Article citation info:
Nowicki M, Gill A. Concept of hazard identification for RAMS specification. Rail Vehicles/Pojazdy Szynowe. 2023;3-4:54-63. https://doi.org/10.53502/RAIL-177619

Rail Vehicles/Pojazdy Szynowe

www.railvehicles.eu

Concept of hazard identification for RAMS specification

Maciej **Nowicki** [a, *], Adrian **Gill** [b]

[a] *Łukasiewicz Research Network – Poznan Institute of Technology, Poznan, Poland*
[b] *Insitute of Transport, Poznan University of Technology, Poznan, Poland*

ARTICLE INFO

Received: 11 December 2023
Revised: 20 December 2023
Accepted: 26 December 2023
Available online: 28 December 2023

KEYWORDS

RAMS
pneumatic boards
safety assessment
hazard identification

In parallel with the dynamic development of rail transport in terms of vehicle design, control systems, infrastructure issues, the development of processes and procedures in the area of safety management must also progress. This growing awareness was confirmed, among other things, by harmonising the content of the regulations on railway safety and interoperability, the safety certification of railway undertakings and the definition of the tasks and roles of national safety authorities. In effect, this was to enable the development of a single European railway area.

An implementation tool that allows for a systematic approach to safety management processes and that enables the above requirements to be met is, among other things, RAMS analyses. A key step in the safety management process for specifying RAMS is hazard identification, which is particularly highlighted in PN EN 50126-2:2018 through the holistic model for risk assessment and control of railway system hazards (hourglass model). It places the hazard identification process in two stages, i.e. in the early development stage of the analysis (similar to other known risk management models) and in the hazard control stage. This positioning alone indicates the importance of the hazard identification process. On the comprehensiveness and detail of its implementation depends the validity of the final outcome of the RAMS analysis. The development of such a process for real technical facilities in a way that is consistent with the needs of RAMS analyses and, at the same time, ensures that satisfactory results of these analyses are achieved, has become the subject of this article.

1. Introduction

The PN-EN 50126-2:2018-1 and PN-EN 50126-2:2018-2 standards (the so called RAMS standards) have made a significant impact on the structuring of general aspects in the area of specifying the reliability, availability, maintainability and safety of railway systems (RAMS), but they have allowed a certain degree of freedom in the choice of methods for applying the systematic RAMS management process, including the assessment of system safety. With this in mind, the assessment of system safety can therefore be performed in a variety of ways, all of which are, of course, within the scope of the standards indicated.

One of the foundations of the safety management process for specifying RAMS is hazard identification. Possible faults or oversights at this stage can have undesirable consequences at further stages of the assessment and, moreover, determine the quality of the results of risk assessments. It is not without reason that the authors of the article [25] call this stage "the heart of the risk management process".

The key role of the hazard identification stage has also been strongly emphasized by Covello and Merkhofer, treating hazard identification as a completely separate process, necessarily carried out before risk assessment [24].

The legislated flexibility in the details of RAMS specification means that the hazard identification phase is conducted using a variety of methods and techniques, although the heuristic ones based on 'brainstorming' are still the most popular.

For example, in the article [25], identifying the hazards of Abuja Mass Transportation (ARTM) in

* Corresponding author: maciej.nowicki@pit.lukasiewicz.gov.pl (M. Nowicki)

Nigeria, a questionnaire interview method was used. According to the authors, this approach was chosen due to the lack of sufficient data to use the most recent hazard identification methods. However, care was taken to identify human error.

Another example of the use of a nonstandard method based on brainstorming – *sticky notes* – is the paper [21]. This method was used to identify the hazards occurring during the replacement of a power pack vehicle as part of an entity in character of maintenance (ECM).

The Fault Tree Analysis (FTA) and Event Tree Analysis (ETA) methods were used to analyze the risks occurring on the Slovak railway network, as discussed in the article [19]. The author of the article [20], on the other hand, points to the HAZOP (Hazard and Operability Study) method, used by DB (Deutsche Bahn) assessors as a compromise between FMEA (Failure mode and effects analysis) and FTA, while pointing out the limitations of this method.

Another example of the use of a well-known method referred to in the standard [15] is the use of Preliminary Hazard Analysis (PHA) used in the analysis of the railway signaling system in the study [9].

In another case, data from the experience of system operation, obtained from the analysis of accident reports or the opinions of railway experts, were used to assess railway accidents [7]. A similar approach was followed for the analysis of incidents at level crossings [12], using internal risk lists, management review reports and safety audit reports, which was supplemented by interviews with operators and infrastructure managers. The last example is particularly noteworthy because a variety of methods were used in the identification exercise, as is also implicit in the concept that is the subject of this article.

In addition, the authors of the article [3] provide interesting information, indicating that among only 6.7% of the analysed reports, which concerned construction projects, it was possible to identify all risks that should be identified on the basis of current knowledge, while the maximum levels of risk identification were, respectively: 89.9% for nuclear construction projects, 72.8% for rail projects and 66.5% for both rail and general construction projects. The above information confirms that the hazard identification stage requires special attention, so it is not surprising that it is a frequent subject of the authors' considerations, as confirmed by the publications quoted in the introduction.

These examples show that different hazard identification methods are used to different extents, depending on the specifics of the assessed system. This conclusion formed the basis for the following aim of this article: to develop and present a hybrid (multi-stage) hazard identification concept for the RAMS specification of rail vehicle systems. The hybridity of identification will consist in the synergistic use of different approaches to finding sources of hazards and threats in technical systems (from a systematic retrospective approach, through heuristic and predictive techniques, to control studies). The multistage nature of the identification will be driven by the system's life phase, imposed by the Model V of the RAMS standards, for which the presented concept is intended. Examples of the results of the hazard identification process according to the developed concept are presented in the form of records of the dedicated hazard register. The records were developed in relation to pneumatic boards of rail vehicles.

2. Theoretical introduction

The subject of broadly defined safety assessments is characterized by heterogeneous nomenclature (resulting, among other things, from the terminological divergence of the RAMS standards and Regulation (EU) 402/2013 [19]). Therefore, in order to fully understand the further parts of the article, the presented hazard identification concept will be preceded by a short theoretical presentation, which is also practical in terms of highlighting the requirements that this hazard identification concept must meet.

According to EN 50126-1, a hazard is understood as a condition that could lead to an accident [14]. It should be added that an accident is additionally defined in the above-mentioned standard as a sequence of events, which indicates that the condition, which is a hazard, may be a set or sequence of events, not only a single event or a set of features/properties of the system or its environment.

The CSM Regulation [19] in this particular case defines hazard in an analogous way treating it as: a condition that may lead to an accident.

The outcome of the hazard identification process should be a formulated hazard. In order for such formulation to be useful in further stages of risk management, it should contain the following elements (according to point 7.4.2.1 [14]):

- identification of sources/causes of danger – e.g. component, subsystem or system failures, human errors, etc.
- undesirable events that can lead to losses during system operation and maintenance
- losses (consequences) associated with undesirable events – from the point of view of railway operation, losses may mean damage to passengers, staff or members of the public, damage to the environment, etc.

− existing control measures to control and limit the occurrence of an undesirable events.

This understanding of hazard is also familiar to other areas of risk management. For example, Vincoli [22] understands a hazard as "a condition or situation that exists in the work environment and may cause an undesirable release of energy resulting in physical injury, wounding and/or damage". Macdonald [12] views hazard as inherent physical or chemical properties that can cause harm to persons, property or the environment.

Whatever the definition of a hazard, they do not indicate that a hazard is often a hypothetical state or situation. According to Aven [1]: "The hazard identification process should be a creative process wherein one also attempts to identify unusual events". Moreover, he is of the opinion [1] that probably 80% of the time will be (and perhaps should be) spent finding these types of hazards and "the unusual and not-experienced events", even though they will constitute 20% of all those identified.

In view of the need to use the results of hazard identification, the hazards formulated should therefore not only be events or states that have occurred, but above all those that are formulated by the identification performer using appropriate inductive or even abductive reasoning. The process of identifying risks therefore contains a certain element of creativity, and is sometimes even a form of guessing what might happen [5].

As part of the requirements to be met by the hazard identification step, it should be pointed out that the RAMS specification standards consider hazards at the system under consideration level and hazards at the railway system level. A hazard, understood as a state, therefore develops at different levels of system decomposition. The relationship between the individual components of such a chain of events and states, according to the RAMS guidelines, is shown schematically in Fig. 1.

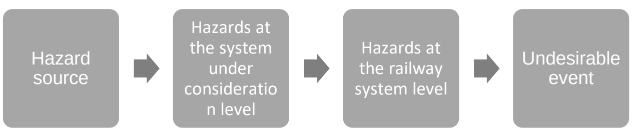

Fig. 1. Evolution of the source of the hazard assuming consideration of the hazard at two levels according to the [15]

For the purposes of the presented concept of hazard identification, in addition to the classification into hazards at the level of the system under consideration and hazards at the level of the railway system, a classification based on the component hazards was introduced:

− a hazard that is a single event or factor (identified mainly at the design stage of systems/facilities in a systematic manner using inductive reasoning and FMEA-type methods)
− hazards which are a set of events and/or properties of the area of analysis (states occurring as a coincidence of sources/hazard factors, identified using methods such as bow-tie or FTA, for example), also referred to in standard [15] in clause [19] point 11.4
− hazards that are sequences of events (usually formulated as the first or last of the adverse events in a sequence of events, identified by inductive reasoning and ETA-type methods).

In addition, the identification of risks can lead to the formulation of risks originating from so-called systematic errors, e.g. in the system design phase, human errors, instruction inadequacies and so called random failure resulting primarily from stress degradation, environmental overloading, etc., as shown in Fig. 2 [14]. Systematic errors happen permanently under certain conditions of handling, storage or use, while accidental errors result from one or more possible degradation mechanisms.

The information listed above should be collected and organized in a risk register. The hazard register forms the basis for current risk management (carried out to achieve and maintain a safe state) as a tool for controlling hazards. The hazard register is updated throughout its life cycle whenever there is a change in the identified hazards or a new hazard is identified. In accordance with point 7.4.2.2 [14].

The hazard register must include or refer to, inter alia:

− the identification of those responsible for managing the hazard
− the likely consequences and frequency of the sequence of events associated with each hazard
− the risk resulting from each hazard (in quantitative or qualitative terms)
− the risk acceptance principles chosen and, in the case of explicit risk estimation, also the risk acceptance criteria for demonstrating the acceptability of the risk control related to the hazards
− for each hazard: the measures taken to reduce the risk to an acceptable level or to remove the risk.

3. Research topic – description of the concept

The trends of hazard identification identified in Chapter 1 and the theoretical introduction in Chapter 2 made it possible to formulate the assumptions of the hybrid (multi-ethereal) hazard identification method for RAMS specification that follows.

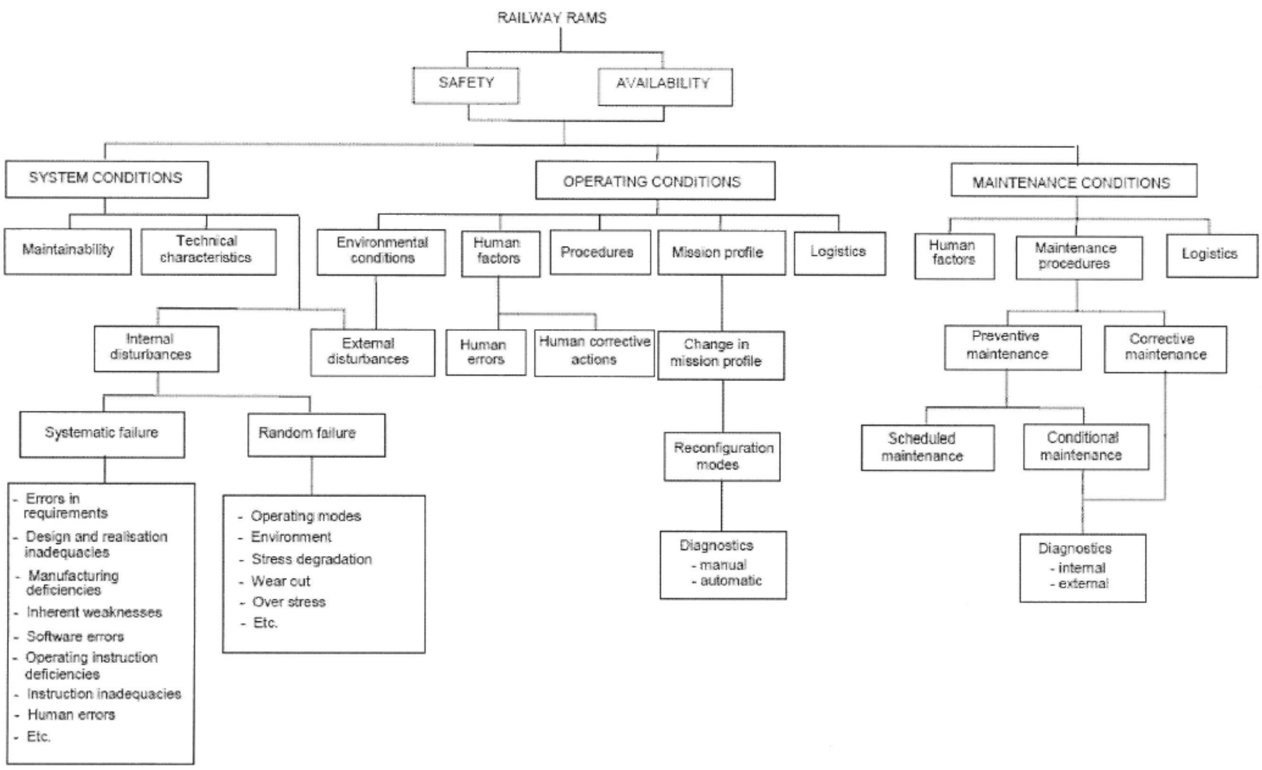

Fig. 2. Factors influencing RAMS [14]

The basic idea is to perform a systematic hazard identification in accordance with the system life cycle, using dedicated identification methods appropriate to the life cycle stages. In order to be in line with the RAMS specification guidelines, the stages of the hazard identification process have been linked to the stages of the system life cycle as indicated by model V [15]. The main emphasis in this identification process will be on the study of the various relationships/influences occurring between elements of the system itself, as well as the system and its environment (i.e. the so-called interfaces). It can be additionally pointed out that these will be both so-called intentional relations (resulting, e.g. from the physical connection of elements) and so-called nonintentional relations (caused, e.g. by the respective forms of errors or system failures).

The hazard identification process will be carried out in the following stages in line with the system life process indicated by the V model [15], as shown in the diagram below Fig. 3.

3.1. Conceptual phase/system requirements specification

According to the RAMS, the task of the conceptual phase is to define the overall scope of the project, to deepen the knowledge of the system (RAMS phase 1) and, in the next step, to specify the system requirements (RAMS phase 4), i.e. to specify the system requirements for the next life-phases, as well as to define acceptance criteria and to define the overall demonstration of compliance.

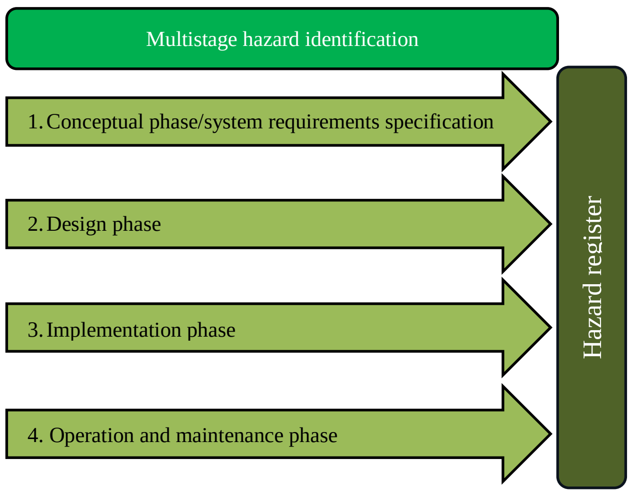

Fig. 3. Schematic of hazard identification steps according to mode V [15] for the concept described

Within this stage of hybrid (multi-stage) hazard identification, an approach based on a systematic review technique of the analysis area is adopted. Hazard identification will therefore be performed by systematically analyzing the records of the system requirements specification and looking for possible deviations in the achievement of the design intentions, operational conditions of the process, procedures or system (or in other words: by questioning the achievement of the design intentions and operational conditions). This approach is in line with the idea of methods such as HAZOP [17]. In the praxis of applying such a stage concept, threats will take the form of negation of the fulfilment of the overall requirements for the system, and will be demonstrated in the collaboration of the project team.

In the field of the CSM Regulation [19] (also referred to in point 6.3 [14]), such a course of action is called a code of conduct, which, in order to qualify as a requirement, must meet the following requirements according to Annex I [19]:

- must be widely recognised within the railway industry. Otherwise the code of practice must be justified and should be acceptable to the assessment body
- must be relevant to the oversight of the considered risks in the assessed system. The successful application of the code of practice for similar cases regarding the management of change and the effective control of identified system risks within the meaning of this Regulation is sufficient to be considered as significant
- must be available to the assessment bodies on request for their assessment or, where appropriate, for mutual recognition, in accordance with Article 15(5), of the appropriate application of the risk management process and its results.

It should be noted that the results of hazard identification at this stage will have a major impact on decisions regarding the implementation of the system design.

An essential element of the assessment performed in accordance with the CMS regulation cited above [19] is a system definition (also described in the RAMS standards in point 7.3.2.1 [14]) containing a series of information such as: the purpose of the system (the intended use); the functions and elements of the system, if applicable (including the human, technical and operational elements); the boundary of the system, taking into account other systems with which the system interacts; the physical interfaces (the systems with which the system interacts) and functional interfaces (inputs and outputs relating to performance); the system environment (e.g. energy and termic flows, shocks, vibrations, electro-magnetic interference, operational purpose) [19].

Referring to the example object of the concept in the form of pneumatic boards, exemplary elements of system definition are presented below in the form of selected basic parameters collected in Table 1.

In addition, Fig. 4 below shows an example of a graphical approach to describing the boundaries or interfaces of a system.

Table 1. Selected basic parameters of pneumatic boards [own elaboration]

No.	Parameter	Description
1.	Highest pressure in the supply line	1000 kPa
2.	Air cleaning equipment incorporated in the board	Cyclone with dehydrator on supply line
3.	PN brake functions accessible via the board	Standby, service braking (8 braking steps), emergency braking, disconnection of the board brake control system from the service line
4.	EP-B brake functions available via the board	Brake released or one of eight brake stages
5.	Possible states of the parking brake	Brake loosened, braked or disengaged
6.	Highest pressure in parking brake spring actuators	Equal to the board supply pressure
Electrical parameters of the boards		
7.	Rated board supply voltage	24 V DC
Working conditions		
8.	Place of work	The driver's cab or its immediate vicinity this cab
9.	Working position	Vertical

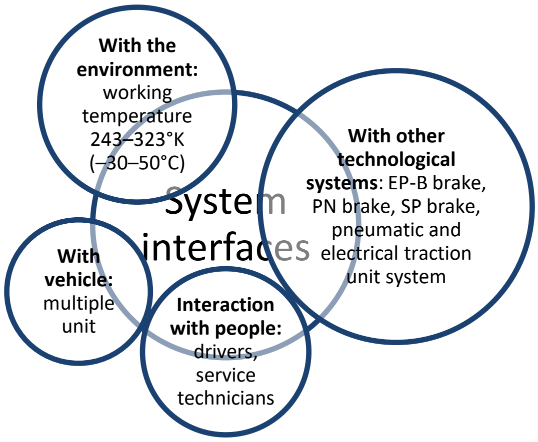

Fig. 4. Graphical presentation of system interfaces in the form of pneumatic boards [own elaboration]

3.2. Design phase

According to the RAMS approach, the objective of the design phase (RAMS Phase 6) is to: design subsystems and components according to RAMS requirements; demonstrate that subsystems and components comply with RAMS requirements; and refine plans for future lifecycle tasks.

According to the presented concept for hazard identification, heuristic methods will be used at the design stage. They are ideal for the prediction of future phenomena, based on creative thinking and logical combinations. However, it has a number of disadvantages, e.g.: the dominance of analysis by the most active members of the expert team monopolises the discussion or pragmatism in the pronouncement of nonobvious ideas for fear of criticism.

With this in mind, the concept presented here therefore proposes the use of a codified approach based on the brainstorming technique and implemented in the form of the sicky notes method. The essence of this method is the exploration of expert knowledge by means of short, concise notes made (usually physically) on small pieces of paper (popular yellow note cards – thus the name of the method). These cards have a dual role, i.e. they are used to stimulate the experts' discernment to look for irregularities in the process under analysis and to record the results of the method. What is valuable from the hazard identification point of view is the fact that experts, seeing such a seemingly less formal way of recording information, are more willing to discuss and report irregularities in the analysed area. In addition, the results obtained (as shown by the authors of the study [21]), sometimes even directly can be used as correctly formulated hazards. The method is particularly applicable to process analysis, but, as the authors of [21] have shown, it can also be used for technical objects and their handling processes.

From a practical point of view, the sticky notes technique consists of the following actions:

- Task 1 Assembling an interoperable group of experts by the facilitator – one of the most important issues determining the outcome of hazard identification at this stage is to involve the right group of experts with knowledge of both the design and practically all stages of the product lifecycle, i.e.: existing requirements, component design, manufacturing and servicing (maintenance).
- Task 2: Define the questions to which answers are sought – in the case of analysis for the purpose of hazard identification, these may take the following form: *How can component "x" fail? What could be the cause of failure of "x"?* and in subsequent iterations: *What could be the consequence of component 'x' being damaged?*
- Task 3 Collecting the answers – each member of the team writes down, based on their knowledge, on separate pieces of paper the proposed answers and then tapes them on the board under the question under consideration.
- Task 4 Analysing the answers – at this stage the results are systematised in several aspects: prioritising the results, grouping the answers, indicating the connecting elements (inter-feeds).
- Task 5. Repetition of Tasks 3 and 4 – if necessary, after the analysis of the collected information, it is possible to refine the questions, which can be done by performing further iterations of Tasks 3 and 4.

A practical aspect is that if it is difficult to gather a group of experts at the same time, a virtual analysis can be carried out, e.g. on a Teams or Sharepoint platform, in a similar way to the above.

This identification will also be complemented by a systematic verification of the validity of the form of component faults cited in the PN-EN 50129:2019-01 [16] standard for components of electrical systems.

Hazard identification at the design stage is of key importance, since risks are considered in practice at virtually every stage of the life cycle of the system under consideration. The aim is to apply appropriate design or system solutions to avoid or minimise them.

3.3. Implementation phase

This hazard identification phase will be implemented over several phases of the system life cycle, according to the part of the V-model corresponding to production (phase 7) and integration (phase 8). The overarching goal of this phase is to produce subsystems and components in line with the previous phases, assemble them and integrate them. According to the provisions of the standard [14], the types of defects associated with RAMS should be inspected and tested in this phase, which will be realised by the following methods:

- direct observation
- acoustic methods
- sticky notes – described in point. 3.2.

Direct observation of production processes aims, among other things, to catch some of the most unpredictable risks originating from the group of errors/human factors, to which a whole team of human reliability analyses is dedicated (HRA – Human Reliability Analysis). Section 5.6.4 of the standard [14] defines human factors as anatomical, physiological and psychological aspects of humans. From this point of view, HRA aims to assess and help prevent the consequences of emerging human factors/errors affecting system performance, operation, reliability and safety [4]. According to the authors of the article [4], during the operation of transport systems such as trains, ships, aircraft and motor vehicles, about 70–90% of accidents are directly or indirectly due to human error and according to the same authors, with the development of technology, the reliability of transport systems has increased over the past decades, while human reliability has remained unchanged over the same period. In the presented concept, the above-mentioned errors are to be identified by direct observation of production processes, which assumes the recognition of hazards arising from, e.g:

- failure to apply the provisions of the instructions and procedures
- rushing the work in progress
- routine in the case of repetitive activities
- difficulties of adaptation to new activities due to modifications of the production processes
- inexperience, especially in the case of newly recruited staff, especially due to high staff turnover.

The above is in line with the provisions of point 11.2 [15] indicating that causal analysis should also identify reliable human error.

In addition, direct observation aims to identify the form of component damage occurring during production, which can be done through organoleptic verification of components at the acceptance stage by the quality department by performing, for example: geometric measurements and functional tests.

The identification of component faults during production also involves the use of acoustic methods, which are well suited to the analysis of mechanical and pneumatic systems such as pneumatic boards. For this purpose, a leak detector can be used in the form of an acoustic trumpet acting as a directional microphone to attenuate disturbing environmental sounds, allowing the exact location of the source of the sounds generated to be determined, even those inaudible to the human ear. The method belongs to the group of passive methods, which means that the apparatus does not emit signals and does not affect the physical state of the tested object; instead, it only registers the physical effects arising in the monitored object itself. In the case of pneumatic systems, the sources of acoustic emission signals are: emerging and propagating microcracks, corrosion processes, cracks causing air leakage through leaks. Looking at the above description, the adopted identification method resembles the acoustic emission method (def. AE – acoustic emission), which belongs to widely used methods of monitoring engineering objects such as: pipelines, compressed gas tanks, combustion engines, power transformers [18]. In contrast to the accepted acoustic trumpet method, the AE method involves recording elastic waves using piezoelectric sensors that convert the AE waves into an electrical signal that is transmitted further to the measurement system [2].

In summary, since human error is currently considered to be the most important source of accidents or incidents in safety-critical systems, the concept described assumes that they are identified as early as the design phase (within sticky notes) and subsequent corresponding production (phase 7) and integration (phase 8) phases.

In addition, it should be noted that the hazards identified at the level of the system under consideration will repeatedly take the form of faults that will be transposed as hazards at the level of the railway system. On the other hand, the acoustic method will also constitute an important element of the control measures (point 7.4.2.1 [14]), which exist to control or limit any undesired event resulting from the hazards.

Figure 5 shows a pneumatic board type 200ZH 94-1 undergoing the direct inspection described above to identify the form of component damage occurring during production.

Fig. 5. Pneumatic board 200ZH 94-1 during acceptance [own drawing courtesy of PIT-Industry]

3.4. Operation and maintenance phase

The last phase of the presented identification concept, concerns the operation, maintenance and monitoring of the system (this is phase 11 of the RAMS V model). This phase involves continuous monitoring and evaluation of the system's RAMS indicators.

In the case of hazard identification carried out for systems already in operation, very valuable is feedback analysis of data from:

- complaint processes during the warranty period of the component (exploitation phase)
- service data during regular maintenance activities (maintenance phase).

This also follows from the obligation in point 7.12.3 [14] stating the need to update the operational hazard register.

The above-mentioned sources of information can be used to indicate the form of damage to the analysed components, and further enable the formulation of risks on their basis.

An additional benefit of this approach will be the ability to extract relevant data on the reliability of systems, e.g. in the form of a damage severity indicator.

4. Example of hazard register created for the hazard identification concept

All hazards identified at the various stages described above should be included in the hazard register created for the specification of the RAMS.

According to [14], the risk register should include:

- purpose of the register
- for each hazard, the specific actor responsible for managing the hazard and the functions or components contributing to the hazard
- the likely consequences and frequencies of occurrence of hazard-related sequences of events
- the risks resulting from each hazard
- selected risk acceptance principles
- the measures applied to reduce the risk to an acceptable level or to remove the risk
- the safety constraints exported

thus completing the provisions of point 7.4.2.1 [14].

The illustrative hazard register created for the concept described is presented in Table 2 below using pneumatic arrays as an example object of analysis.

In addition to the system definition referred to in Section 3.1, pneumatic boards in their various versions are used on all types of rail vehicles to control the braking systems, to supply these systems with compressed air and to distribute compressed air for auxiliary vehicle systems (e.g. supplying the indicators

Table 2. Risk register [own elaboration]

Risk register															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Description						System under consideration **A**			Railway system level **G**						
System element	Function in the system	Responsible entity	Form of failure (Hazard source HS)	Detectability D (HS)[1)]	Probability of occurrence P(HS)[2)]	Hazard (H^A)	Detectability D(H^A)	Probability of occurrence P(H^A)	Hazard (H^G)	The possibility of avoiding D(H^G)	Probability of occurrence P(H^G)	Undesirable event (UE)	Probability of occurrence P(UE)	Losses L(UE)[3)]	Risk R(UE)
			HS_i	$D(HS_i)$	$P(HS_i)$	H_i^A	$D(H_i^A)$	$P(H_i^A)$	H_i^G	$D(H_i^G)$	$P(H_i^G)$	UE_i	$P(UE_i)$	$L(UE_i)$	$R(UE_i)$
Pressure converter	Pneumatic device for direct filling of brake cylinders as a function of the control signal generated by the camshaft valve	Section for the design of pneumatic systems	Rubber bellows rupture	0.98	$2.3 \cdot 10^{-5}$	Air leakage from the gearbox (no possibility of changing (increasing) |cylinder pressures	0.99	$2.3 \cdot 10^{-7}$	Extension of the braking distance of a loaded railway vehicle	0.99	$2.3 \cdot 10^{-9}$	Stopping a vehicle in an unauthorised place	$2.19 \cdot 10^{-9}$	6	$1.31 \cdot 10^{-8}$
												Running into another railway vehicle	$1.15 \cdot 10^{-10}$	8	$9.21 \cdot 10^{-10}$
Distribution valve	Control of control chamber filling/emptying time. Implementation of service braking	Pneumatic systems design section	Damage to the oring between the brake board and the timing valve mounting plate	0.98	$7.63 \cdot 10^{-6}$	Air leakage from the timing valve	0.99	$7.63 \cdot 10^{-8}$	Unwanted stopping of a vehicle on the route	0.99	$7.63 \cdot 10^{-10}$	Stopping a vehicle in an unauthorised place	$7.63 \cdot 10^{-10}$	6	$4.49 \cdot 10^{-9}$

Detectability D(HS) – value approximated by expert knowledge
Probability of occurrence P(HS) – estimated on the basis of operating data
Losses L(ZN) – assigned on the basis of PKP PLK procedure *Technical and operational risk assessment*

for the manual parking brake or the door locking and locking devices). In addition, there are transducers for measuring pressures e.g. in the supply and main lines, brake cylinders, auxiliary reservoirs, etc.

The individual risks have been assigned to the elements of the system being decomposed. For the sake of clarity, only the most relevant information has been included within the framework of this illustrative register, which should be supplemented by the requirements in point 7.4.2.1 [14].

It is important to note that the hazard register should be updated throughout the life cycle, especially when a change occurs in the already identified hazards or a new hazard is identified.

5. Summary

Unlike the literature mentioned in the introduction, the concept of hazard identification for RAMS specification presented in this paper involves the development of a hybrid (multi-stage) method using a number of dedicated methods for the systematic identification of hazards at different stages of the system's life, characterised by different specificities described in Chapter 3.

In line with the concept, threat identification will be initiated at the conceptual/system requirements specification stage, where threats take the form of negation of general requirements, using a systematic analysis of the system requirements specification records.

Hazard identification at the design stage will use a heuristic sticky notes me-method that also takes into account systematic verification of the validity of the form of component faults referenced in PN-EN 50129:2019-01 [16] for electrical system elements.

The use of a combination of several methods – direct observation, acoustic methods and the sticky notes mentioned above – will enable the most effective identification at the implementation stage (realised over several life cycle phases according to the V-model: production (phase 7) and integration (phase 8). In addition, direct observation of production processes aims, among other things, to identify some of the most unpredictable risks from the group of errors/human factors, which is an important added value of the presented concept.

Finally, hazard identification at the operating stage, in addition to the possibility of obtaining important data on the reliability of systems (e.g. in the form of damage severity indexes), will provide information on post-tenuation forms of damage to components that were not anticipated at earlier stages of the analysis.

According to the above information, the described concept will give the possibility to control the hazard identification in the individual system life stages indicated by model V [15] which takes into account the so-called refined identification according to sec. 11.3 [15] capturing unseen risks resulting from :

- new technologies that could not be immediately identified due to lack of experience or knowledge (point 3.1 of the concept)
- additional risks in the existing system due to technology transfer, e.g. from analogue to digital technology (points 3.2 and 3.3 of the concept)
- errors in the new design due to lack of adequate/ appropriate specification (point 3.2 of the concept)
- special operating modes in the existing system which may not fit together adequately and may create new risks related to the activities of the operating, maintenance or other personnel (point 3.4 of the concept)
- design errors that could create new risks (point 3.2 of the concept).

In accordance with the assumptions described in point 2, the concept allows the identification of both systemic and random risks at the level of the system under consideration and at the level of the railway system. This is important, among other things, from the point of view of the risk assessment to be carried out in subsequent steps, which requires grading the consequences of the occurrence of adverse events, which is reflected, among other things, in the illustrative risk register created for the purposes of the described concept presented in Table 1.

The hazard identification performed according to the described concept will allow to proceed to the next stage of the analysis in the form of risk assessment and evaluation.

Acknowledgements

The research was carried out/financed under the Program of the Ministry of Education and Science ”Applied Doctorate” realized in years 2021–2025 (Agreement no DWD/5/0355/2021 as of 01.02.2022).

Nomenclature

H	hazard
HS	hazard source
D	detectability
L	losses
P	probability of occurrence
R	risk
UE	undesirable event

Bibliography

[1] Aven T. Risk analysis. John Wiley & Sons. 2015. https://doi.org/10.1002/9781119057819

[2] Baran I. Non-destructive testing of technical equipment using acoustic emission method (in Polish). Nondestructive Testing and Diagnostics. 2019;4:15-19.

[3] Carter G, Smith AD. Safety hazard identification on construction projects. J Constr Eng M. 2006;132(2): 197-205. https://doi.org/10.1061/(ASCE)0733-9364(2006)132:2(197)

[4] Felice F, Petrillo A. Methodological approach for performing human reliability and error analysis in railway transportation system. International Journal of Engineering and Technology. 2011;3(5):341-353.

[5] Gill A, Kadziński A. Hazard identification model. Proceedings of 20th International Scientific Conference Transport Means (5-7 October 2016, Juodkrante, Lithuania), Kaunas University of Technology. 2016:885-890.

[6] Gill A, Kadziński A. Hazard identification for the analysis domains in railway system (in Polish). Prace Naukowe Politechniki Warszawskiej. Transport. 2017;115: 47-56. https://yadda.icm.edu.pl/yadda/element/bwmeta1.element.baztech-e1dcff14-5607-4e4f-aa35-a1d1cb22f6ca

[7] Gill A, Kadziński A. Hazard record (in Polish). Autobusy technika, eksploatacja, systemy transportowe. 2016;12:158-161. https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-99c81781-6a5a-44b7-ab03-680525a85de2/c/GILL_KADZINSKI.pdf

[8] Gill A, Kobaszyńska-Twardowska A. Identyfikacja zagrożeń w wybranych strefach tramwaju z wykorzystaniem metody Bow-Tie. Logistyka. 2014;6:5514-5521.

[9] Hwang JG, Jo HJ. Hazard identification of railway signaling system using PHA and HAZOP methods. International Journal of Automation and Power Engineering (IJAPE). 2013;2:32-39. https://ia800508.us.archive.org/27/items/IJAPE100/IJAPE100.pdf

[10] Leitner B. A general model for railway systems risk assessment with the use of railway accident scenarios analysis. Procedia Engineering. 2017;187:150-159. https://doi.org/10.1016/j.proeng.2017.04.361

[11] Li Q, Zhang Z, Peng F. Identification for railway accident prevention: complex network-based model development and comparison. Entropy. 2021;23(7):864. https://doi.org/10.3390/e23070864

[12] Macdonald D. Practical industrial safety, risk assessment and shutdown systems for industry. Elsevier 2004. https://doi.org/10.1016/B978-0-7506-5804-1.X5000-9

[13] Nedeliakova E, Hranicky MP, Valla M. Risk identification methodology regarding the safety and quality of railway services. Production Engineering Archives. 2022;28(1):21-29. https://doi.org/10.30657/pea.2022.28.03

[14] PN-EN 50126-1:2018-02. Zastosowania kolejowe – specyfikowanie i wykazywanie niezawodności, dostępności, podatności utrzymaniowej i bezpieczeństwa (RAMS). Część 1: Proces ogólny RAMS. 01.02.2019.

[15] PN-EN 50126-2:2018-02 Zastosowania kolejowe – specyfikowanie i wykazywanie niezawodności, dostępności, podatności utrzymaniowej i bezpieczeństwa (RAMS). – Część 2: Sposoby podejścia do bezpieczeństwa.

[16] PN-EN 50129:2019-01 Zastosowania kolejowe – systemy łączności, przetwarzania danych i sterowania ruchem – Elektroniczne systemy sterowania ruchem związane z bezpieczeństwem.

[17] PN-EN 61882. Badania zagrożeń i zdolności do działania (badania HAZOP) – Przewodnik zastosowań, Polski Komitet Normalizacyjny, Warszawa 2016.

[18] Ranachowski Z. Application of acoustic emission to fault diagnostics in civil engineering (in Polish). Drogi i mosty. 2012;2:151-173. https://www.rabdim.pl/index.php/rb/article/view/v11n2p151/108

[19] Rozporządzenie Wykonawcze Komisji (UE) nr 402/2013 z dnia 30 kwietnia 2013 r. w sprawie wspólnej metody oceny bezpieczeństwa w zakresie wyceny i oceny ryzyka i uchylające rozporządzenie (WE).

[20] Schulze J. Improvement of hazard identification in railway software. Master's Thesis in Secure and Dependable Computer Systems. Chalmers University of Technology. Goteborg 2010. https://publications.lib.chalmers.se/records/fulltext/138837.pdf

[21] Smoczyński P, Gill A, Motyl M, Babiak A. How to do it with sticky notes: a method for exploring expert knowledge to prepare guidelines for practice in railway vehicle maintenance. Transport Problems. 2021;16(1): 153-164. https://bibliotekanauki.pl/articles/2203855.pdf

[22] Vincoli JW. Basic guide to system safety. Third Edition. John Wiley & Sons Inc. Wiley 2014. https://doi.org/10.1002/9781118904589

[23] Wang J, Gao S, Yu L, Zhang D, Xie C, Chen K et al. Data-driven lightning-related failure risk prediction of overhead contact lines based on Bayesian network with spatiotemporal fragility model. Reliab Eng Syst Safe. 2023;231:109016. https://doi.org/10.1016/j.ress.2022.109016

[24] Wang LC. Hazards identification model for rail rapid transit accidents. J Mar Sci Technol. 2004;12(2):78-85. https://doi.org/10.51400/2709-6998.2223

[25] Zhang Y, Fom DD. Hazard identification and risk assessment of Abuja rail mass transit. Transportation Safety and Environment. 2022;4(2):1-8. https://doi.org/10.1093/tse/tdac014