*Human Systems Engineering and Design (IHSED2023),* Vol. 112, 2023, 310–320
https://doi.org/10.54941/ahfe1004142

# Safety Engineering in Design of Autonomous Public Transportation Systems

**Jari Laarni and Antti Väätänen**

VTT Technical Research Centre of Finland Ltd, Espoo, 02044 VTT, Finland

## ABSTRACT

There are several safety challenges in the development of autonomous public transportation systems operating in urban environments. Special methods are needed for the identification and treatment of important human actions and for the recognition and prevention of potential human errors. This paper describes the utilisation of Functional Resonance Analysis Method (FRAM) in development and definition of autonomous tram transportation systems. The results are based on characteristics of tram transportation and human factors in autonomous transportation systems. Also, interviews of tram system operators and tram drivers were used in this study. The paper aims to conclude main safety engineering issues in autonomous tram systems and how to use FRAM approach to identify and solve them.

**Keywords:** Functional resonance analysis method, Task analysis, Human errors, Autonomous transportation system, Tram

## INTRODUCTION

The objective of the present study is to identify safety engineering activities that promote the safety design of public transportation systems. The study is carried out in SmartRail 2 project, in which the SmartRail ecosystem is launched, and tram transportation services are considered from passenger, lifecycle services and autonomous system point of views. The ecosystem will focus on themes such as predictive situational awareness, user-centric solutions, efficiency and impact assessment (SmartRail Ecosystem, 2023). The project considered tram systems in Tampere and Helsinki in Finland, but this paper focusses on the modern Tampere tram transportation system that was taken into use in 2021 and on the smart rail network evolving and extending during the next few years.

There are several safety challenges in the development of autonomous public transportation systems operating in urban environments where high demands are set for sensors and sensor networks aiming at reliable detection of pedestrians and other vehicles (Laarni & Väätänen, 2023). Typically, three kinds of activities can be identified: safety analyses, safety requirements specification and user-centred design of the target systems. In this paper, we focus on primary safety design activities, i.e., task analyses, identification and treatment of important human actions, identification of potential human errors,

 

and potential performance variability. Task analysis focuses on the analysis of human tasks that are needed to support the identified human actions and determines the risk significance levels of the tasks to be analysed. Treatment of important human actions identifies and tracks human actions that may be affected by introducing autonomous transportation systems, including actions that are important to passengers and other road users. Identification of potential human errors aids in identifying potential human errors with important consequences so that these can be adequately treated in the design phase.

Special methods are used in identification and treatment of important human actions and in identification of potential human errors. We have developed an innovative approach in which human actions analysed by hierarchical task analysis methods are further analysed through the following steps: task classification, human error identification, analysis of potential consequences and recovery opportunities, semi-quantitative probability analysis and criticality and remedy analysis. The results of these analyses are then used as an input to functional resonance analysis in which the Functional Resonance Analysis Method (FRAM) is used (Hollnagel, 2012). The FRAM method establishes a model of a certain activity representing the main features of how the activity is performed, and it specifies the potential variability of the system in terms of main functions. The method has shown to be a valuable tool in understanding the reasons behind the gap between work-as-designed and work-as-done (Hollnagel, 2012).

Various data collection methods have been used in identification of operator and transportation service user functions, tasks and activities. Based on collected data, we were able conduct hierarchical task analyses and identify potential human errors and the potential variability associated with operator tasks. The paper will give preliminary examples of analyses and models, and their prospects and limitations are discussed.

## BACKGROUND

### Tram Transport Risks

Even though tram driving is a rather complex task, tram accidents are quite infrequent (Naweed & Rose, 2015). Nevertheless, accidents and collisions occur on tram transportation. Trams are quite dangerous in an urban environment because of their high mass, braking characteristics and low reaction time (Margaritis, 2007). Typically, accidents are categorized as tram to vehicle collisions, tram to pedestrian collisions, tram to tram collisions and passenger falls inside the tram saloon (Naznin et al., 2018).

A common finding is that road users typically underestimate the probability of tramway accidents and incidents due to the fact that trams drive on tracks and their speed is quite low (Guerrieri, 2018). A majority of tram to vehicle collisions occur at intersections. A typical accident at intersections is a collision between a tram and a car turning left at the intersection caused by the fact that car drivers misperceive traffic signs or do not obey them (Guerrieri, 2018). Tram to pedestrian collisions are more common at tram

stops or their vicinity. Pedestrians often do not notice the tram approaching a crossing or a tram stop (Guerrieri, 2018). They step into the street to the front of an approaching tram; nowadays it is also common that they are looking at their mobile device and wear earphones while walking (Guerrieri, 2018). Pedestrians also often run close the front of a stationary tram while hurrying to the tram causing danger if the tram starts to move (Sagberg & Satermo, 1997).

With regard to tram drivers, three causes of accidents have been identified: situation awareness, time pressure and organizational behaviour (Naweed & Rose, 2015). Trams are operating in a mixed traffic environment which is not strictly separated from other road users and pedestrians. This requires higher levels of situation awareness and constant requirements to make predictions. Tram driving also requires that more effort is placed in the supervision of the passenger saloon. It is also challenging to maintain required separation between trams, which may lead to "hurry up and wait" approach (Naweed & Rose, 2015).

Autonomous or semi-autonomous tram system may solve some of the above-mentioned safety challenges, but simultaneously raise some others. Autonomous public transportation vehicles at higher levels of automation (i.e., at SAE levels of 3-5) have to operate smoothly in all kinds of traffic situations. They must perceive and analyse data, make plans and decisions and execute actions in real time. In order to perform these tasks without operator intervention, these vehicles need computer programs, sensors and communication devices for localization, signal and obstacle handling and vehicle control (Figure 1).

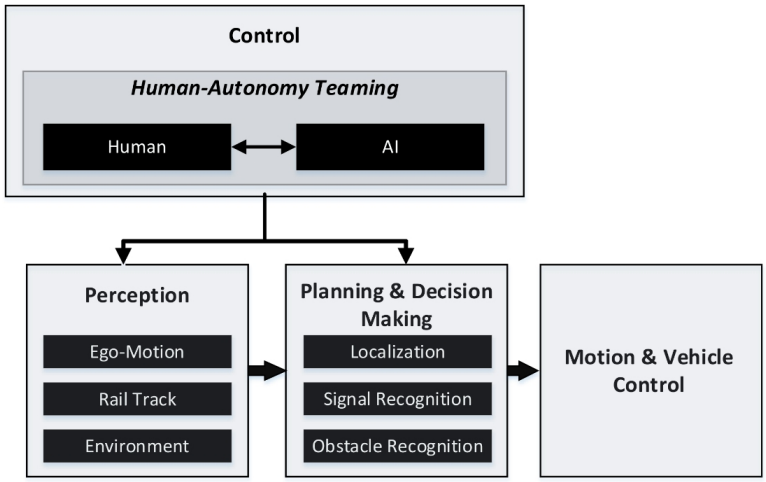


**Figure 1:** High-level system architecture for an autonomous tram system. (Adapted and modified from Ghasemieh & Kashef, 2022 and Palmer et al., 2020.)

Many kinds of risks associated with autonomous tram transportation can be identified such as wrong detection and recognition of other road users, objects and traffic signs, challenges caused by delays and situation awareness problems in transferring the authority from the automated system to

the operator in emergency situations, and cybersecurity hazards caused by unauthorized access to the autonomous control system (e.g., Iclodean et al., 2022).

## Safety Limits in Tram Driving

The concept of 'safety limit' is a useful tool in safety analysis and risk assessment in many domains. Safety limit demonstrates a threshold value that works as a warning signal that should not be exceeded. It is typically discussed in terms of control theory, according to which, there is a comparator comparing the perceived state to the reference value, that is, a safety limit. Based on the result of the comparison, an output function (i.e., a particular behaviour) is generated, which has a specific impact on the environment.

Safety limits are established and maintained in driving. A typical limit a driver has to monitor is the distance to the critical obstacles in the environment. One of the driver's main tasks is to monitor that these distances are kept large enough: the smaller the distance the more probable an error becomes. The ability to maintain the safety limit is dependent on the system's performance capability and task demands: if the performance capability decreases and task demands increase, the system's resilience decreases until it reaches a state where it cannot constantly maintain the safety limit and as a result the probability of an error increases (Figure 2). In order to maintain the safe state, a larger safety limit is needed to keep the probability of an error at a reasonably low level. Many kinds of performance shaping factors (PSFs) have an effect on human performance capability and task demand such as fatigue, stress, driver skills, decision making complexity and time pressure. What complicates the analysis is that the PSFs interact with each other in complicating ways which is nearly impossible to anticipate in detail.

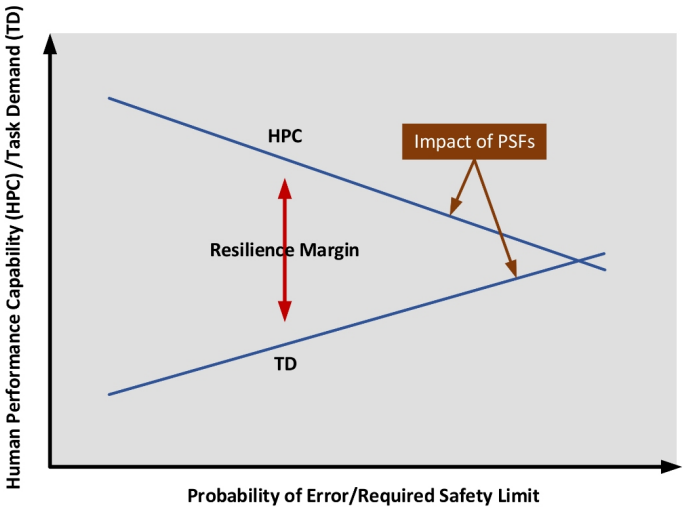


**Figure 2:** Illustration of the dependencies between capability/task demand and probability of error/safety limit. The probability of error/required safety limit increases with a decrease of human performance capability and an increase of task demand. This can also been seen as a decrement of resilience margin. HPC = Human Performance Capability; TD = Task Demand; PSF = Performance Shaping Factor.

Safety limits have to be considered in the design of autonomous transportation systems, that is, they have to be designed in a way that the difference between the perceived state and required value is always above some critical limit for various operations situations which are dependent on control actions. In other words, designers have to estimate the required level of a safety margin that offers a flexible way of acting also in less favourable environmental conditions; they also have to justify why the proposed safety margin is adequate and consider that critical additional uncertainties in limit estimation are accounted for.

There are several possible methods for the estimation of safety limits in autonomous driving. Most of these methods have a similar structure, and they proceed along similar steps. First, they define the task under analysis, determine its sub-goals and decompose these subgoals; second, they classify the sub-tasks according to a particular category; third, they identify potential error types and modes associated with the sub-tasks, determine their possible consequences and how the errors can be recovered.

With regard to task analysis, they should be performed from the vantage points of main stakeholders. For example, we could conduct a hierarchical task analysis of various stakeholders' activities on a tram drive. With regard to tram operation four different operational states are considered: 1) starting a shift at the depots; 2) approaching and stopping at a pedestrian crossing; 3) approaching and passing a tram stop; and 4) crossing other vehicles at intersections (Laarni & Väätänen, 2023). With regard to passengers' activities, three phases of a tram drive can be identified: activities before, during and after the journey. An example is given in Figure 3, which shows a passenger's actions during a tram journey.

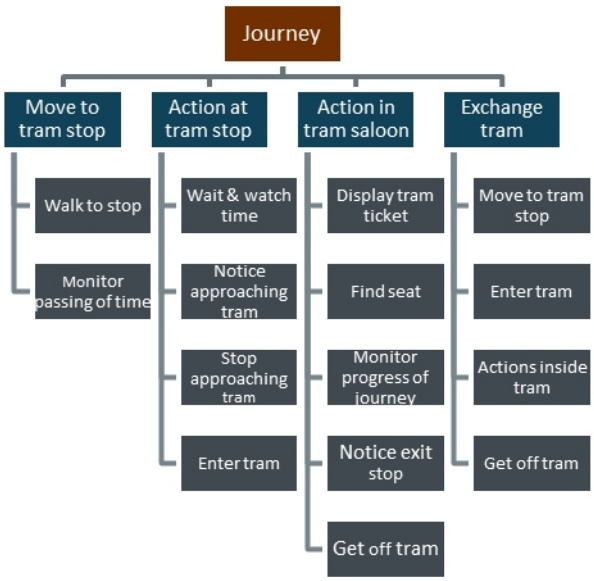


**Figure 3:** Example of a hierarchical task analysis: a passenger's activities during a tram journey.

## DATA COLLECTION

Data for the preliminary safety analysis was gathered through interviews and a workshop session. Tram drivers were interviewed in several sessions. The interviews conformed the semi-structured approach and addressed topics such as:

- Perceived input and effects on own tasks
- Output of own actions
- Work conditions and requirements
- Resources and demanded skills for tram driving
- Monitoring and controlling tram
- Monitoring passenger behaviour
- Issues related to time keeping and schedule.

The autonomous traffic system expert workshop was held in June 2022. Three experts participated in the workshop. The workshop addressed topics such as:

- Challenges, risks and requirements related to the tram stops areas, intersections with other vehicles and pedestrians, and possible obstacles on a track
- Cabin surveillance including getting in and out of the tram
- Remote operation of the trams
- Visions for the future of autonomous tram transportation systems (2-5 years and 5–15 years from now on).

## SAFETY ANALYSIS OF TRAM TRANSPORTATION

### Some Results From Interviews and Workshops

As presented above, the experts thought that deficient monitoring of other vehicles and pedestrians at intersection areas is one of the main risks faced by tram drivers. In addition, it is challenging to ensure safe entering and exiting while opening and closing tram doors, because monitoring of tram saloons and tram stops are mainly camera based.

Tram transportation operators monitor tram traffic, communicate with drivers and other stakeholders, and react to possible problems. A control centre has multiple workstations and monitors, and there is an extensive information flow from sensors and cameras to the control centre. It is important that the received information is relevant and presented in an user-friendly format so that the operators can maintain adequate situation awareness.

The experts visioned the future of autonomous tram transportation. The development of autonomous driving will have an effect on the evolution of tram transportation in the near future (2-5 years from now on). Lidar based sensors are one of the main enablers of autonomous tram transportation. They are especially useful, e.g., in providing spatial information around the tram. Despite of the advanced sensor systems and other enablers of autonomous driving, in emergencies and other exceptional situations there is a need to drive a tram from the control centre. For example, very harsh weather conditions or catching up with the timetable delays might cause the need to operate the trams remotely.

The development of autonomous driving technology will also leverage the development autonomous tram solutions for 5–15 years from now on. The other vehicles can co-operate with autonomous trams, and advanced sensor solutions help trams to adapt to other traffic. It was also visioned that further in future the autonomous trams are able to cope with complicated and sudden exceptions. It was seen that sensors become more versatile and accurate, and there is also a better coverage of the sensors. This will enable self-diagnostic solutions to detect, categorize and retrieve malfunctions.

## FRAM Analysis of Autonomous Tram Driving

Safety analysis of driving automation has to take into account that the traffic system is complex, non-linear and tightly coupled. The classical error identification methods mentioned above cannot fully encompass this complexity, and therefore we have turned to more systemic safety analysis methods, which seem to be more suitable for the analysis of risks associated with autonomous public transportation systems. Examples of such methods are Systems-Theoretic Process Analysis (STPA) and Functional Resonance Analysis Method (FRAM).

FRAM can be used as a tool for understanding the reasons behind the gap between work-as-imagined and work-as-done, from the perspective according to which the autonomous system represents work-as-imagined, and the actual tram operation represents work-as-done. There are some recent studies in which FRAM has been applied in analysis of autonomous driving (Grabbe et al., 2020; Hirose et al., 2021).

A FRAM model was developed by a free software tool called the FRAM Model Visualizer (Hill & Hollnagel, 2016), which is freely available at https://functionalresonance.com/the%20fram%20model%20visualiser/. The basic idea behind the FRAM is to develop questions that are discussed with those who will use the system in their work (Laarni et al., 2020). The objective of these questions is to identify the critical functions related to the operation of a tram system and the interactions of these functions.

FRAM is based on a couple of principles, for example, successes and failures are equally valued, tram operators are considered as proficient in adjusting their behaviour to the contingencies of each phase of the tram drive, and unanticipated events may be caused by unexpected interactions of multiple functions, e.g., in demanding weather conditions. As said, FRAM has shown to be a valuable tool in understanding the reasons behind the gap between work-as-designed and work-as-done (Hollnagel, 2012).

Figure 4 shows a graphical depiction of a FRAM function with the six aspects. Input is something that is transformed by the function (e.g., information about the traffic situation in front of the tram); Output is the result of the function (e.g., decision to start to brake); Precondition specifies conditions for the fulfilment of the function (e.g., fulfilment of critical safety protocols of an autonomous system); Resource specifies what is consumed when the function is executed (e.g., operators located at a control centre); Control specifies rules and regulations followed while the function is conducted (e.g., the road traffic law); and Time specifies temporal restrictions that have to be considered (e.g., tram timetable).

To build the FRAM model, the main functions and their interrelations were first identified and presented by the FRAM notation. Second, the couplings between functions were defined and illustrated by thin lines connecting the functions (Figure 5).

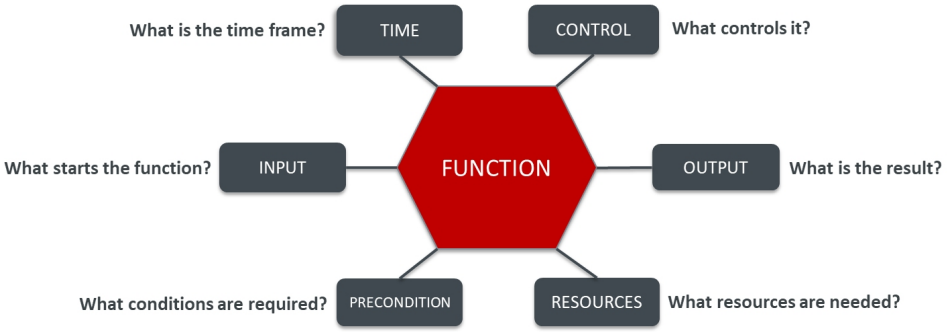


**Figure 4:** Constituents of a FRAM function (adapted from Hollnagel, 2012).

A simple FRAM model for pulling over the tram at the tram stop is presented in Figure 5. Only a small subset of all possible couplings is displayed. The aim is to stop the tram at a predefined position for passengers to board and alight. The main action is represented by two functions 'Approach tram stop' and 'Start braking'. Three functions 'Monitor driving info', 'Monitor pedestrian info' and 'Monitor passenger info' demonstrate building operator situation awareness, and there is an input-output coupling between them and 'Approach tram stop' and 'Start braking' functions. The three monitoring functions are, in turn, coupled with 'Be aware of current situation' function which demonstrates the comprehension of the overall driving situation. The monitoring functions are also coupled with 'Alert operator' function. The comprehension of the situation provides output to the next two functions entitled 'Plan next actions' and 'Pull over tram', which terminates the task.


**Figure 5:** Simple FRAM model with potential couplings related to approaching and stopping at a tram stop.

The next task would be to evaluate the FRAM model with regard to the number of couplings, since according to Laarni et al. (2020) their number is associated with the variability of a particular function so that the variability increases with the number of couplings.

## DISCUSSION

Even though autonomous public transportation systems such as autonomous trams can be safer than the present human-driven system, they have to be developed in a precautionary manner. Since autonomous trams and busses at the highest SAE levels are at present not necessarily safer than operator-driven vehicles, their risks and benefits have to be carefully analysed and evaluated (cf. Resnik & Andrews, 2023). We have proposed FRAM as a useful tool in safety analysis of an autonomous tram system. FRAM could be especially helpful in the analysis of novel technologies of which there is little previous experience. Previous findings suggest that the method is quite sensitive, and it is able to identify hidden couplings and low variability in functions, which may be difficult to identify by more traditional safety analysis methods (Laarni et al., 2020). However, Laarni et al. (2020) proposed that since FRAM may identify negligible couplings and imagined variability, it is important to discuss with tram drivers and other experts whether they consider the variability real or not. It is therefore important that the findings are evaluated against an independent set of criteria.

One problem with the method is that since a hierarchical structure is missing from a FRAM model, it is difficult to zoom in or out on a model and find the optimal level of detail (Laarni et al., 2020). In order to find the optimal level, it is necessary to perform the modelling work at various levels of detail.

In general, safety analyses have to be performed at different levels of detail: higher-level analyses are targeted towards the system's overall performance; lower-level analyses at the sub-system level focus on, e.g., designing the system components for maintaining safety limits. And in order to see the potential safety challenges from different vantage points, safety analyses would have to be performed from the perspectives of main entities of the system, that is, the autonomous tram system itself, passengers and other road users (i.e., vehicles and pedestrians).

Safety analyses provide input not only to the design of autonomous transportation systems, but they give also partial answers to ethical questions and concerns related to autonomous public transportation. Overall, they help us to answer one of the primary questions of autonomous driving: on what time span could we develop and deploy autonomous public transportation systems such as trams and shuttlebuses so that we are able to avoid and minimize all potential risks?

## CONCLUSION

Public transportation has more and more autonomous features, and the results can be used in future autonomous transportation solution development work and studies. Functional Resonance Analysis Method (FRAM)

was used in safety analysis of an autonomous tram system. There is no ready-made safety engineering baselines and guidelines to gather and interpret future autonomous tram transportation systems. FRAM method enables us to identify hidden couplings and low variability in functions, which may be difficult to identify by more traditional safety analysis methods. The FRAM method can help to illustrate possible risk issues and dependences among functionalities in public transportation solutions.

## ACKNOWLEDGMENT

The research was funded by Business Finland under the SmartRail 2 project. We would like to thank all interviewees and workshop participants for their valuable contribution.

## REFERENCES

Ghasemieh, A., Kashef, R. (2022) 3D Object Detection for Autonomous Driving: Methods, Models, Sensors, Data, and Challenges, Transportation Engineering Volume 8 100115.

Grabbe, N., Kellnberger, A., Aydin, B. and Bengler K. (2020) Safety of Automated Driving: The Need for a Systems Approach and Application of the Functional Resonance Analysis Method, Safety Science Volume 126 104665.

Guerrieri, M. (2018) Tramways in Urban Areas: An Overview on Safety at Road Intersections, Urban Rail Transit Volume 4 pp. 223–233.

Hill, R., Hollnagel, E. (2016) Instructions for Use of the FRAM Model Visualiser (FMV) Website: https://zerprize.co.nz/Content/FMV_instructions_2.1.pdf.

Hirose, T., Sawaragi, T., Nomoto, H. and Michiura, Y. (2021) Functional Safety Analysis of SAE Conditional Driving Automation in Time-Critical Situations and Proposals for Its Feasibility, Cognition, Technology & Work Volume 23 pp. 639–657.

Hollnagel, E. (2012) FRAM, the Functional Resonance Analysis Method: Modelling Complex Socio-Technical Systems. Farnham, Surrey, UK: Ashgate.

Iclodean, C., Varga, B. O and Cordos, N. (2022) Autonomous Vehicles for Public Transportation. Cham, Switzerland: Springer.

Laarni, J., Tomminen, J., Liinasuo, M., Pakarinen, S. and Lukander, K. (2020) "Promoting operational readiness through procedures in nuclear domain", in: Engineering Psychology and Cognitive Ergonomics. Cognition and Design. HCII 2020, Harris, D., Li, WC. (Eds.) Lecture Notes in Computer Science Volume 12187. Cham, Switzerland: Springer.

Laarni, J., Väätänen, A. (2023) "Development of a Concept of Operations for an Autonomous Tram System", proceedings of the Intelligent Human Systems Integration (IHSI 2023) 69 pp. 541–549.

Margaritis, D. (2007) Accident Analysis into the Primary and Secondary Safety of City Trams in the Netherlands. Association for European Transport and contributors. Leiden: European Transport Conference.

Naweed, A., Rose, J. (2015) "It's a Frightful Scenario": A Study of Tram Collisions on a Mixed-Traffic Environment in an Australian Metropolitan Setting, Procedia Manufacturing Volume 3 pp. 2706–2713.

Naznin, F., Currie, G. and Logan, D. (2018) Exploring Road Design Factors Influencing Tram Road Safety - Melbourne Tram Driver Focus Groups, Accident Analysis and Prevention Volume 110 pp. 52–61.

Palmer, A. W., Sema, A., Martend, W., Rudolph, P. and Waizenegger, W. (2020) "The Autonomous Siemens Tram", 2020 IEEE 23rd ITSC pp. 1–6.
Resnik, D. B., Andrews, S. L. (2023) A Precautionary Approach to Autonomous Vehicles, AI and Ethics Website: https://doi.org/10.1007/s43681-023-00277-6
Sagberg, F., Saetermo, I.-A. F. (1997) Traffic Safety of Tram Transport in Oslo, TOI Report (367).
SmartRail Ecosystem Website: https://smartrailecosystem.com/ (Retrieved May 19, 2023).