University of Twente

Safety by design

Hyperloop

Author:
Group G1

Supervisor:
dr. M. Rajabali Nejad

January 30, 2021

Name
René Jacobi
Jordan Oost
Marcel Vliem
Evert Willem van den Brink

Contents

Chapter 1

Introduction

The EU aims to develop an efficient transport system to reduce emissions and congestion. In recent years, hyperloop trains are being developed. The virgin hyperloop has transported its first passengers in 2020 [9]. The train can be seen as a capsule which is travelling in a vacuum tube (see figure 1.1). Because of the vacuum, the air resistant is minimal and in theory the transport system could reach transonic speeds [10]. Because of the high speed, the train could compete with traditional means of transport like trains and airplanes. Short air routes could be replaced by a hyperloop, because airplanes have to deal with for example runway taxiing and decent [10]. One of the biggest concerns of this transport system is safety, because of the high speed and enclosed environment. Thereby it is important that this system is investigated from a safety point of view.

Figure 1.1: Hyperloop [8]

Chapter 2

Scope

2.1 Technical system

To be able to give a complete overview of the safety aspects related to the system, a thorough definition of the system is necessary. This includes defining the system, the subsystems of the system and the components of the subsystems. In addition, all system boundaries and their interactions should be defined, including human and environment interactions. The System Under Consideration is called the Hyperloop. This conceptual vacuumtrain has been in development since 2012 by a combined team of companies. The working principle is that small trains called pods are transported through a near vacuum tube which can be located in or above the ground. The system aims to compete with airplanes and cars for short to medium inter-city trips, decreasing traffic jams and air pollution. The system includes the subsystems listed below.

Pod The pod is the cabin where the passengers will be seated. This cabin needs to be pressurised to be survivable. The pod also contains magnetic lifting devices to make the pod hover over the rail. A linear electromagnetic motor is used to accelerate and decelerate the pod.

Tunnel The tunnel is depressurised to create an almost vacuum environment in the tube, this greatly reduces drag and therefore enables the pod to travel at high speeds.

Vacuum generation The vacuum pump(s) generate the vacuum in the tubes by extracting most of the air inside the tube to the environment.

Station The station is the place where passengers wait for a pod, pods are stored and a system is present to allow passengers to enter the pod without losing the vacuum in the main system.

Control facility The control facility makes sure no pods collide, and that there are enough pods at each station for the number of passengers waiting. This acts as a central hub for data management, housing servers that provide and collect data of other sub-systems.

2.1.1 Detailed subsystems

Pod

- Linear propulsion system, electromagnetic motor to accelerate and decelerate the pod.
- Electromagnetic no-contact levitation, for limited friction
- Control, communication, sensors, electronics, feedback etc.
- Cabin
  - Seats
    - Seat belts
  - Cabin pressure must be 1 bar for health reasons
  - Oxygen tanks, oxygen percentage must be maintained over trips
  - Doors
  - Cargo setup (no seats)
- Entertainment and information system

Tunnel

- Switches
- Solar panels, ideally power the system for 100%
- Induction loop to power the pod
- Rails
  - To rest on when no power is supplied
  - Keep the pod in a defined position under unexpected conditions (loss of vacuum for example)
- Walls
  - Provide structural integrity even under extreme weather conditions
  - Must be airtight
- Support columns (above ground), to keep the hole system suspended above the ground to allow construction and traffic underneath.
- Emergency exits

Vacuum generation

- Cybersecure
- Powerfull enough to keep the hole system under vacuum
- Must be as efficient as possible

Station

- Passenger flow control
- Building; walls, roof, stairs etc.
- Connection to pod without losing vacuum
- Park pods

Control facility

- Link pods to passengers
- Control pod destination and speed to avoid collisions
- Section off sections where pressure loss is detected to keep the remaining system operational without extreme power draws for the vacuum pumps
- Direct maintenance crews effectively

2.2 Environment of the system

The environment of the system can have impact on the system and humans which are detrimental to the functioning of the system and therefore safety. As the environment consists of many subsystems only the main interacting subsystems of the environment will be considered from here on. The following six subsystems categories of the environment will be considered.

Physical environment The physical environment contains all the objects physically effecting the system and that the system effects physically. Also defining the temperature and of the outside world. This will limit the systems usage to usage within areas where temperatures are non-lethal in a time span of 2-hours.

Power The system requires electrical power, which can partly be done self-sustaining by using solar panels placed on top of the tube. However on days of minimum solar exposure the system requires stored energy or delivered by the existing power grid.

Internet To make the control station usefull a information flow between the different pods, stations and central is needed. This is done using the internet infrastructure.

Nature Nature is all living things excluding humans, being effected by or effecting the system. For example, the magnetic fields from the pods can effect animals[15].

Regulations Governments and governmental bodies like the European Union can have regulations that hinder the use of the system or building of the system.

Competing systems Competing systems like transportation by aeroplane or train influence the system by profitability.

2.2.1 Detailed environmental factors

The following environmental factors play a significant role within the physical environment system.

Physical environment
- Weather
- Earthquakes
- Wind
- Floodings
- Terrorist attacks

Power
- Generation
- Storage

Internet
- Cables
- Servers

Nature
- Occupied area
- Magnetic/electronic waves effecting animals

Regulations
- European
- Asian
- American
- Etcetra

Collaborating/competing systems
Public image
Designers
Maintenance crew

2.3 Humans

Several stakeholders will have an impact on the construction and operation of a Hyperloop. These will not all have the same influence over each part of the Hyperloop's life-cycle, but all have the capability to influence the design and running.

Primary user This will be the group utilising and eventually paying for a large part of the costs. This group will therefore be fundamental for its economical success. This group is heavily influenced by the general opinion, which should be considered both an asset and a threat. This group will also be influenced by the standard of the travel experience and the price of travel.

General public This group will represent the general opinion and will influence the political landscape. This group could be influenced like the primary user, but the focus will be less on travel experience and travel costs.

Local general public A subgroup of the general public is the local general public. In addition to the concerns the general public will hold, this group will also likely be concerned by the local impact the tube will have on for example the aesthetics, the noise during operation and the building, etcetra.

Environmental impact advocates It is likely that this group will also influence the political landscape. This can be both a strength and a threat. If the public perception will focus on the Hyperloop being an alternative for more polluting forms of transport then it will likely be endorsed. Meanwhile if it is viewed as being harm full to the natural habitat of local species then it can expect political backlash.

Land owners The site of construction is bound to have obstacles, these might be current land owners. A land owner can refuse to sell his or her property or drive up the acquisition price.

Operator This likely to be the investor in the infrastructure but can also be an outsourced party. This party will be responsible for the daily running of the Hyperloop. Traditionally its labor costs will be the largest post on the the lifetime budget of the Hyperloop. As this group will be responsible for the operation of the equipment, it is both one of the largest liabilities and one of the best places to manage risk.

Suppliers This group will be key for a low initial investment, low operating costs and a low downtime due to maintenance. Good suppliers and products can therefore be key in the success of the product[1].

Agencies Agencies will be responsible for implementing the policy set by the general public. As these are often not financially motivated, defects in the relation with these agencies can result in a lot of downtime. These agencies are also the most likely to make sure that safety inspections are being made and that safety equipment functions properly.

Inter-agency bodies When the Hyperloop, for example, crosses borders, it can result in an inter-agency cooperation. In this example custom and immigration agencies from multiple countries have to work together to allow a smooth operation.

Maintenance personnel/companies When the Hyperloop requires inevitable maintenance the most unpredictable part of this process is likely to be the personnel. Having a well trained staff will therefore result in a small amount of downtime and a predictable amount of downtime. This will it make easier to give an accurate prediction to the traveller.

2.3.1 Interaction

To integrate the system safely in a real life application, six aspects are investigated which follow from the safety cube theory. These aspects are the human, technical system, environment and the interaction between those aspects [11]. The interactions are shown in Table 2.1. Note that many interactions are similar for regular train transport. The difference between a hyperloop and a regular train is primarily the use of a vacuum tube. This tube can be build in the ground or above, but will need most likely additional safety requirements. Also the relatively high speed of the hyperloop must be taken into consideration.

Table 2.1: Design structure matrix

	Human	Technical system	Environment
Human	Other train passengers, conductors, other personnel and government regulators	Train operator, the use or abuse by passengers, maintenance. Misbehavior on stations.	Frequency of passing of cart. Regulation changes. Third party transport.
Technical System	Saving time. Economic, safe, punctual and low environmental impact traveling. Maintenance impact on other road users.	Hyperloop	Mechancial and electromagnetic vibrations. Visual intrusion. Competitors.
Environment	Information system, accessibility for passengers and disabled passengers, station location, (low) visibility	natural disasters, weather, pressure difference, ground water, cables and pipes, buildings. System condition sensors. Internet(control) infrastructure. Competitors. Electrical supply. Signal blocking structures (mountains, bridges, etc.). Interfering signals(cell towers, railroad crossings, etc.)	Emergency services. Law's policies and regulations. Climate change.

Chapter 3

Safety objectives

3.1 Level of protection

For the subsystems a certain level of protection is desired. Each subsystem has its own function. When some systems fails, the consequence can be severe. It could lead to legal issues, reputation damage, injuries and potential death. This should be prevented. To structure the level of protection, for each subsystem the level of safety is determined. The 5 levels of safety are:

1. Must always be avoided
2. Changes have to be made in design
3. Technical measures can be taken
4. Information should be provided
5. Risks are acceptable due to low severity

In other words, when a subsystem requires a level of safety of 1, the failure rate must be lowest. A level of safety of 5 can have a higher failure rate, but should still be acceptable. This is similar to the SIL of IEC 61508-1.

3.1.1 Pod

Cabin The pod cabin encloses the passengers and keeps the inside air pressure at 1 bar. When the cabin would fail by for instance mechanical stress, passengers could get hurt or die. This should be prevented at all cost and thereby this subsystem has a desired level of safety of 1.

Seats The pod seat should be comfortable and the seat belt should be safe enough to keep the passenger secure during operation but also during a crash. When it would fail it has severe consequences on the heath of the passengers. Thereby the level of safety is 1.

Entertainment and information system When this system would fail, it has no severe consequences for the passengers. Thereby the desired level of safety is 5.

Levitation The levitation system makes the movement possible. When it would fail, the train will drop onto the rails and slow down till it stops. It is assumed this has not severe consequences, but the experience will most likely be annoying and can result in a shock trough the system. Thereby the level of safety is 2.

Control system The control system controls the pod and makes sure the system works. When it fail it could result in pods crashing into each other. Thereby the required level of safety is 1.

Propulsion system The propulsion can accelerate and decelerate the pod. Breaking is an essential function and should never fail. Thereby the level of safety is 1.

3.1.2 Tunnel

Switches The switches inside the tunnel will direct the train on a specific track. When these would fail, it could lead to a head on collision with another pod. Because of the extreme speeds, this should be avoided at all cost and a level of safety is chosen to be 1.

Solar panels The solar panels are part of the power system of the train. Most likely to have stable power, an outside power source is required. When a solar panel would fail, this will lead to little consequences. Thereby the required level of safety is 5.

Induction loop The induction loop directs the power to the pod. When it would fail, the pod would slow down, but most likely the harm due to failure is limited. Thereby technical measures can be taken to minimise the risk but it is not critical. A level of safety of 3 is thereby required.

Rails When the levitation system fails or is turned down, the cabin must be supported by the rails. When the rails fail in a high speed situation, this has severe consequences. Thereby the level of safety is taken as 1.

Support columns (above ground) The failure of the support structure must be avoided at all cost, because it could damage the tube and in the worst case make the pod crash. Thereby the level of safety is 1.

Emergency exits The emergency exits must always work in a case of a accident. The required level of safety is thereby 1.

Walls The tunnel transports the passengers and the wall is under a large stress because of the vacuum. When it would fail it would have severe consequences and thereby the level of safety is 1.

3.1.3 Vacuum generation

When the pump would fail, the train would (most likely) experience turbulence when the air is sucked in, but afterwards the train is most likely still operational at a lower speed like a more conventional train. The turbulence could lead to disturbance of the pod and technical measures could be taken. Thereby the selected level of safety is 3.

3.1.4 Station

Passenger flow control The station should be save for all passengers. There should not be to many obstructions or an trip point when entering the pod. Thereby the level of safety is 3.

Building The building must withstand the weather conditions and everyday use. Failure would most likely happen over time. When part break off it can lead to injuries. Maintenance is thereby important and should be taken into account during designing and thereby a level of safety of 2 is selected.

Parking pots The parking of the pots must be on a suitable location, but the risks can be accepted due to low severity. Also only staff is allowed in this location and thereby the level of safety required is 5.

Sealed connection to pod This seal is important for the realisation of the vacuum. If it would fail, the pressure would increase in the tube and also the rushing of the air inside the tube will be unpleasant for the passengers. To notify the passengers, information can be provided. The desired level of safety is thereby 4.

3.1.5 Control facility

In the control facility the operation of the entire network is regulated. When it fails it can result in colliding of pods. Thereby the desired level of safety is 1.

3.1.6 Environment of the system

There is little influence by the designer on the environment, but on certain points decisions can be made. A reliable power supplier should be selected to minimise power loss. Furthermore the internet which is used to control the system should be safe to use and reliable. Lastly a appropriate route of the tunnel should be selected such that the damage to nature is limited and there are little points where for instance trees can fall on the tunnel and hinder the operation of the system.

3.2 Regulations and directives

As regulations for Hyperloop transport systems are still under development [6], no regulations can be found specifically for Hyperloop systems. However, regulations concerning railway systems can be give an indication of regulations for Hyperloop systems. A few and their basic description are given below:

3.2.1 Directives

Directive 2009/125/EC Concerning the directives on devices that use energy.
EMC Directive 2014/30/EU Directive on ensuring that the Hyperloop is not effected by or effecting other equipments by means of EMC signals.
Directive 2014/34/EU Concerns explosive environments. Due to the oxygen tanks and batteries, the pod is an explosive environment and therefore the system should take this directive into account.
Directive 2006/95/EC Directive concerning low voltage equipment which is expected to be present in the pod and tunnel, for example (panels, control systems, batteries).
Directive 2006/42/EC Concerning all equipment mounted on the pod, but excluded are the means of transport by rail. However, Hyperloop does not move on rails so this directive should be considered.
Directive 2014/32/EU Concerns all measuring equipment like sensors onboard the Hyperloop system.
Directive 2000/14/EC Concerning all outdoor equipment that emits noise, however excluded are equipment intended for transport of passengers or goods by road, rail, air or water. Hyperloop is a floating pod and therefore it can be seen as transport by air, however this should be checked with governing bodies.
Directive 2014/68/EU The tunnel must be able to withstand a pressure of 1 bar during installation, and therefore must conform to this directive concerning pressure equipment.
Directive 2014/53/EU All radio equipment used within the system is subjected to this directive if it also released into the market.

3.2.2 Harmonised standards

3.2.3 Type B

Type B standards are standards which apply to almost all designs and products.

NEN-EN 15085-3:2007 Is about requirements of welded connections in the design.
NEN-EN 12299:2009 Traveling comfort measuring and evaluation norms.
NEN-EN 13272:2012 Electrical lightening norms.
EN 15179:2007 Concerning braking systems and control of braking. Especially the control of braking can still be applicable to hyperloop systems.
NEN-EN 45545:2020 This EN norm is about material and part requirements concerning fire propagation.
NEN-EN 12299:2009 Regulations on ride comfort of passengers.
UIT 76:2016 Basic regulations on product safety, including circulation, battery specifications and more.
ISO 12100:2010 Concerns the risk assessment and reduction of machinery.
IEC 62236-1:2018, IEC 62236-2:2018 This regulation is an international regulation concerning the maximum electromagnetic emission into the environment.
EN 50160 Supply voltage characteristics in distribution systems, so the connection to the power grid. Or output of a solar panel system.

3.2.4 Type C

Type C standards are standards specifically for a product or industry.

NEN-EN 14067:2003 This EN norm is concerning the aerodynamic phenomena of trains in tunnels.
NEN-EN-IEC 62928:2018 Lion-ithion battery use in railway vehicles.

3.3 History of accidents

The Hyperloop is a transport concept still in its development phase, therefore a small president is available for accidents in its history. However, the main systems that will be used in a hyperloop are already in use in other transport systems.

- The first maglev accident: A hyperloop is likely to use maglev technology. Although also being a relatively new technology, it has already been applied. The first deathly accident from this transport system was in Germany in 2006, but was entirely contributed to human error of the maintenance personnel. [4]
- In the train world we see that one should also take the miss use by the traveller into account. For example: In 2019 at least 77 people died in a train fire caused by an exploding gas stove. In addition the train was overcrowded resulting in a large number of fatalities. [14]
- A hyperloop will be efficient because of its operating environment (vacuum). This will also mean that the vehicle will experience pressurisation. This effect is similar to the pressurisation in the aviation industry and there is therefore some precedence regarding accidents due to pressurisation cause by fatigue damage [12] [3].
- As the hyperloop will run in a tunnel/tube it is very prone to natural disasters. A natural disaster is responsible for the largest loss of life in the train industry till nowadays. This was in Sri Lanka 2004, where a tsunami costs the life of an estimated 800 people. [5]
- Also the likely automation has some cause for concern. In 2019 a driveless metro in Paris did not stop for 3 consecutive stations without clear cause for the passengers resulting in panic. [2]
- As the Hyperloop will run in a vacuum tunnel, it is also important to look at the dangers a tunnel introduces. For many Europeans the Mont Blanc tunnel accident still feels fresh. On the 24th of March 1999 a fire broke out. Due to bad design, the fire department was not able to effectively battle the fire and evacuation of the tunnel was troublesome. As people tried to reach safety the tunnel system drove toxic gasses back in the tunnel faster then it could be outran, claiming the life of 39 people. [13]

3.4 Safety-critical functions

Every system has both functions that are not critical for safety as well as functions that are critical for safety. Here safety-critical functions of each subsystem will be identified. To start of a design system matrix is made, a simplified version can be found in Figure 3.1, the most safety critical interactions (red in Figure 3.1) are elaborated on.

3.4.1 Tunnel

Physical damage/distortion If the tunnel is deformed due to impact or affected by corrosion or degradation it could happen that the path of the pod is distorted enough to become detached from the rail, and in worst case the pod might go through the sides of the tunnel. Damage to the tunnel can also lead to flooding or obstruction of the tunnel which can endanger the occupants.

Known failure modes In all designs failure modes like fatigue can not always be avoided and therefore need to be properly managed.

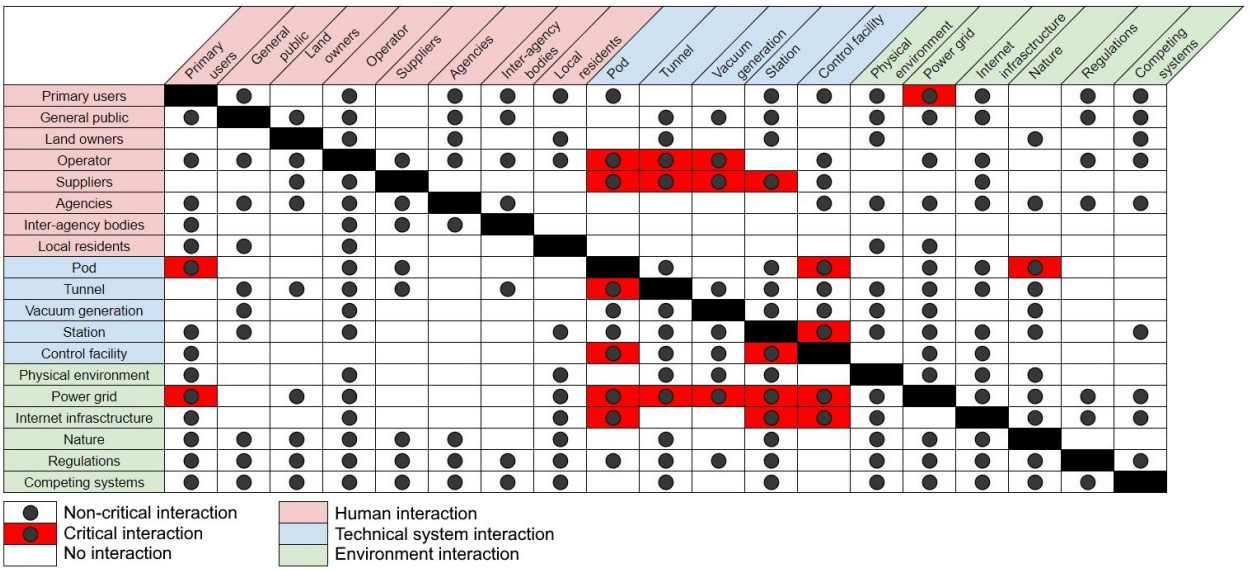

Figure 3.1: Simplified design system matrix, every dot signifies an interaction, all red cells indicate a system critical interaction

Power lines As power lines run through the tunnel, these need to be kept out of reach of the passengers even in emergency situations.

3.4.2 Pod

Life-support Due to the vacuum in the tunnel, the pod needs to be pressurised and supplied with oxygen. If this system fails people can die.

Propelling pod The propelling of the pod using electromagnets can significantly impact nature, due to the electromagnetic fields.

Pod collapse In case of an unexpected stop of a pod or disconnection of a pod with the control system, a different pod can crash into the previous pod.

Interaction with users The users of the pod can get stuck in the pod, feel unsafe or claustrophobic, pass out or become injured or ill. The severity of these events can become worse when the pods lose connection to the outside world.

Fire Although a fire within the tunnel is unlikely when there is a near vacuum, the pod itself can catch fire. This can be caused by defects in the battery or misbehaviour by the users.

3.4.3 Control facility

Power Without power the control system cannot work without redundancy, therefore injuries due to abrupt stops or collision can occur.

Internet infrastructure Loss of connection to either the pods or stations can result in injuries due to loss of control.

3.4.4 Physical environment

Vibrations The traveling of a pod through the tunnel can cause vibrations to the environment. This can cause disturbance or in some cases damage (e.g. with eigenfrequencies).

3.4.5 Power grid

Exposed cabling High power exposed cables can injure users if they are to close to the cables, or during a extreme operating environment(flooding). This can also happen indirectly when the tunnel or pod becomes electrically charged.

Electromagnetic waves High power cables can emit EMP (Electro Magnetic Pulses) which can injure bystanders or occupants. For example the lines over tracks.

3.4.6 Internet infrastructure

Loss of connection All pods must be controlled, therefore position signals to the command center are critical. When signal is lost pods can collide.

Disruption of signals If signals or sensors are disrupted due to external interference, for example: power lines, telescopes, etc.

Hijacking, hacking of The hijacking or hacking of the system by for example terrorists, can not only disrupt the transportation system, but also deliberately make pods crash.

3.4.7 Suppliers

Bad quality/wrong materials If suppliers supply materials which are not as the design specified and certified, unexpected life cycles can occur.

3.4.8 Operator

Maintenance Operators are responsible for maintenance and control of for example fatigue cracks. When these checks are inadequate or not frequent enough critical functions may be lost.

Chapter 4

Hazards identification

4.1 Identifiying the hazards and risk

To identify the most important hazards, a Failure Mode Effect Analysis (FMEA) is made using all DSM's. The failures are ranked using tables A.1, A.2 and A.3. Three factors have been given to each hazard: a severity factor, an occurrence factor and a detection factor. A hazard is considered most important if the severity and occurrence are high and the chance of detection is low. The risk is then calculated by multiplying

the factor. The most important hazards concerning the system are discussed in the next chapter. Checklist from ISO 12100 were not directly used in the FMEA, but were used to identify possible hazards in the FMEA.

4.1.1 Fault tree

An alternative means of identifying hazards and risks is by using a fault tree. This is especially useful when regarding complex sub systems. A fault tree was therefore made for the climate control as it besides heating and cooling also has to provide an oxygen supply and for the vacuum in the tunnel as it is such a massive subsystem. The fault trees can be found in figure B.1 and figure B.2.

Chapter 5

Hazard control

5.1 Unacceptable risks in FMEA

Some risks are unacceptable. These risks should be designed out. If this is not possible, safety devices can be used. When this is also impossible, the last measure is to inform the users about the hazard. In the FMEA, a RPN value was calculated for each of the failure modes (see Appendix A). The most important subsystems are discussed below. The RPN value gives an indication of the risk of the failure mode, but the model is not perfect. Some failure modes are important without a high RPN value.

5.1.1 Pod

The most important failure modes when looking at the FMEA are the pressure failure, oxygen supply failure, uncontrollable movement, fire, sensors measures wrong data, control system receives no signal and control system receives bad data when looking at rather high RPN values.
A potential cause of pressure failure and oxygen supply failure is an empty tank. To prevent this, the tank should be maintained correctly and a sensor should be used to detect anything unusual. During operation the tank should be weight and compared to the flow sensor to detect any leaks. When the system fails, the desired corrective step is to deploy oxygen masks for a pressure failure. To correct the oxygen supply failure, a backup oxygen tank and an emergency exit should be implemented. By implementing these measures the risk of these failure modes will decrease significantly. Most measures are assumed to be rather cheap and thereby are cost effective. Only an emergency exit seems complicated to implement, because of the tunnel wall. The tunnel should depressurise to let people escape to the nearest exit. This will most likely take some time. To solve the risk of panic of the passengers information should be provided to the passenger in cause of a failure.
Another important failure mode is fire. This should be prevented. To prevent overheating of the battery or motor they should be cooled. Furthermore smoke and temperature sensors should be used to detect unusual situations. When a fire occurs it should be corrected by for instance fire extinguishers, sprinklers, insulation and fire proof materials. The circuits could also short. To prevent this the circuit should be tested under normal load and higher loads. To detect a failure, breakers with feedback can be used. To correct the failure, personal can be deployed who are trained on electrical hazards. Using a water based extinction system is most likely not an good idea because of the risk of electrocution. Most measures seems cost-effective. Nevertheless, the pod should not be made of extreme expensive materials. There should be a balance between the cost

and the ability to withstand a fire.
An important failure mode is also a sensor which measures data wrong by for instance interference. To detect any unusual situations, the sensor data should be compared to a second sensor. To minimise the risk of the pod crashing, there should be a crash safety system build inside the pod which monitors the surroundings and breaks automatically. The control system could also receive no signal by for instance broken part or because the signal is blocked. To prevent broken parts, preventive maintenance should be implemented. By looking at the average life expectancy, an maintenance plan can be made. Ideally, it should be predicted when a part fails such that there is no downtime in the system. If it fails inside the pod, a backup communication system should be implemented.. To prevent blocking of the signal the route should be tested extensively and a backup system should be implemented. Furthermore, the control system could receive bad data by disruption. A crash safety system should be implemented to make sure there is no crash by this disruption. These measures will decrease the risk and are essential but the crash safety system can be expensive.
An uncontrollable pod is an important failure mode. A possible cause could be hacking of the pod. Hacking of the pod should be prevented by means of a secure firewall of the system. To detect anything unusual, the connection should be monitored. To correct a potential hack, a manual override switch is recommended. Another important cause are system bugs. This risk should be minimised by testing the software extensively. To detect the failure the control facility should send feedback to the developers. Furthermore a cause is cable interference. To prevent this, interference reducing cables can be used to bundle the lose cables. The solutions proposed for this failure mode seem cost-effective. Still, it should be investigated how extensive the testing can be without running over budged.

5.1.2 Tunnel

The most important failure mode of the tunnel is structural failure of tube for containing the vacuum when looking at the RPN value. Furthermore 'no power transmitted to pod' and electrocution when maintenance is conducted or when there is need for a emergency evacuation are important although the RPN value is lower. Potential causes of structural failure of the tube are natural disasters and impact by equipment which are left inside the tube by maintenance workers. To prevent a failure caused by natural causes, the system should be turned off when there are weather alarms. To detect extreme natural events, a weather station could be implemented into the system, but this seems expensive. Most likely the weather station in the region will be good enough. To prevent equipment laying inside the tube, there should be strict guidelines for the workers working inside the tube and signs should be placed to warn workers of not letting tools inside the system. These measures will most likely not increase the cost significantly and will be essential for the safe operation of the system.
Another potential failure mode is that there is no power power transmitted from the tunnel to the pod. A consequence of this power loss is that the pod cannot decelerate. An important cause for this failure is a broken or corroded cable. To prevent damage, there should be minimal amount of holes where cables are exposed. Also the cable sleeves should be strong enough. To prevent corroded cables, corrosion resistant insulation can be used. To detect damage of corrosion regular visual checks must be conducted and workers should be trained to detect unusual situations. When the failure mode occurs an emergency break should be implemented, which can be build into the pod. The emergency break must require power to not break. When the power is off, it will then be activated. The measures are important and thereby cost is less of an issue. Requirements should be set for the emergency break such that an appropriate solution can be designed.
The tunnel should allow maintenance and emergency evacuation. A potential failure mode could be electrocution because of the high energy need of the system. A cause of this could be unprotected cables. To prevent electrocution, the cable should be well protected. To detected any unusual situations visual checks should be conducted. To prevent electrocution, the electricity should be cut off when there is a shorting. The measures are most likely cost-effective and important to minimise the risks. Like stated before, emergency exits can be hard to implement but is essential.

5.1.3 Control facility

The most important failure mode of the control facility is the crash of pods into each other. The most important cause is that the system is hacked , the software is not good enough or the hardware is broken.
To prevent hacking of the system, the antivirus should be up to date. Furthermore a private network can be used to isolate the system form outside. To detect unusual situations, the connection should be monitored. When the system is hacked there should be a manual override switch. To prevent software bugs, the software should be extensively tested. To detect bugs in the systems, the control facility can give feedback to the developers. To correct any failure, a backup system which uses for instance a previous version of the code can be used. A manual override switch can also be implemented. Another cause of the crashing of the pods could be broken hardware. To prevent this, the maintenance should be done preventive. To detected any hardware problems, the connection should be monitored. To correct when the hardware fails, a backup system should take over the control before repairs can be made. These measures should be important minimising the risks and the measures seem also not expensive. They will limit the downtime of the system and thereby lower the cost.

5.1.4 Vacuum generation

The important failure mode for the vacuum generation is the failing of the compressor. The most important cause is wear. To prevented this, the compressor should be preventive maintained such that the risk of failing during operation is minimised. A backup compressor could be also implemented to eliminate this risk. Because failing will result in downtime of the system, it will cost money. By preventing this, these cost will be minimised and the cost of the measures are justified.

5.2 Monitor system

5.2.1 Lagging and leading indicators

It is not possible to solve all hazards. Thereby the system should be monitored. For this monitoring, there are lagging and leading indicators. Lagging indicators indicate if something bad happened. Leading indicators can be used to notify failures before they happen [7].
Lagging indicator of the SoI are for instance customer complains, the number of fails of the break systems during operation and number of training's missed by the employees.
Leading indicators are for instance safety training's which are planned in the future, the number of near-misses, employee observation and the employee engagement.

5.2.2 Safety culture

To minimise risks in the operation of the system, the users and employees should be aware of the importance of safety. These groups should be involved in the designing process for a safe system, be encouraged to prevent accidents and give feedback on the operation of the system. To improve the safety culture, training's on safety could be given. Furthermore it would be useful to make the employees responsible for parts of the system to prevent accidents. For instance the maintenance crew could distribute the responsibility of certain components. This will most likely make the employee more aware of the risks and can thereby be useful to minimise them.

Chapter 6

Conclusion

In this report the Hyperloop has been analysed for safety critical aspects. This has been done with a systems engineering approach which includes tools to include all relevant aspects of the system of interest. The pod, tunnel, vacuum generation, station and control facility have been identified as the main subsystems. A detailed analysis of these subsystems resulted in a thorough understanding of the system. Next to the system the environment in which the system operates and the relevant human factors have been discussed.
From the detailed system analysis the level of protection was determined for each subsystem based on their functions, from which safety requirements followed.
Because the Hyperloop is still under development only a limited list of previous accidents could be given. Therefore the history of similar means of transportation was studied to find additional safety related functions. For this reason a study of the relevant norms was also performed.
The functions of the system which were safety critical have been found by the construction of a design system matrix. A FMEA was made to identify the most important hazards and risks.
The report is concluded with control and monitor recommendations for the unacceptable hazards and risks of the Hyperloop. They concern the pod, tunnel, control facility and vacuum generation.

Bibliography

[1] Kosten fyra-fiasco bijna 800 miljoen. *NOS - Binnenland*, Jun 2015.

[2] The Local Europe AB. Paris metro passengers get 'fright of their life' on runaway driverless train. http://news.bbc.co.uk/2/hi/south_asia/4132247.stm, 18-9-2019. Accessed on: 4-12-2020.

[3] Aircraft accident investigation commission Ministry of transport. Aircraft accident investigation report japan air lines co.. ltd. boeing 747 sr-100. ja 8110 gunma prefecture. japan. https://www.mlit.go.jp/jtsb/eng-air_report/JA8119.pdf, 19-6-1987. Accessed on: 4-12-2020.

[4] BBC. Deadly crash on german monorail. http://news.bbc.co.uk/2/hi/europe/5370564.stm, 2006. Accessed on: 4-12-2020.

[5] BBC. Survivors tell of tsunami train horror. http://news.bbc.co.uk/2/hi/south_asia/4132247.stm, 30-12-2004. Accessed on: 4-12-2020.

[6] Hyperloop Connected. Regulating the hyperloop. http://hyperloopconnected.org/2019/09/regulating-the-hyperloop/, 26-09-2019. Accessed on: 20-11-2020.

[7] Hyperloop. Understanding leading and lagging indicators of safety. https://www.fldata.com/leading-lagging-indicators-safety-performance, 2020. Accessed on: 2-12-2020.

[8] Hyperloop. Delft hyperloop presenteert nieuw team in kunsthal rotterdam. https://www.emerce.nl/wire/delft-hyperloop-presenteert-nieuw-team-kunsthal-rotterdam, 7-2-2020. Accessed on: 16-11-2020.

[9] Klei K. Virgin hyperloop verscheept eerste passagiers. https://www.kijkmagazine.nl/filmpjes/virgin-hyperloop-verscheept-eerste-passagiers/, 14-11-2020. Accessed on: 16-11-2020.

[10] Opgenoord M. M. J. and Caplan P. C. Aerodynamic design of the hyperloop concept. *AIAA Journal*, 56(11):4261–4270, 2018.

[11] Nejad M. R. *Safety by design Engineering products and systems*. SafetyCube.com, 2020.

[12] Aviation Safety Network. Aloha airlines flight 243 incident report. https://aviation-safety.net/database/record.php?id=19880428-0, 4-12-2020. Accessed on: 4-12-2020.

[13] Duffé P. and Marec M. Task force for technical investigation of the 24 march 1999 fire in the mont blanc vehicular tunnel. https://bit.ly/36F7vG7, 20-6-1999. Accessed on: 4-12-2020.

[14] The Washington Post. At least 73 dead in massive train fire in eastern pakistan. https://www.washingtonpost.com/world/at-least-66-dead-in-massive-train-fire-in-eastern-pakistan/2019/10/31/2a35919a-fba6-11e9-ac8c-8eced29ca6ef_story.html, 31-10-2019. Accessed on: 4-12-2020.

[15] Hai-Ying Wang, Xiao-Bo Zeng, Si-Yuan Guo, and Zong-Tao Li. Effects of magnetic field on the antioxidant defense system of recirculation-cultured chlorella vulgaris. *Bioelectromagnetics*, 29(1):39–46, 2008.

Appendix A

FMEA

A.1 Tables

Table A.1: Severity ratings

Severity	Category	Result
Catastrophic	4	Could result in one or more of the following: death, permanent total disability, irreversible significant environmental impact, or monetary loss equal to or exceeding €10,000,000.
Critical	3	Could result in one or more of the following: permanent partial disability,injuries or occupational illness that may result in hospitalization of at least three personnel, reversible significant environmental impact, or monetary loss equal to or exceeding €1,000,000 but less than €10,000,000.
Marginal	2	Could result in one or more of the following: injury or occupational illness resulting in one or more lost work day(s), reversible moderate environmental impact, or monetary loss equal to or exceeding €100,000 but less than €1,000,000.
Negligible	1	Could result in one or more of the following: injury or occupational illness not resulting in a lost work day, minimal environmental impact, or monetary loss less than €100,000.

Table A.2: Occurrence ratings

Occurrence	Level	Specific item	Fleet or inventory
Frequent	6	Likely to occur often in the life of an item.	Continuously experienced.
Probable	5	Will occur several times in the life of an item	Will occur frequently.
Occasional	4	Likely to occur sometime in the life of an item	Will occur several times.
Remote	3	Unlikely, but possible to occur in the life of an item.	Unlikely, but can reasonably be expected to occur.
Improbable	2	So unlikely, it can be assumed occurrence may not be experienced in the life of an item.	Unlikely to occur, but possible.
Eliminated	1	Incapable of occurence. This level is used when potential hazards are identified and later eliminated.	Incapable of occurence. This level is used when potential hazards are identified and later eliminated.

Table A.3: Detection ratings

Detection	Category
5	Impossible
4	Almost impossible
3	Hard to detect
2	Easy to detect
1	Always detected

A.2 FMEA

										Recommended action(s)		
Part	Function	Potential Failure mode	Potential effect of failure mode	Severity	Potentional causes	Occurance	Means of detection	Detection change	RPN	Preventive	Detective	Corrective
Pod	Support life	Aircondition failure	Freezing	3	Power loss	2	Measure resistance over wire	1	6	Backup local energy source, split into two system redundancy, add insulation	Add temperature sensor with alarm, to prioritse rescue	Backup heat source
					Sensor malfunction	2	Backup sensor to compare results	3	18	Preventive maintenance of sensors	Monitor sensor status, Two sensors for redundancy	Manual override switch
					Hardware failure	3	Measure temperature difference over time	2	18	Preventive maintenance, Multiple units	Do data analysis over multiple trips	
			Overheating	3	Power loss	2	Measure resistance over wire	1	6	Backup battery, split into two system redundancy, add insulation	Add temperature sensor with alarm, to prioritse rescue	
					Sensor malfunction	2	Backup sensor to compare results	3	18	Preventive maintenance of sensors	Monitor sensor status, Two sensors for redundancy	
					Hardware failure	3	Measure temperature difference over time	2	18	Preventive maintenance, Multiple units	Temperature sensor with alarm	
		Pressure failure	People die or get injured	4	Tank empty	4	Flow sensor and pressure sensor	2	32	Preventive maintenance of tank integrity and sensor	Measure weight of tank, and compare to flow sensor data	Oxygen masks deployment
				4	Power loss	3		1	12	Backup energy source		
		Oxygen supply failure	People die or get injured	4	Tank empty	4	Flow sensor and pressure sensor	2	32	Preventive maintenance of tank integrity and sensor	Measure weight of tank, and compare to flow sensor data	Backup oxygen tank, emergency exit
					Power loss	3		1	12			
		Air contamination	People die or get injured	4	Dangerous materials used	2	Sensors for toxic gasses	3	24			
					To low oxygen percentage	3	CO2 sensor	2	24			Shut off air system, use backup system (oxygen masks+tanks)
					Fire	3	CO sensor	2	24	Non toxic materials used		Fire extinguishers, release all air into tube and replace air with air from compressed tank
		Fire	People die or get injured	4	Battery overheating	3	Temperature sensor	2	24	Battery cooling	smoke detector, temperature sensor	fire extinguishers, sprinkler system, physical insulation, fire proof materials
					Motor overheating	2	Temperature sensor	2	16	Motor cooling	temperature sensor	fire extinguishers, sprinkler system, physical insulation, fire proof materials
					Shortcircuit	3	Ground breaker	3	36	Circuit tests, overload tests	Breakers with feedback	Deploy personel, trained on electrical hazards
		Sensors measures wrong data	Pods crashing	4	Sensor measuring interference	4	Compare output with redundancy sensor	4	64		Seperate sensor to compare sensor output	Crash safety systems

	Communicate position to control centre	Control system receives no signal	Pods crashing	4	Communication system is broken	4	No response from system	2	32	Preventive maintenenance		Backup communcication system
					Communication signal is blocked	5	No response from system	2	40	Test routes extensively		Backup less disruptable signaling system
		Control system receives bad data	Pods crashing	4	Communications signal is disrupted	5	Data checker (par, zip like communication)	3	60			Crash safety systems
	Control pod actual movement	Movement out of control	Injury, damage	4	Hacked	3		4	48	Firewall	Monitoring connection of pod	Manual override switch
					Software bugs	4		3	48	Extensive testing of software before use	Feedback from control facility	Backup system
					Motor broken	2		1	8	Preventive maintenance		
					Cables broken/damaged	2	Measure resistance	2	16			
					Cable interference	4		3	48	Add interference reducing cable to bundle		
Tunnel	Contain vacuum	Air seeping into the tunnel	System becomes unoperational	2	Leakage due to fatigue	5	Pressure sensors	2	20	Preventive maintenance		
					Bad maintenance	4	Random quality checks	3	24	Educate mechanics extensively	Quality checks on all operations	Adapt design for design for maintenance
					Bad installment	2	Random quality checks	3	12	Design for installing	Quality checks on each installation	
					Bad supplied part	4	Random quality checks	3	24	Explictite specification of parts and processes of production	Quality check on all supplied parts	
		Failing to maintain pump balance	System becomes unoperational	2	Efficiency loss on pump due to wear	3	Vibration sensors	3	18	Preventive maintenance		Corrective maintenance
					Pump faillure	3	Pressure sensors, Mass flowrate sensors	2	12	Preventive maintenance		Corrective maintenance
		Structural faillure of tube	Death	4	Natural disaster	4	Weather services	3	24	System shutdown for wheather alarms	System shutdown for alarm of own wheather stations	
					Impact with equipment	5	Camera systems	4	40	Strict guidlines for equipment use round the tube		
	Transport Power to pod	No power transmitted	No pod movement	2	Cable broken by animals	2	Measure resistance	2	8	Prevent holes/gaps, Scare off/trap animals	Regular visual checks	Stop following pods
					Cable broken by damage	3	Measure resistance	2	12	Prevent holes/gaps, Tough cable sleeve	Regular visual checks	Stop following pods
					Cable coroded	4	Measure resistance	2	16	Prevent holes/gaps, Corrosion resistant insulation	Regular visual checks	Stop following pods
			Pods cannot decelerate using motors	3	Cable broken by animals	2	Measure resistance	2	12	Prevent holes/gaps, Scare off/trap animals	Regular visual checks	Activate emergency brakes
					Cable broken by damage	3	Measure resistance	2	18	Prevent holes/gaps, Tough cable sleeve	Regular visual checks	Activate emergency brakes
					Cable corroded	4	Measure resistance	2	24	Prevent holes/gaps, Corrosion resistant insulation	Regular visual checks	Activate emergency brakes

	Allow maintenance and emergency evacuation	Electrocution	Death	4	Unprotected cable	2	Visual checks	3	24	Well protected cables	Regular visual checks	Ground breaker
Control facility	Control pod global positioning	Pods crash into eachother	Death/Injury	4	Hacked	3		4	48	Up to date antivirus. Private network	Monitoring connection of pod	Manual override switch
					Software bugs	4		3	48	Extensive testing of software before use	Feedback from control facility	Backup system,Manual override switch
					Broken hardware	4		2	32	Preventive maintenance	Monitor connection	Corrective maintenance, Backup system
		Pod occupieing space waiting for passenger	People get irritated	1	Passenger to late	5	Measure time between arrival message and door closing	2	10			Fine passengers to late
					Passenger chang mind	4	Measure time between arrival message and door closing	3	12			Fine passengers for not denying there own request
		Pod waiting at wrong station	People need to wait for a new pod	1	Wrong user input	4	Compare phone gps position to station entered	4	16	Clear confirmation of trip	Visualisation of trip	Put pod back into to be assigned pool
					Wrong user stepped in	4	Compare phone id to expected passenger phone id	3	12	Clear confirmation of trip	Visualisation of trip	Send pod back
Vacuum generation	Generate almost vaccum in the tunnel	Compressor failing	Pods cannot move through tube	2	Compressor fails unexpected	3	Air flow meter	2	12			Replace compressor, backup compressor
					Power outage	3	Voltage meter	1	6			Backup power
					Wear	6	Vibration meter	3	36	Preventive maintenance		Replace defective part, backup compressor
Station	Accomedate passengers	Not enough room	People cannot get to the pods	1	Events	3	Count in- and outflux	2	6	Dedicated lanes		Close entrance
			Children/groups get lost/seperated	1	Events	3		4	12	Dedicated lanes, with high railings		

Appendix B

Fault trees

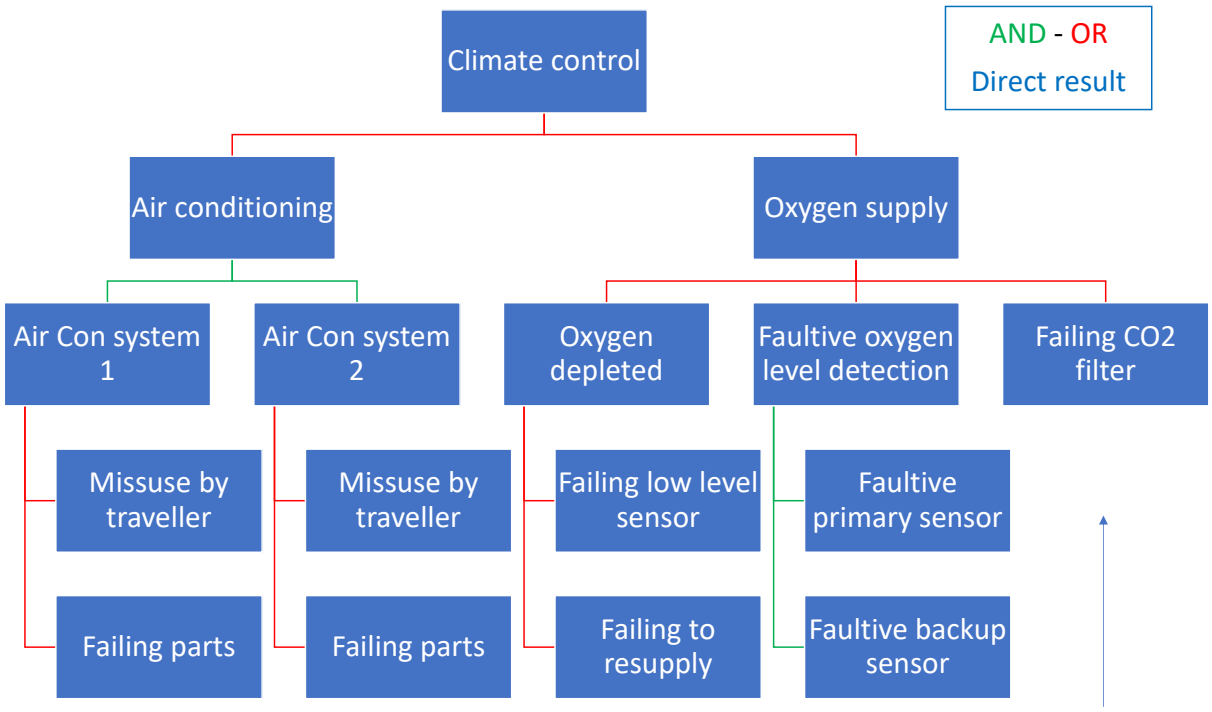

Figure B.1: Fault tree climate control

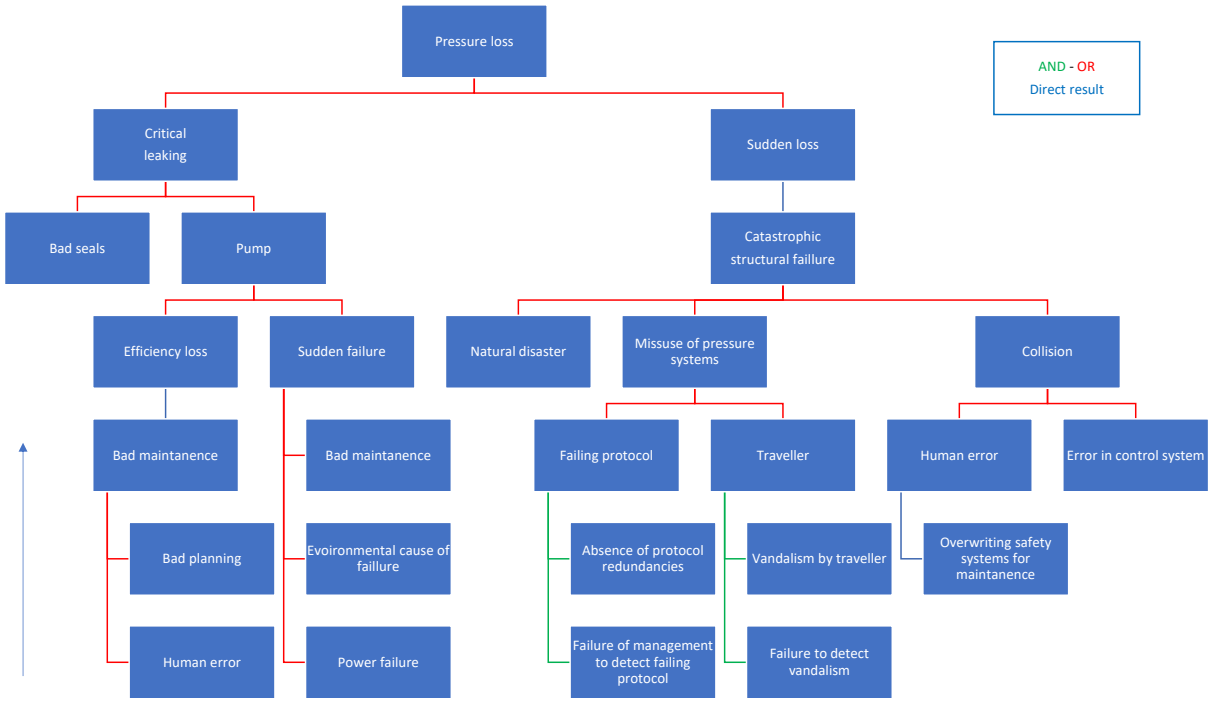

Figure B.2: Fault tree pressure control

The fault trees in figure B.1 and B.2 start with one or multiple events at the bottom. Then moving up the event encounters AND gates, OR gates and direct result. For an AND gate both events have to happen to encounter the output event, compared to a OR gate where only one of them has to occur. For example we take the *failing part* at the left bottom of figure B.1. When the part fails it passes through an OR gate triggering the failure of *Air Con system 1*. However as this runs parallel to *Air Con system 2*, it does not result in an overall failure of the entire *Air conditioning* system. It therefore has an AND gate in between.