Setting safety foundations in the Hyperloop: a first approach to preliminary hazard analysis and safety assurance system

1. Introduction

Hyperloop is the name given to a radically new transport mode. First proposed by Elon Musk in 2013 (Musk, 2013) and boosted trough a university contest, several research teams and start-ups that combine resources from other public and private organizations are working now in its development. This has become a truly global movement that involves hundreds of engineers and other professionals across the world.

In its basic definition, Hyperloop is a mode of transport that consists of two components: a linear infrastructure, in the form of an almost vacuum-sealed tube; and a vehicle (pod) that levitates and advances at high speed (close to 1,000 km/h) along the tube using magnetic and electromagnetic forces (Kumar et al., 2019; Van Goeverden et al., 2018).

The titanic development effort is justified from an environmental point of view, as transportation is responsible for a significant amount of greenhouse gas emissions (GHG). For instance, in the European Union, transport accounts for 31% of the total energy consumption and produces about 1,250 million tonnes of CO_2 equivalent per year (European Commission, 2019). In fact, transport is the only sector where CO_2 emissions have steadily increased from 1990 levels in the EU-28, to the point that it now represents a 30% of the total emissions, compared to just 20% in 1990. This is in part because demand for mobility is also growing steadily, with annual growth rates of 2.4% for passengers and 2% for freight in the EU-28 (European Commission, 2019). Finding ways to reduce GHG emissions from transportation is thus crucial (Chapman, 2007; Uherek et al., 2010) to achieve a more sustainable society.

The main efforts in this direction have been either fuel consumption reduction or more efficient alternative fuels (i.e. electric vehicles). The results from these efforts could however be reaching their limit, as the theory of the innovation S-Curve in technology suggests (Utterback, 1994). Following this theory, we could be in the last part of the S-Curve, where even significant efforts trying to refine the technology do not produce substantial improvements. We need another kind of innovation, meaning disruptive innovation. We have to change to another S-curve. We must turn to technologies that use different logics, and that would probably be in a fermentation stage, in the first part of their S-curves.

The Hyperloop emerges from these disruptive logics, proposing new ways to reduce energy consumption in transportation. Most of the power and, therefore, most of energy consumption in current transport modes is used to overcome friction against the ground and the surrounding air. By levitating the vehicle inside a low-pressure tube, the Hyperloop

dramatically reduces resistance and thus the energy consumption and associated emissions.

As the Hyperloop is still in early stages of development, it is quite difficult to estimate its actual costs and impacts in comparison to existing modes. Nevertheless, a few preliminary assessments have been carried out with somewhat differing results. For instance, Van Goeverden, Milakis and Konings (2018) made a comparison between Hyperloop, high-speed rail and aviation over an average distance of 600 km. They found that the former may outperform the other two in terms of social/environmental impacts but not in terms of economic/financial performance due to much lower capacity, (although the authors admit that this may change depending on the technological development of the Hyperloop).

Janić (2020) studied the energy consumption and CO_2 emissions of Hyperloop, high-speed trains and maglev trains, and found out that the former may be more efficient depending on seat capacity and distance. Finally, Hansen (2020) raises several uncertainties regarding the Hyperloop performance and considers that it will not be able to compete with traditional modes unless it offers clear advantages in terms of reduced travel time, safety and comfort. In any case, all these studies are partially based on assumptions and simplifications regarding this new system, and recognize to some extent the potential of the Hyperloop to become an alternative to traditional transport modes.

However, any transport activity may carry risks for people and goods, risks that can result in the loss of human lives, as well as substantial economic losses. Addressing safety is therefore an essential aspect within the development process of a new transport mode such as the Hyperloop.

On the other hand, safety must be approached from all the perspectives and areas involved in the development and operation of a transportation system. Safety is in this sense an unavoidable component of the system, but also, and at the same time, a systemic emergent of the transport system, its components and the interaction between them (Amalberti, 2001; Gherardi and Nicolini, 2000).

Likewise, safety must be addressed from the very beginning, when the vehicle is conceptualized, the infrastructure is designed and the interactions between the vehicle, the infrastructure, the people and the environment are analysed. Failure to do so, that is, addressing safety afterwards, would entail modifications and redesigns of the system that would imply delays in development and execution deadlines, as well as significant extra costs. This is the core motivation for our study, as we aim to instil that very idea of safety as an essential feature of all the research and development related to the Hyperloop.

That said, as we are dealing with safety in a radically new mode of transport that is in the stage of its initial conception and technical validation (as the Hyperloop is now) we are breaking new ground, and we need to advance the frontiers of knowledge.

The work presented here has therefore a clear exploratory nature. Its first goal is to establish the premises and keys for including safety into the Hyperloop development process, from the beginning and as a foundational criterion. Nevertheless, this exploratory work takes as a starting point the already available knowledge related to safety in other more developed and operating modes of transport. Although the focus is on commercial aviation and railways, other, more innovative modes are also analysed, including autonomous vessels.

Given that the focus of the study is rather broad, we will confine it to the field of safety, which is understood here to be related to the behaviour of the system itself. In other words, we have left for future works another vast field, that we call security, that is related to malicious actions by third parties, such as terrorism, cyberattacks, etc. Analogously, we have left regulatory issues out of this article, because we think it is premature to address them, although our conclusions could pave the way to a regulatory framework for the Hyperloop.

The paper is structured as follows. First, in section 2, a comprehensive analysis of existing modes is presented, in order to extract safety principles and measures that may be applied to the Hyperloop. Afterwards, in section 3, the safety and preliminary hazard analysis methodology used throughout the paper is explained. Then, in section 4, that methodology is applied to the Hyperloop case in order to establish a foundation for safety for this innovative transport mode. Section 5 discusses our main findings and results, as well as the limitations of our study, and a first set of recommendations for practitioners are presented. Section 6 closes the article with the main conclusions.

2. Starting points for introducing safety in the development of the Hyperloop

2.1. Overview

Safety has long been addressed in other modes of transport, using different methodologies. These methodologies range from reactive ones, which propose improvements in the system once events (accidents) have happened; to truly preventive methodologies, through heuristic and experimental procedures that test the systems in order to understand and predict their behaviour.

Safety must be approached from an integral perspective (Stoop and Thissen, 1997), that includes all components involved, i.e. infrastructure, superstructure, moving material (the pod in the case of the Hyperloop), the management system and the human factor. The latter is particularly relevant. It does not include only people on board (passengers and staff), but also risks for other staff working in the system as well as other people who might be close to the infrastructure.

In a first review, we identified several modes of transport that could teach us useful lessons, including commercial aviation, railways, autonomous ships, aerospace navigation and vertical transport (elevators). After a first review, we found the first three particularly useful, and we have reviewed them to take advantage of the knowledge available in the field of safety. Conceptually, the Hyperloop shares more characteristics with aviation and railways than with elevators and spaceships. In fact, one of the Hyperloop promoters described it as an airplane that moves like a railway, during an informal conversation. On the other hand, unmanned vessels show how safety has been addressed in a relatively new mode of transport.

The goal of this review is to use this knowledge as a starting point for its extrapolation to the Hyperloop case, setting up an ex ante approach to safety in a new mode of transport. In the following subsections, we analyse the main findings regarding safety in those three modes and summarise their potential application to the Hyperloop.

2.2. Aviation safety as a reference

A convenient management of the risks associated with commercial aviation has made this mode of transport the safest of those currently existing (Janic, 2000; Oster et al., 2013). It is also the mode of transport that, while transporting a significant volume of passengers, reaches the highest speed. Its usefulness as a reference is therefore more than justified.

A first teaching provided by aviation may be related to the principles that inspire safety management in this mode of transport (Perrin et al., 2005). This is a summary list:

- Everyone (passengers included) is responsible for safety.
- Safety must be approached proactively, and even predictively, as well as reactively.
- Safety must be addressed globally. ICAO (International Civil Aviation Organization) centralizes the issuance of recommendations that national entities responsible for safety will transpose into national laws. It is the case of FAA in the USA (Federal Aviation Administration) and EASA in the European Union (European Union Aviation Safety Agency).
- Safety must be addressed in depth. Accident investigation, for example, should not stop when the immediate or apparent causes are found, but it should aim to identify the root causes and their scope.
- Safety must be comprehensively addressed, i.e. it should cover all the areas involved (aircraft, airport, air traffic, etc.), all the useful tools, the training of the people involved, etc.
- Safety must be addressed in a balanced manner. When investing in resources that avoid incidents and accidents, it is required a good risk evaluation, measuring both the severity of their consequences and the probability of their occurrence.
- Safety must be planned systematically, that is, establishing a powerful SMS (Safety Management System) that includes four components:

    - Safety policy: establishes organizational commitment to safety, as well as the methods to accomplish this commitment, in a written manner.
    - Safety Risk Management: must be able to identify potential safety threats, assess their probability and scope and mitigate their incidence and effects.
    - Safety Assurance: must be able to make evolve the entire system towards increasing levels of safety.
    - Safety Promotion: must be able to boost a safety-oriented culture, through communication, training, incentives, etc.
- Safety management must introduce technological advances related to specific conceptual, methodological and technical tools.

Based on these principles, the list of improvements recently introduced in the field of commercial aviation is spectacular. These include improvements in aircrafts (e.g. reliable engines, structural integrity, resilience against weather conditions, redundant systems, etc.) and airports (e.g. signalling, specific guidelines and procedures for technical operations, etc.). Moreover, every airport is required to have a mandatory AEP (Airport Emergency Plan) that provides detailed response to all kind of abnormal circumstances, such as aircraft accidents, bomb threats, kidnappings, fires, natural disasters, etc.

There is a clear push for automation in this mode of transport to reduce human errors. However, two recent fatal accidents, experience by the new Boeing 737 MAX model in 2018 and 2019, suggest that staff qualifications should not be relaxed assuming automation would cover the difference. Instead, evolving the role of the human factor with a full understanding of the limitations of automation can be crucial (Spielman and Le Blanc, 2021). Another lesson learned from the Boeing 373 MAX case is the importance of meticulously testing a prototype during the new product development stage (Naor et al., 2020).

Additionally, many experts have proposed the simplification of mechanisms and processes as an alternative or complement to automation (Cusick et al., 2017).

Another useful lesson that we can draw from aviation safety management is the use of conceptual models to improve safety. These models help us understand a complex reality, such as air safety, in order to act on it and improve it. Reason's model (or Swiss cheese model), also used in the realm of rail transport, can help in developing a safety framework for the Hyperloop (Cusick et al., 2017).

2.3. Railways safety as a reference

Railways have a long history of operation and safety improvements since their inception in the XIX century. Many systems and procedures have been developed, tested and implemented to ensure a safe and reliable transport of both passengers and goods.

One of these elements, specific to railways, is the blocking system, which avoids rear or head-on collision between two trains. The simplest blocking system ensures for instance a

minimum distance between two trains, by dividing the track in sections, and avoids a train entering a section occupied by another train.

On the other hand, it is necessary to ensure that any change in the signals that govern the movement of the trains does not authorize any dangerous movement or lead to hazardous conditions. Interlocking systems are used for this goal. For example, it prevents access to a track from two others simultaneously. The combination of blocking and interlocking systems makes it possible to safely operate more complex rail networks.

The increasing complexity of railway systems also requires greater automation. Many of the subsystems (signalling, communications, traction, etc.) are controlled electronically, and therefore depend on software for their regulation and proper functioning. Software is, consequently, a critical element for the safety of the railway system. Current automatic locking systems even replace the driver under certain scenarios. For example, the train could be stopped by means of a track beacon, in case the train circulates improperly.

Within this context of growing complexity and demand, there is an extended literature regarding safety features and developments on railways. This includes, for instance, reliable development (Chen et al., 2019; Myklebust et al., 2017), and testing (Li et al., 2016; Lüley et al., 2012) practices for critical software. Other aspects that have encouraged further study and development in recent years are the implementation and enhancement of Safety Management Systems (Accou and Reniers, 2019; Lefsrud et al., 2020), the use of newer accident modelling methods (Alawad et al., 2020; Klockner and Toft, 2015) or the improvement of maintenance assessment and procedures (Barbosa, 2016).

At European level, there is an increasing push for harmonisation of many aspects of railway operation, and that includes all safety aspects. For instance, the adoption of a Common Safety Method (CSM) on risk evaluation and assessment by the European Union (Commission Regulation (EC) Nº 352/2009, 24 April 2009) aims to achieve a standardised safety approach. The implementation of such method may help to address the issue of risk assessment in the Hyperloop.

Safety is related to all the elements of the railway operation: infrastructure (including not only the track itself but all associated systems, such as signalling, electrification, etc.), rolling stock, attached facilities (stations, sidings, workshops, etc.), as well as the different regulations, policies and inspection and maintenance tasks. In most countries, there is national railway organisation responsible for different aspects of railway safety. Within the EU, these include:

- Regular inspections of network safety and reliability.
- Safety certification issuance for railway operators and managers.
- Implementation of regulations.
- Accident investigation.

At the EU level, the European Union Agency for Railways (EURA) assumes these tasks to some extent. This organisation aims to contribute to the effective functioning the Single European Railway Area and to promote a harmonised approach to railway safety. In order to do so, the EURA devises technical and legal framework related, among other areas, to safety, and acts as the European Authority concerning vehicle authorisations and safety certificates.

One of the conditions that the EURA requires for any operator or infrastructure manager that wishes to obtain a Safety Certificate or Safety Authorisation is to define and implement a Safety Management System (SMS) in accordance with EU Directive 2016/798. The purpose of this is to make sure that the applicant complies with all the safety obligations. This kind of certification by national or supranational safety organisations may be incorporated to the Hyperloop as a way to ensure that the system incorporates essential safety features.

The most recent evolution in terms of rail traffic safety, at the European level, is the ERTMS (European Rail Traffic Management System), which is in the process of becoming a standard shared by the entire European railway network to ensure interoperability between different member states. One of its main components is the ETCS (European Train Control System), an advanced blocking and control system for signal compliance and speed limitations. The ETCS is mandatory for any EU funded projects (including new and upgraded lines) since 2009.

There are four main levels of ETCS implementation, and in the highest one (L3), the vehicle position and speed are controlled in real time by means of a GSM-R system (wireless communication between vehicle and track) or GNSS (Global Navigation Satellite System). By doing this, the fixed track sections are replaced by mobile sections associated with each vehicle, hence allowing a safe increase of line capacity and speed. Although the ETCS L3 is still under development, many high-speed lines across Europe have already implement lower ETCS levels, such as the LGV line from Tours to Bordeaux in France (ETCS L2) or the AVE line from Madrid to Barcelona in Spain (ETCS L2).

Finally, and in order to anticipate data related to the operation of railway lines, we can add that lines with double track and a good automatic blocking system can reach capacities of 500 daily trains in each direction. This means a train every 2 minutes in each direction (Losada, 1991). In automated underground lines, where speeds are lower, capacity can increase up to one train per minute. This is the case of the Lille Underground (France) at peak times (González Fernández, 2013).

All things considered, a standardised, highly automated and sophisticated control system similar to the ETCS (and the overall ERTMS system) may be developed and implemented in the Hyperloop to improve both safety and capacity.

2.4. Autonomous vessel safety as a reference

Well-established modes of transport such as aviation and railways may suggest a wide list of safety resources and procedures, developed and applied in both areas over decades. Nevertheless, as we are dealing with a new mode of transport, it could be useful to review how safety has been addressed in other innovative modes, even if they are not as disruptive as the Hyperloop. In order to do so, we explored the most cited literature related to unmanned vehicles, such as autonomous vessels and drones. In a first approach, we found the literature regarding the later more dispersed and less useful as a reference for our study. On the other hand, literature on autonomous vessels (or ships) seems more useful, particularly with regard to the subject of methodology.

An autonomous vessel or ship is 'a merchant vessel which would travers the ocean without having any crew on board or even being controlled remotely' (Wróbel, Montewka and Kujala, 2018, pg. 209). Its development is the object of a few current projects. Physically, an autonomous vessel is not as radically new as the Hyperloop but, conceptually, it introduces disruptive challenges, particularly in relation to safety. In fact, research related to safety in autonomous vessels has grown dramatically over the last decade. Some of the most cited articles on this subject focus on analysing systemic hazards, thus in line with the purpose of our work.

Safety hazards must be addressed before the planning of the ship (Valdez Banda et al., 2019). The literature on unmanned vessels safety proposes different available methodologies to identify and control hazards on this topic. Rødseth and Burmeister (2015) use a framework based on the Formal Safety Analysis suggested by IMO (2007), although they recommend keeping the system complexity as low as possible, simplifying the mission and the environmental constraints.

Some articles use a methodology named System Theoretic Process Analysis (STPA), proposed by Leveson (2011). Valdez Banda *et al.* (2019) define a process that includes these steps: 0) pre-concept design; 1) definition of accidents and identification of hazards; 2) detailed hazards description and initial definition of mitigation actions; 3) definition of the safety controls; 4) identification of the unsafe control actions and redefinition of the safety controls; and 5) representation of the initial safety management strategy.

Wrobel, Montewka and Kujala use STPA methodology in order to identify how the safety constraints may be violated and how to prevent such violations (Wróbel et al., 2018b). These authors found this technique useful to system developers to incorporate a holistic safety approach to design unmanned ships (Wróbel et al., 2018a).

Some conclusions of this literature could be transferred to other transport fields. Reliability of technical systems and increased redundancy are crucial (Hoem et al., 2019). Even fully autonomous vessels are expected to include humans in the safety loops, although endowed with new tasks and abilities (Ventikos et al., 2020).

3. Methodology

Hazard and risk analyses are always iterative processes. An exhausted analysis from scratch is hardly possible, particularly when the object of the analysis is only in a pre-design stage. The goals of the hazard and risk analyses are in this case limited to find a list of hazards as wider as possible, as well as an initial definition of mitigation actions and safety controls.

Rausand and Haugen find three hazard identification methods to be good or suitable for hazard identification when the system is in its early design: Checklists, Preliminary Hazard Analysis (PHA) and Structured What-If Technique (SWIFT) (Rausand and Haugen, 2020). Checklists are based on past experience, hence it is not a method that can be applied to the Hyperloop. We also discard more sophisticated methods used in other new modes of transportation, like STPA in unmanned vessels. In practice, an unmanned vessel is the same vehicle as a piloted one. Changes are limited. It is not the case of a completely new vehicle, like the Hyperloop. Nevertheless, Fleming applied STPA methodology to early concept development (Fleming, 2015), defining Systems Theoretic Early Concept Analysis (STECA). We found this methodology useful for a second iteration of the hazard analysis process, with a better-defined Hyperloop design. At the current stage of design there are many undefined components and relations among them, which make it difficult to build the control loops that are the backbone of this methodology. In fact, Fleming and Leveson (2016) applied STECA to the new Trajectory-based Operations (TBO), which is a shift from the current Air Traffic Management, but it is not so radically new.

SWIFT offers a more systematic procedure to identify hazardous events. In fact, it is this procedure what gives name to the method. SWIFT proposes the use of what-if questions during brainstorming sessions, in order to identify possible hazard events, their causes, consequences and existing barriers and, then, to suggest alternatives for risk reduction. What-if questions can include What if…?, Is it possible that…?, How could…?, etc. As an example, a brainstorming group would ask ‘How could the pod collide against the tube?’, looking for possible causes of this hazardous event. Figure 1 summarizes our methodology.

No hazard identification method can guarantee that all potential causes of one hazardous situation are identified (Jagtman et al., 2006). Nevertheless, we tried to get an exhausting list of potential causes using two techniques. First, we asked What-If question three times in a row, as suggested by Semler (2004) in order to identify the basic causes. We found that asking What-If question five times in a row, as suggested by Ohno (1988), was not useful, because we did not have enough details to answer these additional questions. Consider for instance and accident produced by the collision of the pod against an object. Why did the pod collide against an object? Because it was located inside the tube. Why the obstacle was inside the tube? Because it fell from another pod. Why did it fall from another pod? Because it was not correctly fixed.

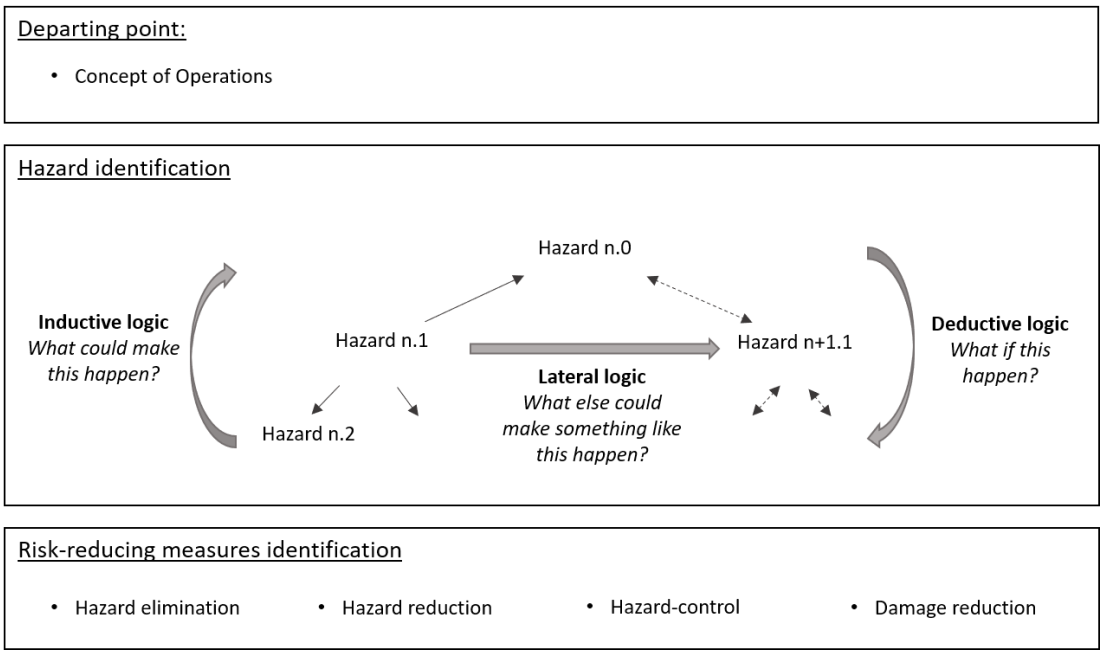

Figure 1.- Our methodology

Second, we used the 'Concept fan', a creative technique proposed by Edward De Bono (De Bono, 1992). Once we have a specific cause, we can go backwards to find the general concept that includes this cause, and then forward to identify similar causes. In practice this is equivalent to moving laterally. For instance, in the example above, the object could fall from a pod, but it could be also a mechanical component that came off the tube, or something that someone forgot during a maintenance revision. All these alternative explanations open new paths in the prospective causal map.

In order to get an exhaustive map of potential hazards, we applied SWIFT going forward and backward. We think SWIFT offers its best results alternating between deductive causal approach and inductive causal approach. Mazouni et al. suggest something similar for PHA (Mazouni et al., 2007). Considering both, deductive and inductive logics, the Bow-tie method is also conceptually similar to our method (Rausand and Haugen, 2020).

To suggest risk-reducing measures, we used as a guide the four categories suggested by Leveson: hazard elimination, hazard reduction, hazard control and damage reduction (Levenson, 2011), thus matching what other authors did with unmanned vessels safety (Valdez Banda et al., 2019; Wróbel et al., 2018b).

The best way to minimize the consequences of an accident is to prevent it from happening, that is, to design the transport system so that accidents are impossible. In other words, the system and its components should be organised so that the accident cannot occur. This will be particularly important in the case of those risks whose consequences are not tolerable,

whether due to their severity (catastrophic) or the frequency of their occurrences (frequent, even probable). The best way to do so is eliminating or reducing hazards.

Even with a design that avoids accidents, they will eventually occur, thus making methods for failure detection and correction necessary. In some cases, because the design has not taken them into account (due to its infrequency and low severity). In other cases, due to unforeseen or poorly predicted risks. These latter cases will require an in-depth review (accident analysis), a possible reconsideration of the risks and an eventual redesign of the system. Ultimately, this further proves that safety must be addressed as a process, not as a state, and one of continuous improvement. In any case, it is necessary to understand the occurrence of one of these safety failures as a hole in the first barrier of the Reason model (constituted by the set of decisions and procedures established by the organization management to ensure a safe operation). The system must therefore include other barriers, in order to react and avoid the accident.

Finally, if neither the design of the system nor the previous control mechanisms have managed to avoid the accident, a third type of measures must be put into action, aimed at minimizing the consequences of the accident.

4. Addressing safety in the Hyperloop

4.1. Initial settings for the Hyperloop

Although the final Hyperloop parameters are yet to be set, a risk analysis should refer to an already defined system with clearly defined conditions, something like a preliminary Concept of Operations. Therefore, a basic definition should been set to serve as a basis for the application of the theoretical framework described above to the Hyperloop. Future changes to these parameters will require the revision of the conclusions related to safety obtained from them. Safety management is essentially a continuous improvement process.

These are the starting parameters:

- The vehicle is initially designed for 50 to 100 passengers, with a length of approximately 40 to 50 meters, and will be constructed with composite materials to ensure its lightness.
- The vehicle levitates along a monorail or a similar configuration attached to the tube bottom and, in addition to the electromagnetic effects, an air compressor established at the rear of the vehicle pushes it. This makes unfeasible to introduce bi-directionality in the vehicle.
- An alternative impulsion system is added to the vehicle, since the compressor will not be effective below a certain speed.

- To embark and disembark people and personal belongings, a double gate system is proposed. This facilitates the maintenance of the vacuum in the main tube, isolating it from the atmosphere in the stations.
- Figure 2 advances a basic configuration of the infrastructure. It proposes two solutions for the change of direction in terminal stations. The first one, on the left, uses a loop. The second one, on the right, uses a turntable. The proposed configurations are similar to those used for magnetic levitation systems currently in service, such as the Transrapid, built in Emsland, Germany (Cassat and Bourquin, 2011).
- We pursue a speed close to one thousand kilometres per hour. Current systems based on electromagnetic levitation have reached speeds of 600 km/h.
- In order to achieve profitable capacities, it is required a frequency of 24 vehicles per hour in each direction (one vehicle every 2.5 minutes).
- The specific technologies to be used for the different vehicle subsystems (levitation, driving, cooling, navigation, power supply, etc.), as well as on the infrastructure (vacuum generation, energy transmission, vehicle guidance, information transmission, etc.) and the control system, are currently under development, and protected by confidentiality agreements.

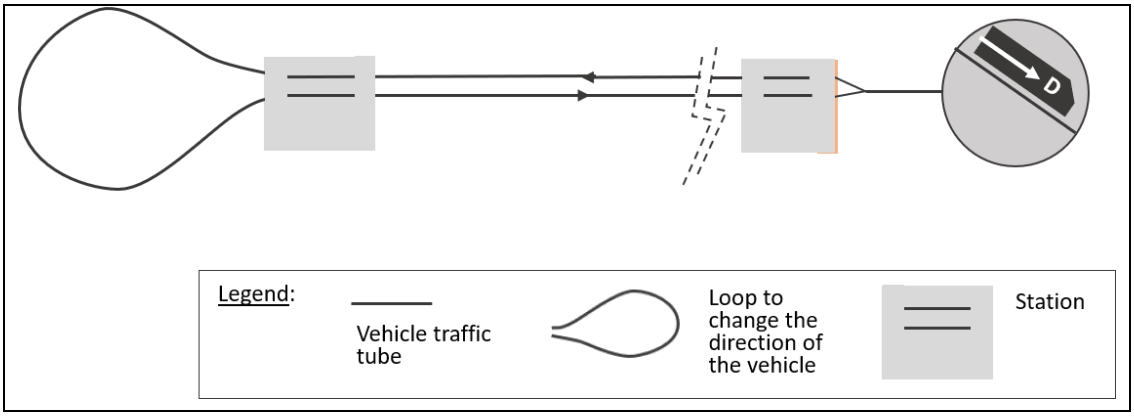

Figure 2.- Basic configuration of the Hyperloop

4.2. Safety responsibility

Safety must be addressed with a systemic approach, as it is done in other modes of transport. Since there is no such system yet, the first task should be its initial definition and implementation. For this, it is essential to appoint a person responsible for that purpose,

vested with both the authority and the power given by his or her attribution. This Safety Officer must assume different roles, which can be classified into three categories:

- Safety promotion roles:
    - To provide a safety perspective to all of organizational tasks performed for the Hyperloop development.
    - To promote the assumption of this perspective by each and every person involved in this development.
    - To promote the assumption of this perspective at a higher level, that is, beyond the company limits, actively participating in any initiative promoted to improve safety globally.
- Development of policies and instruments for safety management:
    - To set safety policies that inspire new developments in this area.
    - To develop a first risk analysis that can grow with the transport system itself. We will build on this later.
    - To develop training programmes that include policies and instruments, and deliver these programmes to the staff and other actors involved in the Hyperloop development.
- Safety management system development roles:
    - To identify new hazards and risks.
    - To measure hazards and risks frequency.
    - To measure and forecast the impacts produced by the identified risks.
    - To propose improvements related to safety in all of the systems at the design level.
    - To propose improvements related to safety in all of the systems at the operational level.
    - To propose improvements in failure alert and diagnosis systems.
    - To propose improvements in damage mitigation systems.

The Safety Officer should occupy a position at the organizational upper echelons, in order to ensure that safety receives significant attention. Alternatively, this responsibility may be assigned to a member of the strategic apex.

In summary, the Safety Officer must have enough power (being part of the strategic apex), authority (by experience and qualification) and leadership (awareness on safety issues). Of course, this not denies the fact that safety is everyone's responsibility.

4.3. Towards a safety management system in the Hyperloop

The development of the Hyperloop is an exceptionally ambitious project that cannot be approached by a single company alone. This kind of projects involve the development of one or several innovative technologies, as well as numerous specific complementary

systems required by those technologies. In this kind of projects, the attitude of the organizations involved should not be to compete with each other, at least at the beginning. It is rather to create firstly a new product (a mode of transport in this case) and then to create a new market.

Innovation barriers are powerful in this kind of projects (Mateu and March-Chorda, 2016), and the synergies of a certain kind of collaboration are essential to overcome such barriers. The collaboration must reach at least those areas of the project that are key to the creation of the market. Seeking the collaboration of institutional leaders is one of these areas. These leaders may contribute to give visibility to the project, promote the required changes in the legal framework and provide different means, like financial resources, grants, etc.

In many other areas, such as product development in search of setting a standard (Utterback, 1994), organizations will compete, but the coexistence of both attitudes (Co-opetition) has proved viable and profitable in other areas and sectors (Brandeburger and Nalebuff, 1996). Under a market creation logic coopetition is required. The businesses must cooperate because consensus is needed to establish institutional standards, although they compete with each other to promote their own technology (Mione, 2009).

Safety must undoubtedly be guided by collaboration, rather than competition. Other modes of transport, such as those analysed in this paper, point in the same direction. Another sound argument when aiming to create a market for a new mode of transport is that potential users will demand safety to be a priority for everyone, in order to obtain the highest level of safety.

In this sense, it is recommendable to associate organizations that work in the development of the Hyperloop in a higher-level entity dedicated to safety. This could be, among other things, a precursor to a future organization that deals with global safety or, at least, the contribution of the industry (the sector) to an entity potentially promoted by public administrations.

4.4. A preliminary hazard analysis in the Hyperloop usual operations

Although the Hyperloop definitive parameters are yet to be fixed, it has already been said that a preliminary hazard analysis must refer to a previously defined system. Consequently, we will use the basic system definition set out in section 4.1. This can and should be specified and complemented in parallel with the Hyperloop development.

In a first approach, we focused on the identification of the main hazards of the system, i.e., those that may have catastrophic consequences. Our analysis identified seven main categories of potential accidents during usual operations: pod collision against the tube, pod collision against an obstacle or person in the tube, collision between pods, hazardous conditions inside the pod and specific hazards on stations, deviations and scape gates in the tube. We present now the results of our hazard identification method (described in section

3) applied to the first four categories. The results for the fifth one, specific hazards on stations, will be presented below. Specific hazards on deviations and scape gates will not be treated in this article, because their configuration is far from being defined.

The results for the first four categories analysis are summarized and presented in Figure 3 (some repeated statements have been omitted in order to simplify the figure, as well as details in hazards that are well known and managed in other environments, like fire and electrical hazards).

Many of the hazards presented in Figure 3 can have extremely serious consequences (catastrophic) because of the high speed, so they must be addressed in depth. Although this is difficult in the current situation, we propose a first analysis that serves as a starting point for further development. Table 1 undertakes this analysis for the most important hazards, cataloguing corrective measures by its nature: elimination or reduction hazard measures from design, hazard control and damage reduction. In order to simplify the table, some repetitions have been omitted.

Figure 3.- First map of potential hazards

	MEASURES		
RISK/SEVERITY	Of design	Related to control and response	Mitigation of unwanted effects
Collision against obstacle at high speed due to deformation, or persons or obstacles in the tube. CATASTROPHIC	Tube robustness. Good materials and good manufacturing practices. Resilient design. Consistent fit pod/track Good constructive practices. Good maintenance protocols. Limited access to the tube vicinity	Sensors along the tube or/and in the pod. Resilient and redundant telecommunication systems Automatic mechanisms to stop the vehicle in case of anomalies. Redundant brake systems. Alarms in case of malfunction or loss of integrity. Alternative power supply.	Rigidity and shock absorption in the vehicle. Particularly between the cabin and the turbine. Protocols and devices to reduce harm to persons. Rescue procedures.
Buckling on the tube surface due to compression forces plus loss of geometry CATASTROPHIC	(All of the above) Extra thickness. Building materials that behave better against buckling. Telescoping mechanisms. Heat attenuation mechanisms	(All of the above)	(All of the above)
Fast pressurization on the tube by a puncture or similar CATASTROPHIC	(All of the above) Aerodynamic design of the vehicle	(All of the above)	(All of the above)

Catching up another vehicle (stopped or slowed down). CATASTROPHIC	(All of the above) Automatic blocking system. Redundant vehicle monitoring system.	(All of the above) Autonomous inter-pods communication system	(All of the above)
Loss of pressurization in cabin CATASTROPHIC	Good materials and good manufacturing practices. Resilient design. Pressurization assurance systems.	Pressure indicators. Leakage alarms. Oxygen reserves automatic triggering.	Alternative breathing systems (oxygen masks). Escape stations.
Loss of levitation CRITICAL/CATASTROPHIC	Good materials and good manufacturing practices. Resilient design. Energy supply assurance systems. Levitation assurance systems.	Levitation indicators and alarms. Vehicle location monitoring. Impulse system without levitation. Redundant power supply.	Soft landing system on the ground tube. Escape stations.
Loss of power CRITICAL/CATASTROPHIC	Impulse assurance systems. Energy supply assurance systems.	Alternative impulse system. Redundant power supply. Towing mechanisms.	Escape stations. Recovery mechanisms and protocols.
Loss of communication CRITICAL/CATASTROPHIC	Good equipment and installation practices. Redundant channels and equipment. Robust software.	Good protocols for discrepancy events. Automatic on-board systems. General shutdown mechanisms in case of disconnection of any component of the network. Alarms.	Escape stations. Recovery mechanisms and protocols.

Table 1. Initial proposed measures (1) of design to avoid hazards, (2) to control and quick response and (3) to mitigate damage.

Anomalous circumstances in the tube could have their origin either in natural disasters (earthquakes, landslides near the tube, etc.) or in constructive or maintenance errors. Each of these origins will require a specific preventive treatment that we will address later.

Collisions between vehicles could have their origin in functional vehicle or infrastructure failures. Figure 3 shows how an important part of the list of potential failures may produce crashes between vehicles, because all these failures involve slowing down or stopping the vehicle.

On the other hand, Hyperloop developers might be paying less attention to the tube than to the vehicle, thus taking for granted decisions that could be questionable, such as the constituent material of the tube (steel). The tube is under unusual stresses which should be studied. Atmospheric pressure outside the tube is not offset by internal pressure, because an almost complete vacuum has been made inside. Additionally, thermal expansion along hundreds of kilometres of steel tube would introduce high longitudinal pressures. The sum of these stresses would probability facilitate buckling, if any structural damage compromises the geometry of the tube. This is an already well-known phenomenon in railways, where the use of Continuous Welded Rail (CWR) in new lines requires a careful consideration of temperatures during track construction, and yet rail buckling is still one of the most important causes of traffic interruptions and accidents (Dobney et al., 2009; Villalba Sanchis et al., 2020).

Additional risks can be produced by the internal vacuum. A puncture on the tube, for instance, might produce a strong flow of air entering the tube. We estimate that the effect on the vehicle would be temporary and not very harsh, except if the vehicle passes through the section of the tube where the puncture is located.

Another implication of the vacuum made in the tube is the demanding efforts required of the turbine that must propel the vehicle, which could produce vibrations and turbine failures, with blades thrown at high speed.

Overall, good materials, good manufacturing, construction and maintenance practices, as well as a resilient design are the best tools for designing a safety mode of transport.

On the other hand, barriers or mechanisms to control and response in case of incident can be of two types: (1) alarms or other mechanisms that urge human reaction and (2) automatic mechanisms that act on the transport system. Many of these mechanisms, in the case of railways, cause the train to stop. In the case of aviation, this measure (i.e. stopping the aircraft) may be counterproductive, and cause an accident of worse consequences. Railway recommendation is applicable to the Hyperloop case.

Finally, if neither the design of the system nor the previous control mechanisms have managed to avoid the accident, a third type of measures must be put into action, aimed at

minimizing the consequences of the accident. These measures are classified in a wide list of categories:

- Those related to the design and manufacture of the vehicle: collision energy absorption capacity, deformation resistance of inhabited spaces, materials that prevent an escalation of direct accident effects (e.g. flame-retardant materials).
- Those related to the design and manufacture of the infrastructure: capability to brake the vehicle in case of loss of control, energy absorption capacity, etc.
- Those related to the response of people involved: procedures for a fast and tidy evacuation, staff and passengers training, instructions in case of accident published in visible places, etc.
- Those related to the expected rescue subsystem response: provision of rapid response rescue mechanisms, training of people whose participation is required in these mechanisms, etc.
- Those related to rescue resources not included in the transport system (civil protection, firefighters, police, hospitals, etc.): ensure knowledge of the risks by these agents, training courses for them, immediate information and mobilization mechanisms, etc.

We must not forget the Titanic experience. Although we have manufactured a supposedly indestructible ship, it is convenient to have enough lifeboats on board.

In view of the measures suggested by Table 1, we add some detail to the most relevant issues:

4.4.1. Indications for infrastructure construction

The high speed planned for the Hyperloop would turn any tube deformation into a catastrophe, independently of the control and mitigation measures we could add. Maintaining the tube geometry against any type of natural catastrophe, human or mechanical action is therefore essential. Best practices applied in linear infrastructure planification and construction will be useful, even testing the tube behaviour under seismic actions. Seismic actions to be taken into account by building regulations can define the minimum threshold, although the specific characteristics of the tube infrastructure may require dedicated analysis and the development of new seismic-resistant elements and methods (Heaton, 2017).

Buckling effects due to differential pressure outside and inside the tube and thermal expansion of the constituent material play against the stability of the tube. Designers could use thickness as a design parameter, but they could also test other materials for the tube, such as prestressed concrete with sheet steel covering, that have been successfully used for other uses where tightness is crucial. Additionally, if steel is finally used, it could be useful to cover the tube with solar photovoltaic panels. The idea was already proposed in the Hyperloop Alpha document, in order to get energy for the system (Musk, 2013), but it could

also be used for protecting the tube from the sun, thus reducing its thermal expansion. Another measure to be studied is the use of telescopic mechanisms, perhaps placing them in the escape stations, to which we will refer later.

Preventing access to the vicinity of the tube is also crucial.

Likewise, once the tube geometry has been altered, the importance of control mechanisms to avoid collision becomes crucial.

4.4.2. Indications for infrastructure maintenance

Similarly, guaranteeing the inviolability of the tube against intruders is vital. It should be added that this inviolability should be occasionally suspended, to allow maintenance, repair, improvement, etc. This is the kind of situation in which a robust safety system relaxes, resulting in more than one incident. This will therefore require a particular protocol of action for these cases.

4.4.3. Automatic blocking system

The planned speed for the Hyperloop makes it impossible to manually operate the system. Thus, an automatic blocking system is required. Automation also allows using a mobile blocking system, i.e., distances between vehicles may be guaranteed through software, regardless of the specific point of the infrastructure in which they are located (allowing mobile track sections as in the ETCS L3 system designed for European Railways).

In addition, the vehicles' position must be accurately monitored at all times, as this is essential for any automated control system. The guidelines established for ERTMS may be the starting point to define the Hyperloop automated blocking system.

4.4.4. Mobile track section length, acceleration and capacity

The length of the mobile track section must allow braking the vehicle in a given timespan that depends on the initial speed and deceleration, as well as other technical conditions. For instance, common service braking in trains yields a deceleration of 1.2 m/s^2. This allows passengers to move freely inside the train. The Transrapid is able to stop in 5 km and 72 seconds, with an average deceleration of 1.93 m/s^2. This deceleration would require almost 2.5 minutes and 20 km to stop a vehicle running at a thousand kilometres per hour. Assuming these conditions for the Hyperloop, capacities of 20 vehicles per hour could be achieved. However, safety margins should be added in order to prevent acceleration effects induced by decompression effects or others.

4.4.5. Requirements regarding the constituent materials of the vehicle

The vehicle configuration must harmonise requirements related to its robustness while remaining light, in order to facilitate its levitation. On the other hand, electromagnetic effects play an essential role in the system, which will probably add new requirements to the vehicle's constituent materials. We understand that a substantial part of the vehicle

must be made of composite materials, capable to deliver the required dielectric properties, under magnetism, lightness, resistance to stress, fatigue, corrosion, etc. (de Santis, 2015). These required properties will have a direct impact on safety under normal and extraordinary effects (such as those produced in an eventual accident). It is also recommended to protect the cabin from a catastrophic failure of the turbine, with a scratch resistant layer.

4.4.6. Special requirements for vehicle design

We must also approach the vehicle behaviour in case of impact, because it is both a possible risk and a risk of serious consequences. A few complementary measures can minimize the consequences of a collision: reinforcing stiffening (by means of a thicker perimeter for instance) or adding an aerodynamic front device to absorb energy in case of impact (by means of deformation, for instance), and to reduce pressure in case of a recompression event in the tube.

4.4.7. Measures to respond to possible levitation failures

The procedures and mechanisms used to produce the vehicle levitation should be analysed in depth once they had been perfectly defined. However, our preliminary analysis suggests equipping the vehicle with an alternative motion system, in case of levitation failure. One possible option would be to provide the vehicle with wheels, temporarily turning it into a conventional railway or a kind of bus (using tyres in this case).

4.4.8. Measures to respond to power failures

This kind of failure does not seem to be critical, but it could be if it coincides with other kind of failures, or if it triggers other kind of failures. This would be the case if it coincides with failures in the blocking system or in the levitation system.

Stays of extended or unknown duration inside the vehicle could cause serious situations of passenger anxiety. Consequently, alternative drive systems must be available.

Another solution that may be implemented for these situations is the use of towing mechanisms, although this solution can be more expensive and problematic (the crane could find obstacles to reach the stopped vehicle). Another solution would be the installation of escape stations along the tube, in order to evacuate the passage from the tube in case of failure. Since distances are important, a significant number of these stations should be built along the tube.

4.4.9. Pressurization failure in the passenger cabin

This kind of failure may be catastrophic, if the cabin air is diluted into the vacuum of the surrounding infrastructure (i.e. the tube). This situation should be addressed in-depth, in conjunction with system design, in order to refine measures to control, response and minimize the effects of this kind of failure. Since human lives are at stake, our preliminary analysis recommends the joint use of measures that may include rapid evacuation

mechanisms, the injection of emergency oxygen reserves into the passenger cabin or the release of oxygen masks (as in airplanes). This analysis could even suggest less demanding tube pressure conditions than the 100 Pa initially proposed (Dudnikov, 2018).

4.4.10. Measures to assure communication

This kind of failure may be catastrophic if the whole system is not well designed for it. Integrity, availability, authenticity and reliability of the information and communication technology, services and applications must be guaranteed through high-quality materials, system robustness, and channels and equipment redundancy. Software should be prepared to prioritize inputs in case of discrepancy. The on-board automatic system must be able to stop the pod as a last resort, assuring at the same time that the rest of the system is aware of this situation. In the event of losing communication with a pod, the system should be completely stopped.

4.5. An approach to the risks at the stations

The basic configuration proposed in section 3.1 (Figure 2) has helped us to explore the most immediate requirements related to safety in the Hyperloop. We focus now on safety in the context of stations, particularly on passage boarding and disembarking, trying to infer some exploitation parameters.

Underground networks operated automatically allow high frequencies, up to one per minute (see section 2.3). As long as intermediate stops are short, they do not delay this frequency. In the case of the Hyperloop, intermediate stops could be longer. Firstly, because being a long-haul trip, the luggage could be bulky. Secondly, it could be necessary to devote time to accommodate passengers in their seats, secure them, communicate safety measures, etc. The stop time at the station could be even increased for technical reasons (such as recharging batteries).

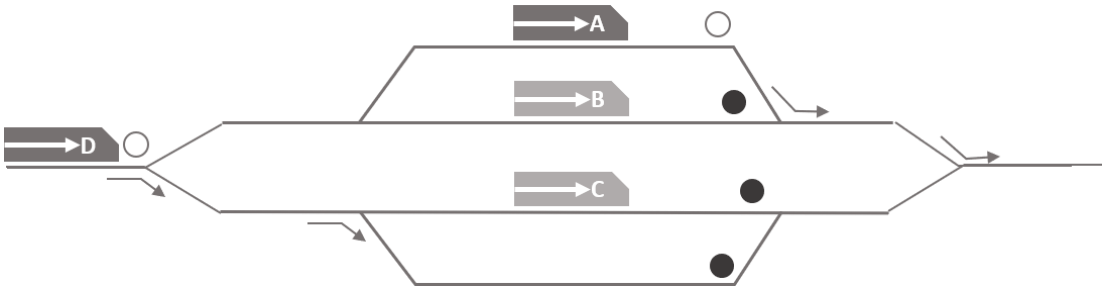

Figure 4.- Station configuration with capacity for attending high frequencies

Consequently, in order to reach high frequencies, it will be necessary to unfold the tracks at the stations. The station depicted in Figure 4 could receive a vehicle every 2.5 minutes, provided that the vehicle stopping time at the station is less than ten minutes. In a more general calculation, the number of tracks in the station should be equal to the stop time at the station of each vehicle divided by the time interval between circulations in the tube.

A station configuration like the one shown in Figure 4 introduces new technical requirements, as well as significant safety ones. The technical requirements refer to maintaining functionality with a more complex configuration, as keeping the vacuum and magnetic levitation in these new conditions is a new challenge. On the other hand, creating the equivalent of a railway switch is another development challenge. The elements proposed in section 4.4.8, related to the alternative drive system (to allow low-speed movement) and a double door lock system to access the station (for maintaining the vacuum inside the tube) are useful here.

All these aspects should be progressively introduced at the design level. The recommendation is, again, that this design should include the safety perspective.

The diversion is a challenge in itself, partly resolved by the existing magnetic levitation monorails. These diversions must include from the beginning an automatic interlocking system that only gives access to one vehicle to each branch. Analogously, the system should give access to the main tube with the required time between vehicles. This automatic interlocking system should be managed by robust software.

Both the system designed to produce the diversion, and the station automatic interlocking system and its software, have to be validated by a thorough and detailed risk analysis, and tested with appropriate simulators (probably ad-hoc designed and developed ones).

Automatic systems also require adapting the station, with adaptations like those already introduced in automatic underground lines. The platform doors are a good example of complements required for this automatic operation. These doors are equipped, among other mechanisms, with sensors, warnings and software capable of identifying problems like obstacles blocking the doors, people close to them, etc.

Finally, with regard to terminal stations, and once bidirectional vehicles have been discarded, two alternatives are proposed:

- The loops originally proposed for change direction in the simplified scheme of Figure 2 have the advantage of avoiding line ends and, therefore, an element that introduces risks in the operation: derail buffers. It is worth remembering the accidents produced in 2009 and 2012 at the Salamanca station, in Spain (Iturralde, 2012).
- Terminal station with change of direction of the vehicles. Although some of the currently operational monorails can use curves of only 50 meters of radius (Cassat and Bourquin, 2011), fitting the loops of the terminal stations shown in Figure 2

may be complicated and economically unfeasible, because of their proximity to city centres. An alternative solution could be the use of turntables (such as those used in railways, now in disuse, as shown in Figure 5). This configuration also presents, however, conflicting points related to safety, which would require a new in-depth risk analysis.

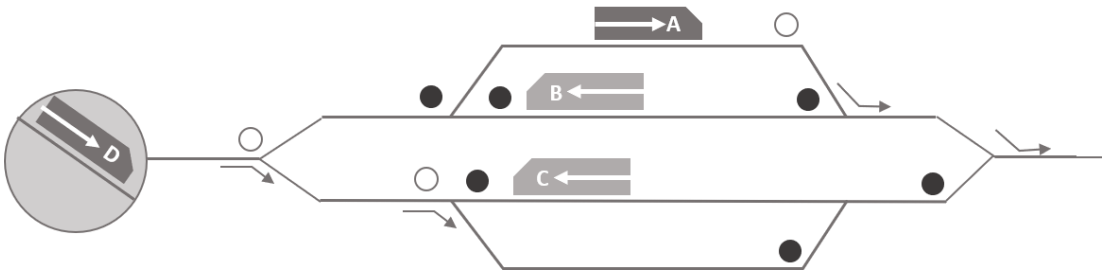

Figure 5.- Operational scheme of a terminal station with sidings and a turntable for change of direction.

4.6. The role of the human factor in the safety of the Hyperloop

The Hyperloop expected speed exceeds human reaction time. Therefore, total system automation is mandatory. This automation must include the system response to incidents. For example, when an obstacle is detected inside the tube, it is not enough to activate alarms to warn staff to stop the vehicle, it must be the system itself that automatically brakes and stops. It is appropriate to apply here the criteria used on railways, i.e. automatic train detention in the event of any contingency to reduce the risk of an accident.

Once the vehicles have been stopped, what actions should be planned thereafter? The obstacle that has triggered the automatic stop system may have very different origins (an intrusion into the tube, a part detached from a vehicle, a part detached from the infrastructure, a part or tool forgotten in a previous maintenance operation, etc.). These origins are difficult to list at the moment, especially with the comprehensiveness that would be necessary. In any case, staff should follow a protocol specifically designed for this type of situation.

Those responsible for applying this kind of protocol must have a comprehensive and complete information of the entire system, including vehicles and every tube section. This suggests the following recommendations:

- Decision makers must be located in a place that control the entire system (a Single Control Centre, or SCC).
- This SCC must have all the information related to the system in a precise, complete and updated way.

- This SCC must have the capability to activate and manage all the systems, ordinary and extraordinary (rescue), to solve the situation and restore the operation if this is possible.

All these circumstances allow us to identify a new list of potential risks that could result in critical or even catastrophic situations (Table 2).

	MEASURES		
RISKS	Of design	Related to control and response	Mitigation of unwanted effects
There are no people with the ability to make sound decisions under pressure in the SCC.	Recruiting and hiring plan. Training programs. Detailed and well-known controllers scheduling.	Staff on duty. Skills tested in simulator.	Protocols of response in case of eventuality affecting human resources.
The information is not available to the SCC or arrives incomplete, biased or delayed.	Telecommunications system protected against faults.	Check-lists. Redundant telecommunication systems (*backups*). Alarms in case of malfunction.	Protocols of response in case of eventuality affecting the telecommunication system.
Ordinary systems are not under the control of the SCC.	Ordinary systems protected against faults.	Check-lists. Permanent monitoring systems of all processes. Individual and general automatic stop mechanisms. Alarms in case of malfunction.	Protocols of response in case of eventuality affecting any of the ordinary systems.
Extraordinary systems are not under the control of the SCC.	Extraordinary systems protected against faults.	Check-lists. Permanent monitoring systems of all emergency resources. Alarms in case of unavailability.	Protocols of response in case of eventuality affecting any of the extraordinary systems.

Table 2.- Risks and measures related to control from the SCC

Some risks that might be relevant have been omitted from Table 2. This is an intentional omission, in order to introduce them now in greater detail. We have talked about the possible impact that an unscheduled stop of the system may produce on the passage. It is clear that, should the incident be resolved shortly, it would be enough to inform the passage from the SCC through intercoms or other similar means. However, if the detention is prolonged, anxiety or even more serious situations (panic attacks, attempts to force doors, etc.) could happen.

We list some measures aimed at alleviating these effects in the passage:

- Protocols to reassure the passage, such as comforting phrases (perfectly studied in terms of content, tone and timing of the speech).
- Vandal-proof measures on doors and other sensitive points of the vehicle.
- Passage evacuation measures, including:
    - Decision protocols on the evacuation of the passage, taking into consideration the possible effects of long detentions.
    - Incorporation of escape stations in the Hyperloop tube.
    - Provision of ways to move the vehicle or its passage to the nearest escape station without risk.
- Temporary or permanent staff embarked on the vehicle. This staff would not have operational functions, due to automatization, but they would assume roles related to safety and service quality (marketing):
    - Passenger assistance for accommodation, luggage placement and fixing safety mechanisms (i.e. seat belts).
    - Information on safety protocols (like cabin crew members do on airplanes).
    - Attention to questions asked by the passage (probably more abundant during the first months of operation).
    - Inform and reassure the passage in case of incidents.
    - Proceed in case of anxiety or more serious health problem through first aid techniques and communication to the SCC.
    - Guide the passage in case of evacuation or rescue protocol activation.
    - Act as liaison and collaborator with the SCC during incidents, particularly in case the SCC could not act remotely.

In order to make effective these tasks by embarked staff, it would be necessary:

- The drafting (considering all the relevant perspectives), approval and publication of protocols to guide this staff in ordinary and extraordinary circumstances.
- Staff training in the application of each of the protocols.
- Make available to staff the resources required to carry out their work (first aid equipment with their corresponding resuscitation equipment, for example), and the corresponding checklists.

After this analysis we can conclude that, although the role of staff in the Hyperloop operation and safety seems a priori to be subsidiary (given the high degree of automation present in the system), it is actually vital. The staff represents in fact a safety barrier that can activate alternative solutions and rescue plans that, in the long term, may save human lives.

5. Discussion

In this section, the main findings of our paper are discussed and analysed, taking into account two approaches. First, the methodology used to identify hazards and define measures to deal with them is discussed in more detail, analysing its strengths and weaknesses. Secondly, we assess the measures proposed and identify shortcomings and potential improvements that may be applied when the hyperloop system reaches a more advanced stage of development.

5.1. Methodology discussion, limitations and lessons learned

Our work has started from a very simplified model of the Hyperloop and has used a refined SWIFT method in order to identify the main hazards in this model. This identification process has not been without difficulties and challenges, mainly because it has been focused on a radical innovation in its early development stages. Consequently, we added to our methodology a tool recommended for radical innovation, lateral thinking. As De Bono stated, human brain is good at refining ideas (deductive logic), but it is not so much when working with new ones (De Bono, 1967). Lateral thinking took us to make questions like 'what other differential features are involved?'

Inductive logic has been also useful in this context. Our work suggests going beyond questions like 'What could make this happen?', with questions like 'What have we taken for granted?'

However, we could not avoid working under certain kind of groping (paraphrasing Einstein). In fact, we identified some hazards, that could be relevant, reading journalistic information not entirely rigorous; information that we had to filter and rigorously analyse in order to take out its real scope.

Our attempts to try other methods for preliminary hazard analysis, even those recommended for safety analysis on early concepts, were unsuccessful, because all of them seem to require a more defined Concept of Operations. Nevertheless, STECA aims to be the perfect candidate for a second iteration of the safety analysis. Our attempts suggest that a small refinement in the definition of the system, its components and the interactions among them would be enough for using this technique.

We have developed then a systematic search of measures to eliminate, reduce and control these hazards, as well as measures to reduce damage in case of hazardous incidents, using

the classification proposed by STPA, that have delivered a first list of recommendations for practitioners (see next section).

5.2. Results discussion, limitations and recommendations for practitioners

We show below a wide list of recommendations for practitioners generated by our methodology, a list that summarizes our results for practitioners. This list accomplishes some useful goals: (1) it focuses the attention of practitioners on safety, (2) it guides the first approaches to safety by Hyperloop's designers, and (3) it suggests several lines for further development of safety in the Hyperloop.

This is an initiatory work in the field of safety in the Hyperloop, and thus presents numerous limitations. Several important issues have been excluded of our work, like security issues. Moreover, safety in specific components of the Hyperloop system (such as deviations and scape gates in the tube), have been also omitted, partly because the safety analysis of these components cannot be properly done until they had been better defined. Additionally, our work suffers from a lack of depth and specificity, as a consequence of addressing an area that is still under development. Nevertheless, we consider that the objective excuses and justifies these shortcomings, as we hope to set up a footing for further research in the topic of Hyperloop safety.

1. Appoint a Safety Officer that occupies a high hierarchical position in the Hyperloop development organization, responsible for (1) promoting safety in each and every of the Hyperloop development tasks, (2) defining and communicating policies and instruments for safety management and (3) promoting and managing the development of the Hyperloop Safety Management System.
2. Place safety as a priority, promoting and establishing a common safety framework for all those involved in the Hyperloop development at the global level. Safety must be chaired by cooperation rather than competition
3. Adopt inspiring principles for safety, analogous or close to those proposed for commercial aviation (see section 2.2), maintaining a system perspective and a continuous improvement approach.
4. Consider the safety system as one that incorporates accident prevention measures related to areas such as: infrastructure design and execution, vehicle design and manufacture and the design of the organizational system in charge of providing the transport service. The safety system should also incorporate measures of reaction to the occurrence of incidents and accidents, such as rescue protocols with their corresponding mechanisms and means.

5. Include safety as an essential reference in each step of the Hyperloop development process and for each person involved. State without doubt that safety is an important task for everybody, whatever its role in the development process.
6. Assume the total and absolute automation of Hyperloop's operations, thus ensuring that its projected operational benefits are achieved while remaining a safe mode of transport. People must fulfil a creative role in the definition of the system and its operating rules, while operational management is delegated to machines (computers, in particular).
7. Apply safety control mechanisms similar to those used today in the most advanced rail transport (high-speed trains, magnetic trains and automated underground trains), to fully automatise blocking in the main tube and interlocking in stations, as the only way to safely operate the Hyperloop.
8. Monitor the risks already identified in the first analysis made in this preliminary work and whose consequences could reach a certain level of severity, including both risks related to infrastructure (such as deformation, perforation, intrusion into the tube, loss of vacuum, etc.) and risks related to the vehicle (loss of energy, connectivity, levitation, braking capacity or cabin air pressure).
9. Do not take for granted, at this stage of the Hyperloop development, the adoption of certain fundamental decisions, such as which specific material should be used for the tube. Buckling effects due to different pressure inside and outside the tube and thermal expansion could recommend a material other than steel.
10. Analyse in-depth, and consistently test, the behaviour of the tube under the effect of the real forces that will act in the real configuration.
11. Advance, in parallel to the Hyperloop development process, in the specific definition of some measures proposed in this work that aim to reduce risks related to the appearance of obstacles in the tube. These including design measures (such as tube robustness, access control, best construction practices), control and response measures (redundant detection mechanisms along the tube, automatic stopping mechanisms, alarms in case of malfunction) and measures to mitigate unwanted effects (aerodynamics, rigidity and shock absorption mechanisms in the vehicle, rescue procedures).
12. Analyse in-depth, and consistently test, the behaviour of the pod when moving along the track, particularly along curved sections, thus defining the maximum speed as a function of the radius.
13. The information and telecommunication system robustness has to be extensively checked, forecasting its behaviour under all kind of possible failures. Redundancy measures must be applied where possible, as well as a clear hierarchy in case of

conflicting information. Individual and general automatic stop mechanisms should be activated in case of communication failure.

14. Advance, in parallel to the Hyperloop development process, in the definition of experiments and tests that show both the vehicle response in case of collision at different speeds, and the effectiveness of the aforementioned mechanisms (e.g. stiffness and energy absorption).
15. Advance, in parallel to the Hyperloop development process, in the definition of measures aiming to reduce risks arising from the eventual loss of levitation or power, including design measures (such as assurance of power supply and levitation), control and response measures (indicators, monitoring and alarm systems, alternative power systems) and measures to mitigate unwanted effects (evacuation, towing and rescue systems).
16. Advance, in parallel to the Hyperloop development process, in the definition of measures aiming to reduce risks arising from the eventual loss of air pressure in the cabin of the vehicle, including design measures (power supply and pressurization assurance, automatic adjustments in the air pressure in the tube), control and response measures (pressure and leakage indicators, monitoring and alarm systems, automatic triggering of oxygen reserves) and measures to mitigate unwanted effects (oxygen masks or other alternative breathing systems, evacuation and rescue systems).
17. Apply, as the development of the Hyperloop progresses, an in-depth risk analysis, analogous to those described for rail transport, relative to each different subsystem whose anomalous operation could introduce serious risks (levitation, braking, power supply, connectivity, tube vacuum, cabin pressurization, etc.).
18. Advance, in parallel to the Hyperloop development process, in the analysis of the relationships between certain key vehicle characteristics, its performance as a mode of transport and its safety. As an example, we can mention the existing ones between the vehicle braking capacity, the line capacity and the minimum dimension of the mobile track section that defines the automated blocking system.
19. Apply to the Hyperloop terminals what has been developed and prescribed for the terminals of other modes of transport, such as airport terminals or railway stations, in relation, for example, to mechanical or electrical risks, and, in particular, those that may affect passengers, staff, etc. (elevators or conveyer belts failures, slips and trips, etc.).
20. Apply to the Hyperloop terminals what has been developed and prescribed for automated railway stations, such as platform doors, sensors, warnings, alarms, etc.

21. Apply an in-depth risk analysis to the mechanisms designed for the diversion of the Hyperloop vehicle, with particular attention to the performance and safety implications of the double-door lock system.
22. Apply an in-depth risk analysis to the proposed system for vehicle displacement in the absence of levitation, and extend this analysis to the transition process between them.
23. Apply an in-depth risk analysis to the escape gates along the tube, in parallel with the definition of the optimum frequency and design.
24. Work towards the definition of an organizational operation of the terminal station that specifically takes into account the risks already known in railways. Apply an in-depth risk analysis, with particular attention to the proposed mechanism for changing the direction of the vehicle (turntable, loop).
25. Automate the Hyperloop, not only with regard to system management under normal operational regime, but also with regard to the immediate response to abnormal operational circumstances. The reaction to anomalous situations cannot be entrusted to people when the system travels at a thousand kmh. The response to anomalous circumstances must also be fully automated.
26. Meticulously test the successive prototypes, particularly the interaction between staff and automatic systems, and shield this process from commercial pressures. In other words, it is important to avoid the culture of getting the product into service becoming dominant over the safety-first culture.
27. Carefully define the roles that staff in charge of the Hyperloop operations have in this highly automated operation. These roles should, at least, include two key aspects: (1) the decision to start or restart the system (regardless of whether the stop happened in a planned manner or due to a system failure), and (2) that of guiding and assisting passengers, both in normal operating conditions and in extraordinary circumstances.
28. Define the scope of safety qualifications that should be delivered to the staff.
29. The role of passenger assistance requires, at least in the first moments of the Hyperloop operation, to embark agents in the vehicle that assume the aforementioned guidance and assistance functions, both in normal operational conditions (particularly when boarding and disembarking passengers) and also in extraordinary circumstances (unwanted long stops, incidents in general, etc.).
30. Centralize all the Hyperloop management and control operations in a Single Control Centre that receives all the information (accurate, complete and updated), establishes the operational parameters of the system as a whole and that start and restart the automatic systems when appropriate.

31. Advance to a system starting or restarting protocol that includes an exhaustive check of each and every one of the subsystems involved, by means of monitoring systems, reviewing system alarms, reviewing checklists, etc. following the example of similar mechanisms used today in other modes of transport, such as aviation, and using safety as the guiding priority.
32. Advance to the definition of a protocol for action in case of incident. The incipient protocol set out in section 3.5 of this document may be used as a first draft.
33. Analyse the case of anomalous circumstances that could retain the passage in the vehicle, especially if these circumstances are particularly difficult (high or low temperature, extremely log, with assisted breathing, etc.).
34. Advance the definition of protocols for emergency declaration and rescue plan activation, which may serve as a first draft of an Emergency Plan.

6. Conclusion

Safety is the emergent result of a process. There isn't any such thing as a foolproof system design, particularly when the system is in the early stage of its design. We have done in this article the only things that can be done at this stage of design: (1) to focus the designer's attention on safety, (2) to propose a useful methodology to make a preliminary hazard analysis, and (3) to make a first iteration of the processes included in this methodology.

By doing this, we have tried to highlight a main conclusion, which that addressing safety from the very beginning may avoid redesigns, delays and costs in the development of the Hyperloop. The traditional view of safety had introduced safety when the system design had been more advanced, maybe forcing redesigns and expensive correcting measures. For example, analysing the tube from a safety point of view has suggested that certain decisions that could be being taken for granted could cause important problems in future stages.

Our methodology has been useful to generate a wide and sound first list of recommendations, that can be understood as a platform to build on a safer and more robust mean of transport.

Acknowledgements

The authors would like to thank the Zeleros Global team for their cooperation and positive feedback.

Bibliography

Accou, B., Reniers, G., 2019. Developing a method to improve safety management systems based on accident investigations: The SAfety FRactal ANalysis. Saf. Sci. 115, 285–293.

Alawad, H., Kaewunruen, S., An, M., 2020. Learning from accidents: machine learning for safety at railway stations. IEEE Access 8, 633–648.

Amalberti, R., 2001. The paradoxes of almost totally safe transportation systems. Saf. Sci. 37, 109–126. https://doi.org/10.1016/S0925-7535(00)00045-X

Barbosa, R.S., 2016. Evaluation of railway track safety with a new method for track quality identification. J. Transp. Eng. 142. https://doi.org/10.1061/(ASCE)TE.1943-5436.0000855

Brandeburger, A.M., Nalebuff, B.J., 1996. Co-opetition. Doubleday, New York.

Cassat, A., Bourquin, V., 2011. MAGLEV – Worldwide Status and Technical Review, in: Électrotechnique Du Futur.

Chapman, L., 2007. Transport and climate change: a review. J. Transp. Geogr. 15, 354–367.

Chen, Y., Linder, S., Wigstein, J., 2019. An approach of creating component design specification for safety-related software in railway, in: Proceedings - Annual Reliability and Maintainability Symposium. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/RAMS.2019.8769048

Cusick, S.K., Cortés, A.I., Rodrigues, C.C., 2017. Commercial AVIATION SAFETY. 6th Edition. McGraw-Hill, New York.

De Bono, E., 1992. Serious Creativity. The McQuaig Group, New York.

De Bono, E., 1967. New think. The use of lateral thinking. Basic Books, New York.

de Santis, A.J. de, 2015. Análisis de fallos en sistemas aeronáuticos. Paraninfo, Madrid.

Dobney, K., Baker, C.J., Quinn, A.D., Chapman, L., 2009. Quantifying the effects of high summer temperatures due to climate change on buckling and rail related delays in south-east United Kingdom †. Meteorol. Appl. Meteorol. Appl 16, 245–251. https://doi.org/10.1002/met.114

Dudnikov, E.E., 2018. The Problem of Ensuring the Tightness in Hyperloop Passenger Systems, in: Proceedings of 2018 11th International Conference "Management of Large-Scale System Development", MLSD 2018. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/MLSD.2018.8551881

European Commission, 2019. EU transport in figures - Statistical Pocketbook 2019.

Fleming, C.H., 2015. SAFETY-DRIVEN EARLY CONCEPT ANALYSIS AND DEVELOPMENT. Ph D Thesis. Massachusetts Institute of Technology.

Fleming, C.H., Leveson, N.G., 2016. Early concept development and safety analysis of future transportation systems. IEEE Trans. Intell. Transp. Syst. 17, 3512–3523. https://doi.org/10.1109/TITS.2016.2561409

Gherardi, S., Nicolini, D., 2000. The Organizational Learning of Safety in Communities of Practice. J. Manag. Inq. 9, 7–18.

González Fernández, F.J., 2013. Señalización y seguridad ferroviaria. Ibergarceta publicaciones, S.L., Madrid.

Hansen, I.A., 2020. Hyperloop transport technology assessment and system analysis. Transp. Plan. Technol. 43, 803–820. https://doi.org/10.1080/03081060.2020.1828935

Heaton, T.H., 2017. Inertial forces from earthquakes on a hyperloop pod. Bull. Seismol. Soc. Am. https://doi.org/10.1785/0120170054

Hoem, S., Fjørtoft, K., Rødseth, J., 2019. Addressing the accidental risks of maritime transportation: Could autonomous shipping technology improve the statistics? TransNav 13, 487–494. https://doi.org/10.12716/1001.13.03.01

IMO, 2007. Formal Safety Assessment: Consolidated text of the Guidelines for Formal Safety Assessment (FSA) for use in the IMO rule-making process.

Iturralde, M., 2012. Treneando [WWW Document]. URL https://treneando.com/2012/05/02/descarrila-un-tren-tras-chocar-con-una-topera-en-salamanca-donde-hace-dos-anos-colisiono-otro-tren/

Jagtman, H.M., Hale, A.R., Heijer, T., 2006. Ex ante assessment of safety issues of new technologies in transport. Transp. Res. Part A Policy Pract. 40, 459–474. https://doi.org/10.1016/j.tra.2005.08.007

Janic, M., 2000. An assessment of risk and safety in civil aviation. J. Air Transp. Manag. 6, 43–50. https://doi.org/10.1016/S0969-6997(99)00021-6

Janić, M., 2020. Estimation of direct energy consumption and CO_2 emission by high speed rail, transrapid maglev and hyperloop passenger transport systems. Int. J. Sustain. Transp. 1–22. https://doi.org/10.1080/15568318.2020.1789780

Klockner, K., Toft, Y., 2015. Accident modelling of railway safety occurrences: The safety and failure event network (SAFE-Net) method. Procedia Manuf. 3, 1734–1741.

Kumar, S.D., Namdeo, U., Samadhiya, A., Mishra, P., Krishna, K.D., 2019. Hyper loop transportation system. Int. J. Innov. Technol. Explor. Eng. 8, 2278–3075.

Lefsrud, L., Macciotta, R., Nkoro, A., 2020. Performance-based regulations for safety management systems in the canadian railway industry: An analytical discussion. Can. J. Civ. Eng. https://doi.org/10.1139/cjce-2018-0513

Leveson, N.G., 2011. Engineering a Safer World. The MIT Press, Cambridge, MA.

Li, N., Guo, J., Lei, J., Li, Y., Rao, C., Cao, Y., 2016. Towards Agile Testing for Railway Safety-critical Software *. dl.acm.org 24-May-2016. https://doi.org/10.1145/2962695.2962713

Losada, M., 1991. Curso de ferrocarriles. ETSIC, Madrid.

Lüley, P., Franeková, M., Hudák, M., 2012. Safety and functionality assessment of railway applications in terms of software, in: Communications in Computer and Information Science. pp. 396–405. https://doi.org/10.1007/978-3-642-34050-5_45

Mateu, J.M., March-Chorda, I., 2016. Is experience a useful resource for business model innovation? Technol. Anal. Strateg. Manag. 28, 1195–1209. https://doi.org/10.1080/09537325.2016.1182630

Mazouni, M.H., Bied-Charreton, D., Aubry, J.F., 2007. Proposal of a generic methodology to harmonize Preliminary Hazard Analyses for guided transport, in: 2007 IEEE International Conference on System of Systems Engineering, SOSE. https://doi.org/10.1109/SYSOSE.2007.4304278

Mione, A., 2009. When entrepreneurship requires coopetition: The need for standards in

the creation of a market. Int. J. Entrep. Small Bus. 8, 92–109. https://doi.org/10.1504/IJESB.2009.024107

Musk, E., 2013. Hyperloop Alpha. The first concept of the system.

Myklebust, T., Hanssen, G., Lyngby, N., 2017. A survey of the software and safety case development practice in the railway signalling sector, in: Researchgate.Net.

Naor, M., Adler, N., Pinto, G.D., Dumanis, A., 2020. Psychological safety in aviation new product development teams: Case study of 737 max airplane. Sustain. 12, 1–15. https://doi.org/10.3390/su12218994

Ohno, T., 1988. Toyota production system. Productivity Press, Portland.

Oster, C. V., Strong, J.S., Zorn, C.K., 2013. Analyzing aviation safety: Problems, challenges, opportunities. Res. Transp. Econ. 43, 148–164. https://doi.org/10.1016/J.RETREC.2012.12.001

Perrin, E., Kirwan, B., Stroup, R.L., Allocco, M., Statler, I.C., Blom, H., 2005. Aviation System Safety Principles Safety Action Plan-15 Version 2.0.

Rausand, M., Haugen, S., 2020. Risk Assessment. Theory, Methods, and Applications, Second. ed. Wiley, Hoboken, NJ.

Rødseth, Ø.J., Burmeister, H.-C., 2015. Risk Assessment for an Unmanned Merchant Ship. TransNav, Int. J. Mar. Navig. Saf. Sea Transp. 9, 357–364. https://doi.org/10.12716/1001.09.03.08

Semler, R., 2004. The Seven-Day Weekend. Penguin, New York.

Spielman, Z., Le Blanc, K., 2021. Boeing 737 MAX: Expectation of Human Capability in Highly Automated Systems, in: Advances in Intelligent Systems and Computing. Springer, pp. 64–70. https://doi.org/10.1007/978-3-030-51758-8_9

Stoop, J.A., Thissen, W.A.H., 1997. Transport safety: Trends and challenges from a systems perspective, in: Safety Science. Elsevier Sci B.V., pp. 107–120. https://doi.org/10.1016/S0925-7535(97)00033-7

Uherek, E., Halenka, T., Borken-Kleefeld, J., Balkanski, Y., Berntsen, T., Borrego, C., Gauss, M., Hoor, P., Juda-Rezler, K., Lelieveld, J., Melas, D., Rypdal, K., Schmid, S., 2010. Transport impacts on atmosphere and climate: Land transport. Atmos. Environ. 44, 4772–4816. https://doi.org/10.1016/J.ATMOSENV.2010.01.002

Utterback, J.M., 1994. Mastering the Dynamics of Innovation: How Companies Can Seize Opportunities in the Face of Technological Change. Harvard Business School Press.

Valdez Banda, O.A., Kannos, S., Goerlandt, F., van Gelder, P.H.A.J.M., Bergström, M., Kujala, P., 2019. A systemic hazard analysis and management process for the concept design phase of an autonomous vessel. Reliab. Eng. Syst. Saf. 191. https://doi.org/10.1016/j.ress.2019.106584

Van Goeverden, K., Milakis, D., Konings, R., 2018. Analysis and modelling of performances of the Hyperloop. Eur. Transp. Res. Rev. 10.

Ventikos, N.P., Chmurski, A., Louzis, K., 2020. A systems-based application for autonomous vessels safety: Hazard identification as a function of increasing autonomy levels. Saf. Sci. 131. https://doi.org/10.1016/j.ssci.2020.104919

Villalba Sanchis, I., Insa Franco, R., Martínez Fernández, P., Salvador Zuriaga, P., Font Torres, J.B., 2020. Risk of increasing temperature due to climate change on high-speed rail network in Spain. Transp. Res. Part D Transp. Environ. 82. https://doi.org/10.1016/j.trd.2020.102312

Wróbel, K., Montewka, J., Kujala, P., 2018a. Towards the development of a system-theoretic model for safety assessment of autonomous merchant vessels. Reliab. Eng. Syst. Saf. 178, 209–224. https://doi.org/10.1016/j.ress.2018.05.019

Wróbel, K., Montewka, J., Kujala, P., 2018b. System-theoretic approach to safety of remotely-controlled merchant vessel. Ocean Eng. 152, 334–345. https://doi.org/10.1016/j.oceaneng.2018.01.020