Tchórzewska-Cieślak Barbara

Pietrucha-Urbanik Katarzyna

Szpak Dawid
Rzeszow University of Technology, Rzeszów, Poland

Developing procedures for hazard identification

Keywords

failure, system safety, safety management, threats

Abstract

The reliable operation of critical infrastructure has a direct impact on the energy security of country. Due to the complexity and vastness of such system it is exposed to various types of events that could lead to failure. These risks may result directly from the operation and also be the result of external factors. Especially dangerous are the undesirable events with incidental character or unlikely events that constitute a serious threat to people and the environment and resulting in significant loss.

1. Introduction

The primary objective of risk management is to increase the safety of the technical system. The basis of the risk management process is the identification of threats because effective management without this knowledge is practically impossible. The most important is to recognize the technical threats [15], [23]. Besides, you should pay attention to the human and environmental factor, organizational structures and interrelationships between them [7], [16]. Only this approach guarantees avoiding the so-called unidentified risk. For the so called pure risk, associated with the operation of the technical system, standard actions have been developed. Standard solutions for the protection and safety of the technical system should be adequate to possible threats [9], [13], [18]. Generally, the concept of technical system safety is understood as the system's ability to protect its superior functional properties against internal and external threats [32].
Risk assessment is a three step procedure consisting in [10], [17], [19], [21], [30]:

- hazard identification,
- probability assessment,
- consequence analysis.

The previous analyses show that priority issues related to warning system should include [26]:

- assessment of the response time to take action,
- ways of warning different groups of society (schools, hospitals, etc.),
- developing warning messages in accordance with the scale of threat which will allow implementation of protective procedures,
- scenario of population behaviour in face of warning, an indication of alternative sources for media belonging to the critical infrastructure (drinking water, electrical and thermal energy, natural gas),
- public education on the knowledge of warning and alert systems and types of threats and their consequences,
- functioning of fast response emergency service.

The analysis shows that the warning system is a special type of information system [12]. Using the basic conceptual terminology of system theory in relation to the warning system we can distinguish three main subsystems: functional, structural and utility [11], [20].
The functional subsystem consists of the following elements:

- obtaining warning signals: identifying information needs, definition of the observation area with a possible division, location of information sources, measurement of changes in the monitored parameters,

- analysis of warning signals: determination of changes measurement, the characteristics of the permissible ranges of changes, prioritization of indicators of changes, interpretation and verification of warning parameters size.
- warning signals transmission: determining subjects responsible for transmission, supervision of transmission punctuality and accuracy, reducing disruptions and distortions in the transmission.

The structural subsystem includes such elements as: sources of information (internal, external databases, historical, current, prospective) and operational teams (data collection and analysis, emergency response, emergency management centres) [1], [5].

The utility subsystem consists of the following elements:
- obtaining information: recording data from continuous monitoring, interviews and questionnaires,
- data analysis: methodology, data-processing technique, selection of indicators,
- transmission of information: information technology, data protection methods, methods of computer support in decision-making, the rules of verbal communication.

Early warning system can identify threats and launch procedures for counteracting them. Reduction of negative effects is possible because the warning system is part of response in crisis situations. Warning systems are used in the management of risk because they create possibilities for its assessment - reveal extraordinary threats and contribute to the assessment of negative consequences [6], [8], [31].
Besides, warning system determines the effectiveness of any rescue operations. Precise identification of hazard and the smooth transfer of information allow effective response by means of warnings and alarms [4], [29].
In the risk analysis historical knowledge of the system operation, analytical methods and experience of the operators should be used. In many cases, part of the risk analysis is the analysis of the human factor and reliability analysis of a man - a system dispatcher [3].
The aim of the work is to propose a procedure for the identification of undesirable events, including, among others, failure time, type of failure, location of failure, extent of failure, cause of failure, consequences of failure and actions and equipment used to remove the failure.

2. Hazard identification

Hazard identification is usually made using experts methods. The most important methods of detailed hazard analyses are [24], [32]:
- HAZID (Hazard Identification) – it is the first step in hazard analysis and possible consequences, it is often a prelude to risk analysis in technical systems,
- HAZOP (Hazard and Operability Analysis) – the analysis is carried out by teams of experts under the guidance of a leader. The HAZOP method is performed using a keyword list. It is used primarily in the safety analysis of large industrial systems,
- FMEA (Failure Modes and Effect Analysis) – it is used to analyse security of systems and technical installations. It is based on the reliability analysis of individual system components,
- SWIFT (brainstorming) (Structured What-If Checklist Technique) – it is carried out by a team of experts. Basic questions asked during the session are: "What if ?", "How is it possible ?" and "Is it possible ?". In response the types of hazards and potential accident scenarios of events are obtained,
- Influence Diagrams – they are used to determine statistical relationships between causes and effects, which help to understand the phenomena and uncertainties contained therein.

One of the most common ways to conduct a hazard analysis is the study of threats using the following data [28], [32]:
- previous analyses of safety,
- conclusions from occurred undesirable events and their causes,
- experience from the existing technical systems.

There are the following phases of management in terms of failure [27]:
- phase of prevention and risk reduction - safety management system is based on the functioning of risk management; risk analysis and assessment help determine the likelihood of a major failure and assess the losses associated with it, moreover, you can develop a scenario of progress of emergency situation in time and design barriers ensuring safety and protection, which significantly reduce the severity of the consequences of a major failure,
- stage of readiness - a logistics plan for rescue operations in case of a major failure, the final result is to develop an emergency plan. There are

two aspects in response to the occurrence of a major failure:
- organization, responding to the question "who does what?" - medical service, government and local administration, fire brigade, police,
- hardware, allowing counteract the effects of failure - measures to counter a major failure,

- counteracting phase – it means to run operational and rescue plan; main elements of this phase are: start of emergency procedures, strategy and tactics of rescue operations, management, communication and logistical support system.
- phase of corrective action – it takes place after the end of the state of emergency and relies on feedback leading to improve the organization of system security management, it requires treatment-related actions.

Hazard identification should consider the basic factors affecting safety, which can be divided into [25]:
- external factors, resulting from the events that are not the effect of system operation, e.g. the forces of nature, deliberate action of third parties such as vandalism or terrorist attack,
- internal factors, which include, above all: hydraulic conditions of flow, material defects, ageing processes,
- human factors, that is mistakes made during the design, construction and operation, e.g. the lack of proper monitoring, lack or incorrectly conduced repairs and modernization, lack of risk management.

3. Strategies for safety management in terms of identification of operating states

Safety analysis requires the identification of operating states. From the point of view of the system operator one can distinguish the following states:
- all procedures are followed, the operator takes the correct decisions in accordance with the recommendations and indications of subsystems protecting against undesirable events, there is no failure,
- all procedures are followed, in decision making the operator takes into account the indications of protective subsystems, however, failure occurs,
- violation of procedures, in decision-making the operator does not take into account the indications of protective subsystems, failure does not occur,
- violation of procedures, in decision-making the operator does not take into account the indications of protective subsystems and failure occurs.

Complex ergonomics systems work in varying operational conditions, which implies changeability of safety indicators. Theoretical safety is associated with:
- applicable laws, technical requirements,
- protective systems,
- operating procedures.

Actual system safety is associated with:
- technical condition,
- meteorological conditions,
- efficiency of operation,
- system of stuff training.

The process of ensuring the security requirements of system include:
- procedures and technical measures,
- organization and methods of operation,
- documentation and executive instructions,
- stuff qualification and training programs.

Reactive security management is based on the identification of potential threats on the basis of the hazards existing in Water Supply System. This strategy is not very effective in identifying trends and forecasting future sources of threats.
Proactive security management strategies are oriented towards creating database of undesirable events from different sources. The basic assumption is that the risk can be reduced before it occurs. The basis is a rule to take actions in the range of:
- hazard identification,
- analysis and risk assessment,
- taking adequate preventive and corrective actions in risk management.

System security management means managing by assumed objectives in terms of the system. It is implemented according to the principle " Defence In Depth", consisting of:
- minimizing the risk of failure (prevention),
- minimizing the number of failures (active action),
- minimizing the consequences of failure (passive action).

The source of the necessary data for risk analysis are:
- data gathered from the system operation with water companies,
- measurement data,
- data collected from the experts.

The source of uncertainty in the analysis of the aforementioned data is usually incomplete or uncertain knowledge of:

- quantitative and qualitative database on failures,
- assessment of the technical condition of the system,
- inaccurate and incomplete information concerning the location and identification of failure,
- assess the cause-and-effect relationship between failures,
- assessments and expert opinions.

System security management in the operational sense means risk management [22]. Ex ante approach is based on the proactive concept of avoiding or significantly reducing the consequences of undesirable events. This is a new strategy in relation to the traditional ex post approach characterized by a reactive concept of inference based on information after failure.

There are three phases of risk management:

- risk analysis - threats identification, assessment of their frequency and based on it risk determination,
- risk evaluation - gradation of risk levels and on this basis risk values obtained earlier are assigned to one of three ranges of risk (tolerable, controlled and unacceptable),
- risk control – undertaking actions, within the framework of available economic and social conditions, in order to keep the risk at a tolerable level.

In the assessment of the system safety the following rules are applied:

- if there is the possibility of a major failure in the system one should strive to the level of safety being in force in developed countries,
- security measures for improving safety should be used in areas where they will bring the most effective results,
- no safety measure is perfect, therefore it is required to use several barriers which should provide a compact multi barrier system,
- risk should be considered as an economic category (RCBA – Risk Cost Benefits Analysis).

Safety rules formulated by D. Peterson are as follows:

- safety should be implemented systemically,
- undesirable behavior, conditions and failure are symptoms of irregularities in the security system, causes and circumstances of failures are predictable,
- safety can be managed as any other business,
- safety management procedures help identify and determine the causes of failures,
- dangerous human behavior is a normal reaction to the wrong work environment,
- an effective system of safety is created by technical equipment, employee and management procedures,
- safety system must be adapted to the culture of safety,
- the effectiveness of the security system depends on the weight attributed to safety issues.

4. Registration of undesirable events

For a complete analysis of undesirable events an extensive database of various operating data is required. Information about the failure should be recorded on a specially prepared for this purpose failure cards. The scheme of protocol of failure removal was shown in *Figure 1*. Use of the failure cards will allow to obtain the necessary and accurate data on the performance of the system [14].

The condition for the proper implementation of the process is to oblige the people managing the technical system to currently complete failure cards and periodically provide acquired data to experts in order to verify and assess the obtained information. It should be remembered that the results of work will be visible only in the future. The proposed method of recording failures will allow to gain knowledge necessary for further reliability and safety analyses.

In order to use the obtained data to determine the appropriate reliability parameters at first they must be prepared [2]. The purpose of this preparation is to obtain statistical samples in accordance with adapted structures of dividing examined subsystems into elements and set for them reliability states [14].

Report date: ……

Naftoport Oil Terminal

.....
(Address)

PROTOCOL OF FAILURE REMOVAL OF THE NAFTOPORT OIL TERMINAL - Report No. .....

Date of failure notification:_____ time _____
Details of the failure notifier:_____
(name, address, phone number)
Notification accepted by: _____
(name of an employee of the water supply company)

Place of failure [1]): _____ The failure was reported: _____
Name of failure object: _____
Condition of object before failure: _____
Repairs carried out before the failure [2]):
_____
Description of failure [3]): _____
Cause of failure [4]): _____
Persons removing failure: _____ time from _____ to _____
Losses associated with failure: _____
The duration of the preparatory work (date): _____ time _____
Date of repair start: _____ time _____
Date of completion repair:_____ time _____
Completion of after-failure work (date): _____ time _____
Method of failure removal: _____
Used material and equipment:_____
Difficulties, threats and damages [5]): _____
_____
Measures to prevent the repeating of similar failure in future:
_____
_____

Date: Foreman signature: Supervisor signature:

_____ _____ _____

[1]) construction, route, warehouse, workshop, machine room, others.
[2]) types and date of the last overhaul, the information on the conducted technical acceptance made after the renovation, others
[3]) conduct of staff, operation of protection, protective and signalling devices, others
[4]) determining who caused failure, determining which staff is to blame e.g. supervision, repair team, suppliers, natural disasters, no information available
[5]) including the cost of man-hour, losses in fixed assets and working capital, the value of uncompleted production, others

Figure 1. The exemplary protocol of the Naftoport Oil Terminal failure

5. Conclusions

- Ensuring the continuity of the technical system requires the use of knowledge about the reliability and security that are very well characterized by the concept of risk. It includes an assessment of the relationship between threats and used protective barriers.
- Issues related to risk are analysed in many scientific disciplines, including widely understood environmental engineering. Although they are not the mainstream of design and

operational analysis, they are presented as a component describing the basic issues of technical systems safety.

- Obtaining reliable operating data relating to failure, repair, overhaul is essential to conduct proper risk management policy.
- Emergency events (catastrophic) do not appear without a reason but there are a chain of undesirable (critical) events. The use of developed failure card will allow to know the causes and the consequences of each undesirable event, as well as the further evaluation of the technical system safety.
- Identification of the system state can be fraught with errors. There is a possibility that the actual state of the system is identified as other state. In case of binary systems the first and second kind errors are possible . The first type error is to qualify system in up state as system in down state. The second type error is to qualify system in down state as system in up state.
- System safety depends on a number of factors, including technical, social, economic, political and environmental. Among the technical factors the reliability of system is crucial. Safety is understood as the ability of the system to protect the internal values from external threats.
- System safety management in the initial phase means to create a database of undesirable events with particular emphasis on their frequency and negative consequences associated with them. In the fundamental phase of safety management decisions are made about the choice of protection measures against risks, introducing them to the practice of exploitation and control of the effectiveness of the used solutions.

References

[1] Apostolakis, G. & Kaplan, S. (1981). Pitfalls in risk calculations. *Reliability Engineering and System Safety* 2, 135–145.

[2] Aven, T. (1992). *Reliability and Risk Analysis*. Copyright by Elsevier.

[3] Billinton, R. & Allan R. N. (1992). *Reliability Evaluation in Engineering Systems. Concepts and Techniques*. Copyright by Plenum Press. London.

[4] Birolini, A. (1990). *Qualität und Zuverlässigkeit technischer Systems. Theorie, Praxis, Management.* Copyright by Springer, Berlin.

[5] Blischke, W. & Murthy D. N. P .(2000). *Reliability: Modeling, Prediction and Optimization.* Copyright by J. Wiley and Sons, New York.

[6] Chen, C. W., Liu, KFR., Tseng, CP. et al. (2012). Hazard management and risk design by optimal statistical analysis. *Natural Hazards* 64, 2, 1707-1716.

[7] Dhillon, S. (1986). *Human Reliability with Human Factors*, Copyright by Pergamon Press. New York.

[8] Faber M. H. & Steward M. G. (2003). Risk Assessment for Civil Engineering Facilities: Critical Overview and Discussion. *Reliability Engineering and System Safety* 80, 173-184.

[9] Guikema, S. D. & Pate-Cornell M. E. (2002). Component choice for managing risk in engineered systems with generalized risk/cost functions. *Reliability Engineering and System Safety* 78, 227-238.

[10] Haimes, Y. Y. (1998). *Risk Modelling, Assessment and Management.* Wiley, New York.

[11] Haimes, Y. Y. (2009). On the Complex definition of risk: a systems-based approach, *Risk Analysis* 29, 12, 1647-1654.

[12] Hubbard, D. W. (2009). *The failure of risk management*, Wiley. New York.

[13] Kuo, W. & Zuo, M. J. (2003). *Optimal reliability modeling*. Copyright by Wiley, New Jersey.

[14] Kwietniewski, M., Roman, M. & Kłoss-Trębaczkiewicz, H. (1993). *Niezawodność wodociągów i kanalizacji*. Wydawnictwo Arkady, Warszawa.

[15] McGill, W. L., Ayyub, B. A. & Kaminskiy, M. (2005). *Risk Analysis for Critical Asset Protection*. Risk Analysis, Wiley Blackwell 27, 5, 1265-1281.

[16] Pham, H. (2003). *Handbook of Reliability Engineering*. Copyright by Springer, London.

[17] Rak, J. (2003). Metoda szacowania ryzyka zagrożenia systemu zaopatrzenia w wodę. PZITS O/Dolnośląski, *Ochrona Środowiska* 2, 33-36.

[18] Rak, J. (2003). Ryzyko w funkcjonowaniu operatora SZW - analiza ergonomiczna. Wydawnictwo Sigma Not, *Gaz, Woda i Technika Sanitarna*, t.LXXVII 6, 211-214.

[19] Rak, J. (2004). Metody matrycowe oceny ryzyka w systemach zaopatrzenia w wodę. Ośrodek Informacji "Technika Instalacyjna w Budownictwie", *INSTAL* 3, 42-45.

[20] Rak, J. (2005). *Istota ryzyka w funkcjonowaniu systemu zaopatrzenia w wodę.* Oficyna Wydawnicza Politechniki Rzeszowskiej.

[21] Rak, J. (2005). *Podstawy bezpieczeństwa systemów zaopatrzenia w wodę*. Wydawnictwo – Drukarnia LIBER DUO KOLOR Lublin, Monografie Komitetu Inżynierii Środowiska PAN, Lublin, vol. 28, 1-215.

[22] Rak, J. (2009). *Bezpieczeństwo systemów zaopatrzenia w wodę*. PAN, Instytut Badań Systemowych. Warszawa.

[23] Rak, J. & Kwietniewski, M. (2011). *Bezpieczeństwo i zagrożenia systemów zbiorowego zaopatrzenia w wodę.* Oficyna Wydawnicza Politechniki Rzeszowskiej.
[24] Rak J., Tchórzewska-Cieślak B. (2003). *Ryzyko w eksploatacji systemów zbiorowego zaopatrzenia w wodę.* Wydawnictwo Seidel-Przywecki Sp. z o.o.
[25] Rak, J. & Tchórzewska-Cieslak, B. (2006). Metoda zintegrowanej oceny ryzyka awarii w podsystemie dystrybucji wody. Wydawnictwo Sigma NOT. *Gaz, Woda i Technika Sanitarna* 1, 11-15.
[26] Rak, J. & Tchórzewska-Cieślak, B. (2005). *Metody analizy i oceny ryzyka w systemie zaopatrzenia w wodę*. Oficyna Wydawnicza Politechniki Rzeszowskiej.
[27] Rak, J. R. & Tchórzewska-Cieślak, B. (2007). *Czynniki ryzyka w eksploatacji systemów zaopatrzenia w wodę.* Oficyna Wydawnicza Politechniki Rzeszowskiej.
[28] Schneeweiss, W. G. (2001). *Reliability Modeling*. Copyright by Lilole – Verlag, Hagen.
[29] Smith, D. J. (2001). *Reliability, Maintainability and Risk*. Copyright by Butterworth – Heinemann.
[30] Tchórzewska-Cieślak, B. (2009). Water supply system reliability management. *Environmental Protection Engineering* 35, 29-35.
[31] Tchórzewska-Cieślak, B. (2010). Failure risk analysis in the water distribution system. *Summer Safety & Reliability Seminars. Journal of Polish Safety and Reliability Association* 1, 247–255.
[32] Tchórzewska-Cieślak, B. (2011). *Metody analizy i oceny ryzyka awarii podsystemu dystrybucji wody*. Oficyna Wydawnicza Politechniki Rzeszowskiej. Rzeszów.