

Article

Analysis and Assessment of Railway CCTV System Operating Reliability

Miroslaw Siergiejczyk ¹, Zbigniew Kasprzyk ^{1,*}, Mariusz Rychlicki ¹ and Piotr Szmigiel ²

¹ Department of Telecommunications in Transport, Faculty of Transport, Warsaw University of Technology, Koszykowa 75 Street, 00-662 Warsaw, Poland; mirosław.siergiejczyk@pw.edu.pl (M.S.); mariusz.rychlicki@pw.edu.pl (M.R.)

² PKP Polish Railway Lines S.A, Targowa 74 Street, 03-734 Warsaw, Poland; piotr.szmigiel@plk-sa.pl

* Correspondence: zbigniew.kasprzyk@pw.edu.pl

Abstract: The article reviews the history and the direction of development for railway CCTV (Closed-Circuit TeleVision) systems. The authors described the CCTV system at PKP Polskie Linie Kolejowe S.A. and the associated network and server infrastructure. The authors proposed an operational model for a centralized CCTV system that assumes states of partial fitness, in accordance with the regulations of the national railway infrastructure administrator. The aim of the paper is to review, analyse, and evaluate the operational reliability of railroad video monitoring systems in relation to the assumptions of the national railroad infrastructure manager using an operational model. A unified system structure is presented in the article. The model was used as a base to calculate the probabilities for the system while staying in the assumed states. Calculations showed that a centralized CCTV system is characterized by high reliability and satisfies the expectations of PKP Polskie Linie Kolejowe S.A. in this respect. The obtained result of 99.88% probability of leaving the analysed video surveillance system in a fully operational condition within a year indicates a high level of security of the applied solutions in such a large system. The analysed system is one of the largest such solutions designed in the European Union and the largest in Poland, which is an important contribution to the development and implementation of such extensive video surveillance systems in the future. The research question is whether the extensive centralized railway CCTV systems will meet the requirements of PKP Polskie Linie Kolejowe S.A.

Keywords: video surveillance; railway safety systems; rail safety systems



Citation: Siergiejczyk, M.; Kasprzyk, Z.; Rychlicki, M.; Szmigiel, P. Analysis and Assessment of Railway CCTV System Operating Reliability. *Energies* **2022**, *15*, 1701. <https://doi.org/10.3390/en15051701>

Academic Editors: Stanisław Duer and Ahmadiyah Khanesar Mojtaba

Received: 9 January 2022

Accepted: 22 February 2022

Published: 24 February 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction and Analysis of the Issue

Until 2017, only 170 stations and stops out of 2563 active facilities managed by PKP Polskie Linie Kolejowe S.A. (Polish railway infrastructure administrator) had site CCTV, with as many as 100 being obsolete analogue systems. The company lacked regulations on CCTV systems dedicated to passenger infrastructure, which is why newly built systems were non-uniform and/or functionally poor. Only island-type systems were constructed, without the possibility for remote operation. Viewing stations were located typically in Local Control Centres (LCC) or command signal boxes, with viewing conducted locally and occasionally by employees dealing with railway traffic management, which resulted in a low effectiveness relative to the assumed objectives, i.e., protection of people and property.

The previous lack of widespread application of CCTV systems contributed to the low feeling of passenger safety. In a 2017 survey that covered 800 passengers, the main threats indicated in relation to train stations were banditry and the unpredictable behaviour of intoxicated or mentally unstable people [1] (Figure 1). The national infrastructure administrator was approached with questions about surveillance systems—both by passengers and local government authorities. In addition, the existing scientific studies indicated the significant role of CCTV systems in preventing crime at local railway facilities [2].

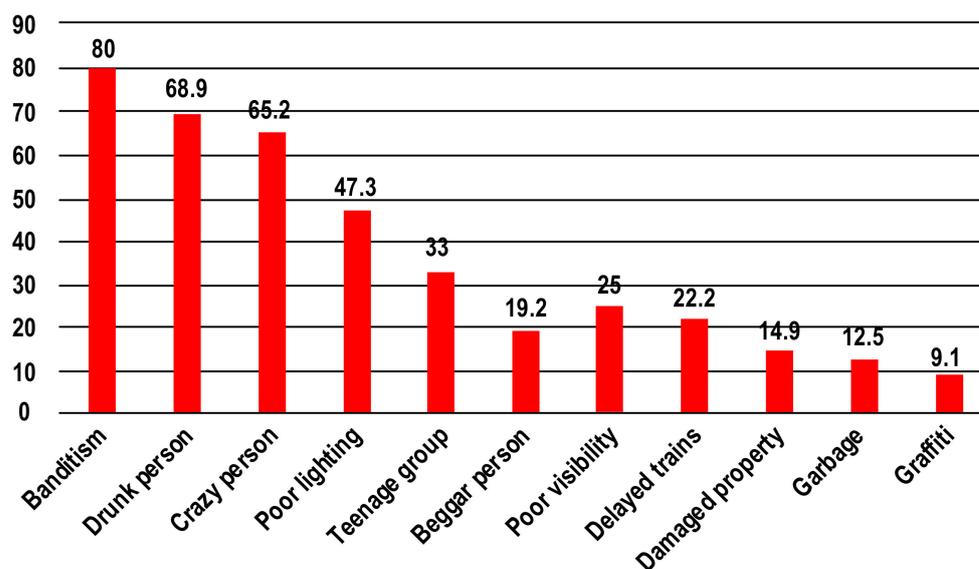


Figure 1. The causes for fear among Polish passengers at railway stations. Source: own study based on [1].

Trying to meet the safety-related expectations of the passengers halfway, as well as in recognition of the threat associated with terrorist attacks in Europe, the national railway infrastructure administrator in Poland decided to respond through developing and implementing a centralized CCTV system that would ultimately cover all the largest passenger stations and stops in Poland. The Ipi-4 instruction entitled “Guidelines for designing and constructing Closed-Circuit Television (CCTV) systems at passenger handling facilities” has been in force at the Polish railway since 2017. It sets out the principles in terms of designing, constructing and operating a modern CCTV system within passenger infrastructure areas at railway stations. The first CCTV systems based on these instructions were commissioned in 2020, upon the commissioning of the modernized railway line No. 447, and the following stations were covered by a surveillance system satisfying the requirements [3]: Warszawa Włochy, Warszawa Ursus, Warszawa Ursus Niedźwiadek, Piastów, Pruszków, Parzniew, Brwinów and Milanówek. The number of train stations with installed modern surveillance systems has been systematically growing ever since.

The next step of PKP Polskie Linie Kolejowe S.A. was announcing a tender to the execution of central system parts—a server room with a planned integration platform that constitutes a key element of the system, as well as a supervision centre that will monitor all railway stations equipped with a surveillance system in line with [3] 24 h a day. A contract for the execution of this task was concluded in 2020—the selected contractor is the Spanish company Aldesa. It is anticipated that the centralized surveillance system will cover 200 railway stations by 2023, with a target of approximately 1050 stations.

There are numerous solutions in terms of video surveillance in the world; however, most of them are not directly associated with railways, and the CCTV structures are significantly different than the one described in this paper.

The authors of [4] believe that video recordings collected and processed in CCTV systems contain important personal data, the reliable protection of which is one of the key operating parameters. Given the fact that the development of artificial technologies in the coming years will probably contribute to an equally dynamic development of intelligent video analysis, decisive measures have to be taken, aimed at protecting such data. Traditional video data protection methods involve masking or simple encryption and do not offer efficient and safe CCTV video search algorithms that are based on video metadata. Moreover, such data are usually stored in the form of plain text. Based on these premises, the authors of this article propose a COP transformation technique, which has the advantage of significantly increasing the efficiency and safety of video metadata. This

is possible owing to the fact that a query is sent to a database in the same manner as for text files, not leaving plaintext within the processed files. The authors indicated that in the course of creating queries for searching metadata, the data that utilize COP transformation offer higher query processing efficiency versus traditional data utilizing text files. In other words, databases implemented within COP transformation may not only execute matching and range queries, but also queries that utilize join-based for multiple base tables. Moreover, they can create simple queries during a statistical analysis of meta-information.

The publication in [5] is also noteworthy. The implementation and provision of communication between vehicles through a wide range of additional application and services have significant impacts on their operation, from safety on roads for wheeled and rail vehicles, to supervision and management of traffic, and even infotainment. However, each application imposes its own limitations regarding the quality of service (QoS) on information exchange. The required efficiency of offered services significantly differs in terms of bandwidth, latency and communication reliability. For example, high-bandwidth applications, such as video streaming, require highly reliable communication. However, damping of an IEEE 802.11p/DSRC communication link caused by static and mobile blocking objects deteriorates link quality and may threaten QoS requirements of supported apps. In contrast, hybrid architecture with two interfaces may offer an emergency switching or backup route creation mechanism and be used for occasionally offloading transmission through more reliable links, such as cellular networks.

The authors of this article propose an approach towards hybrid communication that is based on 4G/LTE and IEEE 802.11p technologies in order to support V2X video streaming applications. The authors conducted extensive studies based on measurements using a field station configuration with a software protocol stack. Field results were collected under various network conditions and in the presence of various blocking objects (LOS, NLOS_V and NLOS_B). The results show that the proposed solution is practically feasible and offers a significant increase in communication reliability. It also enables one to expand the reliable communication range. Furthermore, smooth network switching owing to RAT selection taking into account QoS and the VHO algorithm enables trouble-free and reliable video streaming without failures and interruptions. The proposed approach is a manifestation of an effective compromise between using the IEEE 802.11p/DSCR interface and ensuring a better-quality video streaming service.

Paper [6] presented a traditional CCTV system with marked operational limitations, mainly due to a fixed and preset surveillance pattern. This may reduce system reliability and cause increased generation of false alarms, which translates to increased system processing activity, leading to increased consumption of system resources and energy. In their work, the authors suggested improving these CCTV system operating parameters through a smart combination of a sensor assembly with two cameras, actuators and a lighting module, as well as an implementation of economic built-in processors. The key to success was keeping most CCTV system elements on standby. An exception was made only for system sensors with low power consumption. An effective combination of a sensor assembly with a developed classifier enables one to reduce the generation of a false alarm and improve the reliability of the entire system. In addition, the result was a reduced use of system memory and energy consumption, as well as transmission link capacity, compared to traditional counterparts, which significantly contributed to improved operating parameters of the analysed video surveillance system parameters.

The authors of [7] presented an issue associated with data encryption processes that are a significant burden for the efficiency of modern CCTV systems. These processes are simultaneously the basic protection mechanism for collected and processed data, which is an extremely important issue from the perspective of the reliability and operation of such systems. The hardware support for this process may considerably impact the improvement of these parameters. The authors discussed a systematic real-time video data encryption and decryption methodology based on the idea of chaos in terms of system engineering and analysing data processing algorithms. The proposed system design and the conducted

algorithm analyses were verified using an FPGA hardware platform, employing the Verilog hardware description language (Verilog HDL). The results of the analysis conducted using TETU01 statistical test sets and a differential analysis confirmed increased efficiency and reliability of such solutions relative to CCTV systems.

In [8], the authors proposed a method for improving image quality through the application of data matching with the histogram shaping technique. Image quality is one of the basic parameters of video surveillance systems. It is of particular importance in relation to the systems operated by the railway, where reliability and safety aspects are especially emphasized. Experiments were conducted using 1280×780 px images collected from a CCTV System. The .jpg image format in the form of RGB42 and an .avi video file were selected for analysis. The results of the experiment conducted within a railway station CCTV system indicated satisfactory efficiency of the utilized histogram shaping method for image detection under good and satisfactory lighting conditions, significantly contributing to improving the operating parameters of the system.

The authors of [9] present an underground railway communication system with installed DDS data exchange intermediary software that offers QoS at a preset reliability level. This can be a solution that enables one to maintain information traffic within the network. In such applications as a DDS system for monitoring passenger traffic, it can store the data captured from video file via CCTV cameras distributed within the network, regardless of the encountered communication interruptions. In the phase of contact between stations, data exchanged between train carriage and railway stations upon a stopping train may still be stored, even if the train is disconnected from global networks. This is possible owing to the fact that the system is based on an architecture that comprises more than two domains referenced to broader general architecture, with each of the domains representing an element of an underground railway station. The first domain is the one inside the carriage. The second is located at the train station platform. Further ones are locations at upper station floors. The study involved a simulation aimed at testing the exchange of system video data with two domains, through changing the number of subscribers and the size of sent messages. The results showed that adding a larger number of subscribers did not impact system efficiency. Owing to this, in order to improve the reliability parameters, one can conveniently implement such a system for continuous transmission and collection of centralized information.

In [10], the authors presented an approach to the CCTV analysis of the crowd and of human behaviour in dangerous situations at railway stations. Railway stations are public places that experience significant concentrations of people. For this reason, they are facilities highly exposed to the hazard of crowd panic that can result from a catastrophe or a terrorist attack. Crowd analysis is essential from the perspective of security and surveillance, as it detects abnormal behaviour, thus contributing to reducing the risk of an accident. However, most classic approaches to controlling overload and congestion are based on a hardware approach. This article proposed an approach based on software and an early warning system (CCEWS) for controlling overload through the object detection and tracking technique. Object detection was conducted in accordance with the faster R-CNN architecture. The results revealed that the faster R-CNN model, together with the Google inception resnet v2 CNN model, provided significantly better outcomes, detecting people in appropriate frames of a CCTV image with an accuracy of 93.503% at a 28 FPS. Therefore, it was demonstrated that the general human detection accuracy and FPS result for the Faster R-CNN were significantly better than in the case of other methods. It was also shown that it was possible, under normal CCTV operating conditions, for alarm signals to be generated for each frame with a higher possibility of unfortunate event potential, such as panic due to crowd traffic congestion within a railway facility.

The authors of [11] discuss the issue of the accumulation of a large number of people at railway stations—hence potential targets of terrorist attacks. Access to railway stations is open and is subject to less control than, e.g., airports. For this reason, the reliability of CCTV systems is the key element in terms of improving security at such facilities. One

of the fundamental aspects is efficient, rapid and reliable detection of left objects, such as abandoned luggage. The proposed algorithm can detect lighting changes and adapt to them, which enables one to avoid the generation of false stationary objects associated with poor efficiency. This significantly impacts CCTV system reliability.

Paper [12] presented an issue related to threats within railway facilities that arise from intrusion and property theft, often of considerable value. In order to prevent them, protection systems based on video surveillance are widely used in modern railway systems. It uses an adaptive feature distribution extractor to segment railway tracks through the complete utilization of strong, linear railway scene characteristics and typical categories of local monitored areas. Owing to the application of the presented algorithm, a railway intrusion detection system can automatically and accurately define the boundaries of a monitored scene in real-time and significantly improve its operating efficiency.

The authors of [13] also discuss the issue of threats associated with physical assault and banditry, which are some of the main concerns of rail transport passengers. In order to eliminate such behaviour, it is crucial to introduce reliable and highly efficient CCTV systems. However, their popularization and expansion lead to a situation in which their operators are not able to process the huge amount of information that such systems continuously provide. For this reason, efficient operation of such systems requires the implementation of efficient algorithms supporting automatic and reliable detection of specific situations, such as violence against passengers. In their paper, the authors proposed a three-tier, comprehensive violence detection framework based on deep learning. The experimental results obtained in the course of the studies on various comparative data sets confirm that the proposed method is best suited for detecting violence within CCTV systems and leads to improving their operating parameters, since it achieves higher accuracy than a number of techniques currently applied in this respect. The method is thus efficient that the authors intend to ensure its implementation on devices with limited resources, which will enable its effective deployment even on IoT devices.

Paper [14], which presents the issue of crowd analysis, is also noteworthy. Paper [14] describes the development and evaluation of a multi-stream, convolutional neural network that receives image as input data and generates a density map that comprehensively shows the spatial distribution of people. In order to solve the assumed problems associated with crowd counting, such as extremely unlimited scale and perspective changes, the network architecture utilizes vulnerable fields of various size for each stream. Furthermore, the impact of the two most common trends on generating truths is tested, and a hybrid method based on detecting small faces and scale interpolation is proposed. The experiments conducted on two data sets, UCF-CC-50 and ShanghaiTech, demonstrate that the application of basic truth generation methods enables one to obtain excellent results.

Another study was described in [15]. The paper proposes a smart video surveillance system for level crossings. In this case, a smart video surveillance system starts with extraction, detection and tracking objects moving within a level crossing area (threat area), using the proposed variance-based method. This new method is based on subtracting five background frames, differentiating five frames and calculating variance in order to detect and track objects. The variance-based method involves calculating the variability of columns and rows in video frames, where image pixel intensity changes determine the position of a moving object and is used to locate and track objects in a video. This algorithm enables accurate detection of an object within a hazardous area, with minimum calculation times.

Paper [16] presents issues related to the impact of electromagnetic interference on track-side cabinets of closed-circuit television system operating in the railroad transport environment. The paper develops an operational model including electromagnetic interference. The presented results allow for a numerical evaluation of different types of solutions that can be used to mitigate the impact of electromagnetic interference on the functioning of the system.

Paper [17] presents a study on traffic analysis using computer vision techniques. The traffic volume analysis is based on a CCTV system. This method is challenging in the perspective when there are many vehicle traffic streams at the intersection. In this paper, research is conducted on the processes of improving CCTV-based vehicle counting for traffic analysis. In particular, a comprehensive framework with multiple classes and movements for vehicle counting has been proposed. This paper presents deep learning methods for vehicle detection and tracking. A suitable trajectory approach for monitoring vehicle movements using highlighted region tracking to improve counting performance is presented.

Paper [18] proposes a video-based smoke detection technique for early warning in fire surveillance systems. The paper presents an algorithm to detect smoke in a limited video surveillance environment, both indoors and outdoors. The proposed method uses Kalman estimator, colour analysis, image segmentation, speckle labelling, geometric feature analysis, and M of N decoders to extract the alarm signal at a well-defined time. The proposed smoke detection technique is flexible in terms of input camera type, size, and frame rate and has been implemented on a low-cost platform accessible through a web browser.

2. PKP Polskie Linie Kolejowe S.A. CCTV System Architecture

The central part of the planned CCTV system of PKP Polskie Linie Kolejowe S.A. is the Main Server Room (GS), which houses central and executive system elements. The most important element is the integrated platform called PSIM (Physical Security Information Management), which is an application installed as a virtual instance on physical servers with internal redundancy (Figure 2). The integration platform acts as an intermediary between all system devices. Using a protocol appropriate for a given device, and through access to an Application Programming Interface (API), the PSIM is able to ensure communication between devices, regardless of the ICT standards of such devices. In other words, even in the case of using devices that operate solely based on protocols native for a given manufacturer, it enables the system to operate as a uniform whole, ensuring full control over all processes. PSIM ensures a uniform graphical user interface, regardless of the integrated solution, which is why operators do not have to learn the operation of each added system. This is particularly important in the case of operating and management systems on video recording devices (VMS—Video Management System). These systems significantly differ in terms of interface and are designed based on various management methods. A VMS administrator guidebook can be several hundred pages long, and the same functions may be called and implemented differently, depending on the manufacturer. System operators and administrators at CBIP (Passenger Infrastructure Security Centre) have PSIM-access to all systems through a PSIM client application installed on workstations.

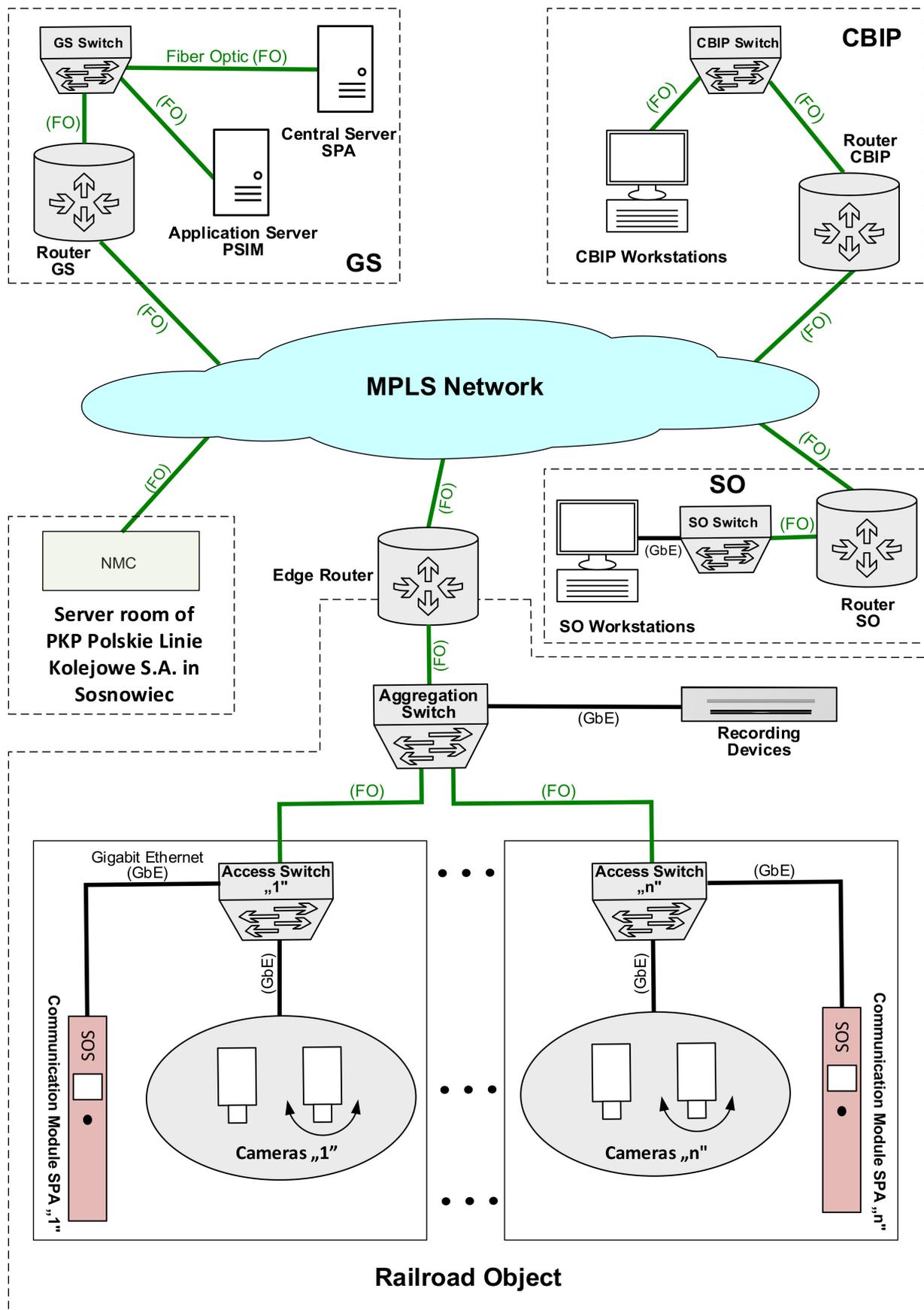


Figure 2. CCTV architecture. Source: own study based on [19–21].

The following systems are subject to integration:

- Facility CCTV—through VMS integration, less often directly through integrating individual cameras through the ONVIF protocol—an open-source protocol that ensures a uniform camera management and communication standard.
- CAS—through integration of a central server located in the GS—a VoIP (Voice over IP) switchboard. The integration is achieved only through ensuring a uniform system operation interface, but also enables functionally linking CAS and CCTV, e.g., through the CBIP—displaying image from a camera installed nearest to the SPA communication module upon an emergency call.
- ACS—Access Control System located in ICT racks. CBIP operators receive information on employee access to the racks.
- IDS—Intrusion Detection system located in ICT racks. Racks are equipped with door opening sensors, as well as vibration sensors, which is why not only unauthorized rack opening is signalled, but also, e.g., attempts to overturn it.

PSIM also ensures the integration of peripherals (air conditioning units in ICT racks, managed power supply strips—CBIP operators are able to monitor their condition). The GS also houses authentication servers (conducted with the use of a device-specific protocol, e.g., RADIUS—Remote Authentication Dial In User Service) and update servers (their role is to update software and the microcode of all PSIM-integrated devices, executing test and collective updates, and the potential restoration of previous versions using an update schedule, e.g., several devices are ongoing test updates; after verifying their efficiency, the updates are executed in packages of several dozen devices, in order not to make the entire system inefficient for the duration of a software/microcode update).

All devices in the GS utilize a common data repository, i.e., drive matrices equipped with an appropriate number of HDD SAS (Serial Attached SCSI) hard drives. Site CCTV is installed at individual railway stations. The system consists of an assembly of executive devices (cameras, infrared radiators, train start/end sensors) as well as CAS communication modules. Camera video streams are sent to an assigned recording device.

A native resolution image is saved on a recording device drive and is available on demand for CBIP operators—such a solution has been adopted to reduce network load since a single 4K camera is able to generate 20 Mbit, even when using the most up-to-date H.265+ compression. One or several stations are monitored live at Viewing Stations (VS) located in their direct vicinity and equipped with a single workstation (identical to CBIP) vs. being usually located in railway utility buildings and operated typically by Railway Security (SOK) employees. They do not allow for administrative access—they can be managed only from the CBIP. From the network perspective, each station has a LAN network, the access switches of which supply actuators through PoE (Power over Ethernet). These switches, as well as the recording devices, are coupled to an aggregation switch cooperating with a site router (demarcation point)—this is the point of contact with the WAN network, where site routers connect with WAN edge devices. An access network diagram is shown in Figure 3.

The IP MPLS backbone network owned by PKP Polskie Linie Kolejowe S.A. is the WAN. This network is to ultimately cover the entire country and consists of thousands of kilometres of fibre optic cables. It is based on a multiple-ring topology—it has three router layers (access, aggregation and backbone). The topology has been selected in order to ensure high accessibility, important in terms of network purpose—it is not only used for CCTV or CAS, but also for railway communication and control systems, e.g., GSM-R and ETCS. A teletransmission network diagram is shown in Figure 4. Network elements are managed at the network management centre in Sosnowiec and, complementary, at CBIP. The network is managed by PKP Polskie Linie Kolejowe S.A.

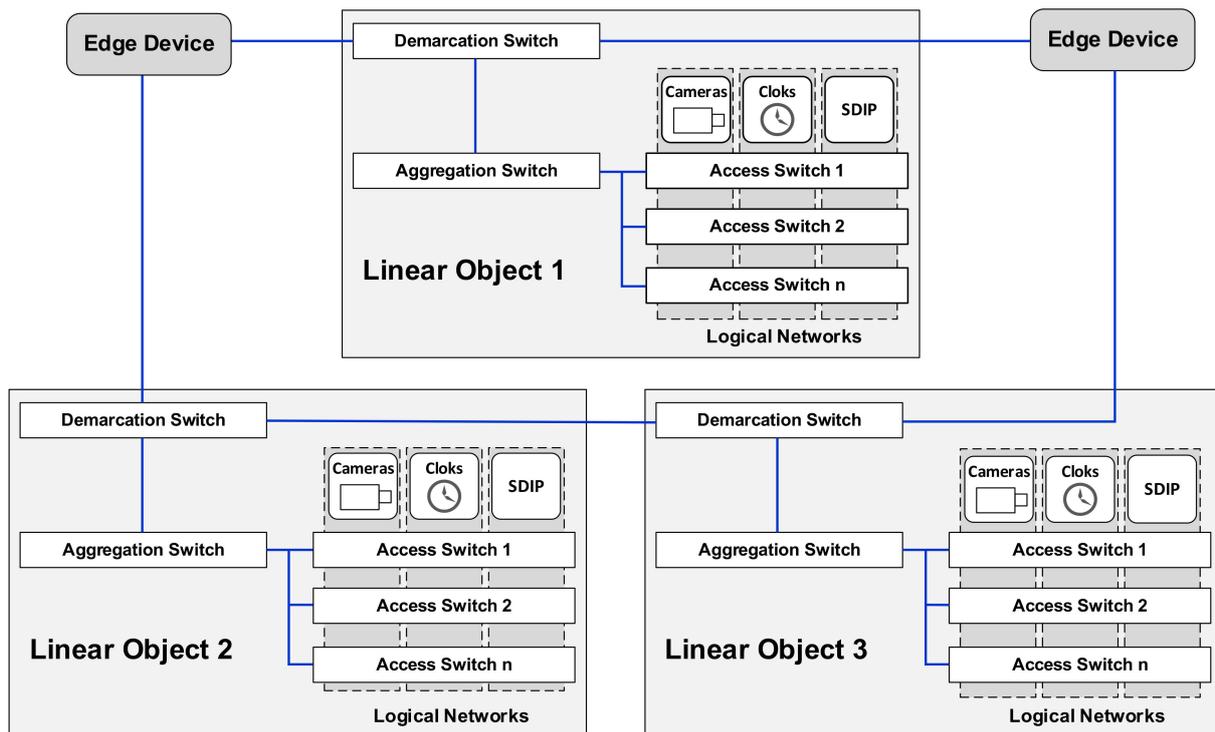


Figure 3. Diagram of a line railway facility access network. Source: own study based on [22].

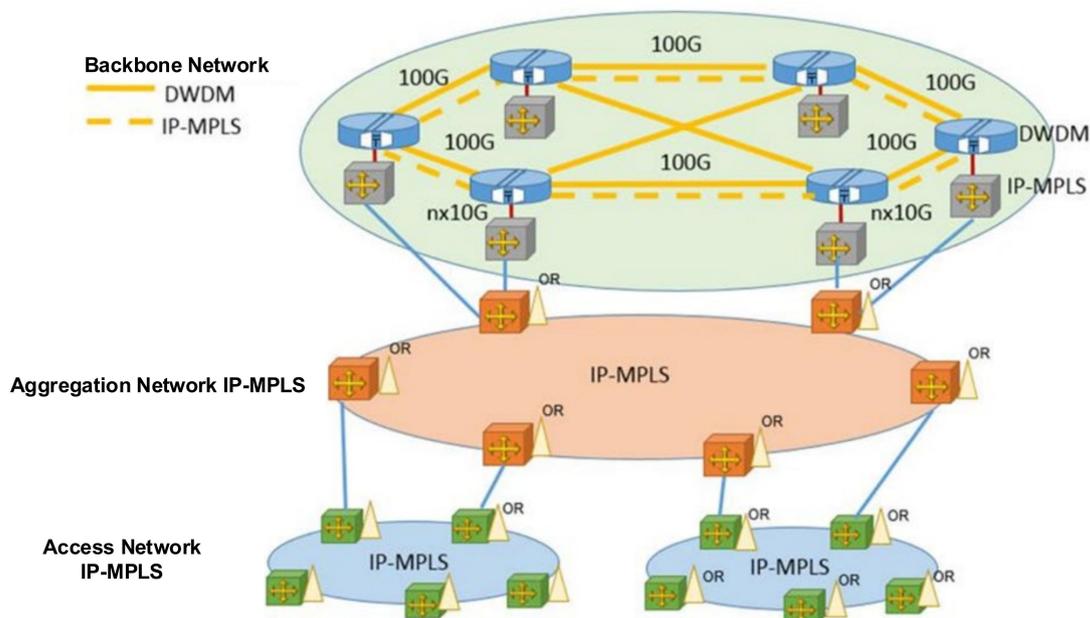


Figure 4. PKP Polskie Linie Kolejowe S.A. teletransmissions network diagram. Source: own study based on [22].

3. PKP Polskie Linie Kolejowe S.A. CCTV System Operating Model

The reliability model was developed in accordance with generally accepted reliability analysis of telecommunication networks using Markov models [18]. The following assumptions were adopted for the development of a PKP Polskie Linie Kolejowe S.A. closed-circuit television system:

- The system is in the state of full fitness (S_1) if and only if its objective function is fulfilled, i.e., assumptions from [19]: 100% of the passenger infrastructure area at each

railway facility is covered by monitoring, with mapping detail appropriate for the category (class) of the stop/station where the system is installed—expressed in pixels per metre.

- Damage to a single camera will mean the creation of a dead zone (facility coverage will drop below 100%) or a zone with reduced mapping detail relative to the requirements [19]. Therefore, the system will cease to satisfy the requirements; however, this will apply only to a certain area of a single railway facility. The system can essentially be considered operable, however not exhibiting the expected parameters (S_2). The system will not transition into state S_2 due to short-term signal losses—cameras are equipped with SD cards that the video stream is sent to when it is impossible to establish a connection with the recording device—the system will then remain in the state of fitness S_1 ;
- Damage to one of the access switches (that ensure not only data transmission, but also power for cameras via the Power over Ethernet—PoE) will result in a lack of monitoring coverage of the entire area, e.g., a given station platform. The switches serve independent areas of a railway facility. Access switches are not ensured by any kind of hardware redundancy. The system ceases to fulfil its task for one of the areas; however, it will still be possible to establish alarm communication with other areas of the facility (e.g., underground passages, other platforms). Therefore, the system will transition to the state of partial fitness S_3 .
- An event that takes an entire service out of operation is damage to the aggregation switch, a pair of aggregation routers (fibre optic loop start and end for a certain line segment) or a pair of backbone network edge routers. This will make video monitoring and alarm communication impossible for one or numerous railway facilities, while resulting in a transition into the state of partial system unfitness S_4 .
- Due to no GS georedundance, any event that leads to the unfitness of key system elements (e.g., PSIM hardware platform) results in the full unfitness of the entire system— S_5 —since a damage to server room elements causes the system to stop working. The PSIM platform has been constructed with local hardware redundancy, which is why in the event of hardware platform failures, the S_5 state may be considered only in the case of a simultaneous damage to both physical PSIM servers or a damage to the redundant pair of switches/routers in the GS.
- Repair times result from the assumptions adopted in [19–21] and are implemented by the hardware vendor and by a service contractor under a maintenance contract, after the warranty period expires.
- Transitions from less severe failure states to more severe are possible; however, repair in such an event is simultaneous for all damaged devices—for logistic reasons. Therefore, there is no probability of a transition from a state of a more severe failure to a state of less severe system failure. The operational model is shown in Figure 5.

The designations in Figure 5 show the following system functions and transition intensities:

- $R_0(t)$ —probability function for a CCTV system in the state of full fitness S_1 ;
- $Q_2(t)$ —probability function for a CCTV system in the state of partial fitness S_2 ;
- $Q_3(t)$ —probability function for a CCTV system in the state of partial fitness S_3 ;
- $Q_4(t)$ —probability function for a CCTV system in the state of partial unfitness S_4 ;
- $Q_5(t)$ —probability function for a CCTV system in the state of full unfitness S_5 ;
- λ_{12} —intensity of transitions from the state of full fitness S_1 to the state of partial fitness S_2 ;
- μ_{21} —intensity of transitions from the state of partial fitness S_2 to the state of full fitness S_1 ;
- λ_{13} —intensity of transitions from the state of full fitness S_1 to the state of partial fitness S_3 ;
- μ_{31} —intensity of transitions from the state of partial fitness S_3 to the state of full fitness S_1 ;

- λ_{14} —intensity of transitions from the state of full fitness S_1 to the state of partial unfitness S_4 ;
- μ_{41} —intensity of transitions from the state of partial unfitness S_4 to the state of full fitness S_1 ;
- λ_{15} —intensity of transitions from the state of full fitness S_1 to the state of full unfitness S_5 ;
- μ_{51} —intensity of transitions from the state of full unfitness S_5 to the state of full fitness S_1 ;
- λ_{23} —intensity of transitions from the state of partial fitness S_2 to the state of partial fitness S_3 ;
- λ_{34} —intensity of transitions from the state of partial fitness S_3 to the state of partial unfitness S_4 ;
- λ_{45} —intensity of transitions from the state of partial unfitness S_4 to the state of full unfitness S_5 .

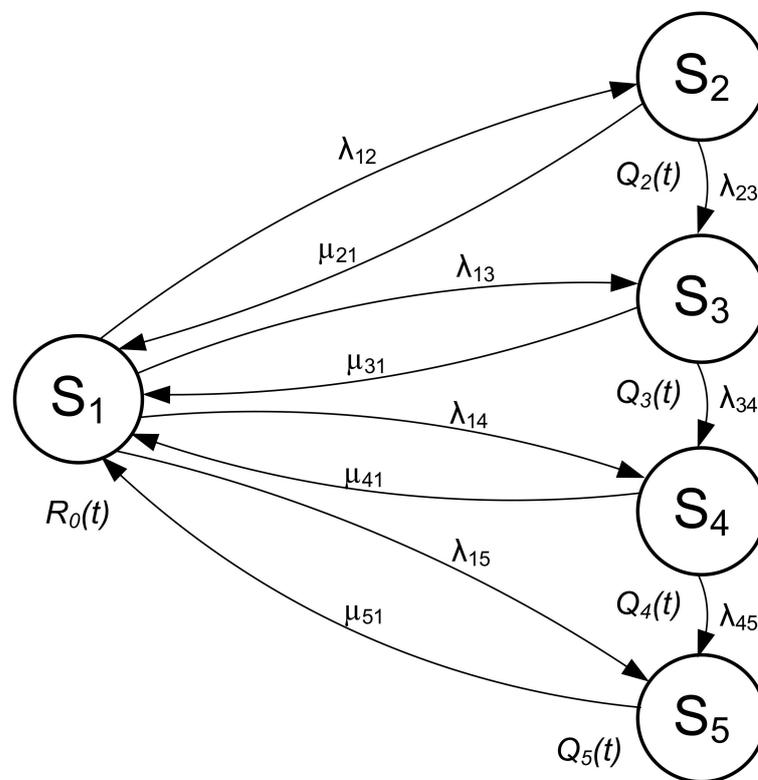


Figure 5. Operational model of a CCTV system. Source: own study.

The operating model in Figure 5 is shown in the form of Kolmogorov–Chapman equations.

$$R'_0(t) = -\lambda_{12} \cdot R_0(t) + \mu_{21} \cdot Q_2(t) - \lambda_{13} \cdot R_0(t) + \mu_{31} \cdot Q_3(t) - \lambda_{14} \cdot R_0(t) + \mu_{41} \cdot Q_4(t) - \lambda_{15} \cdot R_0(t) + \mu_{51} \cdot Q_5(t) \quad (1)$$

$$Q'_2(t) = \lambda_{12} \cdot R_0(t) - \mu_{21} \cdot Q_2(t) - \lambda_{23} \cdot Q_2(t) \quad (2)$$

$$Q'_3(t) = \lambda_{13} \cdot R_0(t) - \mu_{31} \cdot Q_3(t) - \lambda_{34} \cdot Q_3(t) + \lambda_{23} \cdot Q_2(t) \quad (3)$$

$$Q'_4(t) = \lambda_{14} \cdot R_0(t) - \mu_{41} \cdot Q_4(t) - \lambda_{45} \cdot Q_4(t) + \lambda_{34} \cdot Q_3(t) \quad (4)$$

$$Q'_5(t) = \lambda_{15} \cdot R_0(t) - \mu_{51} \cdot Q_5(t) + \lambda_{45} \cdot Q_4(t) \quad (5)$$

Assuming baseline conditions:

$$R_0(0) = 1 \quad (6)$$

$$Q_2(0) = Q_3(0) = Q_4(0) = Q_5(0) = 0 \quad (7)$$

Applying the Laplace transform, the following system of linear equations is obtained:

$$s \cdot R^*_0(s) - 1 = -\lambda_{12} \cdot R^*_0(s) + \mu_{21} \cdot Q^*_2(s) - \lambda_{13} \cdot R^*_0(s) + \mu_{31} \cdot Q^*_3(s) - \lambda_{14} \cdot R^*_0(s) + \mu_{41} \cdot Q^*_4(s) - \lambda_{15} \cdot R^*_0(s) + \mu_{51} \cdot Q^*_5(s) \quad (8)$$

$$s \cdot Q^*_2(s) = \lambda_{12} \cdot R^*_0(s) - \mu_{21} \cdot Q^*_2(s) - \lambda_{23} \cdot Q^*_2(s) \quad (9)$$

$$s \cdot Q^*_3(s) = \lambda_{13} \cdot R^*_0(s) - \mu_{31} \cdot Q^*_3(s) - \lambda_{34} \cdot Q^*_3(s) + \lambda_{23} \cdot Q^*_2(s) \quad (10)$$

$$s \cdot Q^*_4(s) = \lambda_{14} \cdot R^*_0(s) - \mu_{41} \cdot Q^*_4(s) - \lambda_{45} \cdot Q^*_4(s) + \lambda_{34} \cdot Q^*_3(s) \quad (11)$$

$$s \cdot Q^*_5(s) = \lambda_{15} \cdot R^*_0(s) - \mu_{51} \cdot Q^*_5(s) + \lambda_{45} \cdot Q^*_4(s) \quad (12)$$

The probabilities for a video surveillance system to stay in given operating states of the system are as follows:

$$R^*_0(s) = \frac{(\lambda_{23} + s + \mu_{21}) \cdot (\lambda_{34} + s + \mu_{31}) \cdot (\lambda_{45} + s + \mu_{41}) \cdot (s + \mu_{51})}{(\lambda_{13} \cdot (\lambda_{23} \cdot \mu_{31} \cdot (\lambda_{45} + s + \mu_{41}) \cdot (s + \mu_{51}) + \mu_{21} \cdot (\lambda_{34} + s + \mu_{31}) \cdot (\lambda_{45} + s + \mu_{41}) \cdot (s + \mu_{51}) + \lambda_{23} \cdot \lambda_{34} \cdot (s \cdot \mu_{41} + (\lambda_{45} + \mu_{41}) \cdot \mu_{51})) + (\lambda_{23} + s + \mu_{21}) \cdot (\lambda_{13} \cdot (\lambda_{34} \cdot \lambda_{45} \cdot \mu_{51} + \lambda_{34} \cdot \mu_{41} \cdot (s + \mu_{51}) + \mu_{31} \cdot (\lambda_{45} + s + \mu_{41}) \cdot (s + \mu_{51})) + (\lambda_{34} + s + \mu_{31}) \cdot (\lambda_{14} \cdot (s \cdot \mu_{41} + (\lambda_{45} + \mu_{41}) \cdot \mu_{51}) + (\lambda_{45} + s + \mu_{41}) \cdot (\lambda_{15} \cdot \mu_{51} - (\lambda_{12} + \lambda_{13} + \lambda_{14} + \lambda_{15} + s) \cdot (s + \mu_{51}))))))} \quad (13)$$

$$Q^*_2(s) = \frac{(\lambda_{12} \cdot (\lambda_{34} + s + \mu_{31}) \cdot (\lambda_{45} + s + \mu_{41}) \cdot (s + \mu_{51}))}{(s \cdot (\lambda_{12} \cdot (\lambda_{23} \cdot (\lambda_{45} + s + \mu_{41}) \cdot (s + \mu_{51}) + (\lambda_{34} + s + \mu_{31}) \cdot (\lambda_{45} + s + \mu_{41}) \cdot (s + \mu_{51}) + \lambda_{23} \cdot \lambda_{34} \cdot (\lambda_{45} + s + \mu_{51})) + (\lambda_{23} + s + \mu_{21}) \cdot ((\lambda_{34} + s + \mu_{31}) \cdot ((\lambda_{45} + s + \mu_{41}) \cdot (\lambda_{15} + s + \mu_{51}) + \lambda_{14} \cdot (\lambda_{45} + s + \mu_{51})) + \lambda_{13} \cdot ((\lambda_{45} + s + \mu_{41}) \cdot (s + \mu_{51}) + \lambda_{34} \cdot (\lambda_{45} + s + \mu_{51}))))))} \quad (14)$$

$$Q^*_3(s) = \frac{((\lambda_{12} \cdot \lambda_{23} + \lambda_{13} \cdot (\lambda_{23} + s + \mu_{21})) \cdot (\lambda_{45} + s + \mu_{41}) \cdot (s + \mu_{51}))}{(s \cdot (\lambda_{12} \cdot (\lambda_{23} \cdot (\lambda_{45} + s + \mu_{41}) \cdot (s + \mu_{51}) + (\lambda_{34} + s + \mu_{31}) \cdot (\lambda_{45} + s + \mu_{41}) \cdot (s + \mu_{51}) + \lambda_{23} \cdot \lambda_{34} \cdot (\lambda_{45} + s + \mu_{51})) + (\lambda_{23} + s + \mu_{21}) \cdot ((\lambda_{34} + s + \mu_{31}) \cdot ((\lambda_{45} + s + \mu_{41}) \cdot (\lambda_{15} + s + \mu_{51}) + \lambda_{14} \cdot (\lambda_{45} + s + \mu_{51})) + \lambda_{13} \cdot ((\lambda_{45} + s + \mu_{41}) \cdot (s + \mu_{51}) + \lambda_{34} \cdot (\lambda_{45} + s + \mu_{51}))))))} \quad (15)$$

$$Q^*_4(s) = \frac{((\lambda_{12} \cdot \lambda_{23} \cdot \lambda_{34} + (\lambda_{23} + s + \mu_{21}) \cdot (\lambda_{13} \cdot \lambda_{34} + \lambda_{14} \cdot (\lambda_{34} + s + \mu_{31}))) \cdot (s + \mu_{51}))}{(s \cdot (\lambda_{12} \cdot (\lambda_{23} \cdot (\lambda_{45} + s + \mu_{41}) \cdot (s + \mu_{51}) + (\lambda_{34} + s + \mu_{31}) \cdot (\lambda_{45} + s + \mu_{41}) \cdot (s + \mu_{51}) + \lambda_{23} \cdot \lambda_{34} \cdot (\lambda_{45} + s + \mu_{51})) + (\lambda_{23} + s + \mu_{21}) \cdot ((\lambda_{34} + s + \mu_{31}) \cdot ((\lambda_{45} + s + \mu_{41}) \cdot (\lambda_{15} + s + \mu_{51}) + \lambda_{14} \cdot (\lambda_{45} + s + \mu_{51})) + \lambda_{13} \cdot ((\lambda_{45} + s + \mu_{41}) \cdot (s + \mu_{51}) + \lambda_{34} \cdot (\lambda_{45} + s + \mu_{51}))))))} \quad (16)$$

$$Q^*_5(s) = \frac{(\lambda_{12} \cdot \lambda_{23} \cdot \lambda_{34} \cdot \lambda_{45} + (\lambda_{23} + s + \mu_{21}) \cdot (\lambda_{13} \cdot \lambda_{34} \cdot \lambda_{45} + (\lambda_{34} + s + \mu_{31}) \cdot (\lambda_{14} \cdot \lambda_{45} + \lambda_{15} \cdot (\lambda_{45} + s + \mu_{41}))))}{(s \cdot (\lambda_{12} \cdot (\lambda_{23} \cdot (\lambda_{45} + s + \mu_{41}) \cdot (s + \mu_{51}) + (\lambda_{34} + s + \mu_{31}) \cdot (\lambda_{45} + s + \mu_{41}) \cdot (s + \mu_{51}) + \lambda_{23} \cdot \lambda_{34} \cdot (\lambda_{45} + s + \mu_{51})) + (\lambda_{23} + s + \mu_{21}) \cdot ((\lambda_{34} + s + \mu_{31}) \cdot ((\lambda_{45} + s + \mu_{41}) \cdot (\lambda_{15} + s + \mu_{51}) + \lambda_{14} \cdot (\lambda_{45} + s + \mu_{51})) + \lambda_{13} \cdot ((\lambda_{45} + s + \mu_{41}) \cdot (s + \mu_{51}) + \lambda_{34} \cdot (\lambda_{45} + s + \mu_{51}))))))} \quad (17)$$

A computer simulation enables one to quickly determine the impact of changes in various reliability and operational indicators on the values of indicators describing the states of the analysed railway video surveillance system. System repair and damage intensities shown in Table 1 were adopted for the analysis. The adopted values were calculated based on [19–22], as well as operational data provided by the Department of Operation and Passenger Service at PKP Polskie Linie Kolejowe S.A.

Table 1. System reliability parameters.

Parameter	Value (1/h)
λ_{12}	0.00001
λ_{13}	0.00002
λ_{14}	0.000025
λ_{15}	0.000004167
λ_{23}	0.00002
λ_{34}	0.000025
λ_{45}	0.000004167
μ_{21}	0.0208
μ_{31}	0.0416
μ_{41}	0.125
μ_{51}	0.5

By adopting Equations (13)–(17), and by applying the reverse Laplace transform and the values from Table 1, we obtain the following probabilities for the tested system to stay in individual operating states, for an exponential distribution:

- duration of the railway video surveillance system test—1 year:

$$t = 8760 \text{ (h)} \quad (18)$$

- probability of the tested video surveillance system remaining in the state of full fitness S_1 for a period of 1 year:

$$R_0(t) = 0.9988319222061706 \quad (19)$$

- probability of the tested video surveillance system remaining in the state of partial fitness S_2 for a period of 1 year:

$$Q_2(t) = 0.00047974636032957274 \quad (20)$$

- probability of the tested video surveillance system remaining in the state of partial fitness S_3 for a period of 1 year:

$$Q_3(t) = 0.00048014975066258263 \quad (21)$$

- probability of the tested video surveillance system remaining in the state of partial unfitness S_4 for a period of 1 year:

$$Q_4(t) = 0.00019985575200001795 \quad (22)$$

- probability of the tested video surveillance system remaining in the state of full unfitness S_5 for a period of 1 year:

$$Q_5(t) = 8.32593 \cdot 10^{-6} = 0.000008325930837503415 \quad (23)$$

A graph of changes in the probability of the analysed railway video surveillance system remaining in the state of full fitness S_1 for a period of 1 year is shown in Figure 6.

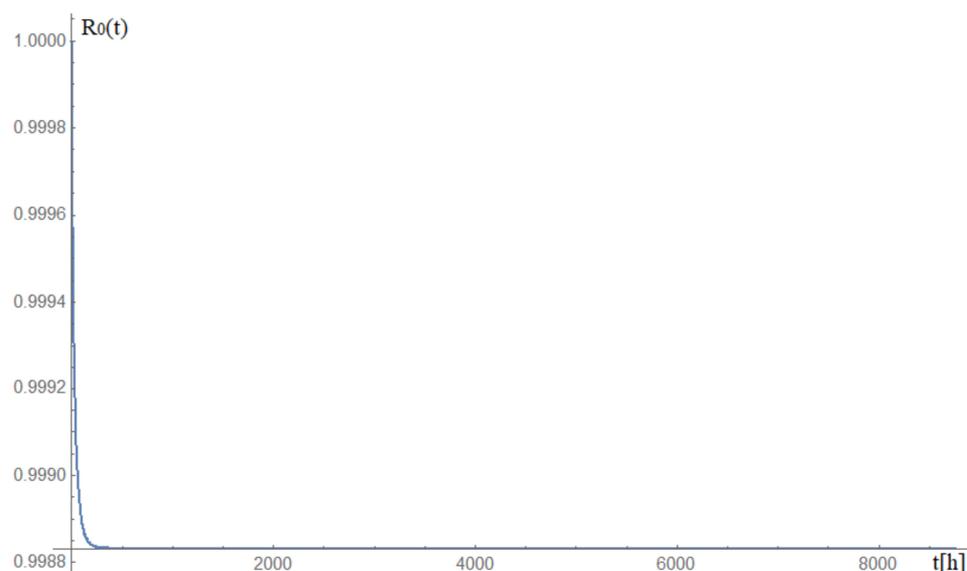


Figure 6. Graph of changes in the probability of the analysed railway video surveillance system remaining in the state of full fitness S_1 for a period of 1 year. Source: own study.

Assuming that the time of restoring the analysed system to the state of full fitness $\mu_{51} = t_{51} - 1$ (h) is confined within a limited range, $t_{51} \in \langle 12; 168 \rangle$ [h]. This means, that within 0.5 to 7 days, it is probable that the analysed CCTV system will find itself in the state of full fitness, which is shown in Figure 7.

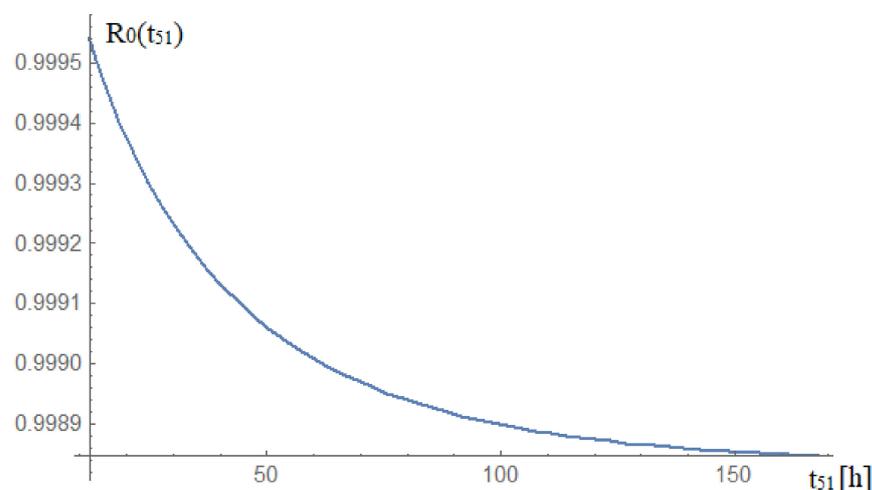


Figure 7. Dependence between the probability of the analysed railway CCTV system staying in the state of full fitness during the restoration of full system fitness. Source: own study.

4. Conclusions

The centralized video surveillance (CCTV) system described in the article is one of the largest solutions of this type under design within the European Union. Current solutions based on an integration platform usually involve single lines or a group of lines with limited territorial coverage (e.g., urban underground).

A centralized CCTV (video surveillance) system satisfies all the requirements that the national railway infrastructure administrator adopted in its regulations and documents that constitute the system basis, i.e., [19–23]. Based on the graph in Figure 7, it is possible to rationalize the actions associated with the possible restoration of full fitness of the analysed railway CCTV system. The time to restore the analysed system to a fully operational state

is within a limited range. The analysed system is in a fully operational state for up to 7 days. The conducted analysis covering the railway CCTV system enables one to assess the security level of the solutions applied therein. A similar operational analysis, but based on the example of GPS receivers, has been conducted and described in [24]. The obtained result, i.e., a ~99.88% probability for a system to stay in the state of full fitness throughout a year, means that the centralized video surveillance system exhibits availability similar to that of other complementary railway systems [25–27], e.g., the GSM-R network (99.95), with 10.5 h downtime per year. Due to the scale and complexity of the system, this is a good result.

This enables one to improve the values of reliability indicators and to rationalize the operation of the tested system. According to [23], further improvement of reliability indicators should be based on increasing the reliability of systems that are not currently redundant (e.g., access switches at railway facilities), and shortening the response times (failure notification and repair) required by [19–22], which will translate to reducing the MTTR Mean Time To Repair parameter, hence improving system reliability. Increasing the requirements in terms of repair speed must be preceded by a profitability analysis; it may entail significantly higher costs.

The resistance of the constructed system to factors not associated with operational damage to the elements will be a separate issue. Both the GS and CBIP are located in the same place (Poznań), and their functions cannot be taken over by any other unit. Therefore, there is a risk that in the event of a natural disaster or a terrorist attack, the centralized CCTV system will remain completely unfit for a prolonged period. It may be justified to implement a redundant server room and service centre located elsewhere, and not in Poznań. Other than that, operational damage was not taken into account in the calculations conducted for the purposes of this article.

The aforementioned article completely omits issues associated with the MPLS backbone network reliability. The analysis of this network's reliability will be the subject matter of another paper. The omission was due to the high reliability resulting from the network structure, i.e., redundant multiple-ring connections. According to the information received from the Department of Operation and Passenger Service at PKP Polskie Linie Kolejowe S.A., the IP MPLS is characterized by reliability exceeding the CCTV system.

Author Contributions: Conceptualization, P.S.; methodology, Z.K., P.S., M.S. and M.R.; validation, Z.K., P.S., M.S. and M.R.; formal analysis, Z.K., P.S., M.S. and M.R.; investigation, Z.K., P.S., M.S. and M.R.; resources, Z.K., P.S., M.S. and M.R.; data curation, P.S. and Z.K. writing—original draft preparation, P.S. and Z.K.; writing—review and editing, P.S. and Z.K.; visualization, P.S. and Z.K.; supervision, P.S. and Z.K.; project administration, P.S. and Z.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Garlikowska, M.; Gondek, P. Sytuacja podróźnych na polskich dworcach kolejowych w aspekcie bezpieczeństwa z uwzględnieniem rozwiązań dla osób niepełnosprawnych. *Prace Instytutu Kolejnictwa* **2017**, *153*, 23–28.
2. Priks, M. The Effects of Surveillance Cameras on Crime: Evidence from the Stockholm Subway. *Econ. J.* **2015**, *125*, 289–305. [[CrossRef](#)]
3. Zarebski, A.; Szmigiel, P. *Wytyczne Dotyczące Projektowania i Budowy Systemów Monitoringu Wizyjnego (SMW) na Obiektach Obsługi Pasażerskiej Ipi-4*; PKP Polskie Linie Kolejowe S.A.: Warszawa, Poland, 2020.
4. Kim, J.; Park, N.; Kim, G.; Jin, S. CCTV video processing metadata security scheme using character order preserving-transformation in the emerging multimedia. *Electronics* **2019**, *8*, 412. [[CrossRef](#)]

5. Brahim, M.B.; Mir, Z.H.; Znaidi, W.; Filali, F.; Hamdi, N. QoS-Aware Video Transmission Over Hybrid Wireless Network for Connected Vehicles. *IEEE Access* **2017**, *5*, 8313–8323. [[CrossRef](#)]
6. Mina Qaisar, S.; Sidiya, D.; Akbar, M.; Subasi, A. An Event-Driven Multiple Objects Surveillance System. *Int. J. Electr. Comput. Eng. Syst.* **2018**, *9*, 35–44. [[CrossRef](#)]
7. Chen, S.; Yu, S.; Lü, J.; Chen, G.; He, J. Design and FPGA-Based Realization of a Chaotic Secure Video Communication System. *IEEE Trans. Circuits Syst. Video Technol.* **2018**, *28*, 2359–2371. [[CrossRef](#)]
8. Chumuang, N.; Ketcham, M.; Yingthawornsuk, T. CCTV based surveillance system for railway station security. In Proceedings of the International Conference on Digital Arts, Media and Technology (ICDAMT), Phayao, Thailand, 25–28 February 2018; pp. 7–12. [[CrossRef](#)]
9. Hadiwardoyo, S.A.; Gao, L. Integrating a Middleware DDS Application for Safety Purposes in an Underground Railway Environment. In Proceedings of the 3rd International Conference on Computer and Communication Systems (ICCCS), Nagoya, Japan, 27–30 April 2018; pp. 46–50. [[CrossRef](#)]
10. Punn, N.S.; Agarwal, S. Crowd Analysis for Congestion Control Early Warning System on Foot Over Bridge. In Proceedings of the 2019 Twelfth International Conference on Contemporary Computing (IC3), Noida, India, 8–10 August 2019; pp. 1–6. [[CrossRef](#)]
11. Park, H.; Park, S.; Joo, Y. Robust Detection of Abandoned Object for Smart Video Surveillance in Illumination Changes. *Sensors* **2019**, *19*, 5114. [[CrossRef](#)] [[PubMed](#)]
12. Wang, Y.; Zhu, L.; Yu, Z.; Guo, B. An Adaptive Track Segmentation Algorithm for a Railway Intrusion Detection System. *Sensors* **2019**, *19*, 2594. [[CrossRef](#)] [[PubMed](#)]
13. Ullah, F.U.M.; Ullah, A.; Muhammad, K.; Haq, I.U.; Baik, S.W. Violence Detection Using Spatiotemporal Features with 3D Convolutional Neural Network. *Sensors* **2019**, *19*, 2472. [[CrossRef](#)] [[PubMed](#)]
14. Rodolfo, Q.; Darwin, T.; Adín, R.; Helio, P. Multi-Stream Networks and Ground Truth Generation for Crowd Counting. *Int. J. Electr. Comput. Eng. Syst.* **2020**, *11*, 33–41. [[CrossRef](#)]
15. Gajbhiye, P.; Naveen, C.; Satpute, V.R. VIRTUe: Video surveillance for rail-road traffic safety at unmanned level crossings. In Proceedings of the 2017 IEEE Region 10 Symposium (TENSYP), Cochin, India, 14–16 July 2017. [[CrossRef](#)]
16. Paś, J.; Rosiński, A.; Białek, K. A reliability-operational analysis of a track-side CCTV cabinet taking into account interference. *Bull. Pol. Acad. Sci. Tech. Sci.* **2021**, *69*, e136747. [[CrossRef](#)]
17. Khac-Hoai Nam, B.; Hongsuk, Y.; Jiho, C. A Multi-Class Multi-Movement Vehicle Counting Framework for Traffic Analysis in Complex Areas Using CCTV Systems. *Energies* **2020**, *13*, 2036. [[CrossRef](#)]
18. Veena, B.M. Reliability Analysis in Telecommunications. *Not. Am. Math. Soc. Commun.* **2020**, *67*, 6. [[CrossRef](#)]
19. Alessio, G.; Sergio, S. AdViSED: Advanced Video Smoke Detection for Real-Time Measurements in Antifire Indoor and Outdoor Systems. *Energies* **2020**, *13*, 2098. [[CrossRef](#)]
20. Zarebski, A.; Szmigiel, P. *Wytyczne Dotyczące Projektowania i Budowy Systemów Monitoringu Wizyjnego (SMW) na Obiektach Obsługi Pasażerskiej Ipi-5; PKP Polskie Linie Kolejowe S.A.: Warsaw, Poland, 2020.*
21. Zarebski, A.; Szmigiel, P. *Appendix No. 4 (Platform integrating PSIM (Physical Security Information Management)) to OPZ for Unlimited Tender on: Zaprojektowanie, dostawa i instalacja elementów prezentacji dynamicznej informacji pasażerskiej oraz systemu monitoringu wizyjnego wraz z infrastrukturą techniczną na dworcach, stacjach i przystankach kolejowych w ramach realizacji projektu pn. Projekt, dostawa i instalacja elementów prezentacji dynamicznej informacji pasażerskiej oraz systemu monitoringu wizyjnego wraz z infrastrukturą techniczną na dworcach, stacjach i przystankach kolejowych; PKP Polskie Linie Kolejowe S.A.: Warsaw, Poland, 2018.*
22. Zarebski, A.; Szmigiel, P. *Appendix No. 7 (Guidelines for a telecommunications container for the needs of GS1 server rooms) to the OPZ for Unlimited Tender for: Zaprojektowanie, dostawa i instalacja elementów prezentacji dynamicznej informacji pasażerskiej oraz systemu monitoringu wizyjnego wraz z infrastrukturą techniczną na dworcach, stacjach i przystankach kolejowych w ramach realizacji projektu pn. Projekt, dostawa i instalacja elementów prezentacji dynamicznej informacji pasażerskiej oraz systemu monitoringu wizyjnego wraz z infrastrukturą techniczną na dworcach, stacjach i przystankach kolejowych; PKP Polskie Linie Kolejowe S.A.: Warsaw, Poland, 2018.*
23. Zarebski, A.; Szmigiel, P. *Wymagania na transmisję danych systemów SMW, SPA i SDIP oraz integrację z siecią teletransmisyjną PKP Polskie Linie Kolejowa S.A. Ie-122; PKP Polskie Linie Kolejowe S.A.: Warsaw, Poland, 2019.*
24. *PN-EN 62676-1-1 Systemy dozоровe CCTV stosowane w zabezpieczeniach—Część 1-1: Wymagania systemowe; PKN Poland: Warsaw, Poland, 2014.*
25. Rychlicki, M.; Kasprzyk, Z.; Rosiński, A. Analysis of Accuracy and Reliability of Different Types of GPS Receivers. *Sensors* **2020**, *20*, 6498. [[CrossRef](#)] [[PubMed](#)]
26. Malfait, W.; Domingo, B.; Spaans, C.; Holvad, T. Operational Requirements Of Railway Radio Communication Systems. Available online: https://www.era.europa.eu/sites/default/files/library/docs/ex_post_evaluation/era_ee_ex_post_operational_radio_requirements_en.pdf (accessed on 20 October 2021).
27. Szmigiel, P.; Kasprzyk, Z. Assessment of Availability of Railway Video Surveillance System. In *Research Methods and Solutions to Current Transport Problems*; Springer: Cham, Switzerland, 2020; pp. 430–439. [[CrossRef](#)]