DOI: 10.2507/34th.daaam.proceedings.xxx

METHODOLOGICAL PROCEDURE TO ENSURE THE SAFETY OF TECHNICAL INSTALLATIONS

Dana Prochazkova, Miroslav Rusko, Georg Rockel & Jan Ilko

This Publication has to be referred as: Prochazkova, D[ana]; Rusko, M[iroslav]; Rockel, G[eorg] & Ilko, J[an] (2023). Methodological Procedure to Ensure the Safety of Technical Installations, Proceedings of the 34th DAAAM International Symposium, pp.xxxx-xxxx, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-xx-x, ISSN 1726-9679, Vienna, Austria
DOI: 10.2507/34th.daaam.proceedings.xxx

Abstract

The paper deals with meaning the term “safety” and concentrates to its sense for technical installations. It shows relations of terms reliability, resiliency, criticality, risk and safety. It characterizes process safety management and safety management system at technical installations. It describes methodology for ensuring the safety of technical installations. The highest quality of each object (i.e. the State, human community, technical installation etc.) is safety, so the highest priority for the object is the overall (integral) safety. This means that it is not only about partial safety such as internal, external, environmental, fire, economic, etc., but about the safety of the whole, which includes partial safety so that the condition of the whole, is optimal. Due to the systemic nature of today's world, integral safety cannot be built without regard to others. Very important is the safety of basic processes, which ensure products and services for human society.

Keywords: Safety; risk management; process safety management; safety management system; methodology.

1. Introduction

The safe community is now at time of globalisation very dependent on a safety level of complex facilities ensuring the territory by basic service necessary for human live, e.g. the electric energy on which there are dependent supplies of good quality drinking water, utility water, information distribution etc. [54]. Based on current knowledge and experience, it is a fact that the quality of life, health and safety of each person depends on the quality of the human community to which they belong. From the reasons of fulfilment of targets of humans (human security and development) that may be only realised if human communities are in safe territory [28], [29]. Ensuring the safe human system is not easy [30], because the human system is a system of systems [31], i.e. system of several mutually interconnected systems of a different nature. Consequences of interconnections (interfaces) are mutual dependences, the character of which is physical, cyber, territorial and organisational [32]. As a consequence of growing globalisation the new sources of disasters take on force, they also cause complex facility failures [33], [34].

Since, according to the EU [1] and the UN [2], the highest quality of each object (i.e. the State, human community, technical installation etc.) is safety, so the highest priority for the object is the overall (integral) safety. This means that it

is not only about partial safety such as internal, external, environmental, fire, economic, etc., but about the safety of the whole, which includes partial safety so that the condition of the whole, is optimal. Due to the systemic nature of today's world, integral safety cannot be built without regard to others. Very important is the safety of basic processes, which ensure products and services for human society.

Climate change, biodiversity loss and pollution - the triple planetary crisis [35] - increasingly threaten the Earth system, necessitating tools such as life-cycle assessment (LCA) that can evaluate the effectiveness of different prevention and mitigation strategies. LCA systematically quantifies the environmental impacts over the whole life cycle of products, processes or policy scenarios [36]. Due to advancements in product design and technology, products in the market today are capable of an extended life cycle by undergoing end-of-life treatments [53]. To enable this, products have to be designed for multiple life cycle (MLC) purposes. Besides that, the presence of technology innovation has led to the generation of multiple products. Therefore, it is crucial to evaluate the life cycle of products in a wider scope. [37]. Design innovation is a key driver to success in the current competitive market by substantially improving product design and features to delight customers' expectations [38]. In view of design innovation, MLC products aim to enhance the value of their life cycle by not only providing satisfactory design functionality, but also proper EOL treatments and a prolongation of their life cycle. This is accomplished by combining relevant strategies of Design for X (DFX), which is a design concept that was recently mentioned as a Design for Multiple Life Cycles (DFMLC). The DFMLC is a sustainable design approach that affords decisive environmental impacts, reduces the amount of waste in landfills, diminishes pollution and the use of natural resources, and protects the quality of natural and built environments [39], [40], [41]. LCA is frequently applied to uncover environmental hotspots and prioritize actions and is increasingly used to assess the environmental impacts of strategy implementation scenarios [42]. Social Life Cycle Assessment (SLCA) is the third assessment dimension and seeks to measure the impact of a product or process on society along the full life cycle. SLCA is similar to LCA in that it follows the LCA four-step procedure [43], providing complementary impact information (social) to the environmental information of LCA and both assessments use a functional unit to define the product system [44]. The differences between them are mainly with respect to interpretations of social impact on people [45]. LCA considers impacts to people indirectly through impacts to the environment, while SLCA more broadly considers many types of impacts directly to people, and the impacts can be positive and negative [44], [46]. Lastly, local and site-specific impacts matter more. The same indicator may show different social impacts to stakeholders based on location [47].

The basic function of the State since its inception has been to ensure the safety of protected assets (interests) of the state and the sustainable development of the State. Protected assets (interests) of the State are the assets of the State that are protected as a priority, i.e. lives, health and security of people, property, environment, public welfare, knowledge, critical technologies and infrastructures. To ensure the safety and development of assets and the State, the State needs to have good management of resources, assets and people under normal, emergency and critical conditions [3].

State safety in its essence is a set of human measures and activities that ensure the security and sustainable development of the State and its assets; i.e. they limit the conditions for realization of danger. To do this, the administration of the State should not only be concerned with survival, power, social compliance and damage prevention, but should solve methodological-conceptual problems and ensure that:

- safety would be considered in a systemic context, i.e. not only in conjunction with a priori defined risks,
- concepts of safety could not be burdened by ideological and political clichés,
- problem solving was based on the results of decision theory,
- the relationship between risk and safety would be correctly understood. The essence of the problem lies in the answer to the question: How are risks and their impacts identified? It is used the answer: They are determined by plausible scenarios. But is there no procedure for how such a scenario should be formed? Usually, the scenario is based on past events and phenomena, and does not consider human violations and the existence of possible surprises caused by the dynamic development of the world and human society,
- the dynamic evolution of the world, which causes changes in the nature of existing risks and brings new risks, would be considered.

The State plays a role that can be described in terms of risk management [3], [4] because it redistributes certain types of risk through decisions about the welfare system/public welfare and health care. The need to consider risks and manage them correctly at all levels of government will prevent failures in the provision of public services.
Risks enter the public domain when they meet any of the following attributes:

- These are externalities that market mechanisms cannot address.
- In connection with legislation, the harmful effects of technology and bad decisions of public administration are imposed on citizens.
- A significant part of the public that disagrees with the concept of managing certain assets is at risk.
- Political decisions, without regard for the safety and development of citizens, give rise to phenomena in which risks are realised.

- Disasters (unacceptable phenomena), which cause unacceptable risks, are distributed in such a way that they disregard political fairness.

Public administrations should therefore analyse the risks both in terms of impacts on society and in terms of impacts on the public administration management system, as a number of examples in the past have shown that public administration decision-making has exacerbated the effects of the emergency situation [5-18]. The steps of the risk management process carried out by public administrations differ from the normal risk management procedure [3] only in that considerable attention should be paid to the formulation of context and risk monitoring from a strategic and procedural point of view, i.e.:

- The capacity of public administrations and other stakeholders to achieve strategic objectives in the areas of safety, security, mobility and environmental conditions (health and environmental risks) should be assessed in a strategic context.
- The problem-solving capacity of public administrations needs to be assessed in an organisational context.
- In the context of risk management, risk thresholds, maximum impact levels and the right priorities for decision-making need to be assessed.

Given the dynamic development of the world, it is necessary for public administration, administrators of all legal organizations of the State (i.e. public institutions and private entities) and individuals to adapt the set of human measures and activities ensuring the security and sustainable development of the State and its assets to the current conditions. This means that permanent risk management is carried out at all levels in favour of integral safety.

The present article examines the problems of safety of the public assets of the State, which belong among technical installations. Their safety depends not only on themselves, but also on the quality of their relationship with public administration. Public administration needs them because they provide products and services to citizens and the State, which thus fulfils many of its basic functions. On the contrary, technical installations need public administration, because it sets and controls the conditions of their activity.

2. Safety and Criticality of Technical Installations

Technology is the application of knowledge to achieve practical goals in a specified and reproducible way. It is a systemic use of knowledge for practical purposes. While technology contributes to economic development and human prosperity, it can also have unacceptable impacts, such as pollution or resource depletion, or cause social damage, such as technological unemployment caused by automation.

Engineering is the process by which technology is developed and operated. This often requires solving problems under strict constraints because the safety of people and other public assets is at stake. Therefore, the management of the safety of technical installations is essential.

The safety management of technical works, which are complex systems of the "systems of - SoS" types, can be defined as the integrated planning, design, optimization, operation and management of products, processes and services for the benefit of people [3], [4-20]. In terms of competitiveness and economy, their performance must also be ensured. This depends on their resilience, which determines how the technical installation responds to harmful phenomena of all kinds. The theory of system management according to [20] implies that the resiliency of the system is related to robustness, redundancy, ingenuity and speed of starting the correct response, Figure 1.

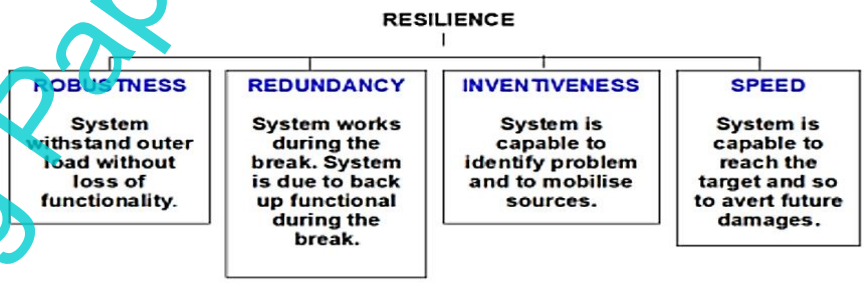

Fig. 1. Context of resiliency of the system with robustness, redundancy, ingenuity and speed [24]

For increasing the safety and reliability of technical installations, it is necessary in terms of references of critical elements and whole to use the disaster sizes with a return period of more than 100 years (current standards consider design disaster for 100 years [20], [24]).

Mistake is that during the design, it is only carried out the protection of elements and objects only for individual listed disasters, i.e. other some possible and unnamed disasters are not considered - it is necessary to use the application called "All Hazards".

As technical facility provides vital functions for humanity, care needs to be taken to ensure the continuity of operations, for which resilience is important. The idea of resilience is portrayed as the intersection of three circles, Figure 2. Resilience means continuously increasing both, the safety and the security while addressing potential conflicts that arise in practice.

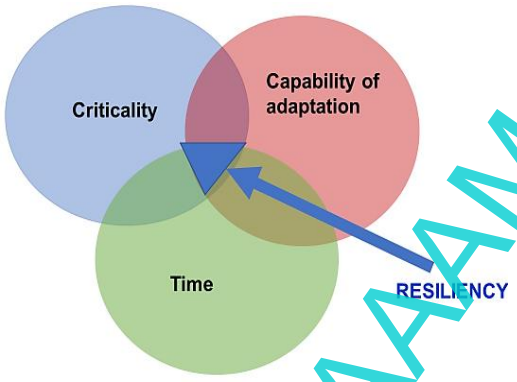

Fig. 2. Critical parameters that are important for resiliency [24]

Resiliency is the potential of a system, which lies in the specific arrangement of the system that maintains the functions and feedbacks of the system in condition, which include the ability of the system to reorganize itself based on changes induced by failures. It follows that sustainability management must be based on resilience management, which has two objectives:

- To prevent so the system could get into unaccepted conditions due to external failures and external stress.
- To preserve the elements activating systemic reorganization and recovery due to massive changes.

Another important characteristic of technical installations is criticality [20], which is a function of resilience and necessity (importance) for the safety of the system. Criticality can be viewed from two points of view, namely from the technical point of view (failure rate of the elements of the system u, i.e. the technical installation) and social (impacts of the non-functioning of the provision of technical installation services to the population). Both aspects are important from the point of view of national safety. From the point of view of the safety of the operation of the technical installation, the first aspect is important; its value is determined by the design.

3. Types of Safety at Technical Installations

With regard to present knowledge and experience, it is currently monitored process safety and the overall (integral) safety of technical installations.

Process Safety is a set of measures and activities that ensure safe operation, i.e. safe operation of processes, e.g. in the case of chemical processes focus on the prevention of fires, explosions and leakage of hazardous substances into the environment [21]. The specific discipline of Process Safety Management (PSM) has been developing over the last 40 years and its aim is to ensure safe processes that take place in technologies, it is the management of principles and systems for the identification of possible threats, understanding and mastering the processes leading to the implementation of threats. It is a complex procedure and requires a multidimensional approach that combines technology and its management [20]. Process safety management is associated with a safety culture and a checklist is often used for safety assessment [22].

Process control is widely used in factories and other automated environments to ensure production efficiency. In general, process control technology is designed to monitor sensors and set important variables according to measured values. This technology allows a relatively small group of people to manage complex operations and helps ensure that the desired outcome is consistently achieved.

System Safety is a set of measures and activities that ensures safe technical installation and its safe surroundings. The discipline in question originated by the application of a systemic approach in engineering fields. Integral (object) safety has its roots in industry safety engineering, which dates back to the 19th century, and which after World War 2 it applied disciplines: systems engineering and systems analysis to solve new and complex engineering problems.

The safety of the system in the monitored concept lies in the application of technical and managerial skills in the identification, analysis, evaluation and management of harmful phenomena and related risks using a systemic approach [4-24].For practical reasons, the approaches used in the area of interest must be effective and affordable. Safety orientation must be part of the company's management system, while respecting the constraints that flow from the outside world. The discipline in question defines:

- technical installation as a system, which is a combination of people, procedures and equipment that are integrated to perform a specific operational task or function in a specific environment,
- the concept of system safety as an application of special technical and organizational skills with the aim of systematically preventing damage and losses to the assets of the system associated with them by identifying threats and managing risks during the entire life of each device or object created and implemented by man.

Over time, the OECD has developed separate concepts for the nuclear and chemical industries [19]. This concept is in work [23] added by cyber security due to increasing role of automatization at present.

System safety in technical installations uses systems system theory and system engineering to prevent predictable accidents and minimize the consequences of unpredictable accidents. In the modern concept, it is generally interested in all losses and damages, and not only in fatal accidents or injuries and damage to property, but also in failure to fulfil a mission (mission, purpose), or environmental damage. The key point of the discipline is to consider losses serious enough that enough time, effort and resources are devoted to their prevention. The size of the investment devoted to accident prevention and/or its impact is substantially dependent on social, political and economic factors. Therefore, for technologies that are likely to have serious consequences, the precautionary requirement is imposed by legislation to ensure the protection of public assets [24].

The primary concern of the safety of technical installations is qualified risk management, i.e.: identification of possible hazards; identification and evaluation of risks; and elimination and/or management through design analysis and/or organizational procedures. The programme for the safety of technical installations must provide for a well-defined procedure for methodological control of safety-related aspects and evaluate the design of the equipment in the sense of identifying possible sources of risk and prescribing time- and costly remedial interventions. The objectives of the system safety programme for technical installations is to ensure:

- the safety of technical installation corresponds to its mission, which is built inherently,
- identifying, assessing, eliminating and/or managing risks to an acceptable level of risk for all risks associated with the system, subsystem and individual parts,
- risk management from threats that cannot be eliminated; i.e. risks must be secured in such a way as to protect personnel, facilities and property,
- the use of new materials and/or products and testing techniques involves only minimal risk,
- the need for corrective measures required to improve safety by temporarily incorporating safety factors is minimised during the inception of the system,
- historical safety data generated by similar safety programs shall be considered and used wherever appropriate.

Industries have either adapted systems safety programs from the military or NASA, or have independently developed their own programs based on the experience gained from the construction of nuclear power plants, from the production of complex, dangerous and expensive equipment. Waiting for accidents to occur and then eliminating the causes has become an uneconomical and sometimes even unacceptable way of modifying and improving systems.

Building many of today's complex systems requires the integration of parts (subsystems and components) made by various independent suppliers and organizations. Even if each supplier maintains the required quality of its parts, combining subsystems introduces new errors and new hazards that are not visible when viewed as separate parts.

Considering the risks associated with a combination of systems and subsystems is referred to in practice as creating inherent security. It has been confirmed in many industrial sectors that incorporating inherent safety into equipment or products can reduce their overall life-cycle costs and that achieving an acceptable level of safety requires advanced recent systems security approaches [24].

System safety-related activities begin at the earliest stages of system concept development and continue through all design, production, testing, operation and shutdown activities. An essential aspect that distinguishes the system safety approach from other approaches used in the field of safety is the primary emphasis on early identification and

classification of hazards so that remedial action can be taken to eliminate or minimize them before the final project decision.

Models trained on large data sets of seismic events can estimate the number of aftershocks better than conventional models do. AI predicts how many earthquake aftershocks will strike — and their strength [48]. Seismologists are finally making traction on one of their most important but challenging goals: using machine learning to improve earthquake forecasts [49]. New machine learning models hold potential for predicting the number of quake aftershocks [50], [51], [52].

Despite the fact that system safety is a relatively new and still evolving discipline, it has its basic ideas, which are preserved in all its manifestations and distinguish it from other approaches to safety and risk management. Principles of system safety management in the recent concept are:

- safety is step by step creating from start of system design and it is not added to the created system,
- safety deals with the system as a whole and not just with subsystems and components,
- safety takes dangers and associated hazards more than just personnel errors,
- safety creating emphasizes analysis rather than experience gained later and standards developed later,
- qualitative approaches are favoured over quantitative ones;
- differentiation of importance of changes and conflicts of goals in a system design is more than system engineering.

The most important aspect of system safety in accident prevention terms is safety management procedures. Effective safety management consists of setting policies and defining safety objectives, i.e. in:

- task and procedure scheduling,
- defining responsibilities and determining competencies,
- documentation and continuous monitoring of threats and resulting hazards, including controls,
- maintenance of the information system for safety management, including feedback and forms of fault/accident reporting, etc.

The safety of the system is responsible for ensuring the security of the system as a whole, including the analysis of the interface between the components. Component safety activities, such as rocket launch pad safety, may be part of general responsibility for system safety, or may be part of component engineering in large and complex projects. For defined types of hazards, such as fires, nuclear safety or explosive atmospheres, a further classification of safety responsibilities may be required.

In any gradation of the breakdown of system safety efforts, system safety engineers are responsible for integrating individual security activities and information. The safety of a system is usually linked to corresponding engineering and/or scientific disciplines such as reliability engineering, quality assurance, human factor, etc. What processes and tasks of system safety will be performed in a particular project depends on its size and the risk level of the designed system [24].

System safety and reliability are closely related [20], [25]. In practice, a safe device or a safe system is reliable, but a reliable device or reliable system may not be safe. Reliability engineering preferentially deals with errors and reducing their frequency. Reliability is defined as a characteristic of a given object expressed in terms of the probability that the object will perform in a specified way the functions that are required of it during a specified time interval and under specified or predicted conditions. Representative reliability engineering techniques aimed at minimizing component (component) errors, and thus complex system failures caused by component errors, are: parallel redundancy; back- up device; safety margin; reducing congestion; and usage time limitation.
These techniques have been shown to be effective in increasing reliability, but they do not necessarily increase safety, and may even reduce it under certain circumstances (e.g., incorporating multiple backups into systems can create an environment for unwanted couplings and affinities between components that cause failure under certain conditions). Therefore, risk analyses connected with system safety look at interactions and do not just focus on engineering errors or uncertainties.

Reliability engineers often consider reliability and safety synonymous. This is true only in some special cases. In general, safety has a slightly broader meaning. Normally, reliability and safety have many characteristics in common. However, many crashes occur without a component failing. On the contrary, many times all components in accidents worked as expected and flawlessly [24]. It can also happen that components can fail (fail) without a crash. It is a fact that breakdowns and accidents may be caused by the operation of equipment outside the permitted ranges of parameter values or time limits on which the reliability analyses were based. This means that the system can have high reliability and yet crash. Moreover, generalized probabilities and reliability analyses cannot be directly applied to specific or local conditions. Most importantly, accidents and accidents are often not the result of simple combinations of errors/component failures [24].

Safety is a feature that stands out at the system level when components are operated together. Events leading to an accident can be a complex combination of equipment error, improper maintenance, information and control system problems, human intervention, and design errors. Reliability analyses only look at the probabilities of accidents and error-related accidents; they do not investigate potential damage that may be caused by the correct operation (operation) of individual components. Therefore, it is not possible for reliability engineering to replace system safety engineering, but it can complement it. However, this must be done with the clear knowledge that the ultimate goal is to increase the system's resilience to the risk of accidental errors. It's always better when the device/system is designed in such a way that individually random errors cannot cause an accident.

Great caution should be exercised when applying reliability estimation techniques for safety assessment. Where accidents are not inevitably caused by phenomena which can be expressed in terms of probabilities of occurrence, the degree of probability of the occurrence of a risk cannot be generally applied to them. Probability of occurrence estimates measure the probability of accidental errors occurring, not the probability of the occurrence of the realization of risks, accidents and/or accidents. Practice shows that when a project error is found during the system safety analyses, it is much more effective to fix it than to convince someone using calculated probabilities that the error will never cause a crash. High probability values of reliable behaviour do not guarantee safety, and it is known from practice that safety often does not require ultra-high reliability [24].

Most often, the main drawback of probabilistic models is not what they include, but what they don't. Low values of the probability of unreliable behaviour simply indicate that the system will not fail in the intended way, but says nothing about the fact that the system can fail with a much higher probability in a way that was not considered [24]. Distinguishing accident risk from error is essential to understand the difference between safety and reliability.

For practical reasons, system security approaches and programs must be effective and affordable. The cost recovery of the system safety program is achieved when crashes are avoided.

The effectiveness of a system safety program is very difficult to prove, because measuring something that did not happen is difficult. One indirect way to measure the effectiveness of a system safety program, although not entirely satisfactory due to the lack of factors compared, is to compare the operation of systems that had a system safety program with those that did not and crashed. Another way of determining the effectiveness of the system safety program is to report hazards that were corrected by system safety personnel before the accident occurred or was otherwise detected. The third way of estimating the effectiveness of system security programs is to investigate cases in which the system safety recommendations were not respected and accidents occurred.

4. Procedures for Ensuring the Safety of Technical Installations

Based on the current knowledge summarized in the works [5-20,23,24] the safety management system of the technical installations includes the organizational structure, responsibilities, practices, regulations, procedures and resources for determining and applying disaster prevention or at least mitigating their unacceptable impacts in the territory. As a rule, it covers a number of issues, including but not limited to organisation, personnel, identification and assessment of threats and resulting risks, organisation operations, organisational change management, emergency and crisis planning, security monitoring, audits and reviews [23]. Based on the last cited work, the safety management system (SMS) of technical installation is integrated management of 7 processes:

- The process for the design and implementation of the concept and management, which is further divided into sub-processes to ensure: overall concepts; safety objectives; safety management/direction; safety management system; personnel, which are further divided into the following sections: human resources management, training and education, internal communication/awareness, and the working environment; and reviewing and evaluating the achievement of safety objectives.
- The process for implementation of administrative procedures which is further subdivided into: disaster hazard identification and risk assessment; documentation keeping; procedures (including work permit systems); change management; safety in conjunction with contractors; and product safety oversight.
- The process of technical matters, which is further divided into sub-processes for: research and development; design and assembly; an inherently safer process; industry standards; storage of dangerous substances; and maintenance for integrity and maintenance for equipment and objects.
- The process for external collaboration which is further subdivided into: cooperation with administrations; cooperation with the public and other stakeholders (including academic departments); and cooperation with other businesses.
- The process for emergency preparedness and response, which is further divided into sub-processes for: on-site preparedness planning; facilitating the off-site preparedness planning (under the responsibility of public administration); and coordinating as well as departmental organisations' activities in providing emergency preparedness and response.

- The process for processing the reports and investigation of accidents/ near misses, which is further divided into sub-projects for: processing accident reports, near misses and other learning experiences; investigating undesirable phenomena; and responding to and following up on accidents (including application of lessons learned and information sharing).
- The process for physical and cyber security of a technical installation, which is further divided into support for: physical security; and cyber security against hackers and terrorists.

The safety management system (SMS) of a technical installation is based on the concept of disaster prevention or at least their serious impacts [19], [23, [24], which includes the obligation to implement and maintain a management system in which the following problems are considered:

- the roles and responsibilities of persons involved in the management of major disaster threats at all organisational levels of technical work and training measures aligned with identified training needs,
- plans for the systematic identification of major threats from disasters and the resulting risks associated with normal and abnormal conditions and for assessing their likelihood and severity (magnitude),
- plans and procedures to ensure the safety of all components and functions in and around the technical installation, including the maintenance of objects, equipment,
- plans for the implementation of changes in the technical installation, territory, objects and equipment,
- plans to identify foreseeable emergencies by systematic analysis, including the preparation, testing and assessment of contingency response plans for such emergencies,
- plans for the ongoing evaluation of compliance with the objectives clarified in the safety concept, SMS and mechanisms for investigating and implementing corrective actions in case of failures to achieve the set objectives,
- plans for periodic systematic evaluation of the safety concept, effectiveness and suitability of the SMS and criteria for assessing the level of safety by the top team of technical installation personnel.

Safety is a matter for all involved, i.e. managers, employees and randomly present. In this context, we talk about the ***so-called golden rules of all involved*** [24], which are:

- to prevent disasters or at least their unacceptable impacts by means of preventive measures, to ensure preparedness to deal with unacceptable impacts on protected assets (interests) of the technical installation and the effective response of the technical installation,
- to communicate and cooperate with others involved in all aspects of the prevention, preparedness and response of technical installation,
- to know the hazard from disasters and possible risks in the technical installation and its surroundings,
- to implement and respect a "safety culture" that is respected and promoted by all stakeholders at all times,
- to establish safety management systems, monitor and, if necessary, correct their activities,
- to apply the principles of inherent safety in the design, design and operation of technical installation and its equipment,
- to carefully manage changes in the technical installation,
- to be prepared to cope with any harmful phenomena that may occur,
- to assist other stakeholders in carrying out their roles and responsibilities,
- continuously to improve safety,
- to operate in accordance with safety culture, safe practices and training,
- to strive to keep up to date with all information and information and provide feedback to managers,
- to strive to develop, strengthen and continuously improve safety concepts, regulations and directives,
- to guide and motivate all other stakeholders to fulfil their roles and responsibilities,
- to know the risks within the sphere of their own responsibility, appropriately plan measures for their proper management,
- to apply an appropriate and coherent planning and follow-up policy,
- to be aware of the risks in the technical installation and know what to do if they are realized,
- to participate in emergency planning and response to emergencies.

Safety culture means that a person in all his/her roles (manager, employee, citizen or victim of a disaster) adheres to the principles of safety, i.e. behaves in such a way as not to cause the realization of possible risks and when he becomes a participant in the implementation of risks, to contribute to the effective response, stabilization of protected interests and their restoration and to start their further development. An effective safety culture is an essential element of safety. It reflects the concept of safety and is based on the values, opinions and actions of the organization's top managers and their communication with all stakeholders. It is a clear commitment to actively participate in addressing security issues and promotes that all stakeholders act safely and comply with relevant laws, standards and norms. The rules of safety culture must be incorporated into all activities in the technical installation. They are not based on concentrating on punishing the

culprits/perpetrators of mistakes, but learning from mistakes and introducing corrective measures so that mistakes cannot be repeated or at least significantly reduce their occurrence.

The tool for ensuring a safe technical installation, i.e. a technical installation in which there is an effective safety culture, is the program to increase the safety of the technical installation [24].The procedure for creating a program to increase the safety of technical installation according to [19] consists of the following steps:

- To define the tasks (partial objectives) and strategic objectives of the technical installation with regard to safety.
- For each technical installation sector (connected with processes and subprocesses given above), to select appropriate target and intermediate indicators for assessing safety levels or to develop specific checklists.
- To create a vocabulary for the needs of managing the integral safety of a technical installation.
- To align standards, good practice practices and local practices.
- To modify the list of target indicators or limit values for checklists according to the conditions in the technical installation in question.
- To modify the list of intermediate indicators or limit values for checklists according to the conditions in the technical installation in question.
- To determine how to evaluate target indicators (i.e. value system) or checklists according to the conditions in the technical installation in question.
- To determine the method of evaluation of interim indicators (i.e. value system) or checklists according to the conditions in the technical installation in question.
- To establish a method/scale for measuring a set of indicators (i.e. a set of values) or a set of checklists and limit limits according to the conditions in the technical installation in question.

Figures 3 and 4 show an idea of entity safety management based on the above risk management insights [20]. The first is simpler and the second shows the decision-making method built into the safety management system of a technical installation.

Fig. 3. Milestones determining the safe or dangerous behaviour of a technical installation in the event of a dangerous situation

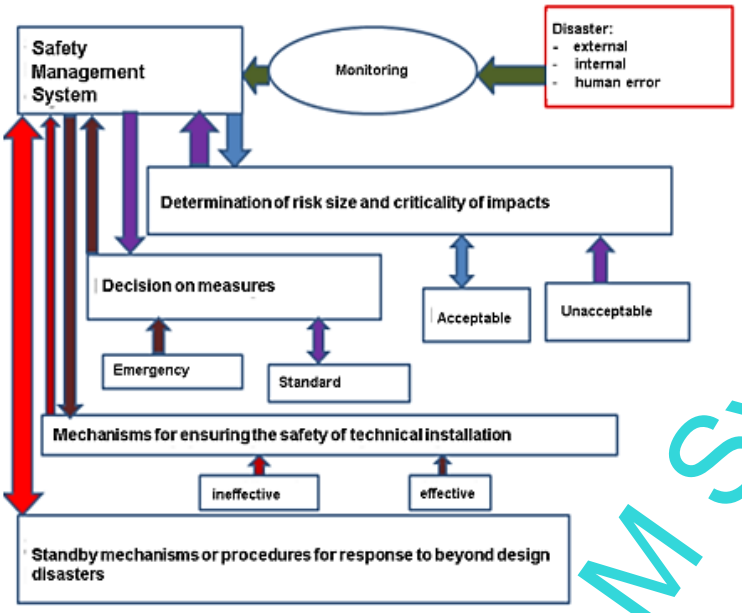

Fig. 4. An idea of the way of managing the safety of a technical installation built into the safety management system

5. Future research plans

Further research is planned to focus mainly on the implementation of the analyzed areas of research in the field of reliability, resistance, criticality, risks and safety in process safety management and especially safety management systems on technical equipment. It will be important to use feedback from practice when applying the described methodology for ensuring the safety of technical equipment and implementing the knowledge gained so far.

6. Conclusion

Safety-oriented engineering also performs safety management tasks, i.e. risk management tasks for the benefit of safety and the development of the human system. In technical slang, we talk about creating inherent safety of a technical installation against design disasters by managing safety. By implementing the precautionary principle, we ensure an increase in resiliency to the unacceptable impacts of over-project disasters that are so unlikely to occur that they are unpredictable. Principles such as "fail safely, perform only specified functions, i.e. if you cannot meet a goal, not do anything" are put into practice in technology[20].

The engineering in question is based on safety management, which is based on specific risk management [20], which is characterized in particular by the following features:

- placement - design - construction - design with minimization of risks, so call: risk-based design, risk-based operation, risk-based maintenance etc.
- operation with the integration of an early warning system and procedures to manage an acceptable level of risk,
- managing the abnormal, emergency and critical conditions during the operation and shutdown.

The specificity of the monitored risk management is that it is the management of risks[4]:

- from all possible disasters at once, with the current list of disasters being determined by the All Hazard Approach [26], [27] (i.e. considering all possible disasters regardless of whether their sources lie inside or outside the system)
- and it is sought optimal solution for relevant possible disasters is sought, while applying the precautionary principle, which includes sustainable development.

Safety-oriented engineering[20]in risks determining the risk uses the principles:

- the risk is determined during the entire life cycle of technical installation, i.e. during the siting, design, construction, operation and decommissioning, and possibly also when the territory is restored to its original state,
- risk determination focuses on user requirements and the level of services provided,
- risks are determined according to the critical impact on processes, services provided and assets determined by the public interest,

- unacceptable risks are mitigated through risk management tools, i.e. technical and organisational measures, standardisation of operational procedures or by automated control.

From the professional point of view, subject engineering is a process that seeks all potential conditions that would endanger the successful functioning of the monitored technical installation at all stages of its lifetime, and identifies possibilities for their management by prevention, preparedness, response and renewal.

Safety-oriented engineering requires the use of advanced safety practices. The implementation of the described methodology for ensuring the safety of technical equipment in practice represents an important element for eliminating risks. It can contribute not only to partial safety such as internal, external, environmental, fire, economic, etc., but also to safety as a whole. Such a comprehensive approach based on current knowledge in the context of the safety management process has the potential to contribute to overall integral safety.

7. References

[1] EU. *Maastricht Treaty*. C 191, 29.7.pp.1–112. Maastricht: EU 1992

[2] UN. *Human Development Report*. New York 1994, www.un.org

[3] Prochazkova, D. (2011). *Strategic Management of Territory and Organization*. ISBN 978-80-01-04844-3. Praha: CTU, 483 p.

[4] Prochazkova, D. (2020). *Analysis, Management and Settlement of Risks Connected with Technical Facilities*. Prague: CTU, 222 p.

[5] Briš, R., Guedes Soares, C. & Martorell, S. [eds.] (2009). *Reliability, Risk and Safety. Theory and Applications*. ISBN 978-0-415-55509-8. London: CRC Press, 2362 p.

[6] Ale, B., Papazoglou, I., Zio, E. [eds.] (2010). *Reliability, Risk and Safety*. ISBN 978-0-415-60427-7. London: Taylor & Francis Group, 2448 p.

[7] Bérenguer, C., Grall, A., Guedes Soares, C. [eds.] (2011). *Advances in Safety, Reliability and Risk Management*. ISBN 978-0-415-68379-1. London: Taylor & Francis Group, 3035 p.

[8] IAPSAM (2012). *Probabilistic Safety Assessment and Management Conference. International. 11th 2012. (Annual European Safety and Reliability Conference*). ISBN: 978-1-62276-436-5. Helsinki: IPSAMESRA, 6889 p.

[9] Steenbergen, R., Van Gelder, P., Miraglia, S., Ton Vrouwenvelder, A. [eds.] (2013). *Safety Reliability and Risk Analysis: Beyond the Horizon*. ISBN 978-1-138-00123-7. London: Taylor & Francis Group, 3387 p.

[10] Nowakowski, T., Mlyńczak, M., Jodejko-Pietruczuk, A., Werbińska-Wojciechowska, S. [eds.] (2014). *Safety and Reliability: Methodology and Application*. ISBN 978-1-138-02681-0. London: Taylor & Francis Group, 2453 p.

[11] Podofillini, L., Sudret, B., Stojadinovic, B., Zio, E., Kröger, W. [eds.] (2015). *Safety and Reliability of Complex Engineered Systems.* ISBN 978-1-138-02879-1. London: CRC Press, 4560 p.

[12] Walls, L., Revie, M., Bedford, T. [eds.] (2016). *Risk, Reliability and Safety: Innovating Theory and Practice: Proceedings of ESREL* ISBN 978-1-315-37496-7. London: CRC Press, 2942 p.

[13] Cepin, M., Bris, R. [eds.] (2017). *Safety and Reliability – Theory and Applications*. ISBN: 978-1-138-62937-0. London: Taylor & Francis Group, 3627 p.

[14] Haugen, S., Vinnem, J., E., Barros, A., Kongsvik, T., Van Gulijk, C. [eds.] (2018). *Safe Societies in a Changing World*. ISBN: 978-0-8153-8682-7. London: Taylor & Francis Group, 3234 p.

[15] Beer, M., Zio, E. [eds.] (2019). *Proceedings of the 29th European Safety and Reliability Conference (ESREL).* ISBN 978-981-11-2724-3. Singapore: ESRA, Research Publishing, 4315 p.

[16] Baraldi, P., Di Maio, F., Zio, E. [eds.] (2020). *Proceedings of the* 30th European Safety and Reliability Conference and *15th Probabilistic Safety Assessment and Management Conference (ESREL2020 PSAM15).* ISBN 978-981-14-8593-0. Singapore: ESRA, Research Publishing, 5067 p.

[17] Castanier, B., Cepin, M., Bigaud, D., Berenguer, C. [eds.] (2021). *Proceedings of the 31st European Safety and Reliability Conference*. ISBN 978-981-18-2016-8. Singapore: ESRA, Research Publishing, 3473 p.

[18] Leva, M.C., Patelli, E., Podofillini, L., Wilson, S. [eds.] (2022). *Proceedings of the 32nd European Safety and Reliability Conference (ESREL 2022).* ISBN 978-981-18-5183-4. Singapore: ESRA, Research Publishing, 3413 p.

[19] OECD. (2002). *Guidance on Safety Performance Indicators. Guidance for Industry, Public Authorities and Communities for Developing SPI Programmes Related to Chemical Accident Prevention, Preparedness and Response*. Paris: OECD, 191 p.

[20] Prochazkova, D. (2017). *Principles of Risk Management of Complex Technological Facility.* ISBN 978-80-01-06180-0, e-ISBN:78-80-01-06182-4. Prague: CTU, 364 p. doi:10.14311%2FBK.9788001061824

[21] EU. *Seveso III Directive (2012/18/EU).* Brussels: EU 2012.

[22] US DOE. *DOE -HDBK-110196. Handbook. No 20585*- Tennessse: US DOE 1996, 180 p.

[23] Prochazka, J., Prochazkova, D. (2022). *Risk Management of Traffic Management Systems*. Prague: CTU, 129 p. doi:10.14311/BK.978 80010 69950

[24] Prochazkova, D., Prochazka, J., Lukavsky, J., Dostal, V., Prochazka, Z., Ouhrabka, L. (2019). *Risk Management of Processes Associated with the Operation of a Technical Facility during Its Lifetime.* ISBN 978-80-01-06675-1. Prague: CTU, 465 p. doi:10.14311%2FBK.978800 1066751

[25] Rausand, M. (2014). *Reliability of Safety-Critical Systems: Theory and Applications*. - John Wiley & Sons, 421 p.

[26] FEMA. *(1996). Guide for All-Hazard Emergency Operations Planning*. State and Local Guide (SLG) 101. Washington: FEMA.

[27] EU. *FOCUS Project*. Brussels: EU 2012 – [on-line] Available on - URL: http://www.focusproject.eu/documents /14976/-5d7 63378-1198-4dc9-86ff-c46959712f8a

[28] Procházková, D., Wessely, E., Rusko, M. & Kralikova, R. (2011). *Human System Safety Management and Environmental Management Relation*. - In DAAAM International Scientific Book 2011. pp. 103-118. ISSN 1726-9687; DOI: 10.2507/daaam.scibook.2011.09

[29] Necesal, L., Lukas, L. & Jasek, R. (2011). *Measures for critical infrastructure protection in the Czech republic*. - Annals of DAAAM for 2011 & Proceedings of the 22nd International DAAAM Symposium, Volume 22, No. 1, ISSN 1726-9679, Katalinic, B. [ed.], Vienna, pp. 0843-0844

[30] Lojan, R. (2015). *Ľudská dôstojnosť a hodnota ľudského života*. - In: Nové horizonty, Bratislava, ISSN 1337-6535, Vol. 9, Issue. 1, pp. 10-14

[31] Prochazkova, D., Prochazka, J., Rusko, M., Mikulova, M. & Ilko, J. (2017). *Model for critical infrastructure safety management*. - In Annals of DAAAM for 2017, Volume 28, No.1. The 28th DAAAM International Symposium. Zadar, Croatia, 08-11th November 2017. Vienna, ISSN 2304-1382, ISBN 978-3-902734-14-3. DOI: 10.2507/28th.daaam.proceedings.085.

[32] Procházková, D. & Rusko, M. (2017). *Relation between human system safety management and environmental management*. - In Journal of Environmental Protection, Safety, Education and Management. Vol. 5, No. 9, ISSN 1339-5270

[33] Kralikova, R., Sokolova, H., Wessely, E. & Polak, J. (2013). *Approaches to assessment of hot environment.* – In DAAAM International Scientific Book 2013. chapter 14. Vienna, pp. 317-328. ISBN 978-3-901509-94-0

[34] Lukas, L. & Hromada, M. (2011). *Risk analysis in context of critical infrastructure protection*. - Annals of DAAAM for 2011 & Proceedings of the 22nd International DAAAM Symposium, Volume 22, No. 1, ISSN 1726-9679, Katalinic, B. [ed.] Published by DAAAM International, Vienna

[35] Steffen, W. et al. (2015). *Planetary boundaries: Guiding human development on a changing planet*. - SCIENCE 15 Jan 2015 Vol 347, Issue 6223, DOI: 10.1126/science.1259855

[36] Kikuchi, Y. (2016). *Chapter 24 - Life Cycle Assessment*. - Plant Factory An Indoor Vertical Farming System for Efficient Quality Food Production, pp. 321-329, https://doi.org/10.1016/B978-0-12-801775-3.00024-X

[37] Suhariyanto, TT, Wahab, D.A. & M.N. Ab. Rahman (2017). *Multi-Life Cycle Assessment for sustainable products: A systematic review*. - Journal of Cleaner Production, Volume 165, 1 November 2017, Pages 677-696, https://doi.org/10.1016/j.jclepro.2017.07.123

[38] Moon, H., Miller, D. R. & Kim, S.H. (2013). *Product Design Innovation and Customer Value: Cross-Cultural Research in the United States and Korea*. - Journal of Product Innovation Management, Volume 30, Issue1, January 2013, pp. 31-43, https://doi.org/10.1111/j.1540-5885.2012.00984.x

[39] Dunmade, I. (2006). *Design for Multi-lifecycle: A sustainable design concept applied to an agroindustrial development project.* - Conference: 2006 ASAE Annual Meeting, Portland, Oregon, July 9-12, 2006, 068059, DOI: 10.13031/2013.21074

[40] Dunmade, I. (2013). *Design for Multi-Lifecycle : A Sustainability Design Concept*. - International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622, Vol. 3, Issue 2, March -April 2013, pp.1413-1418

[41] Go, T.F., Wahab, D.A. & Hishamuddin, H. (2015). *Multiple generation life-cycles for product sustainability: the way forward.* - Journal of Cleaner Production, Volume 95, 15 May 2015, pp. 16-29, https://doi.org/10.1016/j.jclepro.2015.02.065

[42] Hellweg, S., Benetto, E., Huijbregts, M.A.J. et al. (2023). *Life-cycle assessment to guide solutions for the triple planetary crisis.* - Nat Rev Earth Environ 4, 471–486 (2023). https://doi.org/10.1038/s43017-023-00449-2

[43] ISO 14040: 2006 Environmental management — Life cycle assessment — Principles and framework.

[44] UNEP/SETAC (2009) *Guidelines for social life cycle assessment of products. Life-Cycle Initiative*. -United Nations Environment Programme and Society for Environmental Toxicology and Chemistry, Paris, France, http://www.lifecycleinitiative.org/wp-content/uploads/2012/12/2009 - Guidelines for sLCA - EN.pdf

[45] Hoogmartens, R., Passel, S.V., Acker, K.V. & Dubois, M. (2014). *Bridging the gap between LCA, LCC and CBA as sustainability assessment tools.* - Environmental Impact Assessment Review, Volume 48, September 2014, pp. 27-33, https://doi.org/10.1016/j.eiar.2014.05.001

[46] Finkbeiner, M., Schau, E.M., Lehmann, A.. & Traverso, M. (2010). *Towards Life Cycle Sustainability Assessment. Sustainability*. 2010, 2(10), pp. 3309-3322; https://doi.org/10.3390/su2103309

[47] Dyson, B. (2023). *Integration of Life Cycle and Life Cycle Sustainability Assessments Into Decision Analytic Approaches for Sustainable Technologies*. - Reference Module in Earth Systems and Environmental Sciences, Elsevier, https://doi.org/10.1016/B978-0-323-90386-8.00057-7

[48] Witze, A. (2023). *AI predicts how many earthquake aftershocks will strike and their strength*. – Nature, 28 sept. 2023, doi: https://doi.org/10.1038/d41586-023-02934-6

[49] Hall, S. (2023). *What Turkey's earthquake tells us about the science of seismic forecasting*. – Nature 615, 388-389 [2023], doi: https://doi.org/10.1038/d41586-023-00685-y

[50] Dascher-Cousineau, K., Shchur, O., Brodsky, E. E. & Günnemann, S. (2023). *Using Deep Learning for Flexible and Scalable Earthquake Forecasting*. - Geophys. Res. Lett., Vol. 50, Issue 17, https://doi.org/10.1029/2023GL103909

[51] Stockman, S., Lawson, D. J. & Werner, M. J. (2023). *Forecasting the 2016–2017 Central Apennines Earthquake Sequence With a Neural Point Process*. - Earths Future, Vol.11, Issue 9, https://doi.org/10.1029/2023EF003777

[52] Zlydenko, O. et al. (2023). *A neural encoder for earthquake rate forecasting*. - Scientific Reports, vol. 13, 12350 [2023], https://doi.org/10.1038/s41598-023-38033-9

[53] Rusko, M., Kralikova, R., Mikulova, M. & Ilko, J. (2016). *Labeling of Products From the Context of Environment, Quality and Safety*. - In DAAAM International Scientific Book 2016, pp.419-434, B. Katalinic (Ed.), ISBN 978-3-902734-09-9, ISSN 1726-9687, Vienna, Austria. Chapter 37, pp. 419 - 434. DOI: 10.2507/daaam.scibook.2016.37

[54] Prochazkova, D., Prochazka, J., Rusko, M., Kollar, V., Majernik, M. & Ilko, J. (2020). *Safety Management of Complex Facilities*.- In Proceedings of the 31st DAAAM International Symposium, pp.0366-0375, B. Katalinic (Ed.), ISBN 978-3-902734-29-7, ISSN 1726-9679, Vienna, Austria, DOI: 10.2507/31st.daaam.proceedings.051