energies

MDPI

Article

Functional Safety Concept to Support Hazard Assessment and Risk Management in Water-Supply Systems

Barbara Tchórzewska-Cieślak [1], Katarzyna Pietrucha-Urbanik [1,*] and Mohamed Eid [2]

[1] Department of Water Supply and Sewerage Systems, Faculty of Civil, Environmental Engineering and Architecture, Rzeszow University of Technology, Al. Powstancow Warszawy 6, 35-959 Rzeszow, Poland; cbarbara@prz.edu.pl
[2] National Institute of Applied Sciences of Rouen-LMN, INSA-Rouen, 685 Avenue de l'Université-BP 08, 76801 St. Etienne du Rouvray, France; eid.etudes@gmail.com
* Correspondence: kpiet@prz.edu.pl; Tel.: +48-17-865-1703

Abstract: Within the frame of upgrading and modernisation of the Water Supply System (WSS), our work is focussing on the safety systems/devices implemented or that should be implemented in the WSS. The implementation of safety systems is supposed to reduce hazard occurrence and hazardous consequences in case of a WSS unsafe disruption. To assess this reduction, we preconise the use of the safety integrity levels standards. The implementation of the safety systems/devices is undertaken on the ground of the multi-barriers safeguard approach. The "Water Contamination Hazard" is considered in the paper. A case study is presented, assessed and conclusions are drawn. The methodology presented in the paper and the results of the case study assessment will contribute to the decision-making regarding the upgrading of the safety and the performance of the WSS.

Keywords: functional safety; risk; failure analysis

Citation: Tchórzewska-Cieślak, B.; Pietrucha-Urbanik, K.; Eid, M. Functional Safety Concept to Support Hazard Assessment and Risk Management in Water-Supply Systems. *Energies* **2021**, *14*, 947. https://doi.org/10.3390/en14040947

Academic Editor: Abbas Barabadi
Received: 7 January 2021
Accepted: 6 February 2021
Published: 11 February 2021

1. Introduction

A complete analysis and assessment of the safety of water-supply systems is a complex issue. It should cover the analysis of the potential threats, their effects, the inherent system's operational safety, the security systems'/barriers' functional safety, and the procedural and managerial issues. The analysis principally targets the protection of the consumers and the environment.

This holistic and multi-faceted approach provides the necessary support to the decision-making process regarding Poland's WSS modernisation and the implementation of the international standards, the European Union (EU) guidelines and the World Health Organization's water safety plans [1–3]. Within this national holistic program, the paper is reporting on the topic "the security systems' and barriers' functional safety".

Generally, the concept of safety of the technical system is well understood and practiced. System safety assessments focus often on the system's main or top functions. The failure of maintaining any of these top functions within its safe operational limits may result in serious hazards threating the consumer and the environment. To decrease the occurrence frequency of these hazardous system failures, engineers design special safety and security systems or devices to survey and control the safe operations of the system. It is supposed that the implementation of the safety and security systems or devices in a system should reduce the occurrence frequency of hazardous failures. However, the expected reductions should be assessed and proven. If the functional performance of the safety system or device is not proven, its implementation in the technical system will not be approved.

Subsequently, safety systems play a critical role in the protection of WSSs. Their design and the assessment of their safety performance level are receiving increasing interest from

standardisation organisations and inspection authorities. This role is even amplified by the fact that WSSs are considered critical infrastructures.

Critical infrastructure management is an important issue and requires case-by-case analysis in order to build up the holistic approach of WSS safety management according to the seventh goals of the 2030 Agenda for Sustainable Development to fulfil reliable and sustainable energy use.

Within its focus on the safety systems or devices, the paper starts by presenting the concept of "functional safety" and its context, in Section 2.

In Section 3, the paper presents the concept of the safety integrity level (SIL) and its use to assess the functional performance of the safety systems or devices.

In Section 4, we introduce the safety multi-barriers approach and integrate the use of the SIL concept in the WSS safety assessment.

In Section 5, we identify the hazard that will be the focus of the case study in Section 7.

In Section 6, we present the methodology of assessing the safety of the WSS with safety systems or devices implemented in, using the SIL approach, in view of the defined hazard in Section 5, above.

In Section 7, a case study is presented, treated and the results are commented upon.

Finally, Section 8 presents a synthesis of the issue of our research, its context, general conclusions based on the case study, and recommendations concerning decisions to make, concerning the WSS modernisation program in Poland.

Many probabilistic risk-based assessments to support decision making in water supply system risk-management have already been carried out and will be carried out by our team. This paper focuses on the safety systems implemented in the water supply system. The object of the SIL standard methodology is to qualify the effectiveness of the safety systems or devices implemented in a big, complex systems such as the WSS.

2. Functional Safety

The concept of "functional safety" was introduced by International Electrotechnical Commission (IEC) 61,508 standard. IEC 61,508 standard is mainly concerned with Electric, Electronic or Programmable Electronic safety-related systems whose failure could have hazardous impacts on humans and the environment. Functional safety identifies potentially dangerous conditions that could result in hazards and it automatically enables corrective actions to avoid or reduce their impact. It is a part of the overall system safety and depends on automatic safeguards responding to a hazardous event [4].

Detailed functional safety standards are:

- In the field of industrial processes—IEC 61511;
- In the field of machines—IEC 62061;
- In the field of nuclear energy—IEC 61513.

The concept of functional safety relates directly to safety systems (monitoring, warning, control, and safeguard systems). Still, it can be used for the specification and implementation of systems where the functional performance parameter is not safety but, for example, environmental protection or asset protection [5]. In case of emergency, safety systems should ensure that the system is maintained at the required safety level or restored to a safe level. Functional safety does not concern the basic risks related to the inherent system failures in normal (operational) conditions (failures at pumping stations, distribution networks, or treatment plants). It concerns rather those risks that may arise when safety systems or apparatuses fail. In the case of a Water Supply System (WSS), this includes, above all, early-, delayed- or late-warning systems, as well as automatic monitoring and control systems. The task of safety systems is, in case of an inherent system failure, to reduce the occurrence frequency of the resultant hazard, as well as to eliminate/mitigate its consequences [6].

3. The Safety Integrity Level—SIL

Over the past three decades, several initiatives were undertaken to develop guidelines or standards to normalise the safe exploitation of the electrical, electronic, and programmable electronics (E/E/PE) used for safety applications in different engineering sectors. IEC 61,508 standards emerged as the most accomplished result.

Regarding safety systems whose failures may pose a threat to human health and life (especially in the workplace), IEC 61,508 standards have given rise to the concept of the so-called Safety Integrity Level (SIL). In accordance with IEC 61,508 (Functional safety of electrical/electronic/programmable electronic (E/E/PE) safety-related systems—Part 1), the "General Requirements" regarding risk reduction correspond to a "safety integrity level" in line with the risk reduction scale. This SIL concept is increasingly used in the design of safety systems or individual safety/security devices. These systems/devices should meet the SIL requirements in all engineering sectors. It is regularly resorted to in electrical devices and control processes, in the transport sector [7]. Moreover, it is introduced in the machinery engineering sector through EU appropriate standards such as the EU Directive 2006/42/EC MD [8].

In addition, standard EN ISO 13849-1:2008 introduces the concept of the Performance Level (PL) [9]. It assumes that the guarantor of the reliable and safe functioning of a technical system are security systems equipped with automatic monitoring and supervision, under the scrutiny of the Office of Technical Inspection. The highest level of a security automation is achieved by the so-called Safety Instrumented System (SIS), which is responsible for implementing safety instrumented functions (SIFs), with a specific SIL [6]. The SIS is a special-designed solution independent of the automation that controls a process. An SIS is designed to rapidly react to eliminate the effects of detected failure conditions.

Experts at Poland's Office of Technical Inspection are indeed active in running SIL analyses, thereby assessing the performance (SIL) of the Safety Instrumented Systems. There are two divisions of SIL level: a continuous operation division and the so-called request in line with the IEC 61,508 standard division.

SIL is a measure of the degree of risk reduction achieved by safety systems. The greater the potential hazards posed by the processes or the installations, the stricter the requirements for safety systems must be. In other words, the SIL is a measure of the expected performance of a safety function.

To reduce the risk of the "technical-system failures" or "facility failures" categories, appropriate elements of safety systems are used. Their main task is to eliminate hazard sources, reduce possible impacts and prevent escalation, in a severe failure situation. In accordance with the Regulation (352/2009) of the European Commission on the adoption of a common safety methodology for risk assessment, the aim is to attain and/or maintain an acceptable (or at least tolerated) level of risk [10–13].

The use of integrated safety systems with specified SIL levels aims to ensure an acceptable level of an overall risk related to the operational failures of the technical system. The SIL scale contains four levels, in line with EU engineering Safety Standards and practices (EN IEC 61508). Level 4 is the highest level and Level 1 is the lowest. A low SIL (SIL I) means a low expected risk reduction, while the SIL 4 denotes the highest expected risk reduction. The SIL level depends on [4,6]:

- The average per-demand probability of the safety functions' failure (PFDSYS)—for safety systems operating on demand;
- The average per-hour probability of a condition failure (PFHSYS)—for safety systems operating continuously.

In water-supply systems, requirements regarding functional safety apply to individual devices and installations subject to the Office of Technical Inspection supervision. Under standards EN ISO 13849-1 and EN 62061, the so-called Probability of Failure per Hour (PFH), offers a statistical measure of an object's ability to discharge its utility functions. The value in question relates to reliability and service life, as well as the frequency of occurrence

of unsafe failures. Unsafe or hazardous failures have the potential to prevent the safety system from achieving its safety function when there is a true demand [14].

To determine the probability density function (PDF), it is necessary to determine the system failure intensity index [4].

Standard EN IEC 61,508 draws a distinction between:

- Hazardous detectable failure
- Hazardous undetectable failure
- Safe (non-hazardous) detectable failure
- Safe (non-hazardous) undetectable failure.

The total failure intensity is the sum of the occurrence rates for safe undetectable, hazardous undetectable, safe detectable and hazardous detectable failures, and is a function of the so-called Mean Time To Fail (MTTF), as classified by the standard on three levels [15], i.e., as:

- The short MTTF whose value is in the range 3–10 years;
- The average MTTF whose value is in the range 10–30 years;
- The long MTTF whose value is in the range 30–100 years.

4. The Multi-Barrier System

Machine safety standards introduce so-called risk reduction measures by means of inherently safe design measures [16]. According to ISO 12100: "Inherently safe design measures are the first and most important step in the risk reduction process [. . .]. Inherently safe design measures are achieved by avoiding hazards or reducing risks by a suitable choice of design features of the machine itself [. . .]". To ensure the compliance of the chosen solutions with the risk reduction objectives without creating new hazardous situations, the overall risk should be reassessed once the designed solutions are implemented [17].

A risk reduction index is then needed to assess the effectiveness of the designed solutions. This index can be a number, a type, or a degree of the operational reliability [18–20]. It formally determines the effectiveness of the risk reduction expected by the designed security system using, e.g., the Layer of Protection Analysis (LOPA) method, [12]. The concept here assumes multi-layered security barriers being designed, where these layers relate to physical, technical, procedural, and organisational criteria. IEC:61508 stresses on the independence between different layers as part of their definitions.

The SIS are used commonly in process industry [7,10], as well as in the transport sector [21]. Modern SIS implement blocking and automatic security smart algorithms. Their task is to bring the process (i.e., water supply to the consumer in our case) back to a safe functioning [22–24].

More specifically, the multi-barrier systems for WSS are monitoring, controlling, and warning systems, [25]. They are designed to reduce the occurrence probability of a hazard and/or eliminate/reduce/mitigate its consequences [26,27]. Safety barriers can be active or passive. For example, a non-return valve is a passive barrier while a motorised valve is an active barrier. In all cases, safety barriers should be independent. Individual safety barriers may operate in a sequential or in a parallel order.

The introduction of SIS systems into the operations of a WSS entails the design of automation and control systems. In an emergency, they should switch off the supply of the raw water to the water treatment plant (WTP), and safely power down valves, motors, pumps etc. WSS shutdown generates economic losses for the utilities but safeguards consumers and the environment. Subsequently, SIS is assumed to be activated only when hazard occurrence is highly probable or certain. For this reason, the design of lower layers deploying sensors able to detect weak signals and precursors signs may guarantee the elimination of the hazard at earlier stages of the development of the root-causes of hazard, avoiding the activation of the SIS [28,29].

In this regard, water-supply systems should have at least three-layer security systems in place [22]. Indeed, a basic multi-barrier system for a WSS would have components such as [22]:

- A system for the analysis of water quality at the water intake or at the WTP, augmented by biomonitoring that assesses water quality in terms of overall pollution;
- An early warning system—information on water quality provided in advance, and based on automatic and continuous water-quality analysis carried out at a protection-and-warning station located upstream;
- A late warning system—analysis of the quality of water taken into the distribution subsystem run by both the supply company and the relevant department of Sanepid (Poland's sanitary and epidemiological service).

A right decision by a WTP operator requires some time in advance, given that the sooner the operator is informed about a contamination occurrence, the greater the chance is of taking the appropriate measures to minimise/mitigate its consequences. A diagram of the functioning of a pollution warning system is provided in Figure 1 [5].

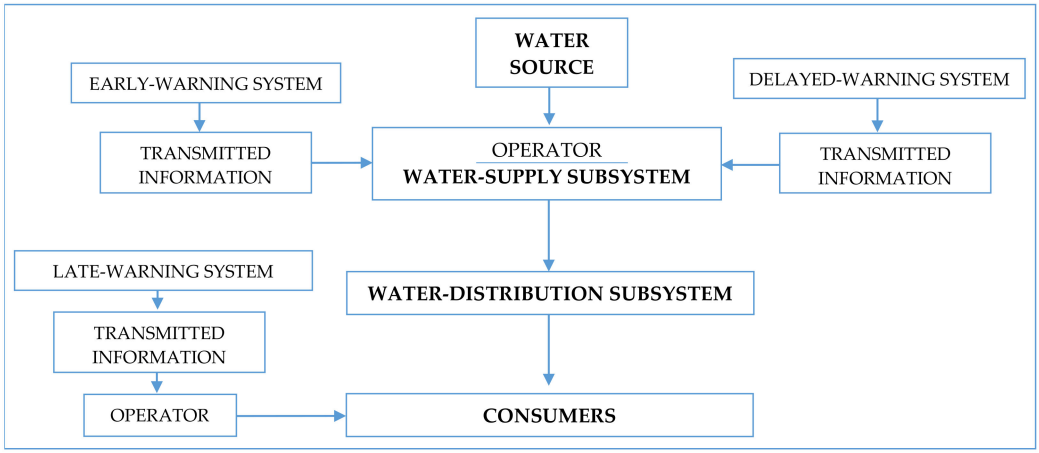

Figure 1. Functional diagram for early-, delayed- and late-warning systems.

The early-warning process is an issue for protection-and-warning stations, whose task is to continuously analyse the specific indicators of water quality, with an automatic real-time transmission of the results thereof to the water treatment plant. Operators at the latter will then be able to intensify (or otherwise modify) the treatment process. This would be very appreciable if the contamination cannot not be cleared and the intake must be shutdown to safeguard the consumers, [1,30].

5. Water Protection and Contamination Hazards

Regarding the WSS, the major hazards are the hazardous contaminants that may bring high risk to human life and the environment. Advanced sensors and E/E/PE devices using technologies to detect and analyse hazardous contaminants in water are available and their technology readiness levels are rapidly increasing with time. The summation of some pollution threating factors pushes the reinforcement of the role of water quality monitoring and early warning functions. These pressing factors are namely: the growing global pollution levels in air and water, the climate changes, the continuous rarefication of global water reserves, and the potential risks of malevolent water contamination acts. Thus, the role of security and warning stations becomes critical.

A protection-and-warning station should be equipped to analyse water quality continuously and reliably. Potential water contaminant categories are inorganic, organic, biological, and radiological. Contaminants can be natural or man-made. However, the most frequently monitored indicators of water quality are actually: turbidity, pH, dissolved oxygen, organic carbon, ammonium–nitrogen, and hydrocarbons. The actual list of systematically monitored contaminants looks short if we consider the potential threating factors mentioned previously.

The actual list of measured contaminants contains [5]:

- Microbiological contaminants;
  - Protection of the intake against cattle and human centres (protection zones of water intakes);
  - Use of early warning systems (e.g., guard stations);
  - Stopping water abstraction during periods of high pollution, such as after storms;
  - Increasing the reliability of treatment by introducing back-up (alternative) systems;
  - Automatic closure systems preventing the supply of inadequately treated water;
  - Devices preventing flow returns.
- Chemical contaminants;
  - Optimisation of chlorine dosing to reduce trichloromethane;
  - Isolation of the system from potential leaks;
  - Risk assessment for suppliers of chemical agents.
- Physical contaminants;
  - Flushing the water supply network of waterworks;
  - New standard maintenance procedures to prevent sludge re-suspension;
  - Anti-flow backflow measures.

Obviously, the choice of indicators for continuous monitoring should be locally adjusted to meet the local specifications of the production and the consumption locations.

Thus far, Poland only has a few such early-warning systems designed and installed. Currently, only large cities can afford them. However, from the theoretical and design points of view, the functioning of warning stations is already a well-known subject, [2,31]. An important characteristic of the WSS is that high quality alarmed data can be monitored before an extreme hazard can definitively propagate in the network and become out of control [32]. It is unfortunately not the case of severe hazards in other engineering sectors with severe accidents such as: electricity blackouts or nuclear powerplant criticality divergence. In other words, hazards propagation in the WSS is governed by a slow dynamic pattern while nuclear criticality divergence is governed by an extremely fast dynamic pattern. That is why early warning monitoring plants have an important role in eliminating and mitigating serious hazards in WSS, while rapid electronic automatic control safety devices have the most critical safety and safeguard functions in nuclear power plants.

The operational experience feedback of WSS distinguishes between two possible types of information-transmission errors, whose occurrence gives rise to different consequences. The first type of errors affects the operational reliability of the WSS while the second affects the WSS safety.

Safety can also be increased by using alternative water-treatment technologies. These are used where contamination cannot be cleared by conventional treatment process.

The most used decontamination processes are related to:

- Modifications in the type or the dose of coagulant or flocculant;
- The use of granular or powdered activated carbon;
- Increasing the dose of disinfectant to eliminate biological contamination.

In the case of a source-water hazardous pollution that cannot be cleared neither by conventional processes nor by alternative proven technologies, the intake will be shut down until the pollution is cleared. The diversification of water supplies is thus strategically important so that the loss of efficiency of the entire WSS may remain as limited as possible, in case of the shutdown of some intakes. In most cases, a large urban WSS will be supplied via several intakes [33,34].

Storage tanks may also constitute reasonable mobile alternatives, in case of serious water shortage crises. Two technological lines of the treatment plants may be distinguished according to the storage tanks classes:

- Raw water storage tanks;
- Clean water storage tanks.

The main goal is the safeguarding of the consumer from the incidental contamination of the water source [35]. Otherwise, raw-water tank operations require an effective protection-and-warning station equipped with an automatic analyser and a continuous transmission of results to the dispatcher of the WTP. This solution allows for appropriate decision-making at the earlier stages of the development of a water shortage crisis [36].

The storage of raw water in a tank can affect the physical, chemical, and microbiological properties of the stored water. The factors most likely to alter the water quality include:

- Time of retention;
- Frequency and scale of changes in level;
- Seasons and weather conditions;
- Type and state of the tank's inner surface;
- Operational and functional conditions;
- Type of flow inside the tank (mixing and replacement of water, absence, or non-absence of zones of dead water).

Treatment technology first and foremost entails raw-water tanks acting as primary settling tanks. Their use limits fluctuations in the quality of the water supplied to the WTP, helping to dampen fluctuations in the quality of the water present in the source of the river. This leaves the possibility of algae reproducing and developing as one of the significant hazards in raw-water storage.

Tanks collecting clean water are most often located within the WTP. Network tanks can thus be starting, central or ending, and most serve as reserve or equalising tanks. The reserve of clean water decreases during long water supply disruptions, while during short ones the reserve increases. The use of tanks with clean water and network tanks allows a steady-state operation of pumps and treatment devices. Tanks' elevation level allows the stabilisation of pressure in the supply network. Reservoirs also store water for firefighting and emergency purposes. The stored water can be used when an intake is shut down or when there is a breakdown along a network. The effect is again to raise the level of consumers' safety.

6. The Risk Reduction Requirements and Methodology

Security systems (classical monitoring, biomonitoring, a control supervision system, etc.) are used to achieve a required safety level. Then, it may be useful to deploy the SIL procedure. This is especially true where WSS automation and control systems are concerned. Deploying SIL standards [7] entails:

- Hardware and software redundancy for control-system components;
- The separation of alarm systems;
- Advanced visuals of the processes relevant to the WSS;
- The training of operators on emergency management;
- The commissioning of current-process diagnostic systems and devices permitting automation;
- The introduction of Fault-Tolerant Control Systems (FTCSs), whereby [37]
  - The place of hardware redundancy in FTC systems is taken by analytical (information) redundancy, and therefore some software redundancy;
  - The place of the dynamic redundancy used primarily in controllers of automation systems is mainly taken by an approach that identifies failures of measuring and actuates devices;
  - Other diagnostic methods are deployed: these can be computer-related regarding controllers and process-related regarding measuring lines and actuators;
  - Dynamic redundancy should be considered at the earliest stages of the design.

Standard EN ISO 13849-1:2008 proposes a risk-assessment method for determining the required level of safety assurance (PL_r). As far as the WSS is concerned, the proposed method encompasses the following parametric scale:

- C—size of probable losses:
  - C_1—small;
  - C_2—medium;
  - C_3—large.
- F—frequency and/or duration of the threat:
  - F_1—rare; fairly frequent and/or short exposure time;
  - F_2—frequent; continuous and/or long exposure.
- E—possibility of the threat being counteracted:
  - E_1—possible;
  - E_2—impossible.

The procedure for determining the required safety level can then be pursued by reference to a standard risk graph (Figure 2).

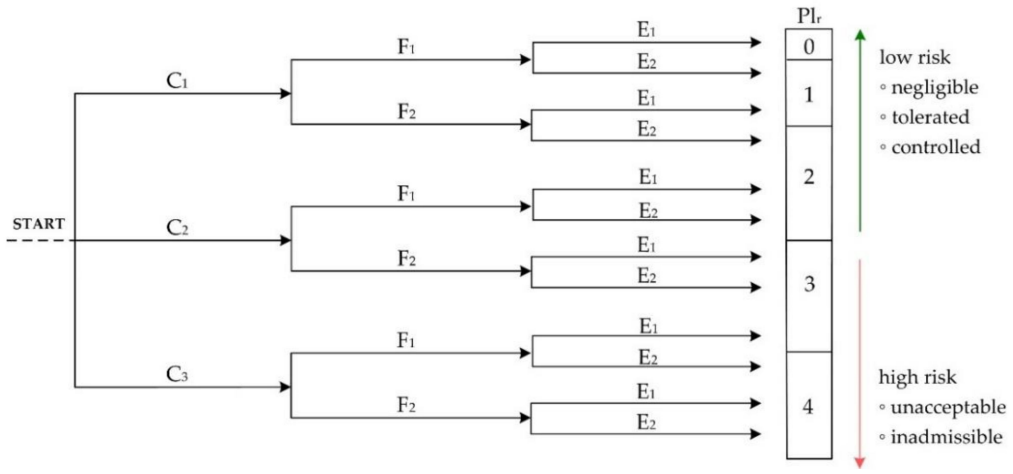

Figure 2. Procedure for determining the required safety assurance (PL_r) level.

The PL level is determined as shown in Figure 2 —in a scale from 0 to 4—the requirements (from most-limited to most-exacting) when it comes to WSS control systems. This scale has been modified due to provisions set on the relevant WSS standard [1,3]. The required PL_r safety level can be achieved by implementing the control system for several different variants, depending on the components' reliability (as evidenced by the mean time to fail, MTTF), and on the type of system used to detect the threats.

7. The Case Study

7.1. Characteristics of the Water System Analysed

The Polish city is supplied with water from a river by means of a bank-chamber water-intake of 84,000 m^3/d capacity. This is treated in a modern two-water treatment plant and meets the quality requirements for water intended for human consumption. At present, the overall water distribution system supplies water to some 190,000 inhabitants of the city and nearby towns. The average daily production amounts to approx. 34,600 m^3/d of treated water, which is enough to fully meet the demand. The municipal "water and sewerage" company also operates: an emergency deep intake of 240 m^3/d capacity, a local water intake, water pumping stations, clean-water equalising tanks and public wells.

7.2. An Example of the Method Being Applied

The city is supplied with drinking water from a central supply system whose source is flowing surface water. Quality monitoring includes an early-warning system (raw water), a delayed-warning system (treated water) and a late-warning system (water in the network). The exposure of the consumers to possible hazards is deemed to be continuous. However, the risk of secondary chemical and microbiological contamination of water in the distribution subsystem should be specified. The classification of risk factors for this specific case is presented in Table 1, according to [10].

Table 1. Classification of risk parameters.

Risk Parameters		Qualitative Classification	Quantitative Classification	Points Scale
Frequency of occurrence of threat/duration of exposure to risk—F	F_1	incredible/negligible	<1 time in 30 years/ <10% of the time	1
	F_2	unlikely/average	1 in >10 to 30 years/ 10–20% of the time	2
	F_3	sporadic/frequent to permanent	1 time in 10 years/≥20% of the time	3
Magnitude of possible consequences—C	C_1	noticeable organoleptic changes in water, a nuisance that is not a health hazard, few consumer complaints	less than 0.01	1
	C_2	quality standards breached slightly, health problems and complaints as regards quality (e.g., odour) among consumers	0.01 to 0.1 probable fatalities per event	2
	C_3	hospitalisation of those exposed is required, information is supplied in public media	>0.1 to 1.0 probable fatalities per event	3
	C_4	threat to the health or lives of consumers, serious toxic effects on indicator organisms, mass hospitalisation, fatal cases, media headlines	>1 probable fatality per event	4
Possibility of the threat being counteracted—E	E_1	routine periodic monitoring of water quality and online monitoring of selected indicators	>90% probability of hazard being avoided	1
	E_2	routine periodic monitoring of water quality	≤90% probability of hazard being avoided	2

The quantitative scale of risk categories is as presented in Table 2.

Table 2. Quantitative scale of risk for the particular water-supply system.

Risk Category	Quantitative Gradation of Risk	PL_r
Inadmissible	16–24	4
Unacceptable	8–12	3
Controlled	3–6	2
Tolerable	2	1
Negligible/No safety requirements	1	0

Quantitative gradation of risk in line with the points-scale weight presented in Table 1 is determined by the following formula:

$$r = C \cdots F \cdots E, \quad (1)$$

where for each threat the characteristics of C, F, and E are determined.

The values of a well-defined risk (r) are determined using an appropriate formula (3). Figure 3 shows the determination of the PL_r levels for the water-supply system under consideration. The risk assessment means the determination of the correspondent "path".

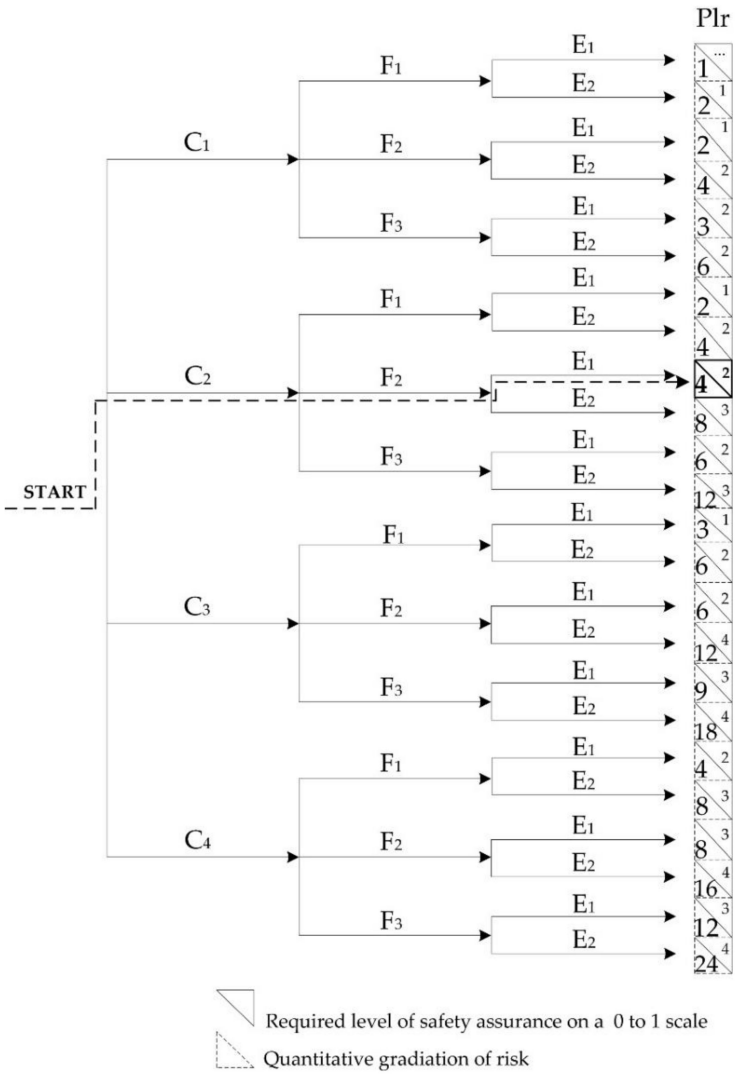

Figure 3. The determination of the PL_r level for the water-supply system (WSS) examined in line with the scenario indicated.

7.3. Discussion of the Obtained Paths

The proposed method takes account of all possible combinations of the risk factors. If a tolerable risk is obtained, threat monitoring is required to maintain the risk in this category. If a controlled risk is obtained, the level of risk need to be lowered to acceptable values. The process is particularly important where points values arise within the range of tolerable risk. Relevant actions have an implication cost that is proportional to any benefits gained. If a risk is unacceptable, actions to reduce it are necessary. Should the emergency scenario associated with the unacceptable risk occur, the shutting-down of the WSS should ensue.

Assessments of elements in relation to the above risk graph were as follows:

- Magnitude of possible consequences—C_2;
- Frequency of occurrence of threat/duration of exposure to risk—F_2;
- Possibility of the threat being counteracted—E_1.

The path for the risk graph obtained is traced in Figure 3. It corresponds to a controlled risk level. Remedial measures to be taken are:

- More-frequent monitoring of the water supply;
- Raising the level of stability of the treated water;
- Possible ozonation and filtration through granular activated carbon

Adequate early detection of contamination enables rational action and protection of consumers against the contaminated water. Taking the right process decisions in terms of water treatment or a decision to warn the public about poor water quality always requires a certain time in advance. Hopefully, the WSS hazards consequences propagation is governed by low dynamic pattern. So, the quicker the system operator receives information about the threat, the greater the possibility will be of making the right decisions. The credibility of the information provided is also of great importance. The introduction of the contaminated water in the WSS means the loss of safety for the consumer and the environment. In turn, sufficiently early detection of incidental contamination in the WSS may lead to the intensification of treatment processes, the introduction of alternative technologies or more periodic control and analyses of the water quality in the WSS.

8. Conclusions

A Risk-based management of the water supply system is needed. That requires the introduction of safety management procedures to minimise the effects of incidental adverse events, to minimise the sanitary hazards exposure of the consumer, and to rationalise decision making regarding WSS management.

One issue is to analyse and assess the reliability of the safety system and its individual components, as a basis to help in decision-making regarding the modernisation, renewal, or repair of the existing systems. Another issue is safety and risk analysis, i.e., regarding threats and their effects, above all for consumers. In this regard, the safety analysis of the system as a whole and of its individual elements should be considered. This should then form the basis for the water safety plan. A comprehensive approach to the safety of a water-supply system should also include the analysis and the assessment of the functional safety of the safety/security systems, e.g., using a multi-barrier approach.

Facing the growing international tensions up to and including potential conflicts over water, as well as climate changes, it seems necessary to have efficient systems of threat early-detection, as well as rapid crisis-response managing systems, in the event of a water shortage or severe contamination crisis.

Further research on the topic should focus first and foremost on modern ICT being deployed and integrated in the risk analysis and assessment, and on the development of decision models for WSS operators. It is also necessary to develop criteria and metrics for quantified risk assessments and for risk reduction indicators.

Author Contributions: All authors equally contributed to the development of this manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: I thank the reviewers for their feedback, which helped to improve the manuscript quality.

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

References

1. Drinking Water Directive (Council Directive 98/83/EC of 3 November 1998 on the Quality of Water Intended for Human Consumption), with Its Latest Amendments Including Commission Directive (EU) 2015/1787 of 6 October 2015. Available online: https://ec.europa.eu/environment/water/water-drink/legislation_en.html (accessed on 6 November 2020).
2. World Health Organization. *Guidelines for Drinking-Water Quality*, 4th ed.; World Health Organization: Geneva, Switzerland, 2011. Available online: https://apps.who.int/iris/bitstream/handle/10665/44584/9789241548151_eng.pdf;jsessionid=FB26DE4E81767BC7525DC61A1537C754?sequence=1 (accessed on 15 December 2020).
3. World Health Organization. *Water Safety Plans, Managing Drinking-Water Quality from Catchment to Consumer, Water, Sanitation and Health*; Protection and the Human Environment World Health Organization: Geneva, Switzerland, 2005.
4. International Electrotechnical Commission (2010). IEC 61508—Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems, Geneva, First Version Issued 1999. Available online: https://webstore.iec.ch/publication/5515 (accessed on 10 December 2020).
5. Tchórzewska-Cieślak, B. *The Multifaceted Analysis of Safety in the Operation of Water Supply Systems*; Publishing House of the Rzeszow University of Technology: Rzeszow, Poland, 2018. Available online: https://eksiegarnia.pl/wieloaspektowa-analiza-bezpieczenstwa-w-eksploatac,3,187,97299 (accessed on 1 December 2020).
6. Borysiewicz, M.; Markowski, A.S. *Acceptability Criteria for Major Industrial Accidents*; Central Institute for Labor Protection: Warsaw, Poland, 2002. Available online: https://www.researchgate.net/profile/Adam_Markowski/publication/268275406_Kryteria_akceptowalnosci_ryzyka_powaznych_awarii_przemyslowych/links/57233daa08ae586b21d87eb3.pdf (accessed on 15 December 2020).
7. Kosmowski, K.T. Risk analysis and functional safety management. *J. Pol. Saf. Reliab. Assoc. Safety Reliab. Semin.* **2011**, *3*, 1–16. Available online: http://ssars.am.gdynia.pl/upload/SSARS2011PDF/VOL3/SSARS2011-Vol3-02Kosmowski.pdf (accessed on 1 December 2020).
8. Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on Machinery, and amending Directive 95/16/ECL 157/24. Available online: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:157:0024:0086:EN:PDF (accessed on 1 December 2020).
9. EN ISO 13849-1:2008. Safety of Machinery. *Safety-Related Parts of Control Systems. General Principles for Design.* Available online: https://shop.bsigroup.com/ProductDetail/?pid=000000000030232654 (accessed on 1 December 2020).
10. Commission Regulation (EC) No 352/2009 of 24 April 2009 Adopting a Common Safety Method for Risk Evaluation and Assessment. *Off. J. Eur. Union.* **2009**. Available online: https://ec.europa.eu/transport/sites/transport/files/celex_32009r0352_en_txt_0.pdf (accessed on 1 December 2020).
11. Markowski, A.S. *Layer of Protection Analysis for the Process Industries*; PAN: Łódź, Poland, 2006; Available online: http://repozytorium.p.lodz.pl/handle/11652/1856 (accessed on 1 December 2020).
12. Markowski, A.; Mannan, S. Fuzzy risk matrix. *J. Hazard. Mater.* **2008**, *59*, 152–156. [CrossRef] [PubMed]
13. McGrill, W.L.; Ayyub, B.A.; Kaminskiy, M. Risk Analysis for Critical Asset Protection. *Risk Anal.* **2007**, *275*, 1265–1281. [CrossRef] [PubMed]
14. API STD 689, Collection and Exchange of Reliability and Maintenance Data for Equipment, First Edition, July 2007. Available online: https://global.ihs.com/doc_detail.cfm?document_name=API%20STD%20689&item_s_key=00496526 (accessed on 1 December 2020).
15. Bell, R. *Introduction to IEC 61508*; Health & Safety Executive Bootle: Bootle, UK.
16. ISO 12100-2:2010. Basic Concepts, General Principles for Design—Part 2: Technical Principles. Available online: https://standards.iteh.ai/catalog/standards/sist/2ca6bc24-071d-4216-ab20-7563e09e3d86/sist-en-iso-12100-2-2004-a1-2010 (accessed on 1 December 2020).
17. CSST & IRSST GUIDE RG-597 Machine Safety: Prevention of Mechanical Hazards. Available online: http://www.irsst.qc.ca/media/documents/pubirsst/rg-597.pdf (accessed on 1 December 2020).
18. Pietrucha-Urbanik, K.; Tchórzewska-Cieślak, B.; Eid, M. Water Network-Failure Data Assessment. *Energies* **2020**, *13*, 2990. [CrossRef]
19. Chybowski, L. Importance Analysis of Components of a Multi-Operational-State Power System Using Fault Tree Models. *Information* **2020**, *11*, 29. [CrossRef]
20. Pietrucha-Urbanik, K.; Rak, J.; Tchórzewska-Cieślak, B. Safety analysis of water supply systems including protection barriers. *J. Pol. Saf. Reliab. Assoc. Safety Reliab. Semin.* **2013**, *3*, 241–248. Available online: http://jpsra.am.gdynia.pl/upload/SSARS2013PDF/VOL2/SSARS2013-PietruchaTchorzewskaRak.pdf (accessed on 1 December 2020).
21. Szymanek, A. Risk Acceptation Principles in Transport. *J. KONBIN* **2008**, *2*, 271–290. [CrossRef]
22. Rybicki, S.A. Multi-barrier system—A way to reduce the risk of delivering water of inadequate quality. *Ochr. Srod.* **2001**, *3*, 7–12. Available online: http://www.os.not.pl/docs/czasopismo/2001/Rybicki_3-2001.pdf (accessed on 1 December 2020).
23. Ondrejka Harbulakova, V.; Estokova, A.; Kovalcikova, M. Correlation Analysis between Different Types of Corrosion of Concrete Containing Sulfate Resisting Cement. *Environments* **2017**, *4*, 44. [CrossRef]
24. Parka, A.; Kuliczkowska, E.; Kuliczkowski, A.; Zwierzchowska, A. Selection of pressure linings used for trenchless renovation of water pipelines. *Tunn. Undergr. Space Technol.* **2019**, *98*, 103218. [CrossRef]
25. Sklet, S. Safety barriers: Definition, classification and performance. *J. Loss Prev. Process Ind.* **2006**, *19*, 494–506. [CrossRef]
26. Urbanik, M.; Tchórzewska-Cieślak, B.; Pietrucha-Urbanik, K. Analysis of the Safety of Functioning Gas Pipelines in Terms of the Occurrence of Failures. *Energies* **2019**, *12*, 3228. [CrossRef]

27. Vališ, D.; Hasilová, K.; Forbelská, M.; Vintr, Z. Reliability modelling and analysis of water distribution network based on backpropagation recursive processes with real field data. *Measurement* **2020**, *149*, 107026. [CrossRef]
28. Zio, E. *An Introduction to the Basics of Reliability and Risk Analysis*; World Scientific Publishing: Singapore, 2007. Available online: https://dl.uswr.ac.ir/bitstream/Hannan/131120/1/Enrico_Zio_An_Introduction_to_the_Basics_of_Reliability_and_Risk_Analysis_Series_on_Quality%2C_Reliability_and_Engineering_Statistics_Series_on_Quality%2C_Reliabi.pdf (accessed on 1 December 2020).
29. Zieja, M.; Wazny, M.; Stepien, S. Outline of a method for estimating the durability of components or device assemblies while maintaining the required reliability level. *Maint. Reliab.* **2018**, *20*, 260–266. [CrossRef]
30. Rak, J.R.; Tchórzewska-Cieślak, B.; Pietrucha-Urbanik, K. A Hazard Assessment Method for Waterworks Systems Operating in Self-Government Units. *Int. J. Environ. Res. Public Health* **2019**, *16*, 767. [CrossRef] [PubMed]
31. The Act of 20 July 2017—Water Law. Available online: http://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20170001566/T/D20171566L.pdf (accessed on 1 December 2020).
32. Bondoc, I.; European Regulation in the Veterinary Sanitary and Food Safety Area, a Component of the European Policies on the Safety of Food Products and the Protection of Consumer Interests: A 2007 Retrospective. Part One: The Role of European Institutions in Laying Down and Passing Laws Specific to the Veterinary Sanitary and Food Safety Area. *Universul Jurid. Supl. 2016, 12–15.* Available online: https://www.researchgate.net/publication/316716657_EUROPEAN_REGULATION_IN_THE_VETERINARY_SANITARY_AND_FOOD_SAFETY_AREA_A_COMPONENT_OF_THE_EUROPEAN_POLICIES_ON_THE_SAFETY_OF_FOOD_PRODUCTS_AND_THE_PROTECTION_OF_CONSUMER_INTERESTS_A_2007_RETROSPECTIVE_PA (accessed on 1 December 2020).
33. Geng, Z.Q.; Wang, Z.; Hu, H.X.; Han, Y.M.; Lin, X.Y.; Zhong, Y.H. A fault detection method based on horizontal visibility graph-integrated complex networks: Application to complex chemical processes. *Can. J. Chem. Eng.* **2019**, *97*, 1129–1138. [CrossRef]
34. Mens, M.J.P.; Gilroy, K.; Williams, D. Developing system robustness analysis for drought risk management, an application on a water supply reservoir. *Nat. Hazard Earth Syst.* **2015**, *15*, 1933–1940. [CrossRef]
35. Zielina, M. Particle Shapes in the Drinking Water Filtration Process. *Clean-Soil Air Water* **2011**, *39*, 941–946. [CrossRef]
36. Pawlak, M.; Kościelny, J.M.; Wasiewicz, P. Method of increasing the reliability and safety of the processes through the use of fault tolerant control systems. *Eksploat. Niezawodn.* **2015**, *17*, 398–407. [CrossRef]
37. EN 15975-2:2013. Security of Drinking Water Supply. *Guidelines for Risk and Crisis Management. Risk Management.* Available online: https://standards.iteh.ai/catalog/standards/sist/dd2df50c-59ec-40f4-845a-00b83dfdd6df/sist-en-15975-2-2013 (accessed on 1 December 2020).