

Article

Not peer-reviewed version

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

[Tomáš Loveček](#), [Ladislav Mariš](#)^{*}, Katarína Petrlová

Posted Date: 29 June 2023

doi: 10.20944/preprints202306.2014.v1

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



Preprints.org is a free multidiscipline platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Article

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

Tomáš Loveček ¹, Ladislav Mariš ^{2,*} and Katarína Petrlová ³

¹ Faculty of Security Engineering, University of Žilina, Slovakia, tomas.lovecek@uniza.sk

² Faculty of Security Engineering, University of Žilina, Slovakia, ladislav.maris@uniza.sk

³ Mathematical Institute in Opava, Silesian University in Opava, Na Rybníčku 626/1, 74 601 Opava, Czech Republic, Katarina.Petrlova@math.slu.cz

* Author to whom correspondence should be addressed (ladislav.maris@uniza.sk, Tel.: +421 902 544 534)

Abstract: Water management systems help allocate water resources effectively, considering various demands such as agriculture, industry, domestic use, and environmental needs. They optimise water distribution and ensure equitable access, minimising water scarcity and conflicts. Critical elements of this system are often the target of various attacks. Depending on the target of the attack, different scenarios based on physical, cyber, or combined forms of attacks can be used. Requirements for the protection of water objects forming part of the critical infrastructure system are determined primarily by generally binding legal regulations, technical standards, or other requirements of third parties. These requirements imply the need to adopt certain protective measures. Physical protection system (PPS), as a convenient way of organising protective measures, makes it possible to prevent an unauthorised person from achieving his goal. Current procedures aimed at protecting objects use a qualitative or quantitative approach. The article presents the use case of a possible way to protect a selected water reservoir that has been identified as a national element of critical infrastructure in the subsector Drinking Water Provision. The use case is based on the analysis of safety requirements and subsequent design of the PPS water reservoir. To verify the functionality of the proposed PPS, a quantitative PPS model was created using a software tool, and four possible attack scenarios were simulated.

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

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. Next 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 *E. 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 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]. In 2013, a lone hacker remotely accessed the Supervisory Control and Data Acquisition (SCADA) system controlling the Bowman Avenue Dam in Rye Brook, New York. Although the attack did not cause any operational impact due to the dam's offline status, it raised concerns about the vulnerability of critical 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]. 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 security, safety and reliability 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 (EPA) provides guidance for assessing the security risks to water utilities and developing mitigation strategies in their document "Security Risk Assessment for Water Utilities" [7]. 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" [8]. The World Health Organization (WHO) has published "Water Security Handbook: Planning for and Responding to Drinking Water Contamination Threats and Incidents" [9], which provides guidance for developing water security plans and responding to 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" [10]. The book "Security of Water Supply Systems: From Source to Tap" provides a comprehensive overview of the security issues related to water supply systems, including risk assessment, physical security, and cybersecurity [11]. In addition to these resources, the National Institute of Standards and Technology (NIST) provides a framework for improving critical infrastructure cybersecurity in their document "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1" [12]. The American Water Works Association (AWWA) has also published a document on risk assessment and management for water and wastewater utilities [13], while the Water Research Foundation offers a resource on security risk assessment and management for small and medium water systems [14]. Overall, the state of the art in water reservoir security involves a multidisciplinary approach that addresses physical security, cybersecurity, and risk management references.

2. Materials and Methods

The requirements for the protection of objects against intentionally acting unauthorised persons with the aim of damaging, destroying, or stealing protected tangible or intangible property located in the object that is owned or managed by a natural or legal person are determined primarily by generally binding legal regulations, technical, national, or international norms and standards, the requirements of insurance companies or other third parties such as parent companies or strategic customers.

Those requirements imply the need to adopt certain protective measures, which should be organised in such a way as to ensure the protection of the property of the owner or operator. If asset protection is the process of establishing a state of security using protective measures aimed at

preventing or stopping any undesirable activities or events (e.g., an electrical short circuit and subsequent fire) that are contrary to the interests of the owner or manager of that property, then the physical protection system (PPS) is the instrument used to achieve this state.

Physical protection system (PPS), as a convenient way of organising protection measures, allows an unauthorised person to achieve his goal, which may be, for example, theft, damage, or destruction of a protected asset. Such a system of protection can be understood as a system implemented by technical and regime protection measures or elements, which can be divided into alarm systems, mechanical barriers, security services, and regime measures. Mechanical barriers serve to deter, slow down, or stop an unauthorised person or intruder, while alarm systems serve to subsequently detect it and trigger an alarm state. An integral part of the protection system are security services, which ensure timely intervention and apprehension of the intruder. Regime protection ensures the proper functioning of those protective measures [15].

In the planning phase, design, implementation, or operation of building protection systems, it is possible to talk about the functionality, economic efficiency, reliability, or quality of PPS from the point of view of their evaluation [16].

A functional PPS shall be considered to be one that fulfils the basic condition that from the initial detection point the attack time is greater (including the total breaking time of mechanical barriers and the time of intruder movements) than the response time of the intervention unit. This means that the PPS is operational if the ratio of these times in that order is greater than one. In the case of an intruder whose aim is to steal a protected interest for its later monetization, it is sufficient to detain him at the latest at the time of leakage, thereby prolonging the total disposition time of the intervention unit. In the case of an intruder whose object is to damage or destroy a protected interest in the form of sabotage or a terrorist attack, it is necessary to detain him before he achieves his objective, i.e. before the protected interest is damaged or destroyed. In this case, we cannot calculate the time of its leakage [15,17].

In practice, a credible demonstration of the fulfilment of this basic condition for the functionality of the system is often difficult to achieve. Existing procedures for object protection use one of two basic approaches [18]:

- qualitative approach,
- quantitative approach.

Procedures using a qualitative approach shall be based on expert estimates by evaluators, where it is not possible to verify precisely the sufficiency of the proposed level of protection and it is necessary to rely on the expertise of the designers of these procedures. In this case, it is not possible to verify whether the PPS is undersized or, on the contrary, oversized in view of the proposed protective measures.

Procedures based on a quantitative approach make it possible to demonstrate precisely the justification of the proposed protection measures using measurable input and output quantities. In this case, it is already possible to verify that the PPS, in view of the proposed protection measures, is not undersized or oversized.

There are currently several tools (software) using one of those approaches for evaluating the functionality of a protection system [19]:

- qualitative approach: RiskWatch (USA), CRAMM (UK),
- quantitative approach: SAVI, ASSESS (Sandia National Laboratories, USA), Sprut (Scientific and Production Enterprise ISTA SYSTEMS JS Co., Russia), SAPE (Korea Institute of Nuclear Non-proliferation and Control, South Korea), SATANO (University of Žilina, Faculty of Security Engineering, the Slovak republic).

In practice, a qualitative approach is mainly used, although it brings a considerable degree of subjectivity to the PPS proposal. The main reason for this is the fact that in practice real values of input quantities are missing, such as:

- breakthrough resistances of mechanical barriers, varying depending on the type of tool used to overcome them,

- probability of detection by alarm systems, which vary depending on the intruder's knowledge of the technologies used (e.g. method of evaluating the change in physical quantity due to the violation of the protected area),
- reliability of alarm system elements,
- reliability of the human factor.

For these reasons, these instruments are used in practice only in a specific area (e.g. nuclear protection) respectively are still in the development phase at various research institutions. In practice, procedures based on a qualitative approach are used much more frequently, which can be further subdivided into [15]:

- directive approach, where protective measures are precisely defined, regardless of the specifics of the operation and the environment in which the object is located,
- variant approach, where it is possible to choose from a finite number of proposed solutions, combining various protective measures, which will allow to take into account to some extent not only the specifics of the operation and environment, but also the financial, technical, or personnel possibilities and capacities of the owner or manager of the facility.

The first and most important step in the TSO design process is to determine the minimum level of protection, which subsequently determines the choice: technical solutions for alarm systems and mechanical barriers, dislocation, parameters and functionalities. The minimum level of protection determines which protective measures are to be implemented, in what proportion and with what characteristics (e.g. security degree/class, purpose of use, key parameters of system elements, dislocation).

The minimum level of protection may result from the so-called safety requirements, which may be given:

- an essential condition for the functionality of the protection system,
- third party:
 - the state, through generally binding legal regulations,
 - standards bodies, by means of a normative standard,
 - an insurance company, through terms and conditions,
 - the customer, in the form of contractual terms or recommendations,
 - the parent company, in the form of internal organisational regulations,
 - another third party, through a regulation, contract, regulation, norms, standards, etc.

In the case of setting a minimum level of protection, based on the fulfilment of the basic condition of functionality of the protection system, a quantitative approach shall be used, using time and probabilistic bases of input and output quantities values (e.g. breakthrough times, transfer and reaction times, detection probabilities, etc.). When setting a minimum level of protection based on meeting the security requirements of third parties, a qualitative approach is used in most cases, either a directive approach or a variant approach.

In many cases, the setting of a minimum level of protection is linked to the risk management process, where the requirements for protective measures increase in scope, respectively become stricter with increasing risk levels (e.g. the safety class of alarm systems increases). Even if the risk management process does not affect the resulting minimum level of protection (i.e. it is directly defined), it has a significant influence in determining the dislocation of elements of protection measures (e.g. cameras, detectors, mechanical barriers, etc.). The requirement for the risk assessment process related to the protection of objects against anthropogenic intentional threats is determined by international and national generally binding regulations, norms and standards focused on a certain field of application (e.g. classified information, protection of critical infrastructure, protection of banking entities, protection of residential premises, etc.).

After establishing a minimum level of protection, which defines which protection measures are to be implemented, with which characteristics and parameters (level, resp. security class, purpose of use, key parameters of system elements), it is necessary to decide on the location of individual protection measures, systems, respectively their elements (e.g. location of cameras, detectors, mechanical barriers, etc.).

The position of individual TSO elements is influenced by a number of requirements, of which the most important include:

- 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.

Only after determining the parameters, operating conditions, it is possible to look for a specific manufacturer or seller on the market who offers a product that meets all defined conditions. Where such a product does not exist on the market or is economically disadvantageous, it is necessary to ensure these requirements by combining several products, but in such a way that the required minimum level of protection, the purpose of individual protective measures, or the dislocation of protective measures are not altered. For example, a dedicated area can be covered by several elements of alarm systems (e.g. detectors or cameras). In the case of the design of the system, we can talk about a certain variation, but it is necessary to bear in mind the preservation of the intended purpose of individual protective measures and also the maintenance of the required minimum level of protection.

3. Results

This chapter specifically elaborates on the safety requirements of the physical protection system 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 safety plan.

The selected object Vodňany water reservoir as an engineering structure defined by its boundary and perimeter, the disturbance or destruction of which, according to sectoral and cross-sectional criteria, would have serious adverse consequences on the quality of life of residents in terms of protection of their life and health, as well as the environment, is an element of critical infrastructure (CIE) within the meaning of the Critical Infrastructure Act [20].

At the same time, according to the Water Act [21], 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. And is 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, it is obliged [20]:

- apply technology that ensures its protection when modernising an element,
 - implement a safety plan.
- In order to draw up a safety plan, the operator must [20]:
- determine the importance of the equipment of the element (water reservoir),
 - evaluate the risk of threat of disturbance or destruction of individual equipment of the reservoir, their vulnerabilities, the expected consequences of their disturbance or destruction on the functionality, integrity and continuity of the operation of the element,
 - select the main security measures for the protection of the element, in particular: mechanical barriers, alarm systems, security elements of information systems, organisational measures with an emphasis on notification and warning procedures, as well as crisis management, training of persons and control measures for 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 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 Ministry of Economy of the Slovak Republic issued a Methodological Guideline on Security Measures for the Protection of Critical Infrastructure Elements 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 [22]. 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 products subsector, including, for example, pumping stations, can be selected as the most appropriate.

Certain requirements are imposed on this type of objects in a specially secured zone. The analysis of these requirements reveals the following minimum level of protection requirements for the reservoir:

- Video Surveillance System (VSS) – 4th level of security [23], purpose: perimeter monitoring and input identification,
- Intrusion and Hold-up Alarm Systems (I&HAS) – 4th level of security [24], perimeter detection, motion and door opening detectors, local optical-acoustic signalling,
- Access Control Systems (ACS) – 4th level of security [25], interconnection with mechanical barriers,
- backup power supply for alarm systems,
- IP protection or anti-vandalism,
- connection of alarm systems to the centralized protection desk with "24/7" operation,
- requirement for an integrated alarm system,
- perimeter: solid fencing, top barrier, lockable gate,
- casing: a door of solid construction equipped with a security locking mechanism or an electronic lock,
- physical protection requirements,
- organisational measures.

It follows that the minimum level of protection requirements apply not only to the representation of specific mechanical barriers and alarm systems, their degree of security, but also to their possible dislocation 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 [26], 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 [20], 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 of disruption or destruction of individual 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 (toxication 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 national level,

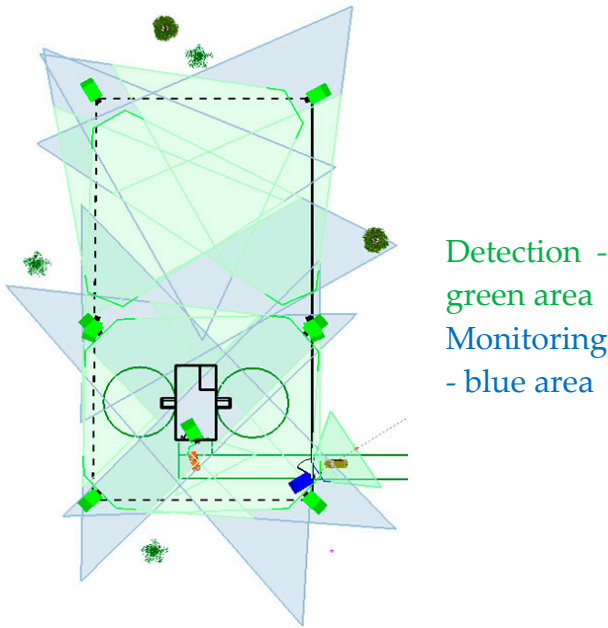
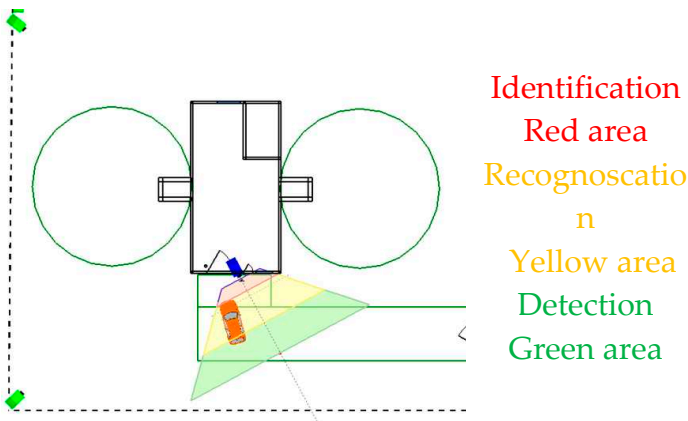


Figure 2. Coverage of the object by a camera system with detection and monitoring functions.



Resolution:
1920 x 1080
Chip size: 1/3";
16:9
Focal length:
4.3
Camera
height: 1.7 m
Tilt: 14°
Field of view:
63°; 38°
Distance: 6.9
m
View width: 8
m

Figure 3. Dislocation of cameras for identification using IP VIDEO System Design Tool software.

In the case of ACS, the dislocation of the individual protection elements is directly determined by the minimum protection level requirements:

- the access control system must allow controlled and regulated access of authorised persons from/to the facility,
- manually and electronically (locally and remotely) controlled entrance gates and gates and a system for monitoring the movement of persons with a connection to the access control system.

The dislocation of mechanical barriers is determined by the requirements for a minimum level of protection and the existing structural arrangement of the object itself (e.g. perimeter of the object, structure, room, opening fillings). Their dislocation in relation to their passive (breakthrough) resistance shall be designed to meet the minimum level of protection requirements for the overall functionality of the system.

The dislocation of physical protection determines the required or expected arrival time of the intervention unit. For the purpose of this study, the response of the intervention unit is determined with a range time of no more than 8 minutes from the place of first detection of the intruder. At an average travel speed of 70 km/h, we have a radius of 9 km from the water tower, in which the centralised protection desk with an intervention unit should be situated.

A functional PPS of objects is considered to be such a system that fulfils the basic condition that from the first place of detection, the attack time is greater than the reaction time of the intervention unit. For this particular case, the minimum level of protection, satisfying the basic condition for the functionality of the system, is determined by the extreme values of the parameters:

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

These extreme parameter values determine how many mechanical barriers with overall breakthrough resistance should be implemented at a specified total reaction time of the intervention unit. Furthermore, the outliers of the parameters indicate the initial place of detection. As stated above, the operator must evaluate (consider) the risks (scenarios) of the threat of disruption or destruction of individual CIE facilities, their vulnerabilities and the anticipated consequences of their disruption or destruction. Four risks (scenarios) of threat of disturbance or destruction of the reservoir are specified for this case of use (Table 1). These scenarios are evaluated using the SATANO software tool, in the form of calculations of individual parameters, critical paths, a graphical display of the initial place of detection, and the timeline of the attack

Possible attack risk scenarios:

Attack scenario 1: An external intruder uses freely available tools to overcome mechanical barriers and alarm systems, where:

- the target of the attack is damage to chlorine equipment resulting in the long-term shutdown of a large number of inhabitants from drinking water supply (Figure 4),
- the intruder proceeds from the public area through the perimeter towards the chlorine room of the water tank building, gradually overcoming standard aperture fillings (Figure 5),
- the expected maximum speed of movement of the intruder in the building is 2 m/s,
- the reaction of the intervention unit from the place of the first detection of the intruder is a maximum of 8 minutes.

Attack scenario 2 differs from the previous first scenario in that the intruder uses a paraglider motor glider to land in areas near chamber 1 and then overcomes standard aperture fillers towards the chlorine room.

Attack scenario 3: An external intruder uses freely available tools and then uses a chemical to contaminate water, where:

- the target of the attack is to poison a large population in a selected consumption area of residential district D5 (Figure 6),
- the intruder proceeds from a public area through the perimeter towards the chlorine room of the water tank building, where he pours a chemical substance into the pumping equipment,
- the expected maximum speed of movement of the intruder in the building is 2 m/s,

- the reaction of the intervention unit from the place of the first detection of the intruder is a maximum of 8 minutes,
- the detection of contamination of drinking water in the water supply network is based on a water pollution detector located at the outlet of chlorine equipment,
- the maximum rate of distribution of drinking water in the water supply network is 1.5 m/s [28],
- the reaction time for shutting off the drinking water supply for residents to residential area D5 is 8 minutes, by mechanically closing the valve after the arrival of employees of the company Vodárne a kanalizácia, s.r.o.

Table 1. Anticipated threat (attack) scenarios.

| Scenario (threat) | | Possibility of occurrence | Consequence | Risk level |
|--|--|---------------------------|-------------|------------|
| Incident | Consequence | <1 - 5> | <1 - 5> | |
| The intruder proceeds from the public area through the perimeter towards the chlorine room of the water tank building, gradually overcoming standard aperture fillings. The goal of the attack is to damage chlorine equipment. | Long-term shutdown of a large number of residents from drinking water supply | 4 | 5 | 20 |
| The intruder uses a paraglider motor glider to land in the premises near chamber No. 1 and subsequently overcomes standard aperture fillings towards the chlorine room. | Long-term shutdown of a large number of residents from drinking water supply | 4 | 5 | 20 |
| An external intruder using freely available tools, which then uses a chemical to contaminate water. | High population toxication | 4 | 5 | 20 |
| The intruder uses a paraglider motor glider to land in the premises near chamber No. 1 and then overcomes standard aperture fillings towards the chlorine room of the water tank building, where it pours chemical substance into the pumping equipment. | High population toxication | 4 | 5 | 20 |

Attack scenario 4 differs from attack scenario 3 in that the intruder reuses a paraglider motor glider to land in areas near chamber 1.

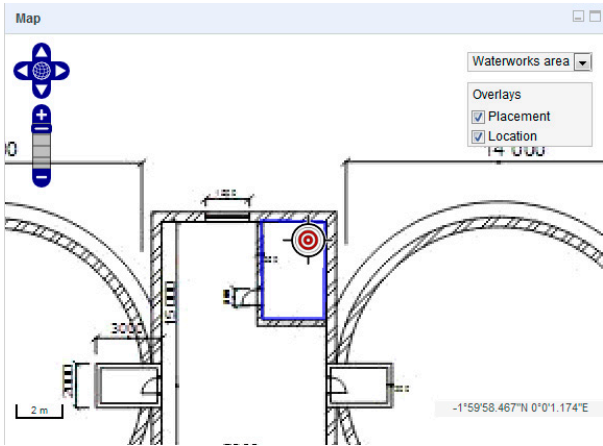


Figure 4. Common target of attacks  in scenarios 1 and 2.

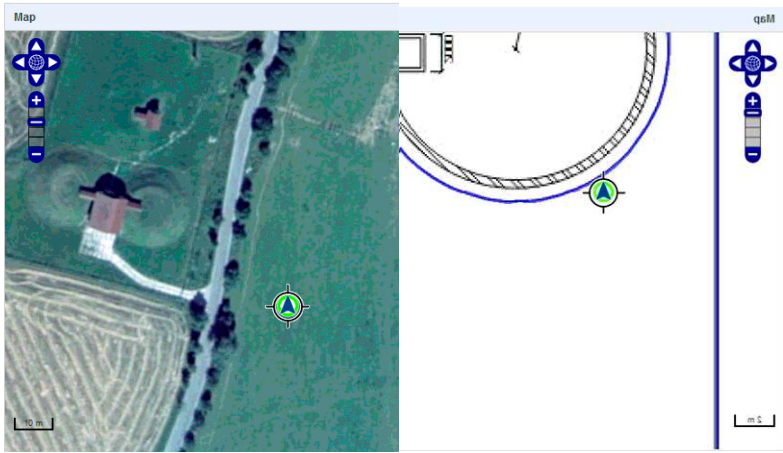


Figure 5. Starting points of the intruder  in scenarios 1 and 3 (left) and scenarios 2 and 4 (right).

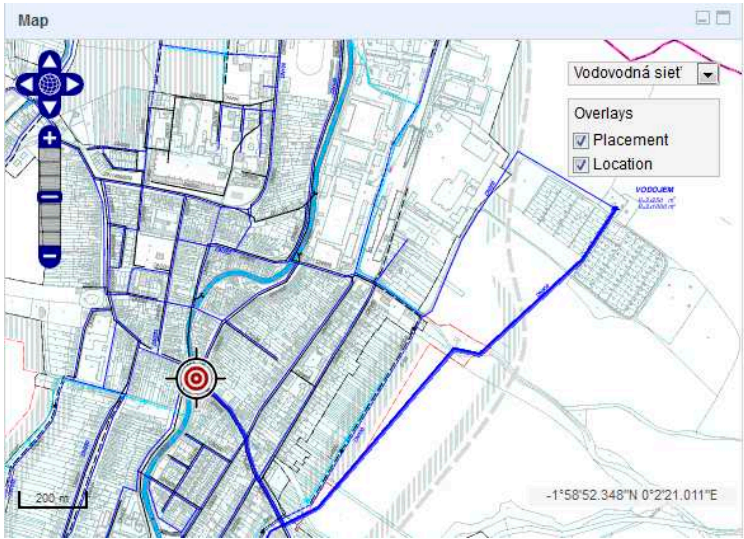



Figure 6. Water supply network Vodňany with the aim of attack  in residential area D5.

For a quantitative assessment of the level of the facility protection system, based on breakthrough resistances of mechanical barriers, probabilities of detection of alarm systems and

reaction times of physical protection. C (Figure 7) and then by simulation of the created scenario to verify the functionality of the given system or to detect its vulnerabilities (e.g. incorrect placement of mechanical barriers and alarm systems, incorrect selection of their parameters, insufficient reaction time of physical protection). Software tool SATANO was developed at the University of Žilina in 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). [29]

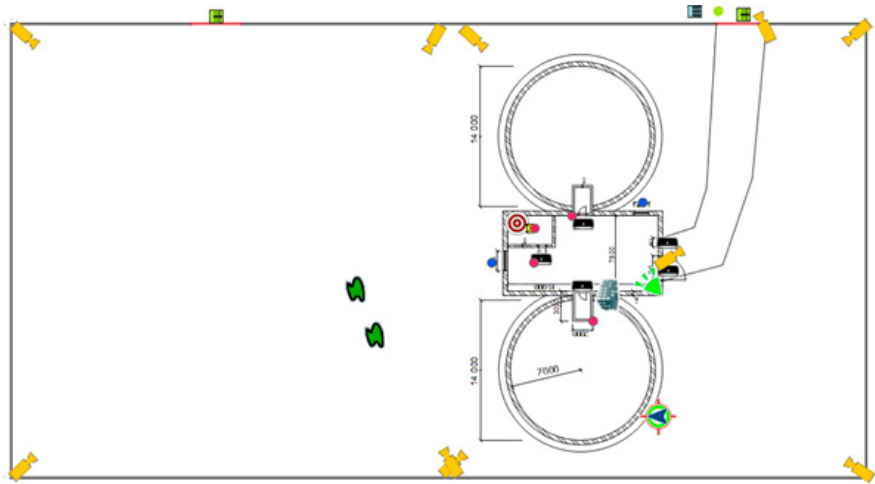


Figure 7. Model of the Vodňany water reservoir protection system processed in the SATANO software tool.

In total, four attack scenarios have been developed, differing in the starting points of the intruder and its attack targets, namely damage to chlorine equipment (scenarios 1 and 2) or contamination of the drinking water source (scenarios 3 and 4). All four attack scenarios were modelled and simulated in the SATANO software tool (where the functionality of the protection system was evaluated if the scenario was executed (Figure 8).

| Attack scenario assessments | | |
|--|------------------------|--|
| <div>Q <input type="text"/> Search</div> | | |
| <div>Delete selected attack scenario assessments 0 of 4 selected</div> | | |
| <input type="checkbox"/> Attack target | Response time | Attack critical path |
| Scenario 1 | | |
| <input type="checkbox"/> Chlorine station | SWAT: 480 [s] | measures efficiency coefficient: 1.057 probability of interruption: 0.562 delay due to passive barriers crossing: 490 [s] total path length: 59.85 [m] total time of attack: 519.92 [s] time of detection: 12.51 [s] time of target being protected by response unit: 492.51 [s] |
| Scenario 2 | | |
| <input type="checkbox"/> Chlorine station | SWAT: 480 [s] | measures efficiency coefficient: 0.476 probability of interruption: 0.051 delay due to passive barriers crossing: 210 [s] total path length: 37.15 [m] total time of attack: 228.57 [s] time of detection: 0 [s] |
| Scenario 3 | | |
| <input type="checkbox"/> Residential district - block D5 | closing valve: 480 [s] | measures efficiency coefficient: (1.057 ; 3.794) probability of interruption: 0.999 delay due to passive barriers crossing: 490 [s] total path length: 2030.5 [m] total time of attack: 1833.69 [s] |
| Scenario 4 | | |
| <input type="checkbox"/> Residential district - block D5 | closing valve: 480 [s] | measures efficiency coefficient: (0.476 ; 3.213) probability of interruption: 0.994 delay due to passive barriers crossing: 210 [s] total path length: 2007.8 [m] total time of attack: 1542.34 [s] |
| Results found: 4 | | |

Figure 8. Results of simulations of four scenarios of attack on the Vodňany water reservoir.

The results of attack scenario simulations 1 to 4 show that the PPS is effective in 3 out of 4 attack scenarios (Table 2). In scenario 2, the PPS needs to be adjusted, either by reducing the reaction time of the intervention unit or by increasing the passive resistance of some of the mechanical barriers in the reservoir object, so as to achieve parameter extremes determining the minimum level of protection.

Table 2. 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 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 TSO) and 3.213 (in the case of drinking water source closure system) | 0.994 | PPS is efficient |

An example of attack scenario 4 visualisation is shown in Figure 9.

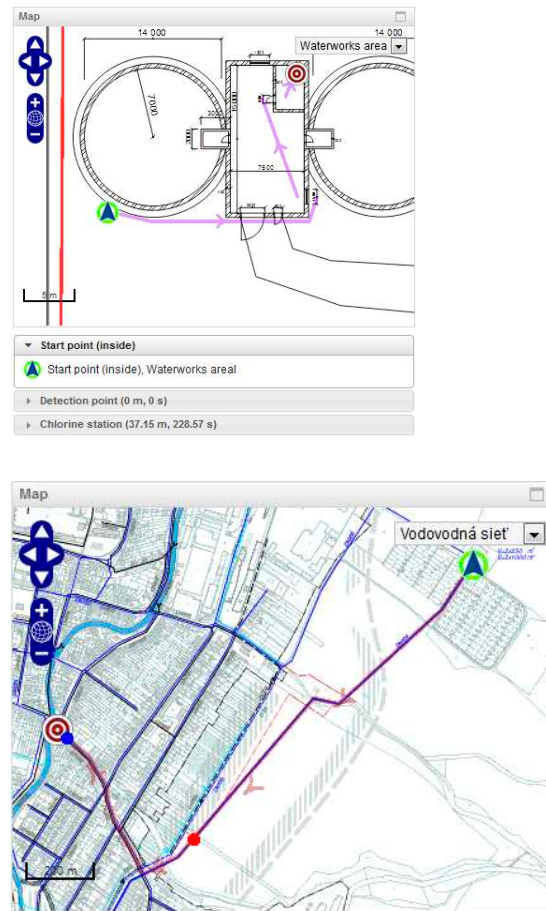


Figure 9. Graphical representation of the critical path of the intruder  in scenario.

4. Discussion

Objects of water management systems are often part of the critical infrastructure of a state or the EU due to the nature of their operation. Since they have a significant impact on the quality of life of citizens in terms of protecting their life and health, they are often the target of various attacks carried out by organised 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 requirements for the protection of objects against intentionally acting unauthorised persons with the aim of damaging, destroying or stealing protected property are determined primarily by generally binding legal regulations, technical, national, or international norms and standards, and the requirements of other third parties.

According to the European Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [26] as well as under the National Law on Critical Infrastructure [20], relevant threat scenarios need to be considered in order to assess vulnerabilities and the potential impact of disruption or destruction of critical infrastructure. In general, in the planning and design phases of physical protection systems (PPSs), it is possible to evaluate their functionality, economic efficiency, reliability and/or quality [16]. A functional PPS shall be considered to be a system which fulfils the basic condition that, from the initial detection point, the attack time is greater than the response time of the intervention unit. Existing methodological

procedures aimed at protecting objects use a qualitative or quantitative approach. Procedures based on a quantitative approach allow measurable input quantities (e.g. probability of detection, time of movement of the intruder, time required to overcome mechanical barriers) and output quantities (e.g. probability of interruption) to demonstrate precisely the justification of the proposed protective measures. One of the tools that uses a quantitative approach is the software tool SATANO (Security Assessment Of Terrorist Attack In A Network Of Objects), which allows to model 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 PPS against individual attacks (Table 2). 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 of the intervention unit).

The aim of the article was to present, at 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. Taking both approaches into account will make it possible to objectify the planning process of any PPS as much as possible

5. Conclusions

Water reservoir security is a dynamic and evolving field, as threats and risks to water infrastructure continue to emerge and change over time. Therefore, it's important for researchers and practitioners to stay up to date with the latest developments in this area. One emerging issue in water reservoir security is the use of advanced technologies, such as smart sensors and IoT devices, to monitor and manage water infrastructure. While these technologies can offer significant benefits in terms of efficiency and performance, they can also introduce new vulnerabilities and risks that need to be carefully managed. Another key consideration in water reservoir security is the need to balance security measures with the operational needs of water utilities. For example, physical security measures, such as fencing and surveillance cameras, can help to deter unauthorized access to water reservoirs, but they can also make it more difficult for utility workers to perform routine maintenance and repairs. Finally, effective communication and collaboration among stakeholders is essential for ensuring the security and protection of water reservoirs. This includes coordination between water utilities, government agencies, law enforcement, and the community at large. In summary, water reservoir security involves a holistic approach that addresses both physical and cybersecurity risks, takes into account the operational needs of water utilities, and emphasizes the importance of communication and collaboration among stakeholders.

Author Contributions: Data curation, formal analysis, data curation: T.L. L.M and. K.P.; writing—original draft, visualization: T.L.; writing—review and editing, methodology, 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. *New England Journal of Medicine*. 331(3). 1994, p.161-167. Available online: <https://pubmed.ncbi.nlm.nih.gov/7818640/> (accessed on 22 May 2023).
2. Hrudey, S. E.; Hrudey, E. J.; *Safe Drinking Water: Lessons from Recent Outbreaks in Affluent Nations*. IWA Publishing. 2004.
 3. Al-Ansari, N.; Al-Hadithi, M.; Knutsson, S.; *Terrorism and Security of Water Supplies: The Threat of Water Terrorism*. *Journal of Water Resource and Protection*, 5(5). 2013. P. 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. (2014); *Water Utility Incident Response Planning: Ensuring Effective Emergency Response to Contamination Events*. In *American Water Works Association (AWWA) Water Quality Technology Conference*.
 6. The Age. (2019). *Terrorism Plot to Poison Water Supply: Inside the Ringwood Conspiracy*. 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. U.S. Environmental Protection Agency (EPA). (2009). *Security Risk Assessment for Water Utilities*. Available online: <https://www.epa.gov/sites/default/files/2015-10/documents/security-risk-assessment-for-water-utilities.pdf> (accessed on 22 May 2023).
 8. U.S. Department of Homeland Security. (2016). *Protecting Critical Infrastructure: Water Sector Security*. Available online: <https://www.dhs.gov/publication/protecting-critical-infrastructure-water-sector-security> (accessed on 22 May 2023).
 9. World Health Organization (WHO). (2011). *Water Security Handbook: Planning for and Responding to Drinking Water Contamination Threats and Incidents*. Available online: https://www.who.int/water_sanitation_health/publications/water_security_handbook/en/ (accessed on 22 May 2023).
 10. Water Environment Federation. (2018). *Cybersecurity and Physical Security: A Unified Approach to Water System Protection*. 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).
 11. Jones, J. P.; Haimes, Y. Y.; (2011). *Security of Water Supply Systems: From Source to Tap*. Springer.
 12. National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. Available online: <https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11> (accessed on 22 May 2023).
 13. American Water Works Association (AWWA). (2013). *Risk Assessment and Risk Management for Water and Wastewater Utilities*. 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).
 14. Water Research Foundation. (2017). *Security Risk Assessment and Risk Management for Small and Medium Water Systems*. Available online: <https://www.waterrf.org/resource/security-risk-assessment-and-risk-management-small-and-medium-water-systems> (accessed on 22 May 2023).
 15. Loveček, T.; Reitšpís, J.; *Designing and evaluation of physical protection systems*, University of Žilina, Žilina, 2011. 281p.
 16. Loveček, T., Mariš, L., Šiser, A. *Planning and designing of physical protection systems*, University of Žilina, Žilina, 2018, 285p.
 17. Garcia, M.L.; *The Design and Evaluation of Physical Protection Systems*, Elsevier, USA, 2001, 370p.
 18. Kampova, K.; Loveček, T.; Řehák, D.; *Quantitative approach to physical protection systems assessment of critical infrastructure elements: Use case in the Slovak Republic*. *International Journal of Critical Infrastructure Protection* 2020, 30, 100376.
 19. Act No. 45/2011 Coll. on the protection of critical infrastructure.
 20. Act No. 364/2004 Coll. on water (Water Act).
 21. 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).
 22. EN 62676-1-1 (2014) *Video surveillance systems for use in security applications - Part 1-1: System requirement*. General. European Committee for Electrotechnical Standardization, Brussels.
 23. EN 50131-1 (2006) *Alarm systems. Intrusion systems. Part 1: System requirements*. General. European Committee for Electrotechnical Standardization, Brussels.
 24. EN 60839-11-1 (2013) *Alarm and electronic security systems - Part 11-1: Electronic access control systems - System and components requirements*. European Committee for Electrotechnical Standardization, Brussels.

25. European Council Directive 2008/114/EC of December 8, 2008 on the identification and marking of European critical infrastructures and the evaluation of the need to improve their protection. Available online: <https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32008L0114&from=EL> (accessed on 22 May 2023).
26. CLC/TS 50131-7 (2010) Alarm systems. Intrusion and hold-up systems. Part 7: Application guidelines. General. European Committee for Electrotechnical Standardization, Brussels.
27. Kriš, J.; Božíková, J.; Čermák, O.; Čermáková, M.; Škultétyová, I.; Tóthová, K.; Waterworks I: Water supply. Bratislava: STU v Bratislave, 2006, 816p.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.