Towards a Fault Tree Analysis of Moving Block and Virtual Coupling Railway Signalling Systems

Aoun, Joelle; Goverde, Rob M.P.; Nardone, Roberto; Quaglietta, Egidio; Vittorini, Valeria

DOI
10.1109/ICSRS56243.2022.10067547

Publication date
2022

Document Version
Final published version

Published in
2022 6th International Conference on System Reliability and Safety, ICSRS 2022

Towards a Fault Tree Analysis of Moving Block and Virtual Coupling Railway Signalling Systems

2022 6th International Conference on System Reliability and Safety (ICSRS) | 978-1-6654-7092-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICSRS56243.2022.10067547

Joelle Aoun
Department of Transport and Planning
Delft University of Technology
Delft, The Netherlands
J.Aoun@tudelft.nl

Rob M. P. Goverde
Department of Transport and Planning
Delft University of Technology
Delft, The Netherlands
R.M.P.Goverde@tudelft.nl

Roberto Nardone
Department of Engineering
University of Naples "Parthenope"
Naples, Italy
roberto.nardone@uniparthenope.it

Egidio Quaglietta
Department of Transport and Planning
Delft University of Technology
Delft, The Netherlands
E.Quaglietta@tudelft.nl

Valeria Vittorini
Department of Electrical Engineering and Information Technology
University of Naples Federico II
Naples, Italy
valeria.vittorini@unina.it

***Abstract*—Railway systems are complex given their interconnectivity with sub-systems wherein each contains multiple components. Virtual Coupling (VC) is a next-generation railway signalling technology that advances Moving Block (MB), also known as European Train Control System Level 3 (ETCS L3). Some pilot implementations exist for MB. However, VC is still a visionary system and involves several safety issues due to the relative braking distance between trains. Therefore, it is important to evaluate the safety of this system to understand whether it is feasible for deployment. This paper performs a preliminary safety and reliability study by introducing a fault tree (FT) model to investigate the possible causes that lead to an unsafe train movement for MB and VC. To this aim, a FT model is initially built for the MB system, considering the system configurations and interactions between wireless devices, onboard and trackside equipment. Then, the FT model of the VC system is derived on top of the one for MB and the differences are highlighted between the FT elements of the two systems.**

Keywords—virtual coupling, moving block, fault trees, railway operations

I. Introduction

The notions of safety and reliability are complex and ambivalent. The complication is mainly caused by the fact that the failure behaviours of the components in complex systems are variable, heterogeneous, and can vary over different constituents. The factors that cause these failures can be related to maintenance regimes, service intensity, operational conditions, geographic constraints (e.g. location, gradients) and exogeneous factors (e.g. climate, weather conditions).

Moving Block (MB) is an innovative and cost-efficient railway signalling system aiming at increasing line capacity and reducing the trackside costs due to less train detection systems to be installed. Virtual Coupling (VC) is still a technology under investigation, whose objective is to further improve capacity and cost-efficiency by enabling convoys where train separation can be reduced to a relative braking distance. Given the very short train separation, the major concerns about this concept regard safety and the critical cascading effects that a failure can have. However, no study has shed light on this essential issue yet. In this paper, we study the different components that constitute MB and VC railway signalling systems, their functions and failure dependencies. In particular, we apply Fault Tree Analyses (FTAs) to understand the cascading effect of one or more failures on a certain top event of a fault tree (FT). We also conduct a comparative study between the elements that constitute a FTA for VC and the ones for MB with a particular focus on a sub-model of the onboard unit (European Vital Computer - EVC).

The paper is organized as follows. Section II provides a brief literature review on the application of FTA and hazard analysis with special emphasis on ERTMS/ETCS systems. Section III briefly describes the MB and VC systems. In Section IV, the main components and functions of the MB and VC systems are introduced. The fault trees development for MB and VC is then explained in Section V, together with a discussion on the comparative analysis between the FTAs of both train signalling systems in Section VI. Finally, the conclusions and future works are presented in Section VII.

II. Related Work: FTA and Hazard Analysis of ERTMS/ETCS

Fault Tree Analysis (FTA) is a well-known deductive technique used to decompose core hazards downward to meet potentially hazardous events [1]. The FTA is based on a backward approach which means that we identify the causal relations leading to events such as those described by event-tree headings [2]. The core tasks on FTA modelling are to determine the top event and find the boundary conditions [3].

By implementing a functional analysis, fault trees (FTs) can represent a system view to understand the criticalities of the system functionality in protecting against the boundary failures that lead to the core/root hazard. A FT is used for recording a functional hierarchy of a system to provide a means of assessing how potentially hazardous events could migrate through the system [4].

The FTA has been widely applied to different areas in the world including aerospace, nuclear power, chemical, pharmaceutical, petrochemical and transportation domains. Examples of FTA in railway applications include the modelling of errors made by train drivers [5], the safety analysis of railway brake system [6] and the reliability evaluation of railway power supply [7]. Li et al. [8] apply a FT model of the train rear-end collision accident.

In railway signalling applications, Flammini et al. [9] choose the basic Mean Time Between Failures (MTBF) value for their FT in accordance with specified Reliability, Availability and Maintainability (RAM) requirements for constituents in the ERTMS/ETCS domain. UNISIG [10] develop FTs for ETCS L2. Several attempts have been made for risk and hazards evaluations for MB, i.e. ETCS L3. Beugin et al. [11] discuss the evolution of the managed risks in ETCS when dealing with MB operation of the ETCS L3 system. X2Rail-3 [12] define hazards and their related causes for MB. ASTRail [13] define a system hazard analysis for the MB system. However, no study has been conducted on the development of FTA models for VC. This paper covers this gap by highlighting the additional functions that a FT for VC adds on top of the one for MB.

III. Moving Block and Virtual Coupling Concepts

Train-centric signalling systems like MB and VC shorten the train separation and provide substantial capacity benefits to railway customers. Both systems are illustrated in Fig. 1.

MB envisages a railway with no more block segregation (as in fixed-block signalling) and track-side safety equipment, where train integrity monitoring (TIM) and safe braking supervision are entirely controlled onboard. MB signalling reduces train separation to an absolute braking distance which is needed by a train to brake to a standstill. The train sends a position report to a Radio Block Centre (RBC), by means of a vehicle-to-infrastructure communication (V2I COM), which in turn broadcasts to the trains the permission to run to a specific location, known as End of Authority (EoA).

The concept of VC is visionary and under investigation. VC can further increase the network capacity to accommodate the forecasted railway demand by the European Commission [14]. VC takes MB train operations to the next stage as it separates trains by a relative braking distance and allows them to move synchronously in platoons where they can be treated as a single train convoy at junctions to increase capacity at bottlenecks. A relative braking distance is defined as the safe separation between a train behind and the rear of its predecessor taking into account the braking characteristics of the train ahead. As in MB, the train position report (TPR) is performed via radio communication by means of a RBC. The Movement Authority (MA) is also broadcasted to trains by the RBC. Given the very short distances between trains under VC, sight reaction times of human drivers are no longer safe and Automatic Train Operation (ATO) shall be equipped for automated driving. The communication via the RBC may also be too time consuming, so it is anticipated that the leader train of the convoy communicates with the RBC while the following trains exchange position, speed and acceleration information via a Vehicle-to-Vehicle communication (V2V COM) architecture [15]. Therefore, a relevant aspect for the development of VC is the communication between trains. With respect to the current signalling systems, in which intelligence and information are centralized, VC is based on automated cooperative driving, where intelligence and relevant information are distributed among the trains moving on the line.

For both MB and VC, a safety margin (SM) must be guaranteed after the braking distance. More details about the components and functions of each system are provided in Section IV.

IV. Systems Components and Functions

The first step in developing a FTA is to define the scope of the study. This is achieved by defining the system's components and identifying their related functions. Fig. 2 presents the breakdown structure of the components that constitute MB or ETCS L3 (blue colour) and VC (orange colour). The elements that have both the blue and orange colours are applicable to both MB and VC. The same significance of colours applies to the basic events (circles) or transfer gates (triangles) in Fig. 3 and Fig. 4.

Some of the MB components are also included in ERTMS/ETCS Level 2 systems. At this level of abstraction, the main differences between ETCS L2 and the MB systems are the following: 1) the onboard system includes a new component, TIM, 2) the track-clear detection is no longer necessary as in fixed-block signalling; 3) trackside functions are new or modified.

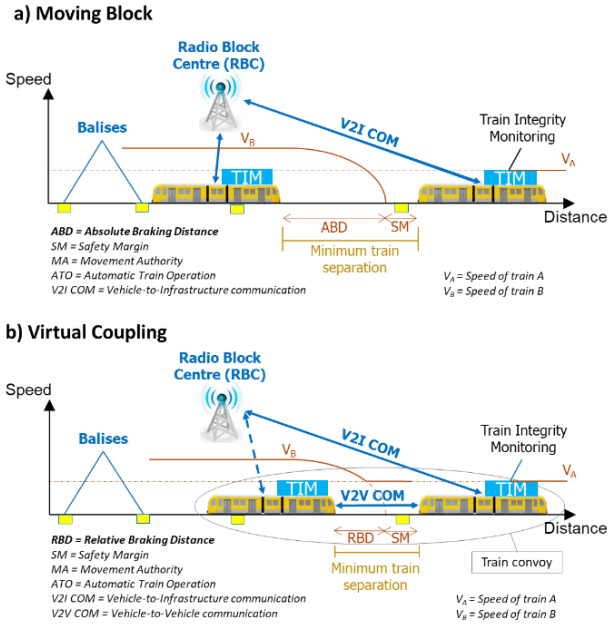

Fig. 1. Schematic architecture of train-centric signalling systems: Moving Block (a) and Virtual Coupling (b).

All the trackside and onboard equipment are common to both MB and VC. However, VC is characterised by the additional V2V COM component.

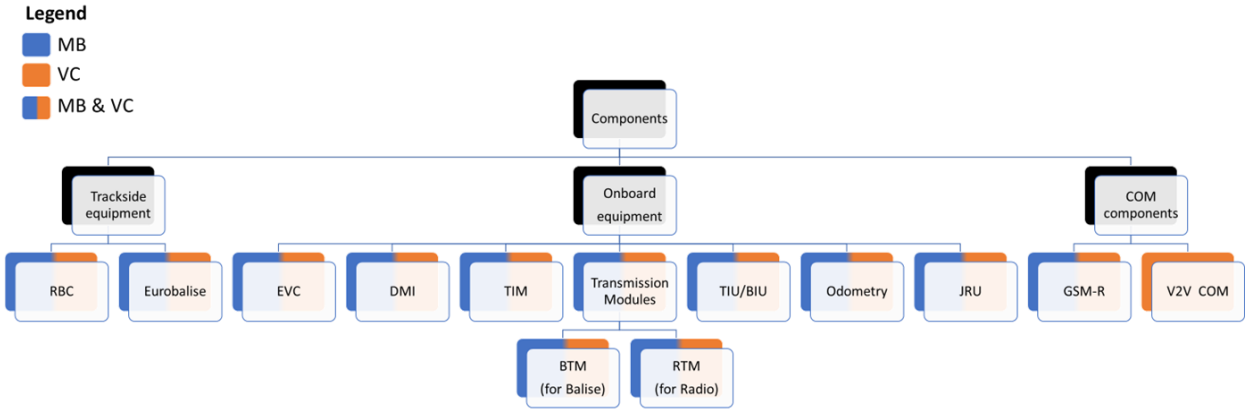

Fig. 2. Components' breakdown structure of moving block (MB) and virtual coupling (VC).

Intuitively, the fewer number of trackside components may increase the system reliability and decrease costs, as it is also envisioned by the European rail initiatives Shift2Rail and EU-Rail [16]. On the other hand, the introduction of new components has to be considered. In the following, a brief description of the components introduced in Fig. 2 is given.

Both MB and VC systems have RBCs and Eurobalises as trackside equipment.

The RBC is a computer-based system that elaborates the messages that need to be sent to the trains. A main goal of the RBC is the management of the MA. The MA provides the maximum distance that a train can safely cross without colliding with another train on the route. In VC, the MA associated to VC, MA_{VC}, combines information from both the RBC and the V2V COM channel, and the speed associated to the End of Authority for VC (EoAvc), is either equal to the speed of the train ahead (if trains are running in a coupled stage), or zero (if trains are decoupling).

The Eurobalise is a transmission device placed between the rail tracks. It is defined as a trackside transponder or electronic beacon acting as a fixed geographical reference point. The main functions of the Eurobalise are to report the train position and to provide the up-link for sending messages to the train onboard system.

The ERTMS/ETCS onboard system is a computer-based system that supervises the movement of trains, on basis of the information exchanged with the trackside system. It is composed of: the Eurocab or European Vital Computer (EVC) where kernel functions are stored, the Driver Machine Interface (DMI), the Balise Transmission Module (BTM), the Train Integrity Monitoring (TIM), the Radio Transmission Module (RTM), the Train/Brake Integrity Unit (TIU/BIU), odometry and the Juridical Recording Unit (JRU).

The EVC monitors continuously the train location by means of an onboard odometer that is regularly calibrated any time the train crosses a balise. It also elaborates MA messages and supervises in real-time a dynamic speed profile including a braking curve that ensures that the train does not overrun the EoA. However, in the case of VC, further functions of the EVC are implemented by considering the supervision of both the EoAvc and the standard EoA (in the operational state of an (un)intentional decoupling). In addition, the EVC for VC predicts the space crossed by the leader during a certain coordination time that is required by the follower to catch up with the leader's speed at the location indicated by the EoAvc within a certain safety margin from the latter's tail.

The DMI provides a bi-directional interface with the train driver and displays relevant information and instructions to the driver.

The TIM verifies that a train is complete while it is in operation. It also guarantees a safe train-rear position and dynamic braking curve supervision.

The BTM detects the presence of a balise and processes the up-link and down-link data. The BTM is interfaced with the ERTMS/ETCS kernel and onboard antenna unit (i.e., Global System for Mobile communications-Railway (GSM-R)).

The RTM provides a bi-directional interface with the trackside.

The TIU and BIU are used as interfaces with the EVC to the train and/or the locomotive for submitting commands or receiving information. The BIU is used for implementing braking instructions commanded by the Train Collision Avoiding System (TCAS) / Distributed Power Control System (DPCS).

The odometry represents the entire process of measuring the train's movement (speed and distance) during a journey along the track.

The JRU is used as a device to record defined data relating to the train's movements for legal purposes. The recorded data shall allow analysing the cause of an accident, incident, or hazardous situation.

The communication components include the GSM-R onboard which applies to both MB and VC and the additional functionality of the V2V COM that is specific for the VC technology.

The GSM-R onboard radio system (antenna) is used for the bi-directional exchange of messages between the onboard EVC and RBC.

978-1-6654-7091-9/22/$31.00 ©2022 IEEE

The V2V COM onboard allows the trains to be separated by less than a relative braking distance. Via onboard antennas, the trains are able to exchange route and kinematic information (e.g., speed, acceleration) and to form a convoy of virtually coupled trains, also known as virtually coupled train set (VCTS).

V. Fault Trees Development

It is well known that a FTA can be performed qualitatively and/or quantitatively. A qualitative analysis provides insights into the structure of the causal chain of failures to analyse system vulnerabilities, whereas a quantitative analysis determines the failure rates of intermediate events and of the top events in sub-trees based on failure rates of basic events.

In this paper, we focus on the qualitative perspective of the FTA since the concept of VC imposes several uncertainties with respect to its implementation. In fact, the novelty of the study presented in this paper is mainly in the systems under study. MB specifications have been defined by the Shift-to-Rail (S2R) X2Rail-1 [17] and X3Rail-3 [19] projects and they are publicly reported in the projects deliverables. VC is still a visionary concept, as explained in Section III. The application conditions of VC have been investigated in S2R X2Rail-3 [19] and further research is planned within Europe's Rail (the successor of the S2R initiative) [20].

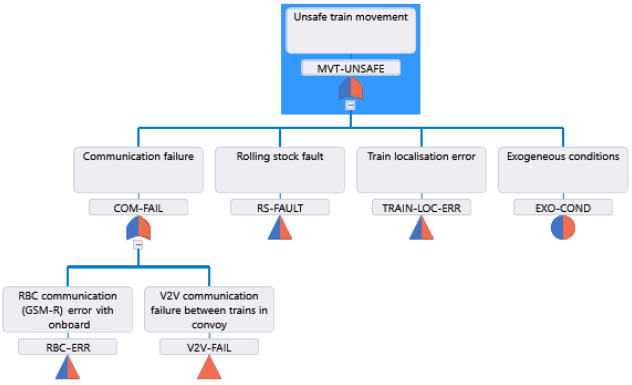

Fig. 3. Preliminary Fault Tree of MB and VC for modeling an unsafe train movement.

Therefore, the aim of this paper is to provide a preliminary study based on the available information and on brainstorming sessions for developing a cascading chain of cause-effect relations to the VC system. The work relies on the hazards analysis for ETCS L3 developed by X2Rail-3 [12], and exploits the FTA for similar previously investigated systems. Specifically, as ETCS L3 is built on top of ETCS L2, the proposed approach leverages on the analyses and results of the FTs developed for ETCS L2 by UNISIG [10]. The developed FTs were then reiterated by looking for identical or similar-meaning events and aggregating the sub-trees for the sake of clearness and simplicity.

The FTs are developed for holistically identifying the causes that might lead to an unsafe train movement (see Fig. 3). We first started by developing a FT for MB, then we extended it to VC by considering the potential failures that might arise from the additional V2V COM component (represented by solely the orange colour). The potential main causes for an unsafe train movement could arise from a communication failure, a rolling stock fault, a train localisation error, or exogeneous conditions like weather conditions, track conditions, interlocking or power supply failure. The driver error was not considered since we consider that the automatic train protection (ATP) would always interfere wherever the reason of driver error is.

The circles are basic events where no further breakdown is possible, whereas the triangles represent a transfer of a FT to another location within the main tree. Therefore, all the triangles represent a further extension to another sub-tree.

VI. Comparative Analysis and Discussion

In this section, we focus on a sub-tree for MB and VC by highlighting in orange the differences between the elements of the FT that are only relevant to the VC system, as illustrated in Fig. 4. We present a sub-tree that shows the potential faults for the provision of data onboard (EVC).

The sub-tree in Fig. 4 is generated from the 'RBC communication (GSM-R) error with onboard' in Fig. 3 through further intermediate events, namely 'Delivering wrong messages' and 'Wrong system data', following a forward approach. This logic emerges from the fact that one of the causes that lead to a RBC communication failure is the wrong messages delivered to the onboard unit (i.e. EVC) that in turn is caused by wrong system data. A wrong provision of data onboard is then considered as one of causes under 'Wrong system data' and is further developed in Fig. 4. The figure shows the cause-effect relationships between the different failures of the components that constitute the MB and VC systems. The reasons for wrong provision of data onboard can be for instance related to failures or errors in the balise, BTM, RBC, RTM (developed inside the sub-tree 'RBC-MSG-WRONG'), TIM or odometry-related component failures.

In the case of VC, we take into account additional components associated to the upgraded functionalities of the EVC that relate to EoA_{VC} and to the V2V COM failure between trains. V2V COM failure could for instance arise from an error in delivering a message from the leader train to the follower trains or if a following train receives a wrong message from its predecessor. Another reason that can lead to a failure in the V2V COM is a train state control error by exogeneous factors.

The other transfer gates in Fig. 4 relate to a wrong transmitted MA message from RBC to onboard, undetected movements, error in elaborating messages onboard and unsafe dynamic speed profile. All the elements under the transfer gate 'RBC-MSG-WRONG' are derived from UNISIG [10], where causes can be related to radio transmission data consistency failure, or wrong radio message received by onboard kernel functions as consistent or an incorrect provision of data (trackside). The sub-tree 'DYN-SPD-UNSAFE' is also developed based on UNISIG's analysis. The 'UNDETECT-MVT' sub-tree is established from the hazards defined by X2Rail-3 [12]. For the error in elaborating messages onboard, reasons could relate to errors in delivering train information to RBC, or an error in Eurobalise or Euroradio transmissions, i.e. BTM or RTM, or an error in detecting the movement of trains. Other reasons relate to the error in route setting and releasing (point control) or an error in delivering a track status message.

Our work and the comparative analysis between the MB and VC sub-trees is also the basis of the apportionment procedure of Tolerable Hazard Rate (THR) to subcomponents. In fact, according to [21], UNISIG define the following maximum THRs:

- 1.0 E-09 / hour for ETCS onboard (installed on a train), and
- 1.0 E-09 / hour for ETCS trackside (installed in an area visited by a train during a reference mission).

Considering that the transmission functions are offered by the joint work of onboard and trackside equipment, UNISIG empirically apportions 1/3 of each hazard rate to the transmission functions. Hence, the THR for ETCS onboard is apportioned as 0.67 E-09 / hour to the onboard functions and 0.33 E-09 / hour to (onboard) transmission functions. Similarly, the THR for trackside functions is apportioned as 0.67 E-09 / hour to the trackside functions and 0.33 E-09 / hour to (trackside) transmission functions. With the increasing complexity of the onboard transmission equipment, which has to support the V2V COM and additional functionalities, this apportionment should be revised. Alternatively, the onboard transmission functions should rely on increased quality equipment to fulfil this rate.

VII. Conclusions and Future Work

This paper consists of applying a faut tree analysis to train-centric signalling systems with particular focus on Virtual Coupling. We analysed the components' functions dependencies for both Moving Block and Virtual Coupling as well as the cascading effects on system failures and unsafe train movements. Differences were highlighted between the fault tree elements that constitute each of the two signalling systems to pinpoint the additional functions that a FT for VC adds on top of the one for MB.

The results can support infrastructure managers, railway undertakings, maintenance service providers and data analysts in identifying the most critical system components based on their defined functions and the developed FTs. The proposed approach also provides an efficient capability of dealing with the core problems of reliability and safety analysis methods.

The work reported in this paper is a first step towards the objective to investigate the failure behaviour of MB and VC systems. To fully reach this goal, more research is needed based on a modular approach to manage the complexity of the model and the usage of Stochastic Activity Networks (SANs) [22]. FT extensions, such as Dynamic Fault Trees (DFTs) [23], can also be used to deal with dynamic redundancies and common cause of failures due to functional dependencies.

Future works will include a quantitative safety analysis of the MB and VC systems, as well as the integration of FTA with Stochastic Activity Networks (SAN) to evaluate the safety-performance effects and behaviours of the MB and VC systems in real-world conditions.

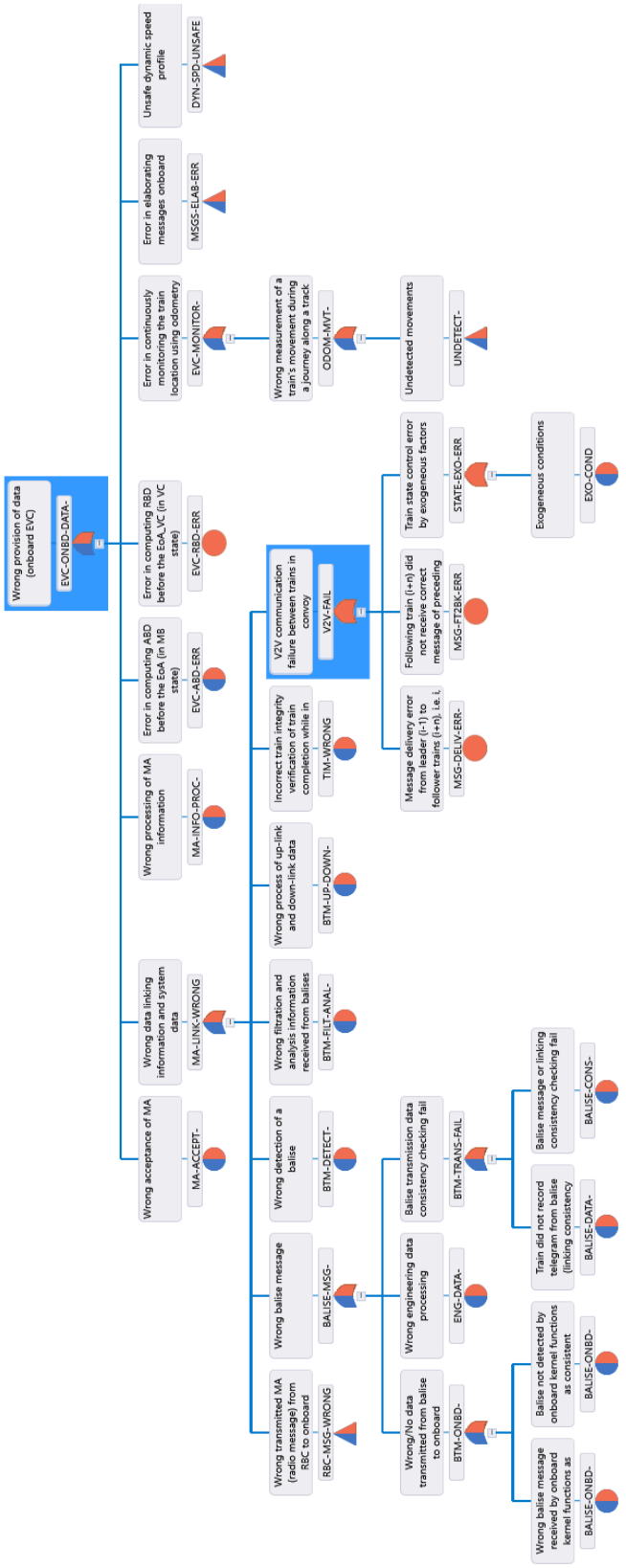

Fig. 4. Fault Tree of MB and VC (additional elements in orange) for a wrong provision of data onboard (EVC).

ACKNOWLEDGMENT

This research has received funding from the Shift2Rail Joint Undertaking (JU) under the European Union's Horizon 2020 research and innovation programme under Grant Agreement N. 101015416 PERFORMINGRAIL.

The JU receives support from the European Union's Horizon 2020 research and innovation program and the Shift2Rail JU members other than the Union. The content of this document reflects only the authors' view — the Joint Undertaking is not responsible for any use that may be made of the information it contains.

REFERENCES

[1] VROM, Methods for determining and processing probabilities 'Red Book', Publication Series on Dangerous Substances 4 (PGS 4), 2017.

[2] H. Kunmamoto, and E. J. Henley, Probabilistic Risk Assessment and Management for Engineers and Scientists, 2nd Ed., IEEE Press, 1996.

[3] E. Ruijters, D. Guck, P. Drolenga, and M. Stoelinga, "Fault Maintenance Trees: Reliability Centered Maintenance via Statistical Model Checking", IEEE Xplore, 2016 Annual Reliability and Maintainability Symposium (RAMS). Tucson, AZ, USA, 2016.

[4] UNISIG, "SUBSET-077 - UNISIG Causal Analysis Process", issue 3.0.0, June 2016.

[5] B. Dhillon, Human Reliability and Error in Transportation Systems. Springer, London, 2007.

[6] L. Zhang, L. Guo, R. Li, and Y. Wang, "A Method for Safety Evaluation of Train Braking System Considering Multiple Types of Preventive Maintenance Cycles", Applied Sciences, mdpi, vol. 12, 2022, 4799.

[7] S. Chen, T. Ho, and B. Mao, "Reliability evaluations of railway power supplies by fault-tree analysis", Electric Power Applications, IET, 1(2), 2007, pp. 161–172.

[8] Y-F. Li, J. Mi, H-Z. Huang, S-P. Zhu, and N. Xiao, "Fault tree analysis of train rear-end collision accident considering common cause failure", Maintenance and Reliability, vol. 15(4), 2013, pp. 403–408.

[9] F. Flammini, S. Marrone, N. Mazzocca, and V. Vittorini, "Modeling system reliability aspects of ERTMS/ETCS by fault trees and Bayesian networks", Safety and Reliability for Managing Risk – Guedes Soares & Zio (eds), Taylor & Francis Group, London, ISBN 0-415-41620-5, 2006.

[10] UNISIG, "SUBSET-088-2 Part 1 - ETCS Application Level 2 - Safety Analysis, Part 1 - Functional Fault Tree", issue 3.7.0, December 2019.

[11] J. Beugin, C. Legrand, J. Marais, M. Berbineau, and El M. El Koursi, "Safety Appraisal of GNSS-Based Localization Systems Used in Train Spacing Control", IEEE Access, IEEE, 2018, 18p. 10.1109/ACCESS.2018.2807127, hal-01724771.

[12] X2Rail-3, "Deliverable D4.2 Moving Block Specifications, Part 6 – Safety Analysis", Shif2Rail, Horizon 2020 EU Funding for Research & Innovation, December 2018.

[13] ASTRail Consortium, "Deliverable 2.2 Moving Block signalling system Hazard Analysis", January 2019.

[14] European Environment Agency, Passenger Transport Demand, Outlook from WBCSD, https://www.eea.europa.eu/data-and-maps/indicators/passenger-transport-demand-version-2/assessment.

[15] I. Mitchell, E. Goddard, F. Montes, P. Stanley, R. Muttram, W. Coenraad, J. Poré, S. Andrews, and L. Lochman, "ERTMS Level 4, Train Convoys or Virtual Coupling", IRSE News, Issue 219, 2016, pp. 1-3.

[16] Shift2Rail Joint Undertaking, Multi-Annual Action Plan, Brussels, November 2015.

[17] X2Rail-1, Start-up activities for Advanced Signalling and Automation Systems, Shift2Rail, 2021.

[18] X2Rail-3, Advanced Signalling, Automation and Communication System (IP2 and IP5) – Prototyping the future by means of capacity increase, autonomy and flexible communication, Shift2Rail, 2021.

[19] X2Rail-3, "Deliverable 6.1 – Virtual Train Coupling System Concept and Application Conditions", No 826141, January 2020.

[20] Europe's Rail, Work Programme 2022-2024 adopted by the EU-Rail Governing Board on 1 March 2022, 2022.

[21] UNISIG, "SUBSET-088 Part 3 – ETCS Application Levels 1 & 2 – Safety Analysis. Part 3 – THR Apportionment", issue 3.7.0, December 2019.

[22] J.F. Meyer, A. Movaghar, and W.H. Sanders, "Stochastic activity networks: structure, behavior, and application", International workshop on timed Petri Nets, IEEE Computer Society, Washington, DC, pp. 106–115, 1985.

[23] J.B. Dugan, S. Bavuso, M. Boyd, "Dynamic fault-tree models for faulttolerant computer systems", IEEE Transactions on Reliability, 41, 363-377, 1992.