Urban Rail Transit (2022) 8:246–266
https://doi.org/10.1007/s40864-022-00181-y

http://www.urt.cn/

ORIGINAL RESEARCH PAPERS

Risk Analysis for Train Collisions Using Fault Tree Analysis: Case Study of the Hanoi Urban Mass Rapid Transit

Thi Hoai An Nguyen[1] · Jochen Trinckauf[2] · Tuan Anh Luong[1,2] · Thanh Tung Truong[3]

Received: 30 January 2022 / Revised: 4 October 2022 / Accepted: 17 October 2022 / Published online: 21 November 2022

Abstract The urban mass rapid transit (UMRT) Line HN2A is the first light rail transit line in Vietnam. It is also the first time the operational safety assessment for the whole life cycle of a railway project is applied and assessed by an applicable scientific tool. While various industry standard methods have been deployed in many countries, their application is not appropriate for assessing the outdated railway infrastructure in Vietnam. This article proposes a method for generating safety risk models for train collisions using the fault tree analysis (FTA) technique. The FTA method comprehensively evaluates the fundamental error and failure probability that could potentially lead to accidents in general and train collisions in particular on Line HN2A. The study describes the procedure for establishing FTA and determining assumptions based on technical specifications and similar railway systems. Compared with the statistical failure results using data from operational tests and commissioning (2018–2021) of the metro line, the results here indicate that this is a reasonable theoretical model applicable to UMRT in Vietnam. The theoretical model will be processed to generate the first-ever scientific risk assessment system based on empirical evidence. In addition, real-time accident and operation data will continue to be collected and compared to the theoretical model to improve its accuracy. The findings of this study could serve as a starting point for risk management on current and future freight, passenger, and metro lines in Vietnam.

Keywords Train collisions · Risk assessment · Fault tree analysis · Human errors · Safety risk function

1 Introduction

Rail transport has become one of the most widely utilized forms of transport thanks to its high level of safety, large capacity, and cost-effectiveness. With the railway network's continuous development including urban rail transit, one of the major areas of focus is ensuring safety through risk management, during both short- and long-term operation, extending throughout the life cycle, through the use of scientific tools such as management of railway operations [1], specifically in developing countries like Vietnam. The current national mainline railway network of Vietnam has been designed, constructed, and operated entirely in a single narrow gauge of 1000 mm since the previous century, with very few updates of the manual operating technology. This significantly highlights that up to now, the conventional technique for managing the safety operation in general, and collisions in particular, of the current Vietnamese railway system and its subsystems is reactionary and based purely on accident statistics. Science-based tools for predicting trends and analyzing the most suitable methods for risk mitigation are

✉ Thi Hoai An Nguyen
nguyenthihoaian@utc.edu.vn

Jochen Trinckauf
jochen.trinckauf@tu-dresden.de

Tuan Anh Luong
anhlt@utc.edu.vn

Thanh Tung Truong
thanhtung.sig@gmail.com

[1] University of Transport and Communications, Hanoi, Vietnam

[2] Technische Universität Dresden, Dresden, Germany

[3] Hanoi Metropolitan Railway Management Board (MRB), Hanoi, Vietnam

Communicated by Baoming Han.

already available in many countries. Accident management of Vietnam railways is currently limited, as it is responsible for accident statistics analysis in order to avoid and minimize the severity of the impact only after an accident has occurred. Statistical analysis of train accident case studies on Vietnam railways demonstrates that hazards and failures have not been identified, recorded, and evaluated to conduct risk analysis using a suitable assessment methodology. Accident and incident prevention and control cannot currently be forecast accurately, increasing the probability and/or severity of failures in future operations. As a result, Vietnam's railway system has a high number of accidents and high failure rates. For example, Vietnam railways' mainline network accounted for approximately 200 railway accidents in 2018, a 3% increase over the previous year, including 163 collisions between trains and road vehicles or persons, resulting in more than 100 fatalities and more than 150 casualties [2]. Thus, the development of a standardized framework safety model for operational and personal safety management of the expanding railway operation in Vietnam should be an area of focus in view of the rapid development of urban rail transport in the country in recent years [3,4].

Urban mass rapid transit (UMRT) Line HN2A in southwest Hanoi is the country's first elevated light rail transit line, which was officially completed and put into commercial service in November 2021. This highlights that the UMRT Line HN2A is the first railway line in Vietnam with an operational safety assessment that was launched and will remain for the whole life cycle. Its advantages include a large capacity and more complicated rolling stock and infrastructure, as well as a modern communication-based train control (CBTC) signaling system and automated driverless train without the need for operator intervention [5]; however, with the increase in modern up-to-date technology, it is vitally important that the Vietnamese railway undertake the promotion of safety in train operations.

A thorough collection and full analysis of the risk data needs to be completed, which of course will take time. Accident and incident scenarios can be predefined to ensure, as far as is reasonably practicable, that the appropriate and proportional risk assessment and mitigation measures are in place to prevent or minimize the severity of future failures of the rail system. Therefore, the research team chose fault tree analysis (FTA) as an easy-to-implement technique that enables quick monitoring and assessment of the risks connected with each set of components in the operating organization. The FTA method is a fairly straightforward technique to expand and update data, as well as other technical research, to increase the model's estimation accuracy. As a result, while this method is not necessarily innovative, it was found to be well adapted to the current development conditions of the Vietnam railway industry. Furthermore, this risk analysis assessment method is compliant with EN 50126, which is in accordance with the latest globally recognized system safety management techniques.

Risk in the railway sector can be defined in relation to accidents and incidents leading to fatalities and/or injuries of people as well as damage to the rail infrastructure or other property [6]. Railway-related accidents/incidents can occur for many reasons during operation, including human error, poor maintenance, and system failure [6, 7]. Amongst these failings, train collisions are one of the most unexpected and damaging in terms of costs and loss of service revenue, as well as the possibility of severe injury (or worse) to passengers during railway operations. Due to high operational frequency, collisions have a potential for greater damage than other forms of railway accidents [7–9]. As a result, studying train collisions for urban railway operations is crucial for increasing operational management capacity. The findings of this study are part of the establishment of the safety management system for Hanoi Metro Company.

From this point of view, the objective of this work is to study and develop the process to fully analyze the probability of generic train collision accidents in metro operations of the elevated light rail transit UMRT Line HN2A, as applicable to partly establishing the safety management system in Hanoi Metro Company. The primary purpose of this paper is to resolve the following research issues:

1. The literature review provides an overview of general published risk management procedures and systematic and precise methods for evidence-based hazard identification and classification influencing operational safety. This section also discusses the applicability of these methods for various types of railways, focusing on the FTA method to identify hazard with a view to further developing collision analysis in Line HN2A.
2. The analysis of generic accidents in the operation of Line HN2A is recommended through the implementation of FTA. To assess the basic error and failure frequency leading to train collisions, two types of collisions based on their design and the results of testing and commissioning will be classified. Following that, the FTA approach is used to determine the probability of each sub-failure and compute the hazard severity and rate of train collision occurrence. To validate and identify deviations and severe errors, the theoretical calculations are compared with error data collected during actual operation of Line HN2A. Sub-failures that deviate significantly from reality and theory must be identified and studied to determine the causes.

3. Based on a comparison with the technical design and the operational plan results using data from operation tests in 2018 and 2020 and commissioning in 2021 of the Hanoi UMRT line, the theoretical model of the FTA method is suitable for the UMRT system in Vietnam. The theoretical model will be further used to develop a new scientific and evidence-based method to perform the risk assessment. The real-time accident and operation data will be collected and compared with the theoretical model to improve the accuracy of the results. This method can be an invaluable tool, not only for the UMRT Line HN2A, but also for all other urban railway systems in Vietnam, thus providing a complete specific and global update of the current risk assessment methodology.
4. The theoretical calculation shows that human error (44%) and vehicle technical conditions (33%) are major factors contributing to train collision probability. Furthermore, real testing data of HN2A indicated the additional problem of wheel–rail adhesion. Therefore, this research suggests several solutions to improve operations through enhancement of human performance, technical testing, and preventative and corrective maintenance, thus providing solutions to improve Vietnam's risk management principles and practices for whole urban railway systems in Vietnam, and ultimately resulting in consumer and stakeholder confidence through a much-improved operational safety regime.

2 Literature Review

2.1 General Risk Management Procedure

Risk management is the process of identifying risks and taking actions to eliminate or mitigate them (to the extent that is deemed reasonably practicable) through the implementation of control mechanisms. Risk management refers to the process of lowering risk to a level that is deemed tolerable and ensuring the control, monitoring, and public communication of those risks [10]. Additionally, risk management can be defined as the collection of cultures, processes, and structures aimed at capitalizing on prospective possibilities while mitigating negative consequences [11]. The risk management procedure applied for a railway system basically follows the common safety method, including (i) establishing the context to determine the situation to be analyzed, (ii) risk (hazard) assessment to determine the risk with respect to a particular situation, through risk identification, risk analysis, and risk evaluation, and (iii) risk mitigation by selecting interventions to reduce risk.

2.1.1 Hazard Identification

From the Office of Rail Regulation (ORR) [12] and Galante [10], in risk analysis, a hazard is described as a condition which can lead to accidents, such as damage to trains, technical equipment, humans, assets, or the environment. The purpose of the hazard identification step is to identify and enumerate all reasonably predictable risks associated with the intended operation of the system in its normal operational environment; these risks are then further analyzed and measured in the next steps [12, 13]. Hazard identification is not only to establish a list of risk factors that can lead to failure and safety breaches, but also to identify the importance of each risk factor and the associated interactions [13, 14]. Based on the guidelines of ORR [12] and Boyle [15] for the systematic identification of hazards, it is imperative to take into account the following factors: (i) system requirement specifications and system design description, (ii) system life cycle including maintenance, (iii) maintained conditions of operation, (iv) human factors influencing the operation, and (v) relevant foreseeable failures. Focusing on assessing the most important risks for operations, hazards will be classified depending on the risk of accidents, with forecasting of the potential severity and possible damage that may occur because of the hazard. There are different methods for systematically identifying hazards. These methods can be used separately or simultaneously, depending on the object in need, and include (i) FTA, (ii) failure mode and effect analysis (FMEA) or failure mode, effect, and criticality analysis (FMECA), and (iii) hazard and operability (HAZOP) studies [10, 11, 14, 16].

Diverse and comprehensive risk identification investigations are a prominent topic of research in railway operations studies. These studies are conducted on several subsystems of the railway system or a particular type of accidents, for instance tracks and infrastructure, [17–19], rolling stock [20, 21], derailments and train collisions [22–26], signaling and control systems [27–29], and railway staff and safety culture [30]. In general, these studies are conducted in one of two ways: (i) by providing an overview of accident statistics and analyzing types of generic hazards, or (ii) by modeling a subsystem or a typical failure/accident/incident using quantitative methods such as Petri nets, Bayesian networks, or Monte Carlo simulation. The outcome of this approach is typical accident patterns and the proportion of common safety hazards, from which one may derive a strategy, regulation, or processes for global safety management legislation, setting out guidelines in the national railway sector. The results of such an approach are frequently employed at the system or subsystem level to increase the capacity or reliability of a component or subsystem. Although these results are very precise and have tremendous value in technical analysis, the system must be operational. From this analysis, it is obvious that there are fundamental differences between establishing risk analysis research in developed railway industries such as Europe, China, the USA, and Japan, which have developed the ability to manufacture their own system components, and in countries with less developed railway systems that do not manufacture their own railway components. To be able to manage the imported modern railway system, these countries require more extensive studies than the aforementioned methods (i), but as of today, they lack the necessary technological basis to conduct studies according to the approach (ii).

2.1.2 Hazard Classification

Hazard classification is the next step after the hazard is identified. The identification of a hazard and all related accidents must be combined with the hazard classification process. The possibility of a risk event occurring is determined, as is the possible impact of that risk not only in the initial cost of re-establishing a safe operating system but additionally the impact to the system's revenue, schedules, and performance, and consumer confidence in using the system. This assessment begins by evaluating these effects and assigning a probability and severity scale score to each using semi-quantitative risk assessment and graphs [5, 31]. Applying this technique to the UMRT management in Vietnam, classification of hazard aims at assessing accidents according to the most important risks in the metro operation and prioritizing hazards to be removed in each operational stage. By classifying and quantifying all of the individual risks, it is possible to determine the risk mitigation [32]. In all subsystems of Hanoi UMRT, and specifically in Line HN2A [4, 33], classified risks will be assigned to one of four groups depending on frequency of occurrence and severity (maximum severity: > 03 fatalities or > 11 injuries or damage > 1.5 billion VND; minimum severity: 1–5 injuries or asset damage from 20–100 million VND).

2.1.3 Hazard Management

Hazard management is regulated so that every hazard, at all levels, potentially affecting the safety of the line operations must be recorded and stored in a hazard log for monitoring, management, and records, throughout the operational life cycle of the line. The information contained within the hazard log is essential for managing risk, and therefore ensuring that the content is accurate and systematic is paramount [16, 32]. The positions allowed to update hazard logs are specified in the regulations of the UMRT Operation and Management (O&M) company. In the first operational stage of Line HN2A, where there are no accident reports or statistics, the line's hazard log will be created based on documents including preliminary hazard analysis (PHA), system hazard analysis (SHA), subsystems hazard analysis (SSHA), and interface hazard analysis (IHA). Documentation of the hazard log in the whole Line HN2A and its subsystems should be used to create a template to be utilized for the whole life cycle of the line.

2.2 Fault Tree and Event Tree Analysis

FTA is a top-down deductive analytical approach for translating a physical system into a logical diagram. FTA may be qualitative, quantitative, or both, depending on the scope of the analysis [10, 16]. The main objectives of FTA are (a) to identify all possible combinations of basic events that may result in a critical event in the system, (b) to find the probability that the critical event will occur during a specified time interval or the frequency of the critical event, and (c) to identify aspects of the system that need to be improved to reduce the probability of the critical event.

All the events in an FTA are connected to logic gates [16, 34]. Logic gates represent the logical relationship between output and input events. In a particular analysis of a system, these logic gates explain how failures of one or several components or subsystems combine and lead to an unexpected consequence. According to [35], the five main logic gates in FTA are as follows: (i) AND gate—the output event occurs only if all input events occur; (ii) OR gate—the output event occurs if any input events occur; (iii) PRIORITY AND gate—the output event occurs only if all the input events occur in a specified sequence, which is usually from left to right; (iv) Exclusive-OR (EXOR) gate—the output event occurs only if exactly one input event occurs, while no other input event occurs; (v) INHIBIT gate—the output event occurs if one input event and additional conditions occurs at the same time.

The study of events using FTA is a probabilistic and graphical approach to modeling and analyzing accident situations [16]. The technique uses inductive and logic methods with a tree-like graphical representation of sequential events. The generated figure depicts several accident scenarios (i.e., event sequences) that might occur in the aftermath of a specified hazardous event. The event tree analysis (ETA) illustrates the system's response to the dangerous occurrence. External events that have an effect on the accident scenario may also be taken into account and included in the ETA [36, 37].

FTA and ETA are widely used in cause–effect analysis of railway accidents and incidents, for example, in the studies of Dindar et al. [38], Ruijters [39], Bearfield and Marsh [40], Liu et al. [41], Lin et al. [42], and Doytchev and Szwillus [43. However, few studies have been conducted on urban railway systems, with the majority of research focusing on risk analysis for high-speed railways or intercity rail passenger and freight lines. There are comparatively very few case studies for developing countries with obsolete railway infrastructure and a lack of managerial expertise. This study focuses on using FTA to analyze generic accidents in metro operations. The content of this article is an integral part in establishing the safety management system in Hanoi Metro Company, as the article will fully analyze a specific type of generic accidents, namely train-to-train collisions.

3 Research Method and Procedure

3.1 Step 1: Overview and Operational Assessment of UMRT Line HN2A

This report provides an overview of the UMRT Line HN2A and its fundamental technical features based on its technical design and operational environment circumstances. The infrastructure is introduced, including the subsystems that comprise the system, most notably the signal and control system. From there, a risk analysis is undertaken on a serious hazard scenario in the railway operation, as a train collision.

3.2 Step 2: Establishing Fault Tree Analysis to Assess the Basic Error and Failure Frequency Leading to Train Collisions

Train collisions are classified into two types: (i) train-to-train collisions and (ii) collisions with a stationary train/or a portion of that train that is not in operation at the time of the impact. Train-to-train collision is caused by six major failures, each of which is further subdivided into particular sub-failures. The reason for a collision with a train or a portion of a train that is not in operation is classified into three major categories of failure, each of which is further subdivided into particular sub-failures. Following that, the research uses the FTA approach to determine the probability of each sub-failure and to compute the hazard rate for train collision occurrence.

Fault tree with a single AND gate: Let $Ei(t)$ indicate that the event Ei (human error or technical failure) occurs at time t, $i = 1,..,n$. Since the TOP event will occur if and only if all the basic events occur, the Boolean representation of the fault tree is

$$\mathrm{TOP}(t) = E_1(t) \cap E_2(t) \cap \ldots \cap E_n(t) \tag{1}$$

The probability that the event occurs at time t is denoted as $Qi(t) = \mathrm{Pr}(Ei(t))$. Assuming that all events $Ei(t)$ are independent, the probability of the TOP event at time t, $Q(t)$, is expressed as

$$Q(t) = Pr(E_1(t) \cap E_2(t) \cap \ldots \cap E_n(t)) = Pr(E_1(t) \cap Pr(E_2(t)) \cap \ldots \cap Pr(E_n(t)))$$

$$Q(t) = q_1(t).q_2(t) \ldots q_n(t) = \prod_{i=1}^{n} q_i(t) \tag{2}$$

Fault tree with a single OR gate: Any of the basic events will cause the TOP event to occur, and the Boolean representation is

$$\mathrm{TOP}\ (t) = E_1(t) \cup E_2(t) \cup \ldots \cup E_n(t) \tag{3}$$

Assuming that all events $Ei(t)$ are independent, the probability of the TOP event at time t, $Q(t)$, is expressed as $Q(t) = Pr(E_1(t) \cup E_2(t) \cup \ldots \cup E_n(t)) = 1 - Pr(\overline{E}_1(t) \cap \overline{E}_2(t) \cap \ldots \cap \overline{E}_n(t))$

$$Q(t) = 1 - \left(1 - q_1(t)\right).\left(1 - q_2(t)\right) \ldots \left(1 - q_n(t)\right) = 1 - \prod_{i=1}^{n}(1 - q_i(t)) \tag{4}$$

Any fault tree diagram can be represented as an alternative fault tree diagram with a single OR gate with all the minimal cut set failures as input events; therefore, the probability $Q_0(t)$ of the top event at time t is expressed as

$$Q_0(t) = \mathrm{Pr}(C_1(t) \cup C_2(t) \cup \ldots \cup C_k(t)) \tag{5}$$

in which $Cj(t)$ is the probability that the minimal cut set j fails at time t, where $j = 1,...,k$. The minimal cut set j will fail at time t when all the basic events $Ej,i(t)$ in Cj occur at time t. The minimal cut set failure, $Ci(t)$, can therefore be represented as a fault tree with a single AND gate. Using m to denote the number of basic events in the minimal cut set Cj, the probability that minimal cut set Cj fails at time t can be expressed as

$$\mathrm{Pr}\left(C_j(t) = \mathrm{Pr}(E_{j,1}(t) \cap E_{j,2}(t) \cap \ldots \cap E_{j,m}(t)\right) \tag{6}$$

We obtain

$$Q_0(t) = \sum_{j=1}^{k} \mathrm{Pr}\left(C_j(t)\right) - \sum_{i<j} \mathrm{Pr}\left(C_i(t) \cap C_j(t)\right) + \sum_{i<j<l} \mathrm{Pr}\left(C_i(t) \cap C_j(t) \cap C_l(t)\right) - \ldots + (-1)^{k+1}.\mathrm{Pr}(C_1(t) \cap C_2(t) \cap \ldots \cap C_n(t)) \tag{7}$$

3.3 Step 3: Comparing the Theoretical Results

The research compares theoretical calculations with error data collected during the testing and commissioning of the UMRT Line HN2A in order to determine whether the theoretical calculations are congruent with reality. Sub-failures that deviate significantly from reality and theory must be identified and studied for causes. ETA is utilized at this stage to determine the probability of train collisions based on the error rate of the sub-failure documented in the operation report.

3.4 Step 4: Recommendations

Through hazard identification and quantification, significant sub-failures which contributed to train collisions will be demonstrated. Additionally, the statistical data gathered reveal significant errors in actual operation. The research also highlights several of the key points of operation and maintenance solutions aimed at enhancing the system's technical conditions, addressing human safety performance concerns, and monitoring and utilizing accident data for risk management.

4 Overview and Operational Assessment of UMRT Line HN2A

4.1 Overview of UMRT Line HN2A

Hanoi Urban Railway Cat Linh–Ha Dong Line UMRT Line HN2A is a 13,021.48-m-long elevated light rail transit project with a total of 12 stations (Fig. 1). With an average distance between stations of 1151 m, this will be the main southwest traffic route in the urban transport network of Hanoi city. One rolling stock depot with an integrated functional maintenance center and operation control center (OCC) is deployed in this line and located at the southeast of Ha Dong station. All 13 trains operate as four-car trains, with a designed maximum speed of 80 km/h, and will be operated in the initial stage of HN2A project with a service speed of 35 km/h. HN2A is a fully automated system, being operated and controlled under a moving block–communications-based train control (CBTC) signaling system (Fig. 2). The trial operation of the HN2A project occurred from October 2018 to December 2018, with a full-scale test run from December 12, 2020, to December 31, 2020, in order to check the operational safety before it was approved for commercial service. On November 6, 2021, Line HN2A was put into commercial operation. The equipment of the entire UMRT Line HN2A Cat Linh–Ha Dong is designed for installation and use for typical environmental conditions of Hanoi city. Outdoor equipment must be suitable for use in naturally occurring environmental conditions and in

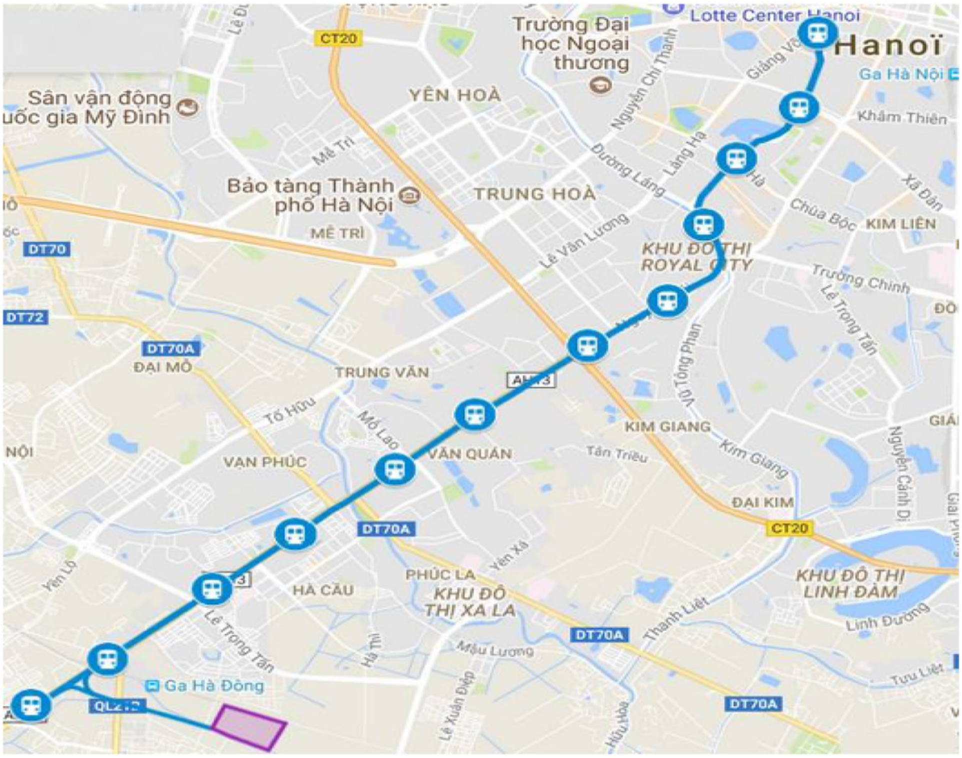

Fig. 1 Overview of Hanoi Urban Railway Cat Linh–Ha Dong Line UMRT Line HN2A

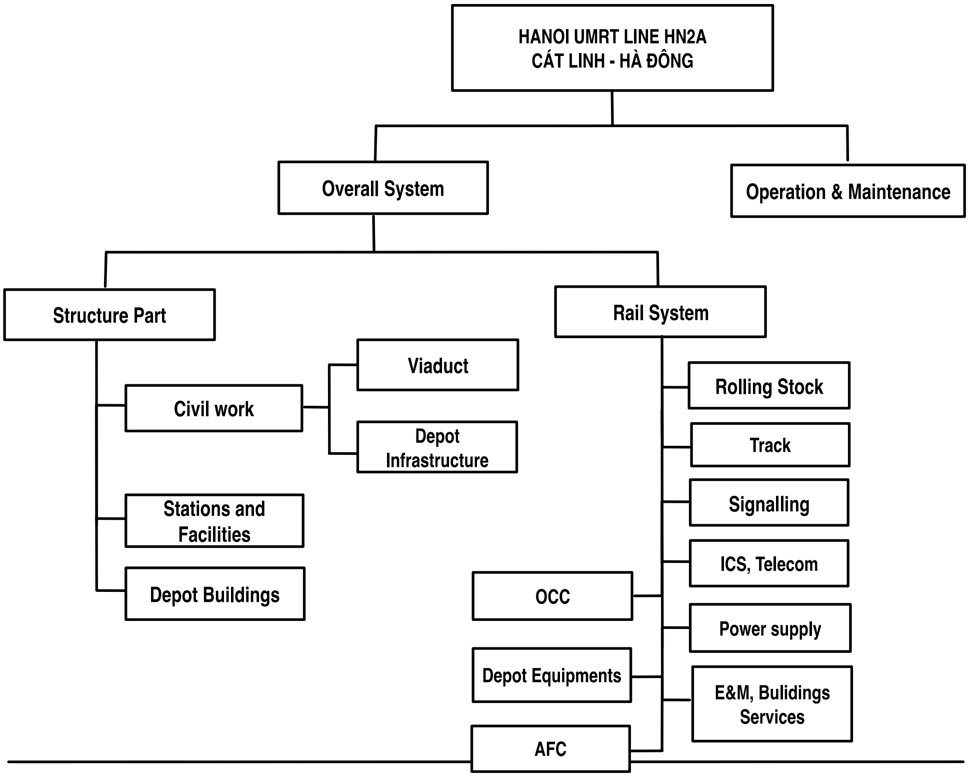

Fig. 2 Structure of UMRT Line HN2A subsystems

natural ventilation, with the ability to resist water, moisture, rain, and flushing ingress. The project's environmental risks mainly comprise earthquakes, floods, and storms.

4.2 Signaling and Control System

Line HN2A is operated under a continuous communications-based system with three operating levels and four driving modes. The three levels of operation are the CBTC, intermittent train control (ITC), and interlocking. CBTC mode is normal mode, and ITC and interlocking are degraded in modes 1 and 2, respectively. The four driving modes for operational use are (i) AM, or automated driving under automatic train protection (ATP) supervision, whereby train operation is granted through a radio system, and track-side signals are set to the "off" position; (ii) CM, which is manual train driving mode under the supervision of ATP, and the track-side signals are set to the "on" position; (iii) RM, which is restricted manual train driving mode, where the safety of train operation is ensured by a combination of interlocking equipment, onboard ATP, dispatch staff, and train drivers; and (iv) NRM, or non-restricted manual mode, in which an onboard signaling system is set to the non-available state, and the train driver operates only with a direct dispatch command and displays of the track-side signals [33, 44].

The CBTC system of Line HN2A is schematically sketched in [44] and shown in Fig. 3. The entire main line

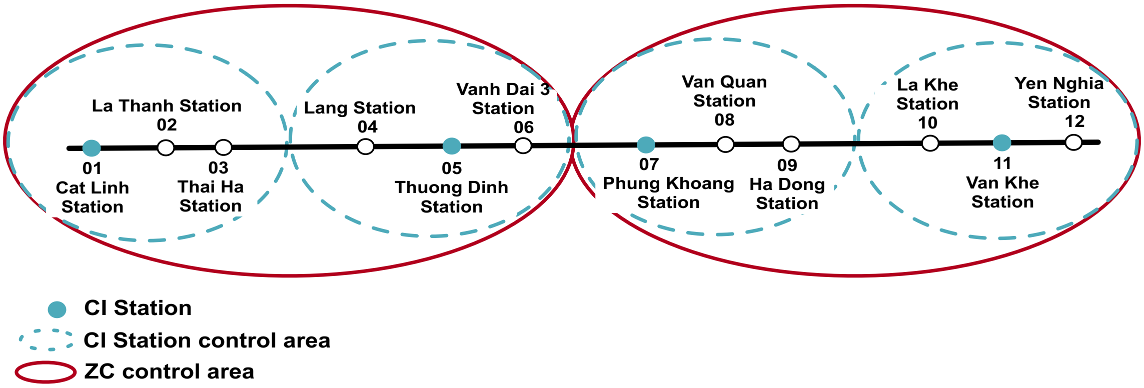

Fig. 3 Zone of interlocking control for UMRT Line HN2A subsystem

is divided into four interlocking zones, each equipped with central interlocking (CI) and local automatic train supervision (ATS) equipment, which is located in Cat Linh, Thuong Dinh, Phung Khoang, and Van Khe stations. Line HN2A adopts the LCF-500 CBTC system from Traffic Control Technology (TCT), which consists of ATP/automatic train operation (ATO), CI, data communication system (DCS), ATS, and maintenance support system (MSS) subsystems. The distributed monitoring system (ATS) and train protection system (ATP) provide train headway control and overspeed protection. The train auxiliary operation system (ATO) is to realize automated operation based on ATS command, with temporary speed restriction/permanent speed restriction (TSR/PSR) conditions which are under ATP protection. Four station control area CIs are failure-safe mode systems, in order to realize normal basic interlocking function. In the CBTC control level, CIs provide related route information in accordance with moving block requirements, and control area zone controllers, whose equipment was installed in the Cat Linh and Van Khe stations, send the movement authority to trains. At the ITC control level, CIs provide related route information in accordance with fixed block requirements and send movement authority via a balise. A data communication system (DCS) realizes data transmission between wayside and onboard systems. MSS offers an equipment work status monitoring and maintenance support function for the CBTC system. Wayside signaling equipment includes signals, switch points, axle counters, Lineside Encoder Unit (LEU), variable balises, and loop and fixed balises.

The driving mode meeting conditions can be manually or automatically activated, and the onboard ATP/ATO equipment records and displays. When the train operates on the access route, it receives the effective ATP information, and the system can automatically activate the train driving mode, or the train driver confirms the driving mode activated. To ensure operational safety, when in the non-automatic train control (ATC) zone, the RM and NRM methods must be used, and the appropriate safety operation must be used. When the train driving mode is degraded, the train must stop and/or not stop to activate the driving mode; when the driving mode is upgraded, it requires no stop to activate. Trains entering and leaving the depot must stop the train and not stop the train to change the driving modes, respectively. The first operation stage uses headway time of 6 min, the second of 4 min, and the next of 2–3 min.

4.3 Determining Risk/Hazard Scenarios

According to EU railway accident classification, railway accidents are classified into six types: train collisions, derailments, level crossing accidents, accidents to persons, fires in rolling stocks, and other accidents [9, 32, 45]. Japan railway accident classification for tramways also includes six types of accidents, namely train collisions, train derailments, level crossing accidents, accidents involving road traffic, and other accidents with casualties [46]. This classification is also in complete alignment with studies of the International Union of Railways [47]. In the UMRT Line HN2A, based on the technical design and the above international practice of classification, risks related to collision (including train-to-train collisions and collisions with an obstacle), derailment, and fire hazards are generic operational risks. In the case of Line HN2A (note that UMRT is the representative name of the urban railway system in Hanoi, in which Line HN2A is a light rail transit system), there is currently no level crossing, and hence it is not taken into consideration in this study. To analyze incidents leading to this accident type, specific conditions must be considered. To analyze and estimate the frequency and risk of each of the collision hazards, FTA is performed as discussed in the next section.

As stated in the preceding paragraph, collisions between trains can be divided into two hazard categories: (i) train-to-train accidents (and train collisions with part of a train not in operation) and (ii) collisions with other objects (components of infrastructure, objects dropped/thrown into areas of operation, vandalism-related objects, and people/animal protected operating areas). For group (i) accidents, subjective system causes such as technical failure, protection system failure, and human error will be the primary causes. This group includes the study of accidents in order to gain a better understanding of the system's possible hazards and to identify technological or procedural solutions for the system. The primary causes of accidents in group (ii) are objective external factors or the violation of railway safety norms by individuals outside the system. The information regarding this type of accident is quite variable. In the early stages of operation, it is impossible to correctly assess the database for these types of accidents. Therefore, for the operating company, safeguarding and rescue measures to cope with this type of accident are more important than evaluating its cause in depth. Thus, train-to-train collisions are the subject of this project's inquiry and analysis.

As there have been no accident reports in the early stages of operation of Line HN2A, the risk frequency estimates are referenced from the technical design of Line HN2A and similar European systems, and the accident data are published in [2, 8, 9]. The risk assessment procedure for Hanoi Metro Company is based on three levels of management: (i) Preliminary hazard analysis (PHA) is used for top-level management or at the initial phase of projects to provide an overview of hazard and risk mitigation and logical thinking of risk identification. FTA is established in the technical management process. This technique is well suited for assessing complicated systems with numerous components and variable hazard occurrence under various operating situations. This technology enables the creation of an open database for the study and updating of discrete components. Bayesian networks (BN) are used in analyzing specific hazard scenarios to assess the impact of each factor in the probability of occurrence, thereby enabling the proposal of appropriate risk control measures. This highlights that, to date, the UMRT Line HN2A is the first and only urban rail line in Vietnam. It was put into commercial service in November 2021 with an operational safety assessment launched for the first time, and remains in effect for the whole life cycle. Meanwhile, all the national main lines with narrow gauge 1000 mm are too old and outdated in terms of infrastructure and technical standards that need to be renovated. Additionally, none of them has been evaluated for proper safety compliance with any standardized method. To the best of our knowledge, this is the first report of the chosen safety assessment method for Line HN2A, and this method is tested with actual data collected by the research team during the testing and commissioning to the date of this article.

The data were collected in two ways: First, for statistics regarding the operations of Vietnam Railway, Metro Line HN2A is the first metro line in Vietnam, and hence no comparable technical systems exist. In this study, however, the working style and safety attitudes of railway personnel are employed to evaluate driver faults. From 2010–2020 accident data and a survey on safety attitudes [48], we demonstrate that the chance of human error in Vietnam is relatively high compared with data collected systematically in Europe and Japan [48]. Consequently, the study focuses on the proportion of driver errors in urban railway accidents, thereby strengthening the solutions linked to the operational process of urban railway systems, which are detailed in the subsequent sections. The second method of data collecting utilizes failure rate or accident raw data extracted from accident reports of urban railway systems/railway systems around the world. When applied to Vietnam's circumstances, these data should be analyzed and modified to accommodate specific operational requirements (operating frequency, passenger traffic, environmental conditions). In the PHA technique, these estimates/changes are made during the system specification, manufacturing, and acceptance phases. These data are referenced and implemented in conjunction with recommendations from manufacturer experts in technical design and safety certification experts in system validation and acceptance. However, these are still theoretical data. Therefore, during the testing phase and initial commercial operation phase, the operating data and actual error data are compared with the theoretical data to determine whether they are accurate. The purpose of this research is to provide an evaluation method and a database for risk evaluation. Consequently, data comparison and completion are performed regularly, both after this paper and in later research.

The evaluation results published in the article show that this first completely new safety assessment method to date is properly applicable for Line HN2A. The research is still continuing to observe up-to-date operational data to perform hazard updates and evaluations of Line HN2A. These findings significantly highlight a straightforward method suitable for safety assessment, which although commonly used for railways in developed countries, is being applied for the first time in Vietnam, approved through application to Line HN2A. In conclusion, these are basic calculations, easily applicable, and could be standardized for technical management of other railway lines in Vietnam. Within the scope of this paper, the research focuses on analyzing and calculating train collision hazards by FTA.

5 Risk Analysis for Collision Hazard by Fault Tree Analysis for UMRT Line HN2A

5.1 Clarifying the Main Failure of Train Collisions in Line HN2A

Train collisions are usually divided into two incident groups: train-to-train collisions and train collisions with a train/part of a train out of operation, as described in the following:

1. Train-to-train collisions might have resulted from C3-Miscommunication, C4-Failure in ATP system, C5-Driver error, C6-Failure of railway vehicle, or C7-Infrastructure problems. Collision with a train or part of a train that is out of operation might have resulted from C8-Failure in ATP system, C9-Failure of railway vehicle, or C10-Driver errors (See Fig. 4).
2. Train collision with a train/part of a train out of operation might have resulted from C8-Failure in ATP, C9-Vehicle failure, or C10-Driver errors. The occurrence of a hazard scenario is contingent upon the breakdown of technical components or human error in operation and the occurrence of a trigger event, such as the presence of a train in a hazardous location. For each case, the chance of a trigger event is different, resulting in a distinct hazard rate; consequently, different probabilities exist for the same failures, such as failure in the ATP system, failure of railway vehicles, and driver failure.

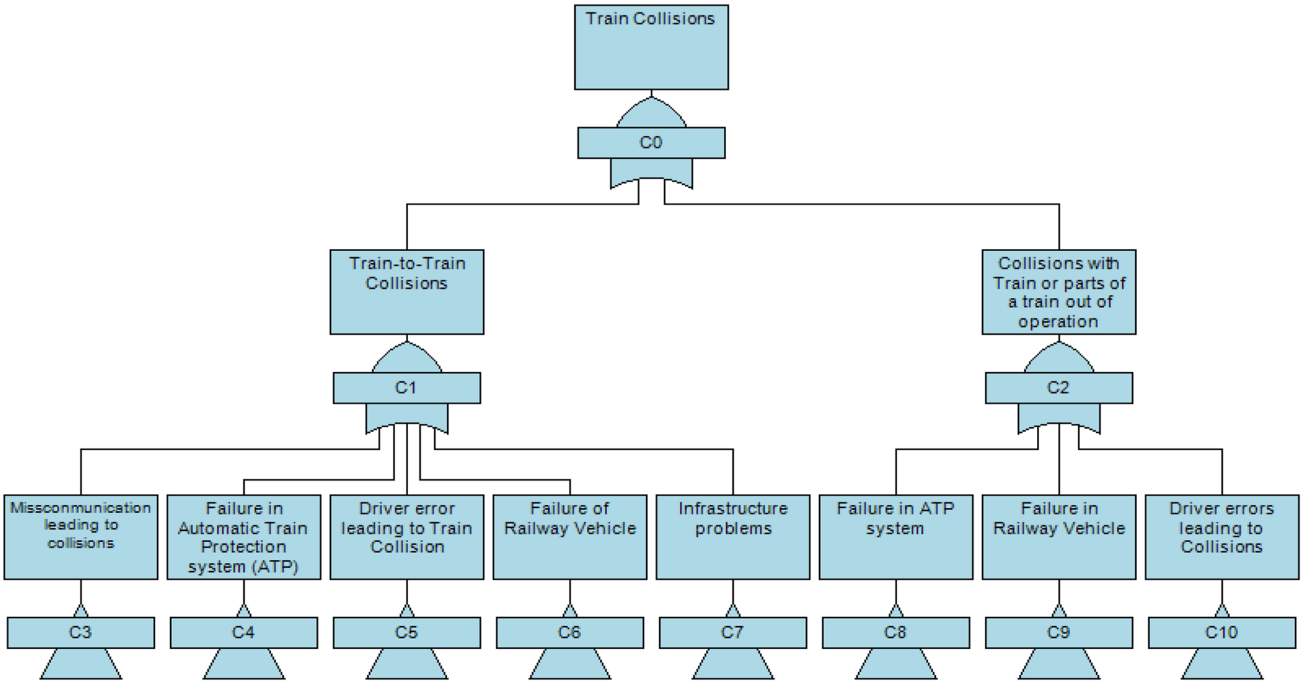
Train Collisions
C0
Train-to-Train Collisions
Collisions with Train or parts of a train out of operation
C1
C2
Missconmunication leading to collisions
Failure in Automatic Train Protection system (ATP)
Driver error leading to Train Collision
Failure of Railway Vehicle
Infrastructure problems
Failure in ATP system
Failure in Railway Vehicle
Driver errors leading to Collisions
C3
C4
C5
C6
C7
C8
C9
C10

Fig. 4 Fault tree analysis of train collisions

5.2 Calculating the Failure: Miscommunication and Failure of ATP

Using modern monitoring and control systems, railway operators in the OCC can remotely control a large area and complex system. Existing signaling systems give us all the information (status) about the signaling elements (points, signals, routes, level crossings, etc.) and ensure that all train movements are coordinated and comply with timetable-based dispatching. The sub-failure and hazard rates are collected and calculated from [49, 50] (Table 1, Fig. 5).

Additional responsibilities associated with modern safety communication systems include operating passenger information systems, monitoring the catenary system, and controlling alarm systems, which are a significant portion of the operator's workload. According to [42, 51], the following are the most common types of operator and ATP system errors:

- Human error comprises the following types of errors: (i) diagnostic and decision-making errors, which are caused by a misunderstanding on the part of operators; (ii) errors of commission, which occur when an operator performs

Table 1 Probability of top event miscommunication and failure in ATP (10^5 km-operation)

No.	Top event	Sub-failure	Hazard rate
C3	*Miscommunication leading to collisions*		*2.92E−03*
C3.1		Wrong information between train driver and dispatcher	1.38E−03
C3.2		Misunderstanding between driver and dispatcher	1.04E−03
C3.3		No information between driver and dispatcher	5.00E−04
C4	*Failure in automatic train protection system (ATP)*		*6.48E−05*
C4.1		Train operated in manual operating mode and not protected against other train operated in ATC and limited operating method	3.19E−05
C4.2		Disruption/corruption of train control and management system	1.02E−06
C4.3		Failure in ATC input data	3.19E−05

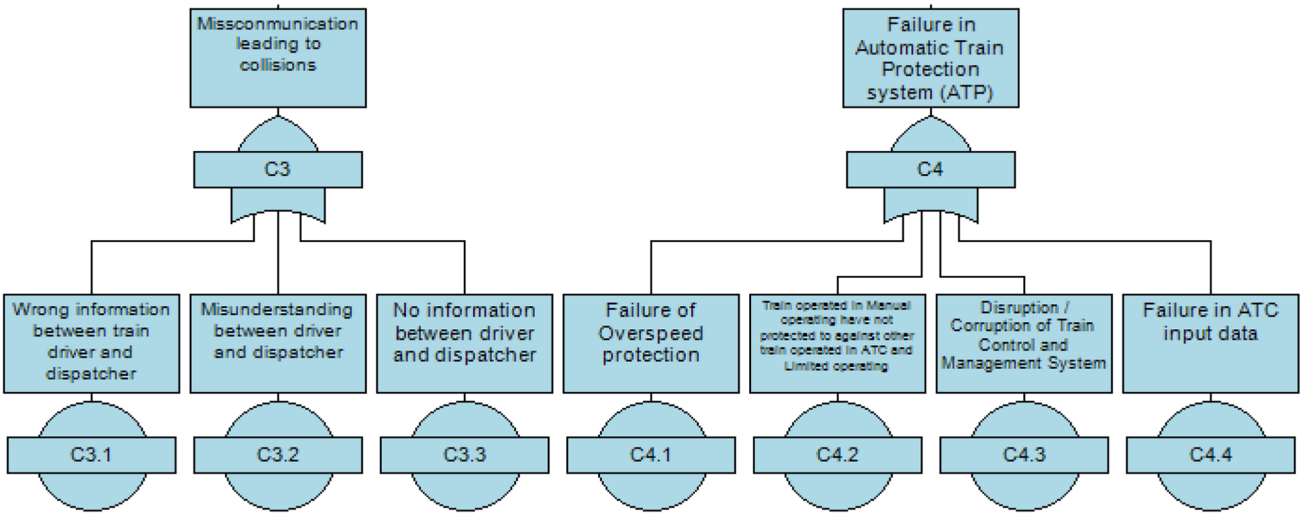
Missconmunication leading to collisions
C3
Wrong information between train driver and dispatcher
Misunderstanding between driver and dispatcher
No information between driver and dispatcher
C3.1
C3.2
C3.3
Failure in Automatic Train Protection system (ATP)
C4
Failure of Overspeed protection
Train operated in Manual operating have not protected to against other train operated in ATC and Limited operating
Disruption / Corruption of Train Control and Management System
Failure in ATC input data
C4.1
C4.2
C4.3
C4.4

Fig. 5 Fault tree analysis of top events: miscommunication and failure in ATP

an action that is both erroneous and not required by the system; (iii) misunderstanding between the operator and the driver as a result of the omission of critical information.

- ATP technological failures include (i) problems in software programming/processing; (ii) failure/corruption of the train control and management system; (iii) disconnection/failure of the data input.

5.3 Calculating the Failure: Driver Error

Driver error and faulty action are frequently combined in a railway accident, leading to the driver's failure to prevent the accident. In an accident, the driver's concentration and assessment are compromised, resulting in judgment errors of approximately 2% to 6% [52]. Based on the support of modern technology in railway control and monitoring, our calculation assumed that this error is around 2.5%. A fatigue problem, attention, violation of regulations, or environmental conditions could all be factors contributing to the errors in judgment. The error actions of the driver might be (i) failing to check aspect of signals, (ii) false reaction to caution signal, (iii) ignoring or violating the safety rules, or (iv) insufficient information from ATC, signal light. Rule violations in the Vietnam railway industry are a significant problem, as in the safety perception survey [39], with a high proportion of answers citing the influence of alcohol or illicit drugs compromising rail safety or using a form of entertainment while on duty (Table 2, Fig. 6).

Table 2 Probability of top events: driver errors leading to collisions (10^5 km-operation)

No.	Top event	Sub-failure	Hazard rate
C5	Driver error leading to train collision		5.12E−03
C5.0	Driver errors		2.56E−01
C5.1		Drivers failed to check aspect of signal/read wrong signal	3.75E−02
C5.2		Drivers failed to react to caution signal/misjudgment	3.75E−02
C5.3		Drivers ignored or violated safety rules	5.00E−02
C5.4		Conflict warnings	5.00E−02
C5.5		Bad visibility from driving cab	6.75E−02
C5.6		Insufficient front/rear lighting in driving by line of sight	1.35E−02
C5.7	Probability of human error resulting in an accident		2.00E−02

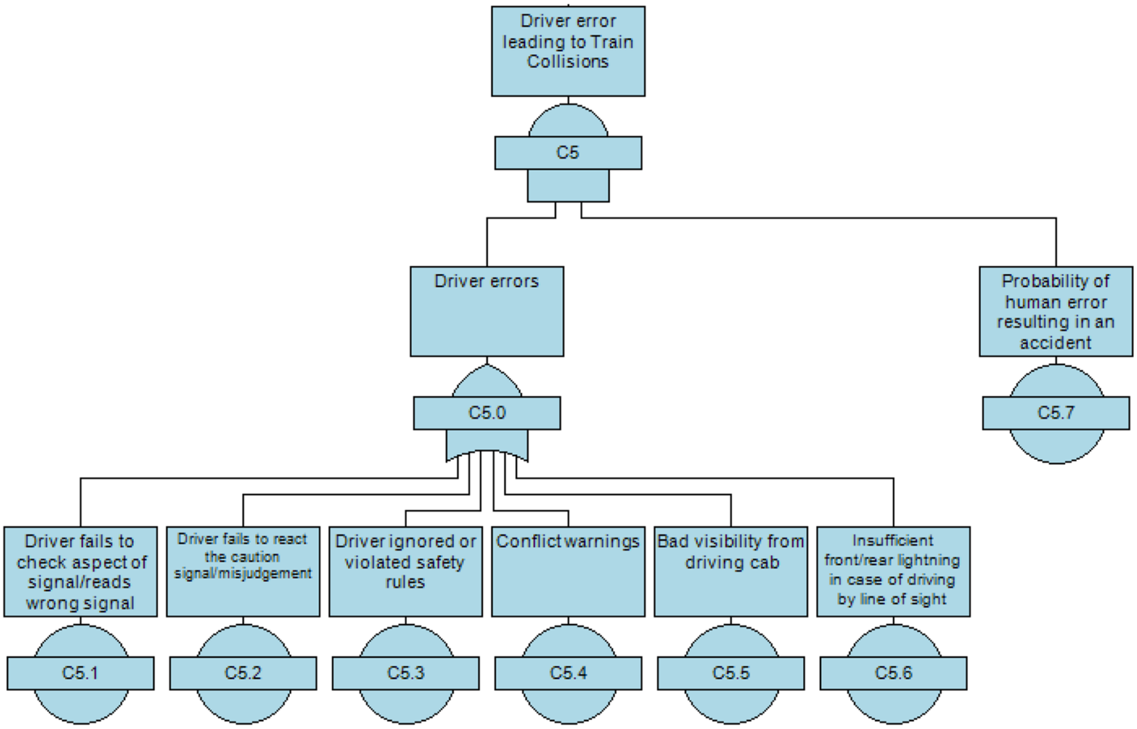
Driver error leading to Train Collisions
C5
Driver errors
C5.0
Probability of human error resulting in an accident
C5.7
Driver fails to check aspect of signal/reads wrong signal
C5.1
Driver fails to react the caution signal/misjudgement
C5.2
Driver ignored or violated safety rules
C5.3
Conflict warnings
C5.4
Bad visibility from driving cab
C5.5
Insufficient front/rear lightning in case of driving by line of sight
C5.6

Fig. 6 Fault tree analysis of top events: driver errors leading to collisions

5.4 Calculating the Failure: Vehicle and Infrastructure

The category of technical equipment factors contains potential failures on the rolling stock or on technical facilities. Rolling stock failures mainly include the following: (i) locomotive—running gear failure, traction motor failure, crank case, oil or fuel fire, electrically caused fire, third rail/pantograph defect, onboard computer failure to respond; (ii) bogie—broken bogie frame, defect on suspension (primary or secondary), failure of the damper; (iii) wheels—broken or damaged flange, broken wheel plate, broken or loose wheel rim, thermal crack; (iv) coupler—broken knuckle, coupler mismatched, broken coupler carrier or shank, failure of articulated connectors; (v) axle set—broken or defective wheel shaft, roller bearing defect, hot box; (vi) vehicle body—broken or defective bolster, broken or defective traction beam, broken or defective center plate, broken draft or center sill, loss of integrity; (vii) brake system—detrition of brake shoe, broken or defective brake disc, blockage of brake line, uncoupled air or hydraulic hose, obstructed brake pipe [53]; (viii) improper structural design of rolling stock [2, 49, 50, 53] (Table 3, Fig. 7).

As a result of the problem with the railway infrastructure in collision accidents, adhesion is diminished. Hence, the ability to stop trains is inhibited, potentially resulting in signals passed at danger (SPADs), station platform overruns, and crashes. Furthermore, it has the potential to cause damage to rails, requiring regrinding and premature replacement, as well as failure to activate track circuits, which could have serious implications.

Table 3 Probability of top events: failure of vehicle and failure of infrastructure (10^5 km-operation)

No.	Top event	Sub-failure	Hazard rate
C6	Failure of railway vehicle		4.49E−03
C6.1		Safety brake failure or inefficiency	1.32E−04
C6.2		Inefficient service braking	1.32E−04
C6.3		Deterioration/cracking of the brake discs due to a parking brake remaining applied or remaining pressure in brake cylinder	6.08E−04
C6.4		Rupture of a semi-automatic coupler/untimely uncoupling	3.02E−04
C6.5		Loss of integrity: poor operation during coupling (excessive speed)	5.08E−04
C6.6/		Overspeed due to traction system failure	2.43E−04
C6.7		Wheelset failure	6.08E−04
C6.8		Low wheel–rail adhesion factor leading to increased stopping distance	3.04E−04
C6.9		Failure of suspension, bogie, connection vehicle-bogie, gauge dynamics, not respecting gauge, interfaces vehicle traction	9.13E−04
C6.10		Loss of car-body integrity	6.08E−04
C6.11		Too high traction effort or inefficient braking when a train is rescued by another one	1.32E−04
C7	Infrastructure problems		1.04E−03
C7.1		Adhesion problem: design of the wheel–rail interface not taken into account	3.02E−04
C7.2		Adhesion problem: presence of external elements compromising the adhesion	7.39E−04

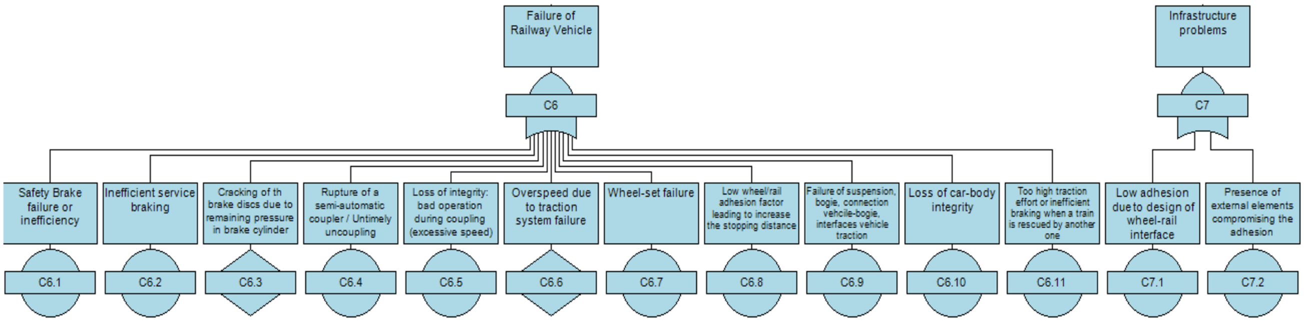
Failure of Railway Vehicle
C6
Infrastructure problems
C7
Safety Brake failure or inefficiency
Inefficient service braking
Cracking of th brake discs due to remaining pressure in brake cylinder
Rupture of a semi-automatic coupler / Untimely uncoupling
Loss of integrity: bad operation during coupling (excessive speed)
Overspeed due to traction system failure
Wheel-set failure
Low wheel/rail adhesion factor leading to increase the stopping distance
Failure of suspension, bogie, connection vehcile-bogie, interfaces vehicle traction
Loss of car-body integrity
Too high traction effort or inefficient braking when a train is rescued by another one
Low adhesion due to design of wheel-rail interface
Presence of external elements compromising the adhesion
C6.1
C6.2
C6.3
C6.4
C6.5
C6.6
C6.7
C6.8
C6.9
C6.10
C6.11
C7.1
C7.2

Fig. 7 Fault tree analysis of top events: failure of vehicle and failure of infrastructure

5.5 Calculating the Failure: Collisions with a Train or Part of a Train Out of Operation

See Table 4, Fig. 8.

Table 4 Probability of top events: train collision with inactive/part of a train (10^5 km-operation)

No.	Top event	Sub-failure	Hazard rate
C8	Failure in ATP system		4.35E−04
C8.1		Failure in emergency braking	4.35E−04
C8.2		Unexpected entrance of a train in the operating area	1.32E−04
C8.3		Disruption/corruption of train control and management system	3.02E−04
C9	Failure of railway vehicle		1.95E−03
C9.1		Failure of parking brake	1.32E−04
C9.2		Emergency brake not activated in loss of integrity situations	9.50E−05
C9.3		Rupture of a semi-automatic coupler/untimely uncoupling	3.02E−04
C9.4		Loss of integrity: bad operation during coupling	5.08E−04
C9.5		Failure of suspension, bogie, connection	9.13E−04
C10	Driver error leading to collision		3.50E−03
C10.0	Driver error		7.00E−02
C10.1		Driver ignored or violated safety rules	5.00E−02
C10.2		Violated the warning signal in shunting movements	2.00E−02
C10.3	Probability of violation leading to hazards		5.00E−02

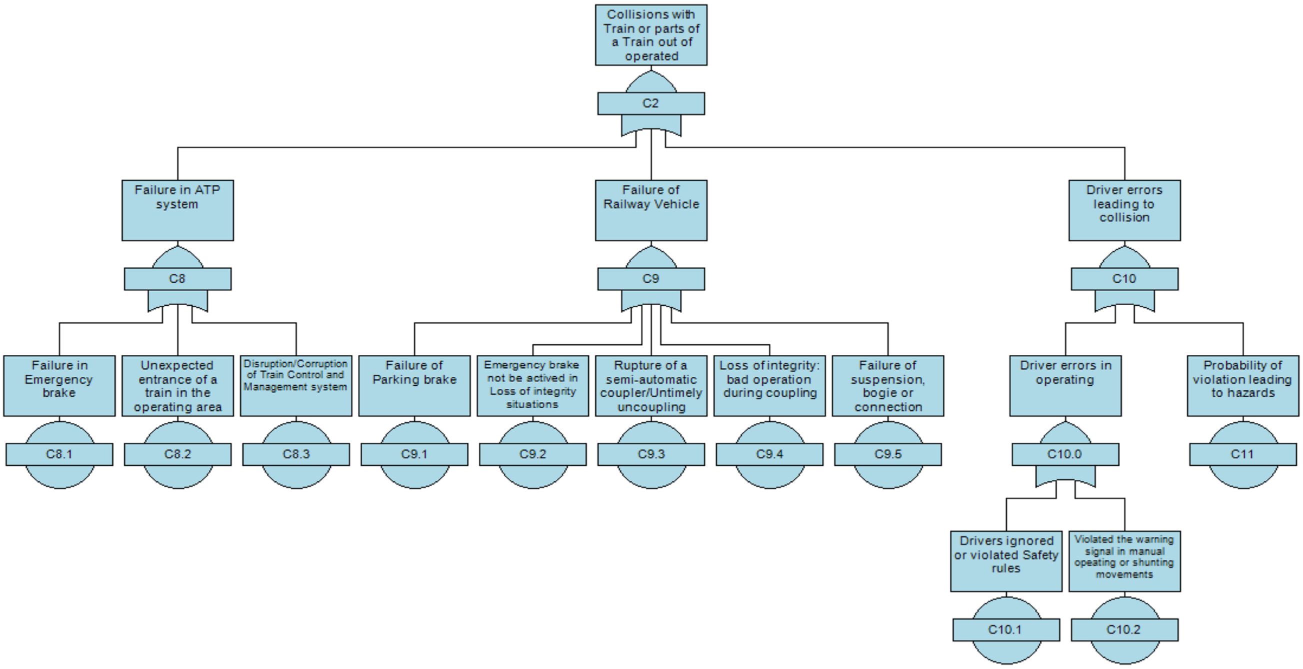
Collisions with Train or parts of a Train out of operated
C2
Failure in ATP system
C8
Failure of Railway Vehicle
C9
Driver errors leading to collision
C10
Failure in Emergency brake
C8.1
Unexpected entrance of a train in the operating area
C8.2
Disruption/Corruption of Train Control and Management system
C8.3
Failure of Parking brake
C9.1
Emergency brake not be actived in Loss of integrity situations
C9.2
Rupture of a semi-automatic coupler/Untimely uncoupling
C9.3
Loss of integrity: bad operation during coupling
C9.4
Failure of suspension, bogie or connection
C9.5
Driver errors in operating
C10.0
Probability of violation leading to hazards
C11
Drivers ignored or violated Safety rules
C10.1
Violated the warning signal in manual opeaing or shunting movements
C10.2

Fig. 8 Fault tree analysis of top events: train collision with inactivated/or a part of a train

5.6 Calculating the Probability of Train Collisions for Line HN2A

Based on the structural function of train collisions and theoretical formulas (1) to (7), the quantitative assessment of collision failures can be calculated. The result is determined as probability of incidents per 100.000 km-operation or number of incidents per year.

The probability of train collisions is calculated by the following Boolean algorithm:

$C0 = C1 \bigcup C2 = (C3 \bigcup C4 \bigcup C5 \bigcup C6 \bigcup C7) \bigcup (C8 \bigcup C9 \bigcup C10) = (C3.1 \bigcup C3.2 \bigcup C3.3) \bigcup (C4.1 \bigcup C4.2 \bigcup C4.3 \bigcup C4.4) \bigcup [(C5.1 \bigcup C5.2 \bigcup C5.3 \bigcup C5.4 \bigcup C5.5 \bigcup C5.6) \cap C5.7] \bigcup (C6.1 \bigcup C6.2 \bigcup C6.3 \bigcup C6.4 \bigcup C6.5 \bigcup C6.6 \bigcup C6.7 \bigcup C6.8 \bigcup C6.9 \bigcup C6.10 \bigcup C6.11) \bigcup (C7.1 \bigcup C7.2) \bigcup (C8.1 \bigcup C8.2 \bigcup 8.3) \bigcup (C9.1 \bigcup C9.2 \bigcup C9.3 \bigcup C9.4 \bigcup C9.5) \bigcup [(C10.1 \bigcup C10.2) \cap C10.3$

= 1.95E−2 (accidents/100.000 km-operation)

Based on the technical design and operational plan of Line HN2A, the total length of this line is 13.02 km. The number of trains operated per day in the first commercial operational phase (2021–2025) is 152 trains/day and in the second commercial operational phase (from 2026) is 252 trains/day. Therefore, the probability of train collisions is:

For 2021–2025, $C0$ = 1.95E−2/10.000 km*13.02 km*152 trains/day*365 days = 0.014 collisions/year

For 2025, $C0$ = 1.95E−2/10.000 km*13.02 km*272 trains/day*365 days = 0.025 collisions/year.

5.7 Comparing the Theoretical Results

These train collision probabilities were calculated using logic in risk analysis, along with data from the technical design of the Line HN2A, as shown above. This result must be compared to real-world operation data and experience from a similar system to ensure it is accurate. The Metro Line HN2A has been in operation since November 6th, 2021, and the most recent statistical data is for the period from November 6th to November 30th, 2021 (25 days). The statistical failure rate from the testing and validation phases was also used in the research, which was clarified in the following manners

Testing operation phase:

- Phase 1 from 01.10.2018 to 10.12.2018 in China: including tested operation and system safety check, operation at 35% operation schedule. Total operation length is 85.455 train-kilometers.
- Phase 2 from 11.12.2018 to 31.12.2018 in China: including tested operation at 100% system capacity with 272 trains/day. The total operation length in this phase is 70.747 train-kilometers.
- Phase 3 from 06.12.2020 to 30.12.2020 in Vietnam: Testing and acceptance phase. Tested operation at 100% system capacity with 272 trains/day. Total operation length in this phase is 84.966 train-operation-kilometers.

Commercial operation (up to 30.11.2021): Operating under a working schedule of 2022–2025 with 152 trains/day. Total operation length in this period is 53.256 train-operation-kilometers.

Therefore, the total length of train-operation-kilometers up to 30.11.2021 is 294.424 train-operation-kilometers. The total of error statistical data in these operation periods is given in Table 5.

The number of failures is the total number of errors in a type of failure which are determined and reported in the operating period, corresponding to the total length of train-operation-kilometers from the testing phase and current commercial operation until November 30, 2021. Therefore, the error rate could be calculated by dividing the number of failures by the total length of train operation kilometers (294.424 train-operation-kilometers).

This total number of failures or error rates reflected dangerous situations/conditions; however, other conditions may be needed simultaneously to lead to an incident or accident. For example, in the case of driver miscommunication to the OCC, it might be a dangerous situation in which the OCC did not have enough real-time information on train operation, and the driver could not receive the control command from OCC. However, this danger alone might not result in train collision, but only when the signal could not be reconnected, the failure in driver recognition and performance simultaneously, and ATC system and emergency brake. We use ETA to calculate the probability leading to collisions., for example as in Fig. 9. The failure probability of the ATC system and vehicle technical errors is usually 1% to 2%, the failure rate of the driver is approximately 2% to 6% [52], and the emergency brake is around 50% due to the evaluation time [39, 53]. Therefore, the calculation of the probability leading to collisions deviates from 0.0005 to 0.002 based on the type of error, as in Table 5. The research on test data indicated several low-significance deviations in the case of sub-failure C5.1, C5.2, and C5.3. This failure group concentrated on human failure. According to the findings of the study [48], there is awareness of human error in the operation of urban railways in Vietnam. The study is based on the statistical analysis and evaluation of the perspectives of researchers, engineers, and local authorities in the railway sector in order to determine workers' perceptions of safety risks and probable safety problems in Vietnam's railway industry. The problems of stress and fatigue and the problem of violation are the most significant issues affecting human performance in railway operations; therefore, human failure estimates are established at a higher level in technical design and theoretical risk assessment, demonstrating the importance and concern of the operator in controlling and managing human performance. This is represented in the company's safety principles, procedures, and safety culture which is specified in the safety management system of the company.

Furthermore, the problem of stress and fatigue among railway workers will not be accurately and completely reflected during the testing phase due to the short time period and the high number of drivers or control/maintenance staff, as well as the fact that there will be almost no absences due to illness. According to [48], the problem of workload is usually a noticeable issue, and the worker is required to work for a long period of time and may suffer from sleep disorders. Workers are rarely encouraged to refrain from reporting to work after a long work shift, and they are also rarely provided with medical or psychological support. As a result, statistics from the operation report and

Table 5 Comparing the hazard rates in theoretical calculations and testing data

No.	Sub-failure	Number of failures/errors per 10^5km-operation	Probability leading to collisions	Hazard rate (100.000 km-operation)		
				Real operation	Theoretical	Deviation
C3.1	Wrong information between train driver and dispatcher	3/1.02	0.002	2.04E−03	1.38E−03	0.68
C3.2	Misunderstanding between driver and dispatcher	5/1.69	0.002	3.40E−03	1.04E−03	0.31
C3.3	No information between driver and dispatcher	–	–	–	5.00E−04	–
C4.1	Train operated in manual operating mode and not protected against other train operated in ATC and limited operating method	1/0.34	0.001	3.40E−4	3.19E−05	0.09
C4.2	Disruption/corruption of train control and management system	–	–	–	1.02E−06	–
C4.3	Failure in ATC input data	1/ 0.34	0.001	3.04E−4	3.19E−05	0.10
C5.1	Drivers failed to check aspect of signal/read wrong signal	1 /0.21	0.02	6.79E−03	3.75E−02	5.52
C5.2	Drivers failed to react to caution signal/misjudgment	2 /0.68	0.02	1.36E−02	3.75E−02	2.76
C5.3	Drivers ignored or violated safety rules	2 /0.68	0.02	1.36E−02	5.00E−02	3.68
C5.4	Conflict warnings	7/ 2.38	0.02	4.76E−02	5.00E−02	1.05
C5.5	Bad visibility from driving cab	14/4.76	0.01	4.76E−02	6.75E−02	1.42
C5.6	Insufficient front/rear lighting in case of driving by line of sight	2/0.68	0.02	1.36E−02	1.35E−02	0.99
C6.1	Safety brake failure or inefficiency	–	–	–	1.32E−04	–
C6.2	Inefficient service braking	–	–	–	1.32E−04	–
C6.3	Deterioration/cracking of the brake discs due to a parking brake remaining applied or remaining pressure in brake cylinder	–	–	–	6.08E−04	–
C6.4	Rupture of a semi-automatic coupler/untimely uncoupling	2/0.68	0.0005	3.40E−04	3.02E−04	0.89
C/6.5	Loss of integrity: bad operation during coupling (excessive speed)	3/1.02	0.0005	5.09E−04	5.08E−04	1.00
C6.6	Overspeed due to traction system failure	2/0.68	0.0005	3.40E−04	2.43E−04	0.71
C6.7	Wheelset failure	2/0.68	0.001	6.79E−04	6.08E−04	0.90
C6.8	Low wheel–rail adhesion factor leading to increased stopping distance (weather conditions included)	3/1.02	0.001	1.02E−03	3.04E−04	0.30
C6.9	Failure of suspension, bogie, connection vehicle bogie, gauge dynamics, not respecting gauge, interfaces vehicle traction	5/1.02	0.0005	8.49E−04	9.13E−04	1.08
C6.10	Loss of car-body integrity	–	–	–	6.08E−04	–
C6.11	Too high traction effort or inefficient braking when a train is rescued by another one	–	–	–	1.32E−04	–
C7.1	Adhesion problem: design of the wheel–rail interface not taken into account	3/1.02	0.0005	5.09E−04	3.02E−04	0.59
C7.2	Adhesion problem: presence of external elements compromising the adhesion	7/2.38	0.0005	1.19E−03	7.39E−04	0.62

error records in the short testing phase will not be able to properly quantify and identify the number of errors that are indirectly caused by human performance.

Additionally, there is some testing data that are substantially greater than the calculation for wheel–rail adhesion. In up to 13 occasions of sub-failure in C6.8 C7.1 and C7.2, the train did not come to a complete stop or emergency stop in the right place. This category does not include failures of the ATP system or the driver's response to braking. These are braking system malfunctions characterized by decreased brake efficacy or a brake system's inability to respond. This is partially explained by the fact that Vietnam's high humidity and wet season limit braking efficiency in certain operating conditions. Additionally, the subjective reason stems

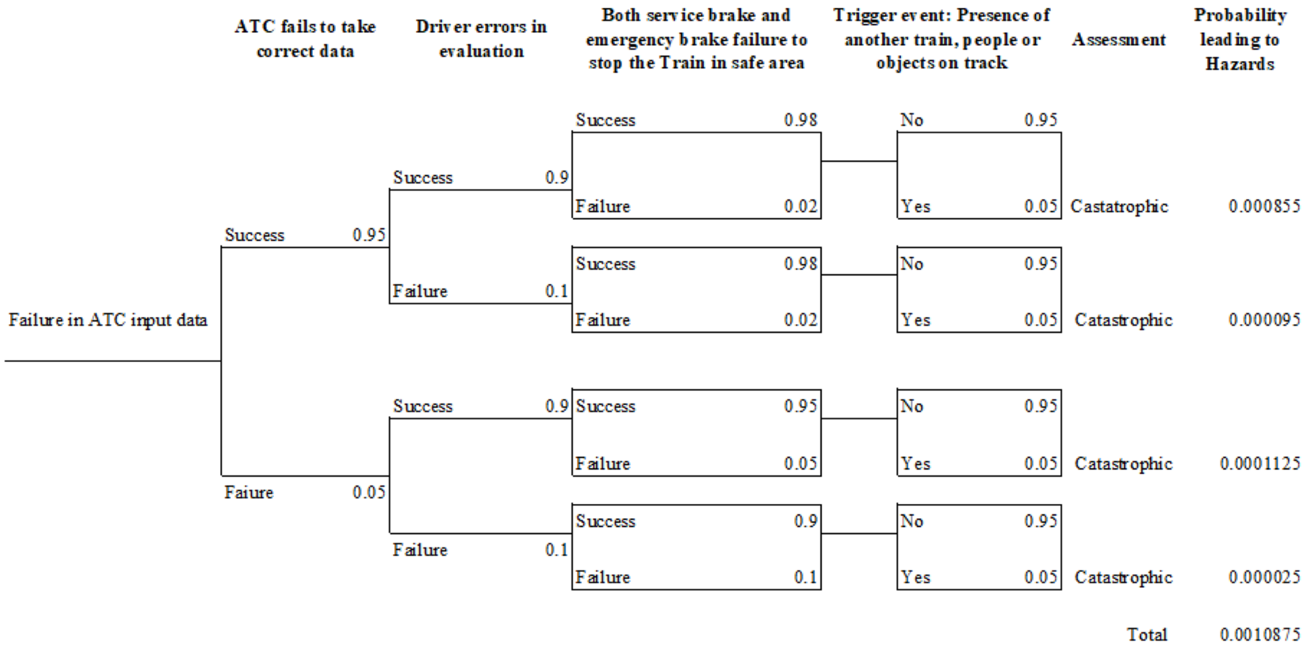

Fig. 9 Principle event tree analysis for failure in automatic train control (ATC) input

from the upkeep of the railway infrastructure and vehicle subsystem. The following section on recommendations will address possible solutions.

5.8 Recommendations

As in the previous theoretical calculation, it is easy to realize the significance of human error (44%) and vehicle technical conditions (33%) contributing to train collision probability. Furthermore, real testing data indicated the additional problem of wheel–rail adhesion. Therefore, the research suggests several solutions to improving human performance and technical testing and maintenance.

5.8.1 Operation and Maintenance

Maintenance is critical to preserving the excellent condition of rolling stock and wagons. The issue is similar to that of infrastructure deficiencies. Additionally, it is a matter of being competent in identifying and resolving safety issues in a timely manner while balancing corporate objectives. This type of issue is addressed by strengthening the safety management and maintenance systems, effective root-cause analysis, and a commitment to continuous reliability improvement.

Securing the brake gear positioned in the wagon's underframe to guarantee that any loose braking components do not fall to the ground and cause a derailment or collision.

Programs for wheelset integrity inspection (ultrasonic). They are also based on other technologies: laser analysis and digital camera photos with lasers or strobe light highlighting the profile. Additionally, wheels must be inspected for material flaws that could result in a rupture.

Conducting visual inspections of train rolling stock axles in accordance with the visual inspection catalogue. A catalogue document has been established that details the problems to be investigated. Double-check signature requirements for safety-classified (S-marked) maintenance operations.

Controlling the technical condition of the track to ensure wheel–rail adhesion, especially in conditions of high humidity and rain.

When passing a signal showing a reduced speed, the driver should initiate the braking or speed reduction action prior to passing the signal, therefore reducing the risk of overspeeding in track deviations.

The ATP system has a function to perform a dynamic brake test on the route to obtain actual test information with regard to the train braking performance.

5.8.2 Human Performance and Safety Culture

Basically, the human factor in railways is contributed by many disciplines including worker psychology, construction engineering, industrial design, environmental and organizational aspects, or operational action. In each phase in the life cycle of a railway project, the compliance of engineers/operators with the above disciplines will influence the rate of human failure, and hence the rate of railway accidents. To ensure good human performance, the system safety management plan of Hanoi Metro Company, which is the Line HN2A operator, clarified several aspects as follows:

Staff competence: The company establishes, assesses, maintains, and records the competence of its employees. No worker will be permitted to undertake rail safety work or be involved in railway operations without the required competency. The competency framework needs to be determined by the accredited organization. There are three procedures for establishing staff competence: (i) determining competency by position description forms, detailing the required levels of competency for all operational positions within the organization; (ii) completing training programs that are accredited and delivered by suitably qualified and recognized training providers; and (iii) maintaining competency, with safety testing assessing the quality of the rail worker.

Internal communications: Recognizes the need for the communication of important rail safety information within the company and for sharing safety information with other rail industry participants. The information sharing in the company is to ensure that workers understand the requirements of the rail safety management system and are kept informed of the company performance.

Training and instructions: A rail safety worker should understand their role and responsibilities as part of the safety management system. The rail transport operator should therefore ensure that its rail safety workers have a working knowledge of the safety management system and how their work relates to it. It must also provide for initial and ongoing training with regard to rail safety including information, instruction and training on new work practices, procedures, policies, and standards, specified hazards, and relevant control measures.

Additionally, special attention should be given to following the train driver's operating procedures in the NRM operating mode, since the train driver's control responsibility is elevated to the maximum level in this operating mode. The ATP system causes essentially minimal interference. At that time, all trains on the line must be halted or converted to RM mode in order to conduct rescue operations for the NRM mode. During the trial operation phase, it was discovered that the driver made an incorrect judgment or followed incorrect procedure, posing a risk of hazardous collisions.

5.8.3 Incident and Failure Database

As previously stated in section 4.4, because the UMRT routes in Hanoi only completed the tests and commissioning and started commercial operation in November 2021, statistical data on incidents and failure rates have not been updated. As a consequence, the qualitative level of this FTA has been reached, as has the quantitative calculation formula.

According to the safety management plan guidelines of the Hanoi UMRT company, the reporting of rail safety-related issues is applicable to all staff involved in railway operations, regardless of whether the issues have a direct influence on railway operations or are perceived as a threat to a railway or its associated infrastructure. These reports include the following: (i) reporting hazards and near-miss incidents; (ii) reporting notifiable occurrences and other incidents relating to health and fatigue risk management, and (iii) reporting rail safety data with (1) monthly data and (2) annual data on human failure, operating performance, and maintenance assessment.

The failure rate data regarding human failure and infrastructure and vehicle condition are assessed by these reports and will be the input for FTA calculation. The calculation of probability of collisions also need to be reevaluated based on the state-of-art research on working behaviors or railway technology to update the reference.

6 Conclusions

The railway system is a highly intricate and interconnected network. Risk assessment for the railway system is never simple. For risk assessment and management of any railway system in general, the data for all system failures and resulting events should be continuously gathered, evaluated, updated, and maintained throughout the system's life cycle, not just for the operating system. Using precise and exhaustive qualitative assessments as the foundation for constructing an evaluation model framework, research and assessment of system failure and other failure should be conducted during the system specification, design/manufacture, and operation phases. Therefore, these investigations and evaluations must be regularly reevaluated and updated. Additionally, it is necessary to consult comparable systems in order to discover any potential problems. Any significant failures that have been recorded by the operation, such as high-frequency failures and human errors, are continuously considered and analyzed. If deemed significant, these failures may be included as additional sources in the risk database by a risk analysis of other railway systems with similar characteristics. Therefore, a continuously updated risk database, as a fundamental part of risk analysis and management methodology, will be shared as an important contribution to the risk assessment not only of this Line HN2A but also of other lines in Vietnam in the future.

This research is a case study of the development of a risk assessment method applicable for UMRT Line HN2A and further development for the UMRT system in Vietnam. Consequently, it concentrates on applying popular ideas to a new application condition and highlighting the distinctions between specific application conditions, thus enhancing the literature on common approaches. This is also the foundation for a more comprehensive quantitative examination of the model based on a comparison between a typical system and the average risk rates in the other system. Calculation results must reflect abnormally high rates in order to focus analysis, conduct research, and identify relevant treatment options (e.g., compliance with regulations or characteristics affecting infrastructure).

The FTA method was selected in the present study for the review and analysis of the methodologies and procedures for hazard identification and evaluation of risk assessment, and was found to be appropriate and can be applied to UMRT in Vietnam as well as Line HN2A, as it provides a risk assessment method that is not overly complicated, is simple to develop, and sufficiently effective for the initial phase of Vietnam's railway industry renovation. The FTA is established in technical management processes. This technique is well suited for assessing complicated systems with numerous components and variable hazard occurrences under various operating situations. This technology enables the creation of an open database for the study and updating of discrete components. The next part of this research focused on developing FTA for train collisions, the most dangerous type of metro accident. The research classifies two types of train collisions and uses the FTA approach to determine the probability of each sub-failure and to compute the hazard rate for train collision occurrence. Data for calculation were collected by the research team from system specification of Line HN2A during its testing and commissioning from November 2021 to the date of publication of the draft article. Based on comparisons of theoretical calculations with error data collected during actual operation of Line HN2A, it can be concluded that despite the small volume of operating data and accident records, technical component failure rates are consistent with theoretical projections (approximately 80–130%). This shows that these assumptions, based on data from analogous urban railway transit systems in Europe and the United States, are accurate, thus confirming that the theoretical calculations and assumptions are reasonable and can continue to be utilized in the Hanoi Metro network monitoring and risk assessment.

On the basis of the study findings, it can be concluded that vehicle-related and human errors have a significant impact on the overall system's hazard rate; consequently, the study provides numerous recommendations for implementing an effective maintenance program to ensure the technical condition of the railway track and vehicles, with a particular emphasis on wheelset and brake system inspection. Additionally, staff competence, training schedules, and the utilization of accident data are highlighted in order to minimize human error.

Acknowledgments We would like to express our special thanks Mr. John Michael Venis (email: jvenis@systra.com) for his proofreading.

Author contributions Conceptualization: Nguyen, Trinckauf and Luong. Methodology: Nguyen, Trinckauf. Software: Luong. Formal analysis and investigation Nguyen, Truong and Luong. Writing—review and editing: Nguyen and Luong. Supervisor: Nguyen and Trinckauf. All authors have read and agreed to the published version of the manuscript.

Funding This research is funded by the University of Transport and Communications (UTC) under Grant Number T2020-KT-001TĐ.

Data availability The authors declare that they are in possession of all data and materials mentioned in this article. This data have been deposited as Supplementary Information in the repositories enabled for this purpose (online resources).

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Ayyub BM (2003) Risk analysis in engineering and economics, Chapman & Hall/CRC.
2. Anderson R, Barkan C (2004) Railroad accident rates for use in transportation risk analysis. Transport Research Board, No. 1863, pp.88-98. National Research Council: Washington DC
3. BEU (2020) Bundesstelle für Eisenbahnunfalluntersuchung: Jahresbericht 2019, Bonn, 2020
4. Bearfield G, Marsch W (2005) Generalising event trees using bayesian networks with a case study of train derailment. In: Conference paper in lecture notes in computer science, September 2005
5. Boyle T (2002) Health and safety: risk management. IOSH Services Ltd., England
6. Braband J (2012) Semi-quantitative risk assessment of technical systems on european railways. In: Flammini F (eds) Railway safety, reliability and security – technologies and systems engineering, pp 54–64
7. Britton M, Asnaashari S, Read G (2017) Analysis of train derailment cause and outcome in Victoria, Australia, between 2007 and 2013: Implications for regulation. J Trans Saf Secur 9(1):45–63
8. BUEDRI (Beijing Urban Engineering Design & Research Institute Co., Ltd) (2012) Hanoi urban railway project: Cat Linh – Ha Dong Line. Volume 2: Traffic Organization and Operation Management. October 2012

9. BUEDRI (Beijing Urban Engineering Design & Research Institute Co., Ltd) (2014) Hanoi urban railway project: Cat Linh – Ha Dong Line. Volume 4: Signal System. December 2014
10. BUEDRI (Beijing Urban Engineering Design & Research Institute Co., Ltd) (2015) Hanoi urban railway project: Cat Linh – Ha Dong Line. Volume 8: Risk Assessments and Safety Management. December 2015
11. CSM (2016) Common safety method on risk evaluation and assessment – amending implementation regulation (EU) No 402/2013
12. Dindar S, Kaewunruen S, An M, Gigante-Barrera A (2017) Derailment-based fault tree analysis on risk management of railway turnout systems. IOP Conf Ser Mater Sci Eng 245:042020. https://doi.org/10.1088/1757-899X/245/4/042020
13. Dingus T, Feng G, Lee S, Antin J, Perez M, Buchanan-King M, Hankey J (2016) Driver crash risk factors and prevalence evaluation using naturalistic driving data. Proc Natl Acad Sci USA 113(10):2636–2641. https://doi.org/10.1073/pnas.1513271113
14. Dinmohammadi F, Alkali B, Shafiee M (2016) Risk evaluation of railway rolling stock failures using FMECA technique: a case study of passenger door system. Urban Rail Transit 2:128–145. https://doi.org/10.1007/s40864-016-0043-z
15. Dodgson J, Spackman M, van der Veer J, Maunder S (2003) Train protection - review of economic aspects of the work of the ERTMS programme team. Health and Safety Executive 2003
16. Doytchev D, Szwillus G (2008) Combining task analysis and fault tree analysis for accident and incident analysis: a case study from Bulgaria. Accident Anal Prevent 41(6):1172–1179
17. Elms D (2014) Rail safety. Reliab Eng Syst Saf 7:291–297
18. EN (1999) EN 50126 – 1999: railway applications: the specification and demonstration of reliability. Railway Application RAMS
19. ERA European Railway Agency (2020) Report pm railway safety and interoperability in the EU, 2020. Publications Office of the European Union, Luxembourg
20. Evans AW (2011a) Fatal train accidents on Europe's railways: 1980–2009. 43(1), 391–401
21. Evans AW (2011b). Fatal accidents at railway level crossing in Great Britain 1946-2009. In: Accidents analysis and prevention , No. 43, pp 1837–1845
22. Evans AW (2021) Fatal train accidents on Europe's railways: an update to 2019. Accid Anal Prevent 158:106182
23. Flammini F, Gaglione A, Mazzocca N, Pragliola C. (2009). Quantitative security risk assessment and management for railway transportation infrastructures. In: CRITIS'08 3rd international workshop on critical information infrastructures security, pp 180–189. Springer, Berlin
24. FRA (Federal Railroad Administration) (2016) FRA accident investigation fact sheet
25. FRAOSA (2021) Federal Railroad Administration Office of Safety Analysis Web Site
26. Fumiaki I (2014) Comparison of safety between Japan and EU railways. JR-EAST Technical Review No.30, p. 17-20. https://www.jreast.co.jp/e/development/tech/pdf_30/tec-30-17-20eng.pdf#
27. Galante E, Bordalo D, Nobrega M (2014) Risk assessment methodology: quantitative HAZOP. J Saf Eng 3:31–36
28. Ghosh S (2004) Identifying and assessing the critical risk factors in an underground rail project in Thailand: a factor analysis approach. Int J Project Manag 22(8):633–643
29. Haimes YY (2009) Risk modeling, assessment and management, 3rd edn. Wiley, New York
30. Hong E-S, Lee I-M, Shin H-S, Nam S-W, Kong J-S (2009) Quantitative risk-evaluation based on event tree analysis technique: application to the design of shield TBM. Tunnel Undergr Space Technol 24:269–277
31. IEC (2006) International electrotechnical commission: IEC 61025: international standard, fault tree analysis (FTA). Geneva, Switzerland. December 2006.
32. IRICEN (Indian Railways Institute of Civil Engineering) (2014). Investigation of derailments. Pune 411001
33. JTSB (Japan National Safety Board) (2022) Statistics of railway accident and statistics of railway serious accident. https://www.mlit.go.jp/jtsb/statistics_rail.html
34. Jurtz S (2019) Untersuchung zur Einführung von ETCS im Kernnetz der S-Bahn Stuttgart: Abschlussbericht. WSP Infrastructure Engineering GmbH, Frankfurt am Main
35. Leitner B (2017) A general model for railway systems risk assessment with the use of railway accident scenarios analysis. Procedia Eng 187:150–159
36. Lin C, Saat M, Barkan C (2012) Analysis of causes of major train derailment and their effect on accidents rates. Transp Res Rec J Transp Board 2289:154–163
37. Lin CY, Saat MR, Barkan CP (2016) Fault tree analysis of adjacent track accidents on shared-use rail corridors. Transp Res Rec 2546(1):129–136
38. Hou L, Peng Y, Sun D (2020) Dynamic analysis of railway vehicle derailment mechanism in train-to-train collision accidents. Proc Inst Mech Eng Part F J Rail Rapid Transit 235(8):1022–1034
39. Li Y, Mi J, Huang H, Zhu S, Xiao N (2013) Fault tree analysis of train rear-end collision accident considering common cause failure. Maintenance Reliabil 15(4):403–408
40. Lindqvist L, Jadhav R (2006) Application of communication based Moving Block systems on existing metro lines. WIT Trans Built Environ 88:391–400
41. Liu P, Yang L, Gao Z, Li S, Gao Y (2014) Fault tree analysis combined with quantitative analysis for high-speed railway accidents. Saf Sci 79:344–357
42. Luong TA, Kunze M, Trinckauf J (2019) Human factor and safety culture in Vietnamese urban railway. J East Asia Soc Transp Stud 13:1905–1926
43. Martani C, Papathanasiou N, Adey TB (2017) A review of the state-of-the-art in railway risk management. IJR Int J Railway 10(1):5–11
44. Matsumoto A, Michitsuji Y, Tobita Y (2016) Analysis of train-overturn derailments caused by excessive curving speed. Int J Railway Technol 5:27–45
45. Milius B (2010) Construction of a semi-quantitative risk graph, PhD thesis. TU Braunschweig
46. NTC National Transport Commission (2017) National standard for health assessment of rail safety workers, 3rd edn. Melbourne, NTC
47. ORR (Office of Rail Regulation) (2013). Common safety method for risk evaluation and assessment. Guidance on the application of Commission Regulation (EU) 402/2013
48. PMURV (Project Management Unit – Rail Vietnam) (2020) Materials of the UMRT line HN2A
49. Profillidis VA (2014) Railway management and engineering. 4th ed. Surrey, United Kingdom: Ashgate Publishing Company
50. Rausand M, Haugen S (2020) Risk assessment: theory, methods, and applications. Wiley
51. Redmill F (2002) Risk analysis – a subjective process. Eng Manag J 12:91–96
52. Ruijters EJJ (2018) Zen and the art of railway maintenance: analysis and optimization of maintenance via fault trees and statistical model checking. University of Twente
53. Sadeghi J, Hasheminezhad A, Essmayil Kaboli M (2015) Investigation of the influences of track superstructure parameters on ballasted railway track design. Civil Eng Infrast J 48(1):157–174
54. Souza A, Tavares F, Bonikowski R, Pereira V (2019) Reduction of number of railroad accidents with locomotive as the main cause. Final Project of Confederação Nacional dos Transportes. Brasilia

55. Sun YQ (2018) Mitigating train derailments due to sharp curve and overspeed. Front Mech Eng 4:8
56. USDT United Stated Department of Transportation (2009) A practical risk assessment methodology for safety-critical train control systems. Office of Research and Development, Washington DC
57. UIC International Union of Railways (2021) UIC safety report 2021. International Union of Railways, Paris
58. VMoT (Vietnam Ministry of Transport) (2016) Circular 16/2016/TT-BGTVT: assessment, certification of urban railway safety
59. VMoT (Vietnam Ministry of Transport) (2018) Circular 16/2016/TT-BGTVT: Procedure, contents, methods for resolving railways incidents, accidents
60. VR (Vietnam Railway Company) (2021) Safety statistic report of Vietnam Railways 2017-2020. July 2021
61. Vu H Tr, Nguyen Th HA (2019) Ensuring safety in urban railway (UMRT) operation in Hanoi. J Transp, Special Issue.
62. Yan J, Wang X (2000) Reliability and safety analysis of automatic train protection system. IFAC Proc 33(9):615–619
63. Wang J (2014) Reliability analysis for CRH2 EMU brake system based on dynamic fault tree. Master thesis. Beijing Jiaotong University
64. Wu C, Cao C, Sun Y, Li K (2015) Modeling and analysis of train rear-end collision accidents based on stochastic petri nets. Special Isssue: Mathematical Problems in Petri Nests Theory and Applications. Mathematical Problems in Engineering. https://doi.org/10.1155/2015/602126