water

MDPI

Article

Use Case of Water Reservoir Protection as a Critical Infrastructure Element in Slovakia Using a Quantitative Approach

Tomáš Loveček [1], Ladislav Mariš [1,*] and Katarína Petrlová [2]

[1] Faculty of Security Engineering, University of Žilina, 010 26 Žilina, Slovakia; tomas.lovecek@uniza.sk
[2] Mathematical Institute in Opava, Silesian University in Opava, Na Rybníčku 626/1, 74 601 Opava, Czech Republic; katarina.petrlova@math.slu.cz
* Correspondence: ladislav.maris@uniza.sk; Tel.: +421-902-544-534

Abstract: Water management systems play a crucial role in efficiently allocating water resources while taking into account various demands such as agriculture, industry, domestic use, and environmental needs. These systems optimize the distribution of water, ensuring fair access and minimizing water scarcity and conflicts. However, these critical systems are vulnerable to different types of attacks. Depending on the target, these attacks can take the form of physical, cyber, or combined assaults. The protection requirements for water objects, which are integral to critical infrastructure, are primarily defined by legal regulations, technical standards, and other third party requirements. These requirements necessitate the implementation of protective measures. One effective approach to implementing protective measures is through a physical protection system (PPS), which prevents unauthorized individuals from achieving their objectives. The current procedures for protecting these objects can be based on either a qualitative or quantitative approach. In this article, we present a use case that demonstrates a possible method for protecting a specific water reservoir, identified as a national element of critical infrastructure in the Drinking Water Provision subsector. The use case involves analyzing security requirements and designing a PPS for the water reservoir. To assess the effectiveness of the proposed PPS, a quantitative PPS model was developed using specialized software. Additionally, four potential attack scenarios were simulated to verify the functionality of the PPS.

Keywords: water reservoir; critical infrastructure elements; physical protection system; model; simulation; physical attack

Citation: Loveček, T.; Mariš, L.; Petrlová, K. Use Case of Water Reservoir Protection as a Critical Infrastructure Element in Slovakia Using a Quantitative Approach. *Water* **2023**, *15*, 2818. https://doi.org/10.3390/w15152818

Academic Editor: Stavroula Tsitsifli

Received: 26 June 2023
Revised: 28 July 2023
Accepted: 1 August 2023
Published: 4 August 2023

1. Introduction

Water reservoirs are susceptible to various types of attacks that can jeopardize water quality, disrupt service, and pose risks to public health and safety. The following text presents real-world examples of attacks on water reservoirs, highlighting their consequences and the lessons learned. In 1993, Milwaukee, Wisconsin, experienced a major outbreak of Cryptosporidium, a waterborne parasite, due to inadequate filtration and disinfection practices. The contamination affected the city's water reservoir and led to over 400,000 cases of illness and 69 deaths. This incident highlighted the need for improved water treatment and surveillance systems to prevent and respond to waterborne disease outbreaks [1]. In May 2000, contaminated groundwater infiltrated the municipal water supply system in Walkerton, Ontario, Canada, leading to a widespread outbreak of *Escherichia coli* infections. The contamination was traced back to a cattle farm near one of the wells supplying the reservoir. The incident resulted from a combination of inadequate water treatment processes, flawed monitoring, and an improper response to the detected contamination [2]. During the Iraq war in 2003, several incidents of deliberate sabotage targeted water reservoirs and treatment facilities. The attackers aimed to disrupt water supply, degrade infrastructure, and create chaos. These acts of sabotage resulted in severe

water shortages and compromised sanitation services in various regions of Iraq [3]. Back in 2013, an individual hacker managed to gain remote access to the Supervisory Control and Data Acquisition (SCADA) system that controlled the Bowman Avenue Dam located in Rye Brook, New York. Despite the fact that the attack had no operational consequences as the dam was offline at the time, it sparked concerns regarding the susceptibility of vital water infrastructure to cyber–physical attacks [4]. In 2014, two individuals attempted to poison the drinking water supply at the Lake Forest Reservoir in California. The attackers, with access to the reservoir site, poured a harmful substance into the water. However, their actions were detected before the contaminated water entered the distribution system. This incident emphasized the importance of rigorous security protocols, surveillance systems, and prompt incident response [5]. In 2019, a group of individuals attempted to poison a water reservoir in regional Victoria, Australia. They released a hazardous substance into the reservoir, targeting a specific community. The plot was detected early, and swift action prevented the contamination from reaching the water supply, underscoring the importance of robust monitoring systems and rapid response protocols [6]. In 2023, an attack on the Nova Kachovka Dam, located in the southern territory of Ukraine, currently occupied by Russia, was recorded. It is one of the biggest industrial and ecological disasters in Europe for decades. It is still impossible to say whether the dam collapsed because it was deliberately targeted or if the breach could have been caused by structural failure [7]. However, it is a fact that Nova Kakhovka is situated in a conflict-affected region due to Russia's aggression against Ukraine. This unfortunate disaster would not have occurred if it were not for the war, which served as an attack vector leading to the event. In times of peace, it would be possible to prevent structural failures. These examples of attacks on water reservoirs illustrate the potential consequences and vulnerabilities associated with such incidents. They emphasize the importance of implementing robust security measures, conducting regular risk assessments, and maintaining strong response capabilities. By learning from these cases, water utilities and stakeholders can enhance the security and resilience of water reservoirs, safeguarding the integrity and availability of clean water for communities.

The security and protection of water reservoirs is crucial to ensure the reliability, safety and security and of our water supplies. The state of the art in this area involves a multidisciplinary approach that includes physical security measures, cybersecurity measures, and risk management strategies. The U.S. Environmental Protection Agency provides guidance for assessing the risks to water facilities and developing mitigation strategies in their document "Security Risk Assessment for Water Utilities" [8]. Similarly, the U.S. Department of Homeland Security offers information on protecting water infrastructure from physical and cyber threats in "Protecting Critical Infrastructure: Water Sector Security" [9]. The World Health Organization (WHO) has published "Water Security Handbook" [10], which provides guidance for developing water security plans for water contamination incidents. The Water Environment Federation also offers a resource on the integration of cybersecurity and physical security measures in protecting water systems in "Cybersecurity and Physical Security: A Unified Approach to Water System Protection" [11]. The book "Security of Water Supply Systems" presents a complex overview of the security issues related to water supply systems, including risk assessment, physical security, and cybersecurity [12]. In addition to these resources, the National Institute of Standards and Technology published a guideline for improving critical infrastructure cybersecurity in their document "Framework for Improving Critical Infrastructure Cybersecurity" [13]. The American Water Works Association (AWWA) has also published a document on management for water facilities [14,15]. In general, ensuring the security of water reservoirs requires a comprehensive approach that encompasses various disciplines such as physical security, cybersecurity, and risk management considerations.

In the European Union, a new directive focused on the resilience of critical entities was adopted in 2022. This directive provides a framework for defining the requirements for protecting critical infrastructure elements [16]. It also obliges member states to incorporate

these security requirements into their national legislation. For example, in the Slovak Republic, this is regulated by the Critical Infrastructure Act [17]. Additionally, standardization organizations such as CENELEC or CEN, responsible for European technical standardization, have issued several technical specifications [18–20] that address the protection of national strategic objects. None of these standards is primarily focused on the protection of water management facilities, as is the case in the United States. Some countries have their own national technical standards issued by their normalization authorities specifically focused to protect critical infrastructure [21]. Regardless of the country of origin, output format, or protected asset, all the aforementioned approaches or standards are based on best practices, but these practices were obtained at a certain time and under specific conditions. However, none of them applies an approach that would allow an objective determination of the level of protection for the protected asset (e.g., water reservoir) based on measurable indicators. The aim of this article is to present, using a specific case study, the possibilities of establishing the minimum level of protection for a water reservoir as a critical infrastructure element, taking into account not only the security requirements of legal regulations and technical standards but also a quantitative approach that enables an objective assessment of the existing or proposed minimum level of physical protection.

2. Materials and Methods

The protection requirements against unauthorized people who intend to cause damage, destruction, or theft of protected physical or non-physical property within an object, which is owned or managed by an individual or organization, are primarily established by legally binding regulations, technical standards, national or international norms, and the demands of insurance companies or other third parties, including parent companies or strategic customers. These requirements necessitate the implementation of specific protective measures that are structured in a manner to safeguard the property of the owner or operator. Asset protection involves establishing a secure state through the utilization of protective measures, which aim to prevent or halt any undesirable activities or events (such as an electrical short circuit and resulting fire) that are contrary to the interests of the property's owner or manager. In this context, the physical protection system (PPS) serves as the means to achieve this secure state.

PPS serves as a convenient and effective means of organizing protective measures to prevent unauthorized individuals from achieving their goals, which may involve activities such as theft, damage, or destruction of protected assets. This system comprises a combination of technical and procedural security measures or components, including alarm systems, mechanical barriers, security services, and procedural measures. Mechanical barriers are designed to deter, impede, or halt the progress of unauthorized individuals or intruders, while alarm systems are responsible for detecting their presence and triggering an alert state. Security services play a crucial role in ensuring timely intervention and apprehension of intruders. Additionally, procedural measures, part of regime protection, are in place to ensure the effective functioning of these protective measures. [22].

During the planning, design, implementation, or operation stages of building protection systems, it is possible to assess the functionality, economic efficiency, reliability, and quality of the PPS from an evaluative perspective. [23].

A functional PPS is one that meets a fundamental requirement, namely that the time it takes for an attack (including the total time for breaching mechanical barriers and the intruder's movement) is longer than the response time of the intervention unit, starting from the initial detection point. This means that the PPS is considered operational if the ratio of these times, in that order, is greater than one.

In the case of an intruder whose intention is to steal a protected asset for subsequent monetization, it is sufficient to detain them at the latest at the point of attempted escape, thereby prolonging the overall response time of the intervention unit. However, when dealing with an intruder whose objective is to cause damage or destroy a protected asset through sabotage or a terrorist attack, it becomes necessary to detain them before they

achieve their goal, i.e., before the protected asset is harmed or destroyed. In such cases, the time of attempted escape cannot be calculated. [22,24].

In practice, it can be challenging to provide a credible demonstration that the system meets the fundamental requirement for its functionality. Existing procedures for object protection use one of two basic approaches [25]:

- A quantitative approach;
- A qualitative approach.

When employing a qualitative approach, procedures rely on expert assessments by evaluators. In these cases, it is not feasible to precisely verify the adequacy of the proposed level of protection. Instead, one must depend on the expertise of the procedure designers. Consequently, it is challenging to determine whether the physical protection system (PPS) is undersized or oversized relative to the proposed protective measures using this approach.

Conversely, procedures that adopt a quantitative approach allow for a precise demonstration of the rationale behind the proposed protection measures. This is achieved by utilizing measurable input and output parameters. In such cases, it becomes possible to verify that the PPS, considering the proposed protection measures, is neither undersized nor oversized. For the purposes of establishing a quantitative approach, four basic models were created [26]: pessimistic, realistic, pragmatic, and optimistic models. The fundamental difference between these models lies in the intruder's decision-making approach (decision-making under certainty and uncertainty) and the method of defining input parameters. Input parameters are considered either constant (deterministic modeling) or random variables defined by the corresponding probability distribution (stochastic modeling). Deterministic models are those that do not use probabilities in their expressions, thereby excluding random variables and emphasizing causality. However, by excluding random variables, inherent internal factors (such as human factors or chance) that can have a significant impact are limited. These models exclude or reduce the influence of the environment, which stochastic models aim to address by introducing an element of randomness into the entire problem (e.g., selecting the intruder's path or the order of tools used).

The pessimistic and realistic models describe the intruder's decision-making under conditions of certainty, while the pragmatic and optimistic models describe decision-making under conditions of uncertainty. In terms of input parameters, the pessimistic and pragmatic models consider them as constant (extreme) values (e.g., the maximum response time of the intervention unit, and minimum breakthrough resistance of barriers), whereas the realistic and optimistic models consider them random variables. There are currently several software tools using quantitative or qualitative approaches for evaluating the functionality of a protection system (Table 1).

Table 1. Software tools using qualitative or quantitative approaches for evaluating the functionality of a PPS [22].

Qualitative Approach		**Quantitative Approach**	
Tool/Software	**Country**	**Tool/Software**	**Country**
Risk Watch	USA	SAVI, ASSESS	Sandia National Laboratories, USA
		Sprut	Scientific and Production Enterprise ISTA SYSTEMS JS Co., Russia
CRAMM	UK	SAPE	Korea Institute of Nuclear Non-proliferation and Control, Republic of Korea
		SATANO	University of Žilina, Faculty of Security Engineering, the Slovak Republic

The software tool SATANO was developed at the University of Žilina, is a simulation tool that allows you to quantitatively assess the level of PPS on various 2D map documents. The software tool was created as one of the outputs of the CI-PAC project, Critical Infrastructure Protection Against Chemical Attack (HOME/2013/CIPS/AG/4000005073). SATANO utilizes a quantitative approach, meaning it is based on the fundamental premise that it is necessary to implement enough protective measures to detect and apprehend

the intruder before they reach their target, which is considered the damage or destruction of the protected asset (e.g., water reservoir). The tool integrates a pessimistic (deterministic) model that excludes any random influences that could occur during an attempt to breach the protected space. It assumes that the intruder has all the necessary information about the protected area (deciding with certainty) and is aware of the critical path to the protected asset. This critical path is characterized by the shortest total time for breaching all barriers, including the time required for the intruder to move from the moment of alarm system detection. From the perspective of input parameters, SATANO takes into account breakthrough resistances of mechanical barriers in relation to the type of tool used, the overall response time of the intervention unit, the intruder's moving times, the probabilities of correct detection by the alarm system, and the detection characteristics of the alarm systems. From the perspective of output parameters, SATANO considers the effectiveness coefficient of protective measures, the probability of eliminating the intruder, and the critical detection point.

The main innovative contribution of the SATANO tool is the ability to create more complex attack scenarios, such as attacks by individuals using different types of tools. Existing tools do not allow for the modeling of more complicated scenarios where the method of attack changes, such as the intruder releasing a chemical substance into the ventilation or pipeline system after overcoming certain barriers. An attack scenario in SATANO represents a description of 1 to N steps in an attack vector, where the vector progressively moves from the access point to the target location and sequentially achieves 0 to N-1 partial objectives of the attack, which can optionally transform into another attack vector. In terms of physical protection, a vector can be designated as an entity that, based on its properties and abilities (physical, chemical, and personal—knowledge, skills, and experience), has the potential to cause a negative consequence. The attack vector is then the environmentally determined approach or method by which the vector (entity) executes the attack in a given space, direction, and time. In order to discuss the effectiveness of PPS, every entity that has the potential to cause a negative consequence must be detected, slowed down, and subsequently eliminated in a timely manner, regardless of whether it is a human proceeding with tools to overcome barriers or a chemical substance spreading in water. Essentially, it still involves the action of an entity and the subsequent reaction of the system, with only the relevant elements of the system designed for detecting, slowing down, or eliminating the specific entity being altered. In practical applications, the qualitative approach is predominantly utilized, despite it introducing a significant level of subjectivity to the proposal of the PPS. This is primarily due to the absence of actual values for important input parameters, including the following:

- The reliability of alarm system components;
- The reliability of the human factor involved;
- The probability of detection by alarm systems, influenced by the intruder's familiarity with the technologies employed (e.g., the method used to assess changes in physical quantities resulting from breaching the protected area);
- The breakthrough resistances of mechanical barriers, which vary based on the specific tools employed to overcome them;
- The lack of precise real values for these input quantities, which contributes to the reliance on subjective assessments within the qualitative approach for PPS proposals.

Due to the aforementioned factors, these tools are currently only applied in specific areas (e.g., nuclear protection) or are still in the developmental stage within various research institutions. In practical applications, procedures based on a qualitative approach are more commonly employed. These procedures can be further categorized as follows [22]:

- The directive approach: This approach involves precisely defining protective measures without considering the operational details or the environment in which the object is situated.
- The variant approach: In this approach, a finite number of proposed solutions are available, allowing for the selection of different combinations of protective measures.

This approach enables some consideration of the operational and environmental specifics, as well as the financial, technical, and personnel capabilities of the facility's owner or manager.

The initial and crucial phase in the design process of the physical protection system (PPS) involves establishing the minimum level of protection. This determination then guides the selection of technical solutions for alarm systems, mechanical barriers, as well as the arrangement, parameters, and functionalities of the system. The minimum level of protection dictates which protective measures should be implemented, their respective proportions, and specific characteristics (such as security degree/class, purpose of use, key parameters of system elements, and their dislocation). The determination of the minimum level of protection can be derived from what is commonly referred to as security requirements. These requirements can originate from various sources, including the following:

- The essential condition for the functionality of the PPS;
- Third parties, which may include the following:
    - Standards organizations, through normative standards;
    - The state, through legally binding regulations;
    - Customers, in the form of contractual terms or recommendations;
    - Insurance companies, through terms and conditions;
    - Parent companies, through internal organizational regulations;
    - Other third parties, through regulations, contracts, norms, standards, and similar guidelines.

When determining the minimum level of protection, a quantitative approach should be employed if it is based on fulfilling the fundamental condition of the protection system's functionality. This approach utilizes time and probabilistic factors to determine input and output quantities such as breakthrough times, transfer and reaction times, and detection probabilities. On the other hand, when establishing the minimum level of protection based on the security requirements set by third parties, a qualitative approach is commonly used. This can involve either a directive approach or a variant approach. In many cases, setting the minimum level of protection is closely linked to the risk management process. As risk levels increase, the requirements for protective measures expand and become more stringent. For example, the security class of alarm systems may need to be elevated. While the risk management process may not directly impact the resulting minimum level of protection, it significantly influences the positioning of protection measure elements, such as cameras, detectors, and mechanical barriers. The risk assessment process concerning the protection of objects against intentional threats is governed by international and national regulations, norms, and standards specific to particular fields of application, such as classified information, the protection of critical infrastructure, safeguarding banking entities, or securing residential premises. Once the minimum level of protection has been determined, outlining the specific protection measures along with their corresponding characteristics and parameters (such as security level or class, intended purpose, and key system element parameters), the next step involves deciding on the placement of individual protection measures, systems, and their components. This entails determining the appropriate locations for cameras, detectors, mechanical barriers, and other relevant elements. The position of individual PPS elements is influenced by a number of requirements, of which the most important include the following:

- Dislocation given by a minimum level of protection;
- Dislocation given by manufacturers' recommendations;
- Dislocation given by the parameters of protective measures;
- Dislocation due to technical regulations;
- Dislocation due to the risk assessment process, or vulnerability analysis;
- Dislocation due to environmental influence.

Once the parameters and operating conditions have been determined, the next step is to search for a specific manufacturer or seller in the market who offers a product that meets all the defined requirements. In cases where such a product is not available or economically disadvantageous, it becomes necessary to achieve these requirements by combining multiple products. However, it is crucial to ensure that the required minimum level of protection, the intended purpose of individual protective measures, and the placement of protective measures remain unaltered. For instance, a dedicated area can be covered by multiple elements of alarm systems, such as detectors or cameras. While some variation may occur in the system design, it is essential to maintain the intended purpose of each protective measure and uphold the required minimum level of protection.

3. Results

This chapter specifically elaborates on the security requirements of the PPS of water reservoir, from the determination of the purpose and the required minimum level of protection, through the dislocation of individual protection elements, to the design of technical solution parameters and operating conditions of the protection system. This use case may be part of the reservoir operator's security plan.

The Vodňany water reservoir, as an engineered structure with a defined boundary and perimeter, is recognized as a critical infrastructure element (CIE) according to sectoral and cross-sectional criteria. The disturbance or destruction of this reservoir could have severe adverse effects on the quality of life for residents, including risks to their safety, health, and the environment. This classification is based on the provisions of the Critical Infrastructure Act. [17]. It is a standalone building located in the outskirts of the city of Žilina, situated in central Slovakia. The water reservoir does not have a permanent presence of staff. It is a building from the 1970s with standard opening fillings and without enhanced passive resistance. Additionally, there are no alarm systems implemented in the facility. Currently, it serves as a source of drinking water for a town with 6000 residents, located approximately 1.5 km away. The Vodňany reservoir is part of the group reservoir Žilina—Southwest. The water reservoir is gradually fed from the water source Fačkov to the intermittent water reservoir Vodňany. The yield of the Fačkov water source is 115 L/s. The volume of the reservoir of Vodňany is 2 × 1000 m^3. The material of the supply pipe is steel with a diameter of 300 mm. The block diagram of the group water supply system is shown in Figure 1.

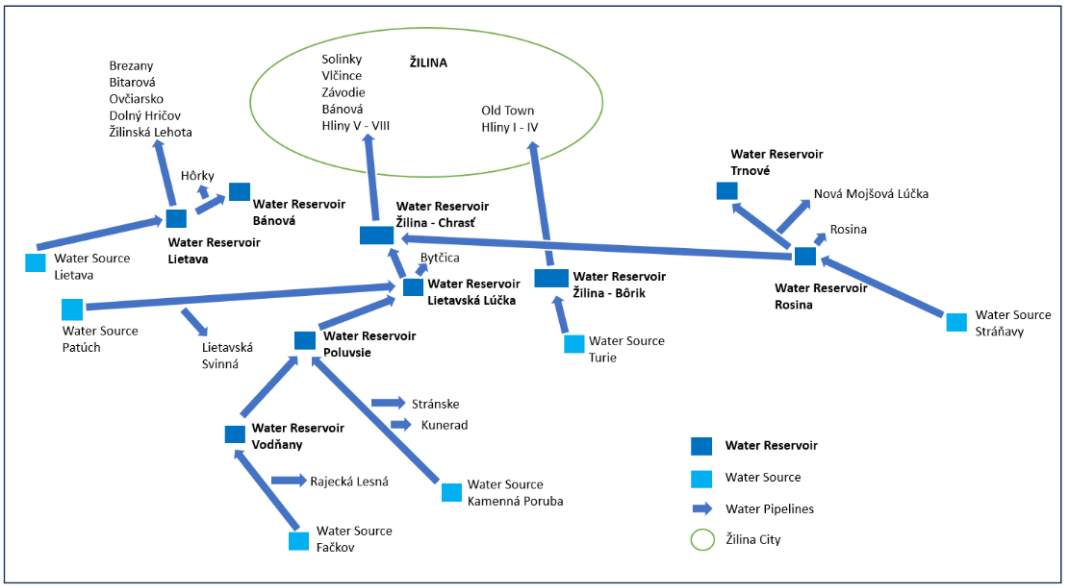

Figure 1. Block diagram of group reservoir Žilina—southwest [27].

At the same time, according to the Water Act [28], the person who handles water is obliged to take care of its protection, make the necessary efforts to improve its condition,

ensure its economical and efficient use according to the conditions and requirements of this Act, and also ensure that the rights of others are not violated. Additionally, they are also obliged to take care of the protection of water conditions and the protection of hydraulic structures. The operator of the reservoir is obliged to protect CIE from disturbance or destruction. To this end, he is obliged to carry out the following [17]:

- Apply technology that ensures its protection when modernizing an element;
- Implement a security plan.

To develop a security plan, the operator must follow the following steps [17]:

- Assess the importance of the equipment within the water reservoir;
- Evaluate the risk of potential threats, such as disturbance or destruction of specific equipment within the reservoir. This evaluation should consider vulnerabilities, as well as the expected consequences on the functionality, integrity, and continuity of the reservoir's operation;
- Choose the primary security measures to protect the reservoir. This includes selecting mechanical barriers, alarm systems, security elements for information systems, and organizational measures.

Emphasis should be placed on notification and warning procedures, crisis management, training individuals, and implementing control measures to ensure compliance with permanent protection measures. It follows that no law specifies how to establish a minimum level of protection that would ensure adequate protection for CIE. According to the Annex to the Critical Infrastructure Act, the water tank belongs to sector 7., water and atmosphere and subdivisions of Drinking Water Provision. This sector falls under the auspices of the Crisis Management and Security Department of the Ministry of Environment of the Slovak Republic. The ministry has no internal regulation that would specify how the operator should apply the legal requirements for the protection of the water tank as CIE.

In 2014, the Slovak Ministry of Economy issued a Guideline on Security Measures for the Protection of CIE in the Energy and Industry Sectors, which can be used to secure CIE from another sector that has similar operating conditions. According to the guidelines for each type of CIE, four protection zones have been defined, namely a separate secure zone, a secure zone, a protected zone, a controlled zone [29]. From the point of view of the nature of operation and construction design of the building, it is appropriate to define the entire area of the water reservoir as a specially secured zone. From the different possible sub-sectors of energy and industry, the oil and petroleum product subsector, including, for example, pumping stations, can be selected as the most appropriate.

Objects in a specially secured zone, such as the reservoir in question, are subject to specific requirements. An analysis of the following requirements determines the minimum level of protection necessary for the reservoir:

- A video surveillance system (VSS), which provides the fourth level of security [30], and the purpose of which is perimeter monitoring and input identification;
- Intrusion and hold-up alarm systems (I&HAS), which provide the fourth level of security [31], including perimeter detection, motion and door opening detectors, local optical-acoustic signaling;
- Access control systems (ACS), which provide the fourth level of security [32], including interconnection with mechanical barriers;
- A backup power supply for alarm systems;
- IP protection or anti-vandalism;
- Connection of alarm systems to the centralized protection desk with "24/7" operation;
- The requirement for an integrated alarm system;
- The perimeter: solid fencing, a top barrier, and a lockable gate;
- The casing: a door of strong construction with a security locking mechanism or an electronic lock;
- Physical protection requirements;
- Organizational measures.

It can be inferred that the minimum level of protection requirements encompass not only the specifications of particular mechanical barriers and alarm systems, including their level of security, but also pertain to their potential placement and functionality.

According to the European Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [16], relevant threat scenarios need to be considered in order to assess vulnerabilities and the potential impact of disruption or destruction of critical infrastructure. The likelihood of possible scenarios of threats of disturbance or destruction of the reservoir in relation to its vulnerabilities has a significant impact on the dislocation of individual elements of the protection system. According to the Critical Infrastructure Act [17], the operator is to draw up a security plan, which also includes an assessment of the risk of threat of disruption or destruction of individual CIE facilities, their vulnerabilities, the anticipated consequences of their disruption or destruction on the functionality, integrity and continuity of operation of the element.

Neither European nor national legislation of general application specifies how the risks (scenarios) of threats to CIEs are to be considered or evaluated.

Already in the previous step, when determining the security level of VSS, I&HAS and ACS ad hoc, the overall level of risk of disruption or destruction of the reservoir was evaluated as "high". This conclusion is based on the assumption that the probability of a threat of disturbance or destruction of the reservoir is high (based on the current geopolitical situation in the EU), as well as the anticipated consequences of the disturbance or destruction being of high importance (intoxication of a large population due to contamination of the water source or long-term shutdown of the population from drinking water supply). The determination of a high level of security risk is also confirmed by the fact that the water reservoir has been classified as a critical infrastructure element at the national level, based on a detailed assessment according to criteria (sectoral and cross-cutting). A risk assessment from the perspective of the probabilities of specific threat scenarios will be presented in the next part of the article.

Once the minimum level of protection has been established, along with the specific protection measures to be implemented (such as VSS, I&HAS, and ACS) and their corresponding functionalities and boundary parameters (such as security degree or class and person identification), the next step is to determine the placement or dislocation of individual systems and their components (including cameras, detectors, and mechanical barriers). In certain instances, the dislocation of protective elements is directly dictated by the requirements for achieving the minimum level of protection, such as intrusion detection at the perimeter of the object. However, it is also essential to consider the dislocation of protective measures in the context of risk assessment and the vulnerability of the reservoir.

The risk assessment process can be applied at a micro level, where the objective is to make decisions about the location of protective measures primarily based on evaluating the probability of potential risks. In this case, risks refer to possible scenarios through which an intruder could achieve their objective. This process is also known as vulnerability analysis. Regarding the water reservoir, vulnerabilities were assessed, leading to the creation of four highly probable attack scenarios. The resulting risk level associated with these scenarios was deemed unacceptable.

The anticipated direction and tactics of attack were taken into account in the overall design of protective measures.

The technical standard for I&HAS [33] recommends where and how individual elements (e.g., detectors) should be implemented in a given facility, based on the appropriate degree of security. In the case of dislocation, I&HAS is determined by the following requirements: perimeter detection, motion and door opening detectors and local optical-acoustic signaling. When dislocating motion detectors cover the designated area, it is advisable to apply the software that can visualize the detection characteristics on a 2D map base (Figure 2).

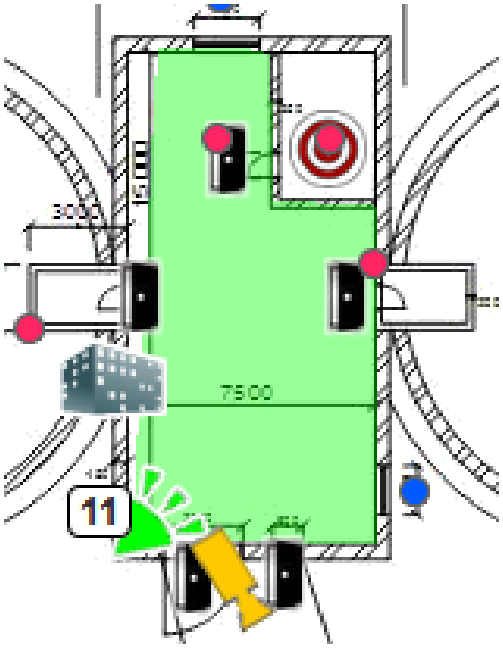

Figure 2. Coverage of the reservoir building with the I&HAS system detector using SATANO software.

When determining the placement of VSS cameras, their location is based on the requirements for effective identification and monitoring capabilities.

To assist in the process of camera placement, it is recommended to utilize software tools that can generate a visual representation of the coverage area on a 2D map background. These tools enable the visualization of camera coverage, typically represented with color coding to indicate specific functions such as monitoring, detection, or identification (Figures 3 and 4).

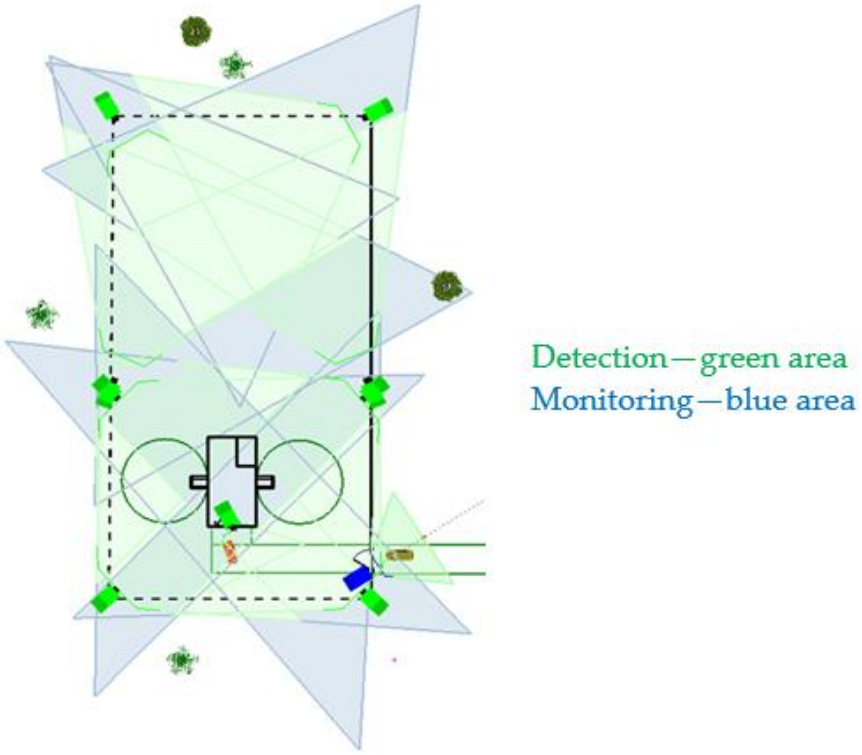

Figure 3. Coverage of an object of a camera system with detection and monitoring functions.

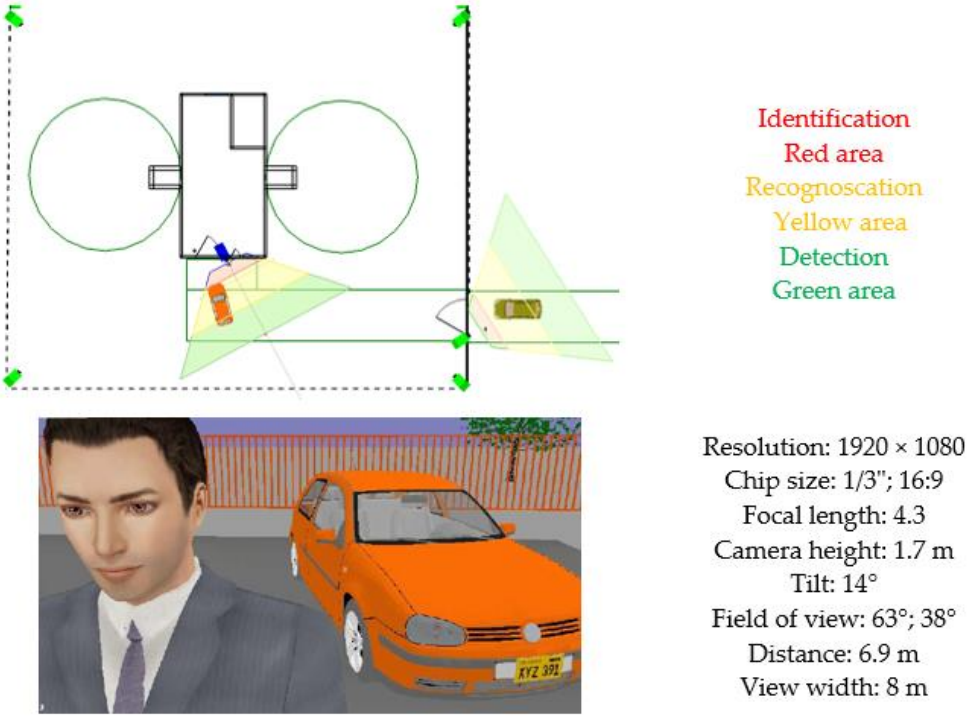

Figure 4. Dislocation of cameras for identification using IP VIDEO System Design Tool software.

For the ACS (Access Control System), the placement of individual protection elements is directly dictated by the minimum protection level requirements. These requirements include the following:

- The facilitation of controlled and regulated access by the access control system for authorized individuals entering or exiting the facility.
- The presence of manually and electronically controlled entrance gates and doors, both at the local site and accessible remotely.
- The implementation of a system to monitor the movement of individuals, which is connected to the access control system.

The placement of mechanical barriers is determined based on two factors: the minimum level of protection requirements and the existing structural configuration of the object. The dislocation of these barriers is determined in relation to their passive resistance against breakthrough. The design ensures that their placement aligns with the minimum level of protection requirements, thereby contributing to the overall functionality of the system. The placement of physical protection measures is determined based on the desired arrival time of the intervention unit. In this study, the response time of the intervention unit is set within a range of no more than 8 min from the initial detection of the intruder. Assuming an average travel speed of 70 km/h, this results in a radius of approximately 9 km from the water tower. Consequently, the centralized protection desk, along with the intervention unit, should be situated within this designated radius.

A functional physical protection system (PPS) for objects is defined as a system that satisfies the fundamental requirement of having an attack time greater than the reaction time of the intervention unit, starting from the first detection point. In this specific case, the minimum level of protection necessary to meet this requirement is determined by extreme values of the following parameters:

- The effectiveness index of protective measures (>1).
- The probability of eliminating the intruder (>0.5).

These extreme parameter values dictate the implementation of an appropriate number of mechanical barriers with combined breakthrough resistance, considering a specified total

reaction time of the intervention unit. Moreover, the outliers of these parameters indicate the initial detection location.

As mentioned earlier, the operator must assess and consider the risks and potential scenarios involving the disruption or destruction of critical infrastructure facilities, their vulnerabilities, and the anticipated consequences of such events. In this case, four specific risks (scenarios) related to the disturbance or destruction of the reservoir (Table 2) are identified and evaluated using the SATANO software tool. This evaluation involves calculations of individual parameters, the identification of critical paths, a graphical representation of the initial detection location, and a timeline of the attack.

Table 2. Anticipated threat (attack) scenarios.

Scenario (Threat)		Possibility of Occurrence <1–5>	Consequence <1–5>	Risk Level
Incident	**Consequence**			
The intruder advances from the public area, navigating through the perimeter towards the chlorine room in the water tank building. Throughout this process, they gradually overcome standard mechanical barriers. The objective of the attack is to cause damage to the chlorine equipment.	As a consequence, a significant portion of the local population would face an extended interruption in their access to the drinking water supply	4	5	20
The intruder employs a paraglider motor glider to land within the vicinity of chamber No. 1 and subsequently proceeds to overcome standard aperture fillings as they make their way towards the chlorine room.	As a consequence, a significant portion of the local population would face an extended interruption in their access to the drinking water supply	4	5	20
An external intruder, equipped with free available tools, utilizes a chemical substance to intentionally contaminate the water supply.	High population toxication	4	5	20
The intruder employs a paraglider motor glider to land near chamber No. 1 within the premises. Subsequently, he overcomes standard aperture fillings as they make their way towards the chlorine room in the water tank building. Once there, the intruder proceeds to pour a chemical substance into the pumping equipment.	High population toxication	4	5	20

Possible attack risk scenarios:

Attack Scenario 1:

In this scenario, an external intruder utilizes freely available tools to overcome mechanical barriers and alarm systems. The objective of the attack is to damage the chlorine equipment, leading to a long-term shutdown of the drinking water supply for a significant number of residents (Figure 5). The intruder enters from a public area, progresses through the perimeter, and gradually overcomes standard aperture fillings within the water tank building (Figure 6). The maximum speed of movement inside the building is expected to be 2 m/s. The intervention unit is expected to react within a maximum of 8 min from the initial detection of the intruder.

Attack Scenario 2:

This scenario differs from the previous one as the intruder employs a motor paraglider to land near chamber 1 before overcoming standard aperture fillings en route to the chlorine room.

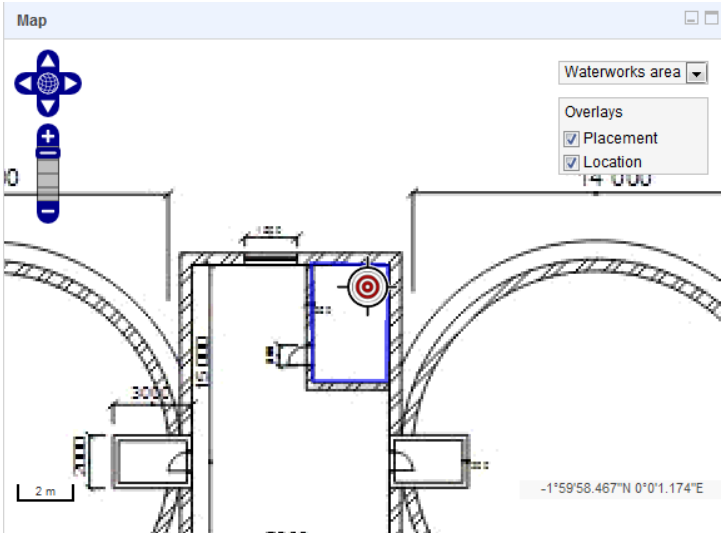

Figure 5. Common target of attacks in scenarios 1 and 2.

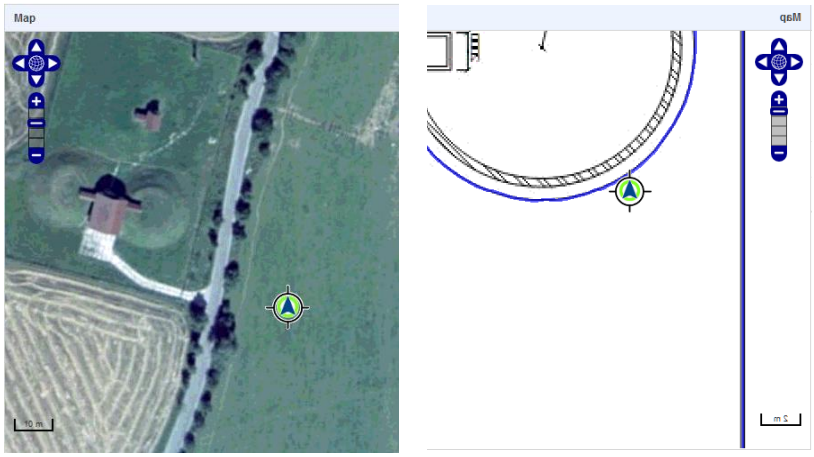

Figure 6. Starting points of the intruder in scenarios 1 and 3 (**left**) and scenarios 2 and 4 (**right**).

Attack Scenario 3:

In this scenario, an external intruder uses freely available tools and a chemical substance to contaminate the water supply. The target of the attack is to poison a significant population residing in a selected consumption area within residential district D5 (Figure 7). The intruder proceeds from a public area through the perimeter towards the chlorine room in the water tank building, where they pour the chemical substance into the pumping equipment. The maximum speed of movement inside the building is expected to be 2 m/s. The intervention unit is expected to react within a maximum of 8 min from the initial detection of the intruder. The detection of water contamination in the supply network is based on a water pollution detector located at the outlet of the chlorine equipment. The maximum rate of drinking water distribution in the network is 1.5 m/s [33]. To mitigate the threat, the drinking water supply for residents in residential area D5 can be mechanically shut off by closing the valve after the employees of Vodárne a kanalizácia, s.r.o. arrive within an 8 min reaction time.

Attack Scenario 4:

This scenario is similar to attack scenario 3, in that the intruder also employs a motor paraglider to land near chamber 1.

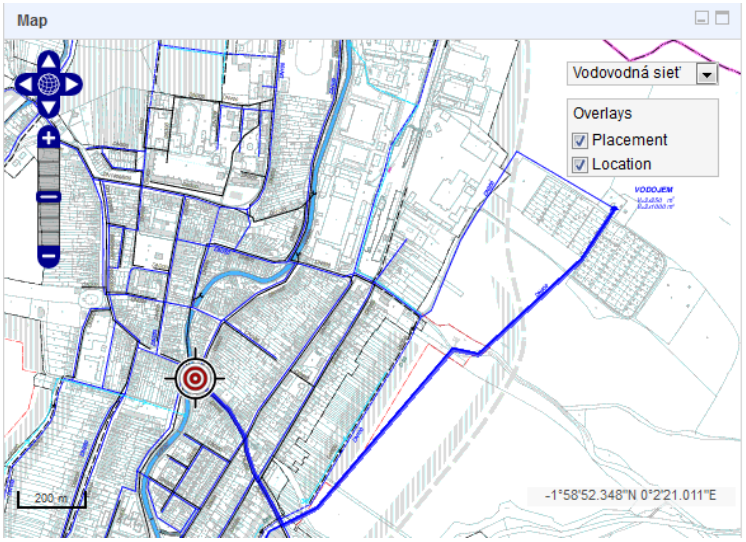

Figure 7. Water supply network Vodňany with the aim of attack in residential area D5.

To quantitatively assess the level of protection within the facility, a comprehensive analysis is conducted. This assessment involves considering the breakthrough resistances of mechanical barriers, the detection probabilities of alarm systems, and the reaction times of physical protection. By incorporating these factors, the effectiveness of the facility's protection system can be evaluated. Furthermore, modeling (Figure 8) and simulation are performed using the created scenario to verify the functionality of the system and identify any potential vulnerabilities. This simulation helps identify issues such as the incorrect placement of mechanical barriers and alarm systems, improper selection of their parameters, or insufficient reaction time of the physical protection measures. By conducting such assessments and simulations, the overall effectiveness and integrity of the protection system can be determined.

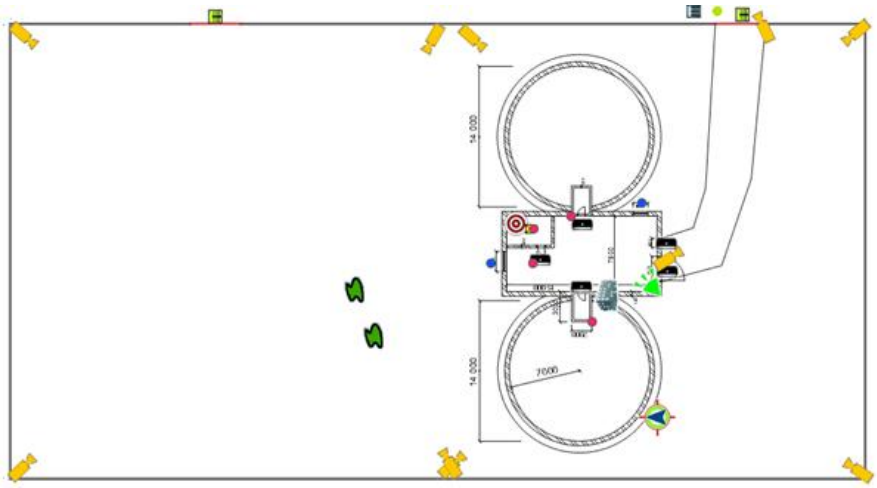

Figure 8. Model of the Vodňany water reservoir protection system processed in the SATANO software tool.

In total, four attack scenarios have been developed, differing in the starting points of the intruder and their attack targets, namely damage to chlorine equipment (scenarios 1 and 2) or contamination of the water source (scenarios 3, 4). All four attack scenarios were modeled and simulated in SATANO (where the functionality of the protection system was evaluated if the scenario was executed (Figure 9)).

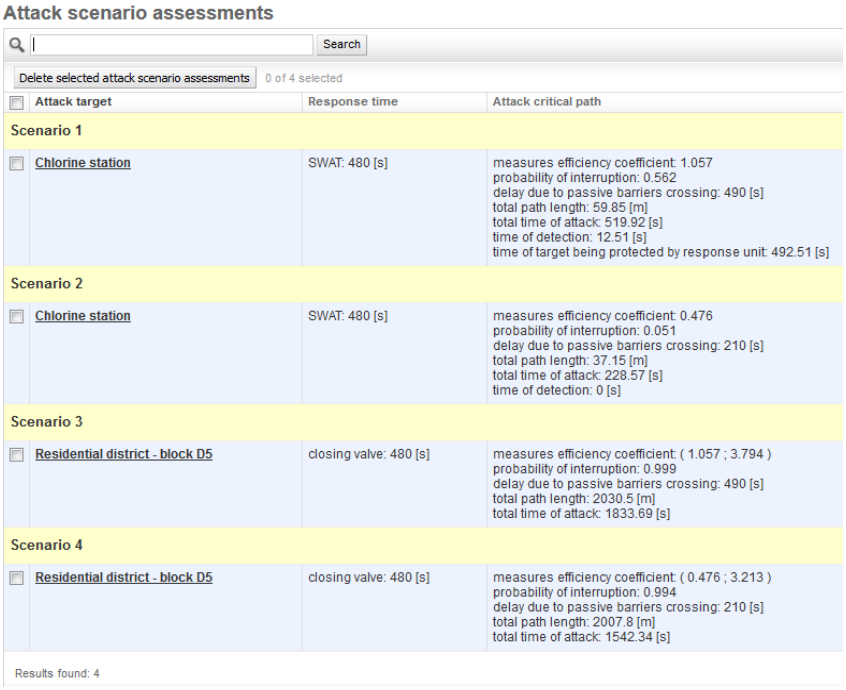

Figure 9. Results of simulations of four scenarios of attack on the Vodňany water reservoir.

In the case of scenario 1, where the intruder's target is to damage the chlorine equipment, the system is effective (all threshold values determining the minimum level of PPS have been achieved) because the delay of the intruder during his path to the target (total time of attack: 519.92 s) is sufficient compared to the response time of the intervention unit (response time: 480 s) from the first moment of detection. The system's effectiveness is indicated by two factors: the measures' efficiency coefficient, 1.057 (must be >1), and the probability of interruption, 0.562 (must be >0.5). Although the "Measures efficiency coefficient" indicates system effectiveness, according to the "Probability of interruption" parameter, which considers input parameters as continuous variables with a normal distribution, the system is effective only with a probability of 0.562.

In scenario 2, where the intruder's objective is again to damage the chlorine equipment, an additional motor glider was used in the attack, reducing the overall intruder delay to 228.57 s. In this scenario, the protection system would be ineffective as the thresholds determining the minimum level of system protection were not achieved (measures' efficiency coefficient: 1.057; probability of interruption: 0.562).

In scenario 3, where the intruder's target is to contaminate the drinking water source, the system is effective with a probability of 0.999. The intruder would be eliminated by the intervention unit (as in scenario 1), and the water supply system would be able to react promptly and shut off the supply of drinking water to the residential district D5. The following factors indicate the system's effectiveness:

- The measures' efficiency coefficient: 1.057 (for the water reservoir protection system) and 3.794 (for the drinking water source closure system) (must be >1);
- The probability of interruption: 0.999 (must be >0.5).

In scenario 4, where the intruder's target is also to contaminate the drinking water source, the system is effective with a probability of 0.994. Although the intruder would not be eliminated by the intervention unit (as in scenario 2), the water supply system would still be able to react promptly and shut off the supply of drinking water to the residential district D5. The following factors indicate the system's effectiveness:

- The measures' efficiency coefficient: 0.476 (for the water reservoir protection system) and 3.213 (for the drinking water source closure system) (must be >1);
- The probability of interruption: 0.994 (must be >1).

The outcomes of the simulated attack scenarios (1 to 4) demonstrate that the PPS proves to be effective in three out of the four scenarios (Table 3). However, in scenario 2, adjustments are necessary for the PPS to enhance its effectiveness. These adjustments can involve either reducing the reaction time of the intervention unit or increasing the passive resistance of specific mechanical barriers within the reservoir object. By achieving these parameter thresholds that determine the minimum level of protection, the PPS can be optimized to address the vulnerabilities identified in scenario 2.

Table 3. Final evaluation of the effectiveness of the proposed protection system for individual water tank attack scenarios.

Scenario	Starting Point	Target of Attack	Coefficient of Effectiveness of Safeguard Measures (>1)	Probability of Eliminating an Intruder (>0.5)	Final Evaluation of the Protection Scheme
1	The intruder proceeds from a public area	damage to chlorine equipment	1.057	0.562	PPS is efficient
2	Landing in premises near chamber No. 1	damage to chlorine equipment	0.476	0.051	PPS is not efficient
3	The intruder proceeds from a public area	contamination of the drinking water source	1.057 (in the case of a water tank PPS) and 3.794 (in the case of a drinking water source closure system)	0.999	PPS is efficient
4	Landing in premises near chamber No. 1	contamination of the drinking water source	0.476 (in the case of a water tank PPS) and 3.213 (in the case of a drinking water source closure system)	0.994	PPS is efficient

An example of attack scenario 4 visualization is shown in Figure 10.

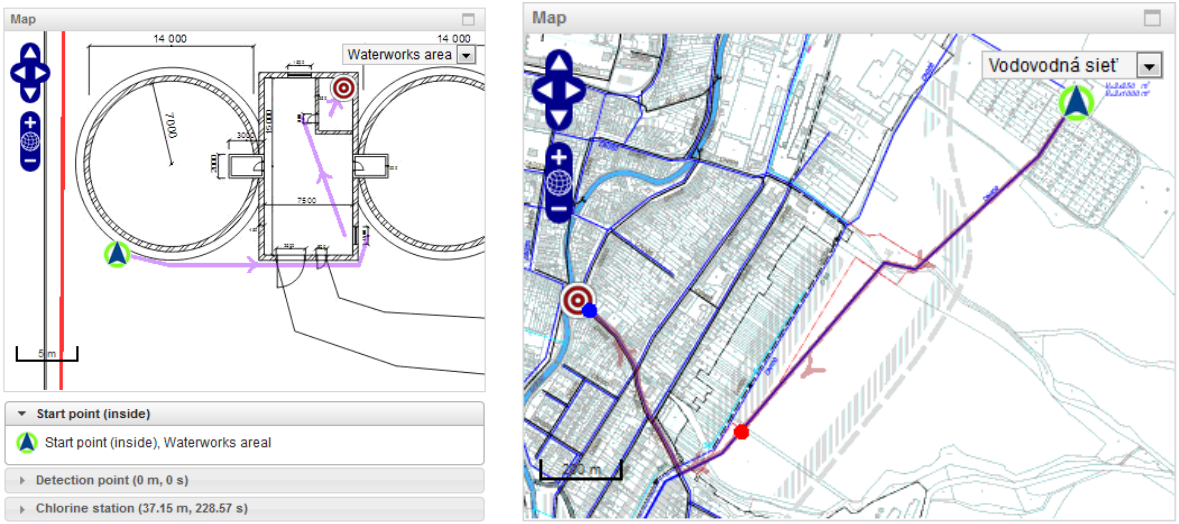

Figure 10. Graphical user interface of the critical path of the intruder → in the scenario.

4. Discussion

Water management system facilities are frequently classified as critical infrastructures at both the state and EU levels due to their operational significance. Given their substantial impact on citizens' quality of life and the imperative to safeguard their health and well-being, these facilities become prime targets for a range of attacks perpetrated by organized groups or individuals. In many cases, these are objects without the permanent presence of an operator, therefore, an attack from the external environment is likely to be assumed. However, an attack from the internal environment is also not excluded. From the perspective of the predicted attack vector, either a physical, cyber or combined attack

can be expected. The article presents the use case of a possible way to protect the selected water reservoir against intentional physical attack from the external environment. The reservoir has been identified as a critical national infrastructure element in the Drinking Water Provision subsector.

The protection requirements for objects against unauthorized people who intend to cause damage, destruction, or theft of protected property are primarily established through legally binding regulations, technical standards, national or international norms, and the stipulations of other third parties. In compliance with the European Directive on the identification and designation of European critical infrastructures and the assessment of their protection improvement needs [16], as well as the National Law on Critical Infrastructure [17], it is essential to consider relevant threat scenarios to evaluate vulnerabilities and the potential consequences resulting from the disruption or destruction of critical infrastructure. During the planning and design phases of PPS, it is possible to assess their functionality, economic efficiency, reliability, and quality [23].

A functional PPS is defined by its ability to satisfy the fundamental requirement that the attack time, starting from the initial detection point, is longer than the response time of the intervention unit. Existing methodologies for protecting objects employ either a qualitative or quantitative approach. Procedures based on a quantitative approach utilize measurable input parameters (such as probability of detection, intruder movement time, time required to overcome mechanical barriers) and output parameters (such as probability of interruption) to precisely justify the effectiveness of proposed protective measures. One of the tools that uses a quantitative approach is the software tool Security Assessment of Terrorist Attack In a Network Of Objects (SATANO), which allows the modeling of a PPS on a 2D map basis and simulate possible physical attacks. This tool was used to model and simulate four attacks on a selected water tower. The objective of these simulations is to verify the functionality of the PPS against individual attacks (Table 3). The results showed that the proposed PPS system is non-functional under certain circumstances (scenario 2) and therefore further protection measures need to be taken (e.g., increasing the passive resistance of mechanical barriers or shortening the response time).

From the above, it can be stated that if the qualitative security requirements arising from legal regulations [16,17], technical standards [13,18–21], or other requirements of third parties [8–12,14,15] were applied without further verification of the proposed PPS, there could be a situation where the PPS would formally meet all requirements but would be ineffective against certain real-world attacks.

For instance, legal regulations [16,17] and technical standards [13,18] require the installation of perimeter fencing, access control systems, or a surveillance system to protect the reservoir from unauthorized entry and potential acts of sabotage. The PPS is designed and implemented based on these requirements, meeting all the specified criteria and standards.

However, in this scenario, the adversaries intending to harm the water reservoir are well-organized and highly skilled. They manage to breach the perimeter fencing using sophisticated techniques, bypass the access control systems with insider knowledge, and manipulate the surveillance cameras to create blind spots. As a result, the PPS, which seemed to meet all the regulatory and technical requirements on paper, proves to be ineffective in preventing an attack.

This example highlights the limitations of solely relying on qualitative security requirements without further validation of the PPS's real-world effectiveness. It emphasizes the importance of adopting a quantitative approach, incorporating simulations and precise measurements, to comprehensively assess the PPS's capabilities against potential threats. By conducting such quantitative evaluations, vulnerabilities can be identified and addressed, ensuring that the protective measures are robust and capable of countering various real-world attacks effectively.

This verification or calibration of the system can be carried out in several ways, either through real physical simulations of attacks or simulations of various attacks using specialized software tools. From the perspective of the input resources expended (e.g.,

financial, human, and material), simulations of attacks based on mathematical models describing the PPS appear to be more advantageous. However, it is necessary to mention that this approach also has certain limits, especially in obtaining values of input parameters, which leads to abstraction from the modeled real protected environment. The need and significance of utilizing quantitative verification of the effectiveness of an existing or proposed protection system should be implemented in all existing or future legal regulations, technical standards, and other methodologies.

5. Conclusions

In conclusion, water reservoirs are vulnerable to various types of attacks that can have significant impacts on water quality, service disruption, and public health and safety. Real-world examples such as the Milwaukee Cryptosporidium outbreak, Walkerton E. coli contamination, deliberate sabotage in Iraq, cyber-physical attacks on the Bowman Avenue Dam, attempted poisoning incidents in California and Australia, and the recent Nova Kachovka Dam disaster in Ukraine highlight the potential consequences and vulnerabilities associated with attacks on water reservoirs.

It is important to note that the existing practices and standards, although based on best practices, were developed under specific conditions and may not objectively determine the level of protection for a water reservoir as critical infrastructure. Therefore, there is a need for a quantitative approach that enables an objective assessment of the minimum level of physical protection for water reservoirs, considering security requirements from legal regulations and technical standards. Such an approach would help ensure the reliability, safety, and security of water supplies and enhance the overall security and resilience of water reservoirs.

When evaluating the functionality of a physical protection system (PPS), a quantitative approach allows for a precise demonstration of the proposed protection measures using measurable input and output parameters. This approach verifies that the PPS is neither undersized nor oversized relative to the proposed protective measures. However, in practice, qualitative approaches are more commonly used, relying on expert assessments and subjective evaluations. This is primarily due to the absence of actual values for important input parameters, such as probability of detection by alarm systems or breakthrough resistances of mechanical barriers, which vary based on the specific tools employed to overcome them. The values of these input parameters should be the subject of further research.

To assess the effectiveness of the proposed PPS, a quantitative PPS model was developed utilizing specialized software. This quantitative approach allows for a precise and measurable evaluation of the protective measures, ensuring the system is optimally calibrated to provide adequate security. Additionally, four potential attack scenarios were simulated to rigorously test and verify the functionality of the PPS, scrutinizing its response to diverse threats.

By combining the use of a quantitative PPS model and simulated attack scenarios, this study demonstrates the efficacy of the proposed protective measures and their ability to fortify water reservoir security. The findings of this research have implications for enhancing the protection of critical water infrastructure, thereby contributing to the resilience of water management systems. In conclusion, adopting a quantitative approach to water reservoir security can bolster protection capabilities and help mitigate the potential consequences of attacks, ultimately securing water resources for the sustainable development and well-being of communities.

The aim of the article was to present, in a specific use case, the establishment of a minimum level of protection based on both qualitative and quantitative approaches. The qualitative approach was applied in determining the security requirements arising from third parties (legislation and technical standards), while the quantitative approach was applied in verifying the basic conditions for the functionality of the PPS regarding four attack scenarios. To verify the functionality of the proposed PPS, the software tool SATANO was used, which is one of the research activities of the authors of the article. Functionality

verification would be possible with other tools, but their possible comparison was not the goal of the article. Taking both approaches into account will make it possible to objectify the planning process of any PPS as much as possible.

Author Contributions: Data curation and formal analysis: T.L., L.M. and. K.P.; writing—original draft, and visualization: T.L.; writing—review and editing, methodology, and supervision: L.M. All authors have read and agreed to the published version of the manuscript.

Funding: The article was created with the support of the project of the University of Zilina in Zilina, The Ministry of Education, Science, Research and Sport of the Slovak Republic: APVV-20-0457 "Monitoring and tracking of movement and contact of persons in health care 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. Mac Kenzie, W.R.; Hoxie, N.J.; Proctor, M.E.; Gradus, M.S.; Blair, K.A.; Peterson, D.E.; Kazmierczak, J.J.; Addiss, D.G.; Fox, K.R.; Rose, J.B. A massive outbreak in Milwaukee of Cryptosporidium infection transmitted through the public water supply. *N. Engl. J. Med.* **1994**, *331*, 161–167. Available online: https://pubmed.ncbi.nlm.nih.gov/7818640/ (accessed on 22 May 2023). [CrossRef]
2. Hrudey, S.E.; Hrudey, E.J. *Safe Drinking Water: Lessons from Recent Outbreaks in Affluent Nations*; IWA Publishing: London, UK, 2004.
3. Al-Ansari, N.; Al-Hadithi, M.; Knutsson, S. Terrorism and Security of Water Supplies: The Threat of Water Terrorism. *J. Water Resour. Protect.* **2013**, *5*, 449–461.
4. U.S. Department of Justice. Bowman Avenue Dam: A Case Study in the Complexity of Responding to Cyber-Physical Attacks. 2016. Available online: https://www.justice.gov/criminal-ccips/file/903036/download (accessed on 22 May 2023).
5. Smarsh, D.J. Water Utility Incident Response Planning: Ensuring Effective Emergency Response to Contamination Events. In Proceedings of the American Water Works Association (AWWA) Water Quality Technology Conference, New Orleans, LA, USA, 16–20 November 2014.
6. The Age. Terrorism Plot to Poison Water Supply: Inside the Ringwood Conspiracy. 2019. Available online: https://www.theage.com.au/national/victoria/terrorism-plot-to-poison-water-supply-inside-the-ringwood-conspiracy-20191118-p53b39.html (accessed on 22 May 2023).
7. CNN. Here are the Key Theories on What Caused Ukraine's Catastrophic Dam Collapse. 2023. Available online: https://edition.cnn.com/2023/06/08/europe/nova-kakhovka-destruction-theories-intl/index.html (accessed on 24 July 2023).
8. U.S. Environmental Protection Agency (EPA). Security Risk Assessment for Water Utilities. 2009. Available online: https://www.epa.gov/sites/default/files/2015-10/documents/security-risk-assessment-for-water-utilities.pdf (accessed on 22 May 2023).
9. U.S. Department of Homeland Security. Protecting Critical Infrastructure: Water Sector Security. 2016. Available online: https://www.dhs.gov/publication/protecting-critical-infrastructure-water-sector-security (accessed on 22 May 2023).
10. World Health Organization (WHO). Water Security Handbook: Planning for and Responding to Drinking Water Contamination Threats and Incidents. 2011. Available online: https://www.who.int/water_sanitation_health/publications/water_security_handbook/en/ (accessed on 22 May 2023).
11. Water Environment Federation. Cybersecurity and Physical Security: A Unified Approach to Water System Protection. 2018. Available online: https://www.wef.org/globalassets/assets-wef/1{-}{-}resources/water-sector-cybersecurity/cybersecurity-physical-security-a-unified-approach-to-water-system-protection.pdf (accessed on 22 May 2023).
12. Jones, J.P.; Haimes, Y.Y. *Security of Water Supply Systems: From Source to Tap*; Springer: Berlin/Heidelberg, Germany, 2011.
13. National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. 2018. Available online: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11 (accessed on 22 May 2023).
14. American Water Works Association (AWWA). Risk Assessment and Risk Management for Water and Wastewater Utilities. 2013. Available online: https://www.awwa.org/Portals/0/AWWA/Government/Security%20and%20Emergency%20Planning/Risk_Assessment_and_Risk_Management_for_Water_and_Wastewater_Utilities.pdf (accessed on 22 May 2023).
15. Water Research Foundation. Security Risk Assessment and Risk Management for Small and Medium Water Systems. 2017. Available online: https://www.waterrf.org/resource/security-risk-assessment-and-risk-management-small-and-medium-water-systems (accessed on 22 May 2023).

16. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2557&qid=1689577224078 (accessed on 17 July 2023).
17. *Act No. 45/2011*; Coll. on the Protection of Critical Infrastructure. European Parliament: Strasbourg, France, 2011.
18. *EN 17483-1:2021*; Private Security Services—Protection of Critical Infrastructure—Part 1: General Requirements. iTeh, Inc.: Newarc, DE, USA, 2021.
19. *CEN/TS 16850:2015*; Societal and Citizen Security—Guidance for Managing Security in Healthcare Facilities. iTeh, Inc.: Newarc, DE, USA, 2015.
20. *P CEN/TR 14383-7:2009*; Prevention of Crime—Urban Planning and Building Design—Part 7: Design and Management of Public Transport Facilities. ASTM: West Conshohocken, PA, USA, 2009.
21. *ČSN P 734450-1*; Physical Protection of the Object of Critical Infrastructure—Part 1: General Requirements. European Commission: Geneva, Switzerland, 2013.
22. Loveček, T.; Reitšpís, J. *Designing and Evaluation of Physical Protection Systems*; University of Žilina: Žilina, Slovakia, 2011; 281p.
23. Loveček, T.; Mariš, L.; Šiser, A. *Planning and Designing of Physical Protection Systems*; University of Žilina: Žilina, Slovakia, 2018; 285p.
24. Garcia, M.L. *The Design and Evaluation of Physical Protection Systems*; Elsevier: Alpharetta, GA, USA, 2001; 370p.
25. Kampova, K.; Loveček, T.; Řehák, D. Quantitative approach to physical protection systems assessment of critical infrastructure elements: Use case in the Slovak Republic. *Int. J. Crit. Infrastruct. Protect.* **2020**, *30*, 100376. [CrossRef]
26. Lovecek, T.; Ristvej, J.; Simak, L. Critical Infrastructure Protection Systems Effectiveness Evaluation. *J. Homeland Secur. Emerg. Manag.* **2010**, *7*, 1–25. [CrossRef]
27. North Slovakia Water Supply and Leverage, Inc. Act No. 364/2004 Coll. on Water (Water Act). Available online: https://www.sevak.sk/wp-content/uploads/2017/12/Skupinov%C3%BD-vodovod-%C5%BDilina-%C4%8Das%C5%A5-Juhoz%C3%A1pad-oblas%C5%A5-Rajeckej-doliny.pdf (accessed on 26 May 2023).
28. Guideline no. 29014/2014-1000-53190 of the Ministry of Economy of the Slovak Republic on Security Measures for the Protection of Critical Infrastructure Elements in the Energy and Industry Sectors. Available online: https://www.economy.gov.sk/uploads/files/J4Vom9oj.pdf (accessed on 22 May 2023).
29. *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.
30. *EN 50131-1*; Alarm SYSTEMS. Intrusion systems. Part 1: System Requirements. General. European Committee for Electrotechnical Standardization: Brussels, Belgium, 2006.
31. *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.
32. *CLC/TS 50131-7*; Alarm Systems. Intrusion and Hold-Up Systems. Part 7: Application Guidelines. General. European Committee for Electrotechnical Standardization: Brussels, Belgium, 2010.
33. Kriš, J.; Božíková, J.; Čermák, O.; Čermáková, M.; Škultétyová, I.; Tóthová, K. *Waterworks I: Water Supply*; STU v Bratislave: Bratislava, Slovakia, 2006; 816p.