VSSs in tunnels.

4. Discussion

Video Surveillance Systems (VSSs) are integral parts of road-tunnel-security and -safety systems. They currently perform a number of functions, such as ensuring the protection of tunnel technologies, monitoring tunnel traffic, or recognising vehicle-license

plates. With the development of new technologies, it is assumed that VSSs will also be used in the future for smart solutions, which will be based on the intelligent video analysis of images. This makes it necessary to assess whether the currently proposed standards for the design of VSSs in road tunnels comply with these new requirements.

Currently, one of the primary tasks of VSS systems is to protect tunnels and their technologies from unauthorised intentional human activity. Here, it is necessary to ensure that the entire physical protection system (PPS) is designed in such a way that the basic requirement for its functionality is met. When it is necessary to objectively assess whether this requirement has been met in the design of the PPS, it is appropriate to use one of the software tools enabling the quantitative evaluation of PPSs, based on measurable output variables (e.g., the probability of intruder elimination). In the article, using the example of tunnel-intrusion simulation, a new tool, SATANO: Security Assessment of Terrorist Attack in a Network of Objects, was presented; this tool makes it possible to evaluate whether the proposed PPS allows an effective response time from the intervention unit, measured from the at which the VSS detects the intruder at the entrance to the tunnel portal. This SW tool has also been applied to other types of object [23,24].

Video surveillance systems enable multiple applications, such as monitoring, detection, recognition, and identification. This article assessed the current standardised requirements for the design of a VSS in a tunnel from the point of view of its possible use for intelligent video analysis, allowing the recognition of various risk situations (e.g., non-standard driver behaviour). To assess the current standardised requirements, the IP Video Design Tool software was used, which made it possible to model the possibilities or limits of using the applicable standard. From the results of the investigation, it can be concluded that at present, VSSs are only capable of motion detection (up to 46%) in a substantial part of the scene being scanned. In the case of the request for the implementation of intelligent video analytics, through which various non-standard behaviours or situations can be automatically recognised, it is necessary either to reduce the spacing of cameras from the current 80 m to a maximum of 50 m, or to increase the requirement for the minimum resolution of cameras from 1 to 5 Mpx [24–26].

In the event that there is a requirement to use the VSS during emergency situations (e.g., a fire in a tunnel), it is necessary to determine the operating conditions and period of time through which the VSS would operate in a given tunnel. The article presented the results of experiments aimed at testing the reliability of cameras in extreme temperature conditions. Subsequently, the results of the simulation of the spread of fire in the tunnel and its possible impact on the operation of the VSS were presented. From the results of the experimental tests, it can be concluded that the reliability of the cameras far exceeded the specified operating ranges (50–55 °C), and the critical limit was around 150 °C. In the event of a fire in the tunnel, this limit temperature would be reached without AEE (e.g., sprinklers) in the order of minutes (depending on the source of combustion, e.g., a passenger car, van, or truck), thus rendering the VSS inoperable. In certain circumstances, depending on the heat source, even AEE would not prevent damage to the cameras.

From the point of view of the modelling and simulation of PPS tunnels, further research is required to obtain a data set with the real values of input variables by using experimental measurements (e.g., the probability of intruder detection, or reaction time by intervention unit) or software simulations (e.g., the breakthrough resistance of a mechanical barrier). At the same time, in the event of the completion of research into the possibility of using VVS in tunnels from the point of view of operating conditions, further research should address possible scenarios involving the non-standard behaviour of drivers in the tunnel.

Author Contributions: Conceptualisation, M.B. and L.M.; methodology, M.B.; software, T.L..; validation M.B. and K.M.; formal analysis, K.M.; investigation, T.L.; resources, K.M.; data curation, L.M.; writing—original draft preparation, M.B. and T.L.; writing—review and editing, L.M.; visualisation, K.M.; supervision, T.L.; project administration, K.M.; funding acquisition, T.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the research project APPV-20-0457 Monitoring and Tracing of Movement and Contacts of Persons in Medical Facilities.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. National Motorway Company. Available online: https://ndsas.sk/uploads/media/551316c1f633d00b96d63faeb9145edc159164c0.pdf (accessed on 10 October 2022).
2. TP 02/2011 Analýza Rizík pre Slovenské Cestné Tunely. Available online: https://www.ssc.sk/files/documents/technicke-predpisy/tp/tp_041.pdf (accessed on 15 October 2022).
3. Nariadenie Vlády SR č. 344/2006 Z.z. o Minimálnych Bezpečnostných Požiadavkách na Tunely v Cestnej Sieti. Available online: https://zakony.judikaty.info/predpis/nariadenie-vlady-344/2006 (accessed on 7 September 2022).
4. Zákon č. 45/2011 Z.z. o Kritickej Infraštruktúre. Available online: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2011/45/20210301.html (accessed on 7 September 2022).
5. Európska Smernica Rady 2008/114/ES z 8. Decembra 2008 o Identifikácii a Označení Európskych Kritických Infraštruktúr a Zhodnotení Potreby Zlepšiť ich Ochranu. Available online: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32008L0114&from=EL (accessed on 9 September 2022).
6. Metodické Usmernenie č. 29014/2014-1000-53190 MH SR o Bezpečnostných Opatreniach na Ochranu Prvkov Kritickej Infraštruktúry v Sektoroch Energetika a Priemysel. Available online: https://www.economy.gov.sk/uploads/files/J4Vom9oj.pdf (accessed on 10 September 2022).
7. Garcia, M.L. *The Design and Evaluation of Physical Protection Systems*; Elsevier: Berkeley, CA, USA, 2001; 370p.
8. Loveček, T.; Mariš, L.; Šiser, A. *Plánovanie a Projektovanie Systémov Ochrany Objektov*; Žilinská univerzita v Žiline: Žilina, Slovakia, 2018; 285p.
9. Loveček, T.; Reitšpís, J. *Projektovanie a Hodnotenie Systémov Ochrany Objektov*; Žilinská univerzita v Žiline: Žilina, Slovakia, 2011; 281p.
10. Lovecek, T.; Ristvej, J.; Simak, L. Critical Infrastructure Protection Systems Effectiveness Evaluation. *J. Homel. Secur. Emerg. Manag.* **2010**, *5*, 1–25. [CrossRef]
11. *EN 62676-1-1*; Video Surveillance Systems for Use in Security Applications—Part 1-1: System Requirement. General. European Committee for Electrotechnical Standardization: Brussels, Belgium, 2014.
12. *EN 50131-1*; Alarm Systems. Intrusion Systems. Part 1: System Requirements. General. European Committee for Electrotechnical Standardization: Brussels, Belgium, 2006.
13. *EN 60839-11-1*; Alarm and Electronic Security Systems—Part 11-1: Electronic Access Control Systems—System and Components Requirements. European Committee for Electrotechnical Standardization: Brussels, Belgium, 2013.
14. *EN 50518*; Monitoring and Alarm Receiving Centre General. European Committee for Electrotechnical Standardization: Brussels, Belgium, 2019.
15. *EN 50136-1*; Alarm Systems. Alarm Transmission Systems and Equipment. Part 1: General Requirements for Alarm Transmission Systems. European Committee for Electrotechnical Standardization: Brussels, Belgium, 2018.
16. *EN 62676-4*; Video Surveillance Systems for Use in Security Applications—Part 4: Application Guidelines. European Committee for Electrotechnical Standardization: Brussels, Belgium, 2015.
17. *ISO 31000*; Risk Management. Principles and Guidelines. International Organization for Standardization: Geneva, Switzerland, 2018; ISBN 978-92-67-10784-4.
18. Kampova, K.; Loveček, T.; Rehak, D. Quantitative approach to physical protection systems assessment of critical infrastructure elements: Use case in the Slovak Republic. *Int. J. Crit. Infrastruct. Prot.* **2020**, *30*, 100376. [CrossRef]
19. Technicko-Kvalitatívne Podmienky (TKP 40) Kamerový Dohľad, Videodetekcia Vrátane ADR—Tunely. Ministerstvo Dopravy, výstavby a Regionálneho Rozvoja SR, Sekcia Cestnej Dopravy a Pozemných Komunikácií. Available online: https://www.ssc.sk/files/documents/technicke-predpisy/tkp/tkp_40_2016.pdf (accessed on 15 November 2022).
20. *EN 50130-5*; Alarm systems—Part 5: Environmental Test Methods. European Committee for Electrotechnical Standardization: Brussels, Belgium, 2011.
21. Madeja, M. *Experimentálne Testovanie Komponentov Kamerových Systémov v Klimatickej Komore*; Diplomová Práca, Žilinská Univerzita v Žiline: Žilina, Slovakia, 2019.
22. Technické Podmienky—Protipožiarna Bezpečnosť Cestných Tunelov. TP 099/2022. Ministerstvo Dopravy, Výstavby a Regionálneho Rozvoja SR, Sekcia Cestnej Dopravy a Pozemných Komunikácií. Účinnosť od 10.06.2022. Available online: https://www.ssc.sk/files/documents/technicke-predpisy/tp/tp_099_2022.pdf (accessed on 20 January 2023).

23. Šiser, A.; Loveček, T.; Mariš, L. Simulation of Possible Assault Vectors in an Attack Using a Real-life Waterworks Object as a Use Case. In Proceedings of the 12th International Scientific Conference Of Young Scientists On Sustainable, Modern and Safe Transport, TRANSCOM 2017, High Tatras, Slovakia, 31 May–2 June 2017.
24. Hsu, W.S.; Huang, Y.H.; Shen, T.S.; Cheng, C.Y.; Chen, T.Y. Analysis of the Hsuehshan Tunnel Fire in Taiwan. *Tunn. Undergr. Space Technol.* **2017**, *69*, 108–115. [CrossRef]
25. Shin-Hung, P.; Shu-Ching, W. Identifying Vehicles Dynamically on Freeway CCTV Images through the YOLO Deep Learning Model. *Sens. Mater.* **2021**, *33*, 1517–1530.
26. Chen, Y.-J.; Shu, C.-M.; Ho, S.-P.; Kung, S.-W.; Ho, H.-H.; Hsu, W.-S. Analysis of smoke movement in the Hsuehshan tunnel fire. *Tunn. Undergr. Space Technol.* **2019**, *84*, 142–150. [CrossRef]