Public

Enablers of Testing Autonomous Vehicle at Existing Proving grounds (ETAVEP)

Project within road safety and automated vehicles - FFI

Datum: 30 March 2022
Authors: Albert Lawenius, Volvo Cars
Arvid Pearson, Volvo Cars
Patrik Nordberg, Volvo Cars
Thomas Broberg, Volvo Cars
Erik Frick, AstaZero
Jenny Viklund, AstaZero
Anna Sjövall, AstaZero
Lukas Wikander, AstaZero
Urban, Dagerhorn, AstaZero
Tomas McKelvey, Chalmers University of Technology
Daniel McKelvey, Chalmers University of Technology
Marvin Damschen, RISE
Anders Thorsén, RISE
Lars Johansson, AB Volvo

FFI Fordonsstrategisk Forskning och Innovation
VINNOVA Energimyndigheten TRAFIKVERKET FKG VOLVO SCANIA VOLVO

Table of Contents

Kort om FFI
FFI är ett samarbete mellan staten och fordonsindustrin om att gemensamt finansiera forsknings- och innovationsaktviteter med fokus på områdena Klimat & Miljö samt Trafiksäkerhet. Satsningen innebär verksamhet för ca 1 miljard kr per år varav de offentliga medlen utgör drygt 400 Mkr.

För närvarande finns fem delprogram; Energi & Miljö, Trafiksäkerhet och automatiserade fordon, Elektronik, mjukvara och kommunikation, Hållbar produktion och Effektiva och uppkopplade transportsystem. Läs mer på www.vinnova.se/ffi.

1 Executive Summary

Testing at proving grounds is a vital stage in the verification and validation chain to ensure both quality and safety of vehicles before they reach the market. This type of testing is facing a new challenge, and that is how to include *testing of autonomous vehicles into normal testing practices.* As these vehicles not necessarily need to have a cab or driving controls, meaning a test driver cannot be in direct control of the vehicle, and thereby cannot guarantee the safety. To solve the issue, there are two obvious solutions, build a new dedicated test track or divide the track time between manually driven vehicles and autonomous self-driven vehicles. The former is extremely expensive, and the latter is not possible as that would prolong the verification time, which is already today a bottleneck in many cases.

ETAVEP has investigated a third option, to integrate autonomous self-driven vehicles into already existing proving grounds operations, hence mixed traffic. The project has addressed what an enabling system, substituting the test driver, needs to fulfill by a proof-of-concept. With its proof-of-concept ETAVEP shows it is possible to integrate self-driven vehicles into existing proving grounds. But it must be done in a systematic and iterative process.

The main objective of the project was to; investigate the possibility to substitute the test driver for self-driven vehicles testing at existing proving ground facilities. To be able to substitute the test driver several research questions need to be answered by a proof-of-concept that embodies state of the art solutions to each research question:

1. Which global monitoring principles need to be applied?
2. Which local monitoring principles need to be applied?
3. Can a type of on-board monitoring for vehicle faults be developed that detects mechanical faults and wear as well as (or better than) an experienced test driver?
4. How to take emergency control over an autonomous vehicle at risk?
5. What is a sufficient set of test cases for validating concepts that have been developed to address 1-4?

Questions one to four were resolved within the project, but the fifth question was too vast to be fitted into the project timeframe, although the project was able to partly answer the question. It is possible to verify but not validate the system as it was shown to be more complicated than initially thought.

The project used a systematic approach to reach the objective that was defined as a layer-based framework. The first step was to understand the proving ground system. When having the knowledge of the system several layers needed to be solved. First layer, is the vehicle safe to drive? If yes, is it possible to stop the vehicle regardless of situation? Is the surrounding safe? Is the movement of the vehicle safe? And finally, is the proving ground operation safe? By finding solutions to each layer, the proof-of-concept shows the possibility to substitute a test driver and address the research questions.

Outcome shows the importance to understand the system by having the right procedures, information and training. To verify the condition of the vehicle an algorithm has been developed to detect non-trivial mechanical faults, using a non-parametric local rational model algorithm. The algorithm was able to differentiate whether the vehicle had any faults or not. The vehicle stop functionality was ensured by using two standalone brake systems to always guarantee stop functionality. To distinguish pedestrians, vehicles or other objects in proximity to the self-driven vehicle, external sensors were integrated to guarantee a safe environment. The developed traffic control system utilizes a safety zone concept showing the potential to make sure vehicle movement remain safe at all-time. If there are vehicle faults or objects in proximity to the vehicle the traffic control sends a stop signal. To ensure the operation stay safe, guidance and routines concerning proving ground design and way of working need to be updated and promptly followed.

As a result of ETAVEP, it is not only shown the possibility and how to integrate self-driven vehicles into existing proving grounds with mixed traffic. But it has also generated several guidelines, best practices, methods, and frameworks of how to do it in a safe way, which has been shared in between the partners. The knowledge gained during the project can be used to; stepwise implement systems which ultimately will enable safe testing of self-driven vehicles at existing proving grounds. The project has also provided a solid foundation for further research to strengthen future systems to enable more advanced testing with higher safety, reliability, performance, and robustness.

An extra attention was given to the proof-of-concept to ensure it is not a specific but a generic concept. Therefore, it is independent of, vehicle type and maturity, weather (excl. snow) and road type (test tracks) and feasible for test speeds up to 80km/h.

Due to COVID-19 situation meetings and demos were made virtually. Dissemination was performed using internal expertise within the partner organizations as well with expertise within SAE together with two academic publications, two demonstrations and a conference workshop. Further, to the content of the project, proving ground design and way of working was added as a result of the initial findings of the project. As the execution continued efficiently, the project managed to rearrange resources to realize this.

The project has shown it is possible to integrate self-driven vehicles into already existing proving grounds if it is done properly with a safety mindset. This is an essential key for Swedish industry to launch self-driven vehicles without risking safety. It contributes to the “Zero Vision” target and increase the Swedish capacity for research and innovation. ETAVEP has not only advanced the development of autonomous testing environments but has also allowed the partners to remain at the forefront in this field.

2 Summering

Testning på provbanor är ett viktigt steg i verifierings- och valideringskedjan för att säkerställa både kvalitet och säkerhet hos fordon innan de når marknaden. Denna typ av testning står inför en ny utmaning, testningen av autonoma fordon. Eftersom dessa fordon inte nödvändigtvis behöver ha hytt eller körreglage innebär det att en testförare inte kan ha direkt kontroll över fordonet och därmed inte kan garantera säkerheten. För att lösa problemet finns det två självklara lösningar; bygga en ny dedikerad provbana eller dela upp bantid mellan manuellt framförda fordon och autonoma självkörande fordon. Det första alternativet är kostsamt och det andra är inte möjligt eftersom det skulle förlänga verifieringstiden, vilket redan idag är en flaskhals.

ETAVEP har undersökt ett tredje alternativ, att integrera autonoma självkörande fordon i redan existerande provningsverksamhet. Projektet har undersökt vad ett system, som ersätter testföraren, behöver uppfylla. Detta genom utvecklingen av ett proof-of-concept. ETAVEP påvisar att det är möjligt att integrera självkörande fordon i befintlig provningsverksamhet men det måste göras systematisk och iterativt.

Huvudsyftet med projektet var att undersöka möjligheten att ersätta de säkerhetsfunktioner en testförare utövar vid framförandet av ett fordon. För att kunna ersätta testföraren måste flera forskningsfrågor besvaras av ett proof-of-concept som materialiserar lösningar på respektive forskningsfråga:

1. Vilka globala övervakningsprinciper måste tillämpas?
2. Vilka lokala övervakningsprinciper måste tillämpas?
3. Kan en typ av övervakning av fordonsfel utvecklas som upptäcker mekaniska fel och slitage lika bra (eller bättre än) en erfaren testförare?
4. Hur tar man kontroll över ett autonomt fordon som är utsatt för risk?
5. Vad är en tillräcklig uppsättning testfall för att validera koncept som har utvecklats för att adressera 1-4?

Fråga ett till fyra besvarades inom projektet men den femte frågan var för omfattande för att passa inom projektets tidsram, även om projektet delvis kunde besvara frågan.

Projektet använde ett systematiskt tillvägagångssätt för att nå målet som definierades som ett lagerbaserat ramverk. Första steget var att förstå provbanans systematik. Genom att förstå systemet behövde flera lager arbetas igenom. Första lagret, är fordonet säkert att framföra? Om ja, är det möjligt att stoppa fordonet oavsett situation? Är omgivningen säker? Är fordonets rörelse säker? Och slutligen, är driften av provbanan säker? Genom att hitta lösningar på varje lager bevisar proof-of-concept möjligheten att ersätta en testförare och ta itu med forskningsfrågorna.

Resultatet visar vikten av att förstå systemet genom att ha rätt rutiner, information och utbildning. För att verifiera fordonets tillstånd har en algoritm utvecklats för att upptäcka icke-triviala mekaniska fel, med hjälp av en icke-parametrisk 'Local Rational Model'-algoritm. Algoritmen kunde skilja på om fordonet hade några fel eller ej. Stoppfunktion av fordon säkerställdes genom att använda två fristående bromssystem för att alltid garantera funktionalitet. För att särskilja fotgängare, fordon eller andra föremål i närheten av det självkörande fordonet integrerades externa sensorer. Trafikkontrollsystemet använder ett säkerhetszonskoncept som visar potentialen för att säkerställa att fordonsrörelsen alltid är säker. Om det finns fordonsfel eller föremål i närheten av fordonet skickar trafikkontrolsystemet en stoppsignal. För att garantera driftsäkerheten behöver riktlinjer och rutiner för provbanedesignen och arbetssätt uppdateras och följas.

Som ett resultat av ETAVEP visas inte bara möjligheten och hur man kan integrera självkörande fordon i befintliga provningsverksamheter utan har också genererat flera riktlinjer, ramverk och metoder för hur det implementeras på ett säkert sätt. Dessa har delats mellan partnerna. Kunskapen som genererats under projektet kan användas för att stegvis implementera system som i slutändan kommer att möjliggöra säker testning av självkörande fordon på befintliga provningsplatser. Projektet har också gett en gedigen grund för vidare forskning för att stärka framtida system vilket möjliggör att mer avancerad testning med högre säkerhet, tillförlitlighet, prestanda och robusthet kan nås.
Extra uppmärksamhet ägnades åt att säkerställa att proof-of-conceptet inte är en unik lösning utan generiskt. Därför är den oberoende av fordonstyp och mognadsgrad av fordon, väder (exkl. snö) och vägtyp (testbanor) samt gällande för testhastigheter upp till 80 km/h.

På grund av COVID-19-situationen hölls möten och demonstrationer virtuellt. Spridningen skedde med hjälp av intern expertis inom partner-organisationerna samt med experter inom SAE, två akademiska publikationer, två demonstrationer och en konferensworkshop. Dessutom adderades leveransen *provbanadesign och arbetssätt* till innehållet i projektet. Eftersom utförandet av projektet fortlöpte effektivt lyckades projektet omorganisera resurserna för att förverkliga detta.

Projektet har visat att det är möjligt att integrera självkörande fordon i redan befintlig provbaneverksamhet om det görs på rätt sätt med hänsyn till säkerhet. Detta är en väsentlig nyckel för svensk industri att lansera självkörande fordon utan att riskera säkerheten. Det bidrar till ”Nollvisionen” och ökar den svenska kapaciteten för forskning och innovation. ETAVEP har inte bara avancerat utvecklingen av autonoma provbanemiljöer utan har också möjliggjort för partnerna att ligga i framkant inom detta område.

3 Background

Testing at proving grounds is a vital stage in the verification and validation chain to ensure both quality and safety of vehicles before they reach the market. This type of testing is facing a new challenge, and that is how to include *testing of autonomous vehicles into normal testing practices.*

To be more precise, the problem is that in today's testing, the core component that keeps the testing of developmental vehicles safe is a skilled, trained, and experienced human test driver. However, many future self-driven vehicles will have no room to fit a test driver. For trucks, several current self-driven concepts are cab-less, see Figure 1. For cars, robotaxi is generally seen as a first application, and these robotaxis will neither have a driver's seat nor physical driver controls, see Figure 2. Since vehicles will either have no room for, or controls available for, a test driver that can guarantee safe testing, other solutions for maintaining safety during developmental testing needs to be found.

Figure 1 Volvo Trucks autonomous concept VERA

Figure 2 Interior view from Volvo Cars 360c Concept Car

At this point, it should be made clear that while the vehicle under test will need to have enough self-driven capability to be able to navigate around the test track (otherwise it cannot perform the required test), it will not be an option to rely solely on that self-driven capability to ensure safety at the proving ground. After all, it is developmental vehicles that are being tested, and these are not yet ready for public road release in terms of hardware and software status. They have yet to be verified to meeting all requirements needed to ensure safe operation.

One solution to the problem of maintaining a safe test environment would be to build a completely separate proving ground for self-driven vehicles. Here, even if vehicles sometimes might crash, at least no humans would be injured. However, building a completely separate test track is very costly, and would not help Swedish industry to stay competitive. Another solution along similar lines would be to time share on existing proving grounds, e.g., manually driven vehicles in the morning and self-driven in the afternoon. Again though, it would make Sweden less competitive in this arena, because all test series now would take twice as long to complete.

For these reasons, it is clear that the first approach that needs to be investigated is whether one can integrate testing of self-driven vehicles into today's proving grounds practices as they are, rather than build something completely new. This would require adding technical capabilities in and around the self-driven vehicles that are able to carry out the same safety management tasks that the test driver currently handles.

To specify the problem being addressed in the current project in more detail, in today's testing, the test driver performs two key tasks. One is ensuring that the test vehicle neither runs off the road nor collides with other traffic participants or objects during testing. The other is monitoring the vehicle for faults that are known to sometimes occur in a vehicle platform under development and which may lead to loss of vehicle control (e.g. thermal activity, functional deviations, and mechanical ruptures in key locations). To replace the test driver in self-driven vehicles under tests, other ways to maintain these two capabilities must be identified and implemented.

Regarding the first capability (safe traffic control), a pre-study was conducted at AstaZero (Viklund, 2019). In this pre-study, vehicles on SAE Level 4 and 5 (SAE International, 2014) were studied, with focus on safe proving ground operations, both on the test tracks and on their way from the workshops to the tracks. It was concluded that while autonomous test vehicles are manageable as long as tests are performed on exclusive tracks, the safety requirements that need to be met when mixing autonomous and manually driven test vehicles requires wholly different supervision and safety systems.

Furthermore, both AstaZero and Volvo Cars are part of the European Proving Ground Safety Association (EPGSA), an association including most proving grounds in Europe. During 2018-2019, AstaZero has led a working group where EPGSA members and clients have discussed testing with self-driven vehicles on proving grounds. The results show that a lot of work remains before the risks related to testing vehicles with no test driver on-board are fully understood and mitigatable, even in a fenced off environment like a test track. Furthermore, while the consensus is that testing of self-driven vehicles is coming, very few have real experience of testing such vehicles, and thus have difficulties developing an informed opinion. These research questions will be investigated in a series of studies with the goal of being able to develop a proof-of-concept that embodies best practice for each research question respectively.

ETAVEP was coordinated by Volvo Cars and executed together with AstaZero, AB Volvo, SafeRadar Research Sweden AB, RISE and Chalmers University of Technology. The project has run for two years with a total budget of MSEK 15.2, with public support of MSEK 7.7

4 Purpose, Research Question and Method

The main purpose of ETAVEP was to investigate the possibility to substitute the safety driver with another solution for self-driven vehicle testing at existing proving ground facilities. To be able to substitute the safety driver several research questions needed to be answered, and in the end of the project present a proof-of-concept that embodies state of the art solutions to each research question.

- **Which global monitoring principles need to be applied?** To what extent does the current proving ground traffic control concept need to be extended and/or changed to adequately supervise autonomous vehicles on test tracks?
- **Which local monitoring principles need to be applied?** Since both living and inanimate objects may appear on the test track unexpectedly (in the sense of a tree falling down, an animal jumping the fence or a road worker experiencing transponder malfunctions), which object detection and classification capabilities need to be installed in addition to those used for continuous traffic control?
- **Can a type of on-board monitoring for vehicle faults be developed that detects mechanical faults and wear as well as (or better than) an experienced test driver?** In particular, will statistical models of expanded non-parametric transmissibility estimates using Local Rational Models (LRM) with a general sensor setup provide a sufficiently robust and accurate performance in this capacity?
- **How to take emergency control over an autonomous vehicle at risk?** If a risk materializes in any of the above monitoring systems, how does one make sure that the autonomous vehicle can be brought to a safe stop?
- **What is a sufficient set of test cases for validating concepts that have been developed to address 1-4?** Since it is impossible to test for all combinations of potential errors, what is an appropriate set of edge cases that if handled will guarantee the desired safety envelope in the four safety aspects described above?

The Project was divided into six work packages, see Figure 3, First, Project management and Demo, focused on coordinating the projects progression and dissemination activities. While the second was dedicated on understanding the system. Third to sixth had the target to develop the proof-of-concept.

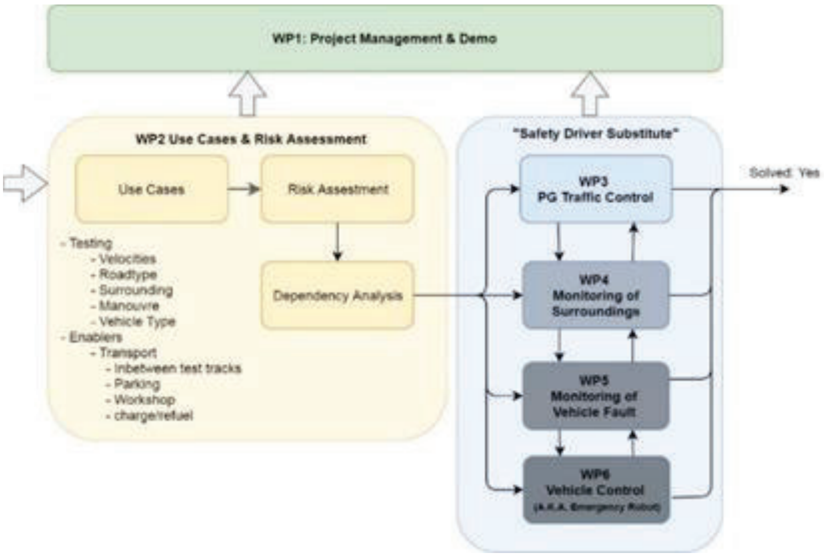


Figure 3 Project structure

ETAVEP has developed a proof-of-concept in several steps, also visualized in Figure 4:

- To understand what a proof-of-concept needs to solve, a stakeholder analysis was performed, use cases were drawn and risk assessment was conducted with experts within the area. (WP2)
- Implement a system to detect non-trivial mechanical faults that could occur during tests, making sure the vehicle itself is safe. (WP5)
- Establish software-based stop functions using the vehicle internal brake system by overriding the vehicle commands. In case the software-based stop function somehow fails a redundant fallback emergency brake system using external actuators is implemented, which will bring the vehicle to a safe stop. (WP6)
- Add capability to monitor the local surrounding of the self-driven vehicle to detect object that can cause safety hazards with stationary sensors (track mounted) and test vehicle mounted sensors. The self-driven vehicle’s own sensors are still under development and cannot be depended upon. (WP4)
- Adding real time supervision functionality (extension of existing conventional traffic monitoring system), taking into account detection from the sensors monitoring the local surround of the self-driven vehicles, positions from vehicle transponder units and proving ground layout. If the movements of the self-driven vehicles are not safe, a stop signal to the vehicle will be sent. (WP3)
- To ensure the operation on proving ground remain safe during operation, a supporting draft of proving ground design and way of working is established. (WP2)
- Integrate all sub-systems into a complete Proof of Concept and verify its functionality with respect to the research questions. (WP2, 3, 4, 5, 6)

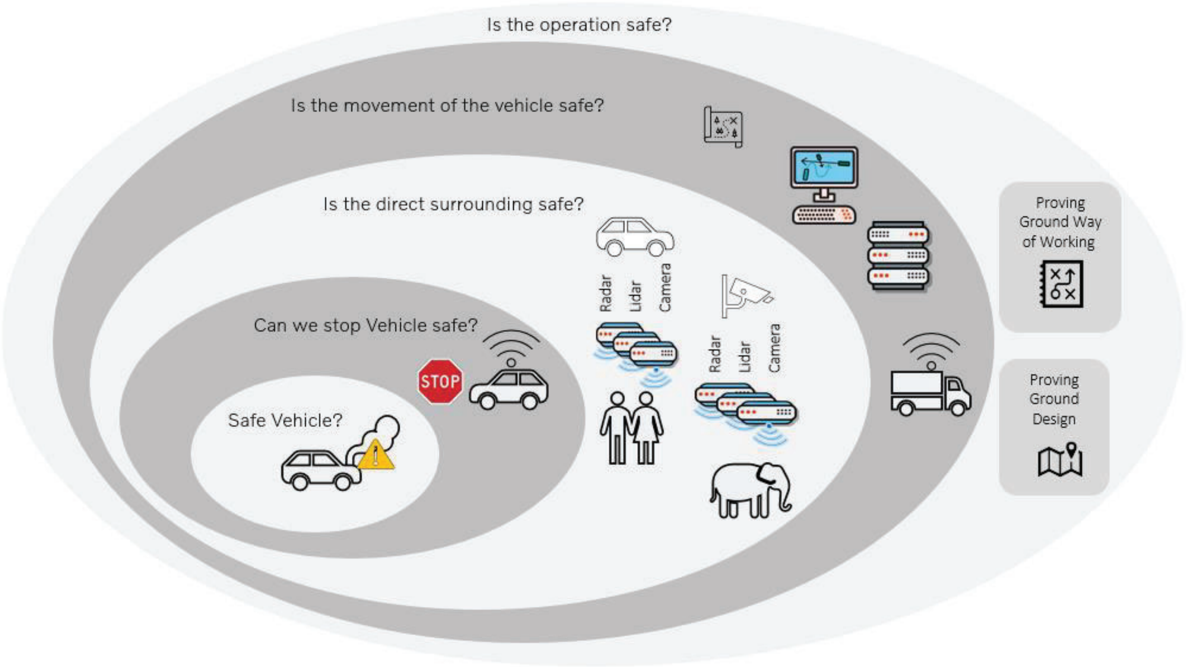


Figure 4 Layer-based framework approach model of how to enable safe operation

5 Objective

The main objective of the project was to develop a proof-of-concept which can enable self-driven vehicles to be integrated into existing proving ground environment. This is not only important for research within the area but also an essential key to launch self-driven vehicles without risking safety, a keystone to reach the "zero vision" target, no one should be killed in a traffic accident.

The project is contributing to *increase the Swedish capacity for research and innovation, thereby ensuring competitiveness and jobs in the field of vehicle industry* through development of existing proving ground to enable testing of self-driven vehicles which is essential for future Swedish automotive industry.
The project has produced international scientific publications and invited international bodies to demonstrations and presentations. Thereby contributing to *developing internationally interconnected and competitive research and innovation environments in Sweden*

The project has been relevant for the program areas of *Traffic safety and automated vehicle*; *A – analysis, knowledge and enabling technology* as the project has increased the competence level of how to test self-driven vehicles in proving ground environments. ETAVEP has with its proof-of-concept found an enabling technology. As a keystone to enable possibility to release safe self-driven vehicle to the market it is contributing to the area *E – Intelligent and crash avoidance systems and vehicle.* To enable safe self-driven vehicles in the transport system, safe and efficient testing need to be done in a confined area, hence ETAVEP is an enabler and contributor to area F – *Automated vehicle in the transport system.*

The objectives were not changed during the project, but the addition of a work task was necessary in addition to the original content, proving ground design and way of working. As the execution continued efficient, the project managed to rearrange resources to realize this.

6 Results and Achievements

ETAVEP has developed a proof-of-concept according to the system view in Figure 5. The proof-of-concept has shown that it is possible to substitute the safety driver, which ultimately shows it is possible to integrate self-driven vehicles into the existing proving ground, an essential keystone to maintain Swedish industry competitive. ETAVEP has shown it has to be done in a systematic and iterative approach. During the project two publications have been published, one conference workshop executed, two live (online) demonstrations conducted, three guidelines, three frameworks and four methods and two checklists have been created and shared in between the project partners.

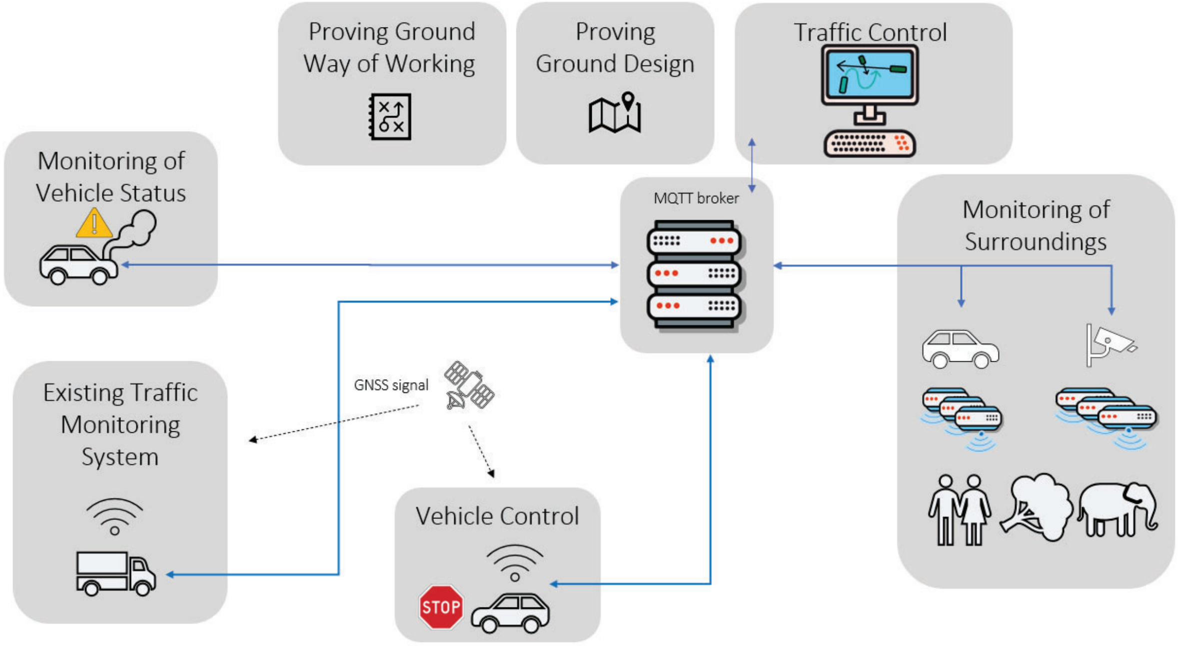


Figure 5 System view of proof-of-concept

6.1 Project Management & Demo

The coordination of the project was done by project management responsible for the project progression, organized dissemination activities, and facilitated meetings with international bodies, among others SAE. The project has organized and conducted two demonstrations, both online due to the COVID situation which has been affecting the project during its complete duration.

Project management was split in two teams:

- Management team; including all work package leaders who have met on a monthly basis to coordinate goals, tasks, deliverables and synchronization.
- Steering group; including project coordinator and industrial representatives (one from each partner), who have met every quarter (and when needed) to oversee the overall project progress.

Beside the monthly management team synchronization meetings, each work package has been working autonomously, having their own regular meetings to coordinate their work to reach the targets. When collaboration in-between work packages were needed it was solved by having jointly meetings and activities such as integration and verification on the test track. This enhanced the project speed of execution while still optimizing the resource utilization.
The COVID situation has interfered with the progression of the project which has resulted in a need to prioritize resources. The prioritization has been to finalize the committed deliveries resulting in a reduced number of scientific publications than intended, reducing from five to two publications and one conference workshop. During the project three student thesis projects have been published.

6.2 Understand your System - Use Cases & Risk Assessment

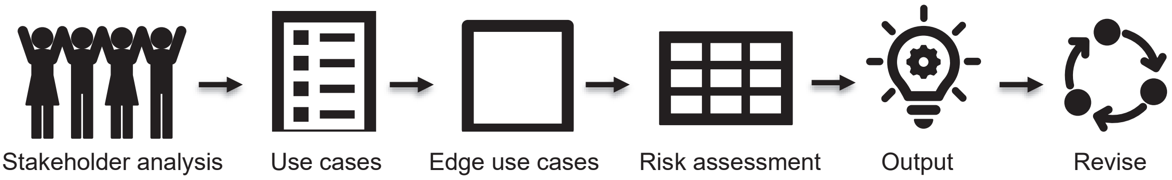
To be able to define and evaluate technical solutions that can replace a skilled and trained test driver, it is necessary to first define the Operational Design Domain (ODD) that needs to be covered during testing. In other testing of autonomous vehicles, an ODD usually describes a set of conditional limitations such as road type, weather, system status, etc., which need to be met for the autonomous vehicle to be allowed to operate.

Within a proving ground, an ODD description will be similar (with road type translated to the test tracks' geographical layouts and types) but there is one key addition, and that is the set of test protocols that are necessary to run during development. Since a key purpose of proving ground testing is to make sure that vehicles perform according to specifications before being allowed on public roads, several protocols are designed to assess vehicle performance at one or more limits, to guarantee future road worthiness.

The number of test protocols run at AstaZero and Hällered Proving Ground (or any proving ground) are too numerous to be effectively covered one by one during this project. However, it stands to reason that a number of safety edge cases, i.e., a compiled set of situations which provide the greatest challenge to a suit of systems replacing the test driver, will be sufficient to adequately dimension the system's capabilities.

Initially it was important for the project to understand the ODD and the reality the project needed to face. A proving ground is normally a very regulated and strict area, and the test protocols are also very well defined. At the same time there must be capacity and suitable structure for experimental testing as the development of vehicles and transportation systems demands it. The project needed to understand both the strict structure but also the need of adaptation.

The initial work done was aimed to support the project to understand the basic conditions of the system by providing the other work packages with information and functional requirements.



Stakeholder analysis – Needs and implications

The initial task for the project was to conduct a stakeholder analysis. The purpose of this analysis was to identify the stakeholders of the project: Who has an interest, influence of the project or who can be affected by the project and its result? Based on interviews with the stakeholders a list of requirements and wishes was compiled.

Identified stakeholders were among others Swedish industry, project partners, test clients, proving ground management and staff. The main requirements and wishes can be summarized with

- Strengthen the competitiveness of Swedish industry
- Build competence and strengthen cooperation within the field of autonomous testing
- Safe work at the test tracks for all kind of staff
- A proof-of-concept traffic management system ready to be put in production at the test tracks together with applicable procedures and regulations
- Build an effective fault reconnaissance system that has the ability to determine the mechanical status of the test object
- Improve the effectiveness of the testing

Identification and selection of use cases

The identification of use cases was based on studies of test protocols which cover a diversity of events, environments, shared test area and rough pavements. Another method to identify use cases was to analyze test tracks or road sections and based on experience produce scenarios originated from existing proving grounds. Collected parameters from the studies were maneuvers, road type, surroundings, interaction between vehicles etcetera.

When all use cases were compiled, the edge use cases like minimum/maximum speed or minimum/maximum acceleration were identified. The use cases were also briefly analyzed due to dependency. From the list of use cases a representative selection was made for further processing:

- Regulated intersection (gates, give way, stop, traffic light)
- Non-regulated intersection (any angle)
- Elevated roads
- Following lane including curves and slopes
- Lane change/merge (up to 4 lanes)
- Overtaking (up to 4 lanes)
- Oncoming
- Change of regulated driving direction (from one way to two way)
- Change of driving direction (from forward to reverse)
- Test area collaboration
- Special events

Next step was to make risk assessments of the use cases. To reach a feasible level of the use cases, each one of them had to be broken down into scenarios. For example, the Regulated intersection was broken down to T-intersection, four-way intersection, roundabout and pedestrian crossing with given properties. At this level the use cases were ready for the risk assessment. Scenarios are presented in Appendix 11.1.

Risk assessment of use cases

The risk assessment model used in low-fi prototyping based workshops is a well proven and efficient risk assessment model. The project has evaluated risks from two perspectives: health and safety, and economic risk. Each risk from the scenarios was assessed based on probability (P) 1-5 and severity (S) 1-5 which gives a risk index. The risks were hereby addressed to the work packages within the project, see Table 1.

Table 1 The Headings in the risk assessment model

Scenario	Possible risk situation – what could fail?	Health and safety risk			Economic risk			Comment	Address to: (Mark with x)				
		P 1-5	S 1-5	Index	P 1-5	S 1-5	Index		WP2	WP3	WP4	WP5	WP6

As an extra safety layer, a number of What-if-questions were added to each scenario. Examples of these questions:
What if…
… something in the vehicle or system would break or stop working?
… someone misunderstood or had false information about something (people in the surroundings, participants, leaders)?
... a person unexpectedly walks, stands, sits or lies on the test track?
... the sight is covered due to dust, fog, glare or spray?
... an on-road obstacle unexpectedly appears?

The project has produced a risk assessment for each scenario. The outcome of the risk assessments has been compiled and presented as requirements to each work package within the project. Since many of the risks occur in many different risk assessments the result has been summarized and prioritized in delivery documents.

The requirements have been categorized in four priorities, presented with examples:

Priority 1: Critical for the project to prove it possible to mix self-driven and manual driven tests but with reduced capacity due to safety or efficiency

- *Detect people on the test track or near the test track.*
- *Fault detection related equipment installed in vehicle must not affect the test results*

Priority 2: Important and necessary to ensure safety and efficiency

- *Handle different regulations for different types of vehicles.*
- *Sensors must communicate status and detections to traffic control with a robust communication*

Priority 3: Nice to have but not critical to the project

- *Based on signal, be able to remotely shift gear from forward to reverse, to be able to reverse a driverless vehicle from tricky or narrow scenarios.*

Priority 4: Impossible or hard to realize

- *Ensure that all vehicles use direction indicators (indicator lamps or other solution) when perform a lane change.*

Sometimes the requirements from the risk assessments have been irrelevant to the project or too demanding to meet. E.g., detection of thermal event in a vehicle. It is of great importance that this feature is working but it is not in the scope of the project. Therefore, some of the requirements were rejected. The delivery documents have been followed up and revised during the project, due to status and relevance.

Conclusions

Outcomes from the project shows how important it is to understand the environment, the vehicles and the tests that will be put together as a system. The project also visualizes the must of being specific enough when you evaluate the conditions, to reach a feasible foundation as reference for further development or needed adjustments. The slightest change can have a decisive impact on the safe operation.

No matter how competent technique one develops, it is still the interface between (wo)man and machine that is the crucial safety aspect. Systems will always need to be complemented by information, training and procedures. The project was complemented by Proving Ground Design and Way of Working to also cover these aspects.

6.3 Monitoring the Vehicle Status

A key role for test drivers during test driving is to monitor the vehicle for faults that may occur while a vehicle platform is under development and which may lead to loss of vehicle control (e.g., thermal events, mechanical ruptures in key locations, severe software bugs, etc.). To be able to replace the test driver, other means to maintain this fault detection capability need to be developed.

Fault detection is currently a vast and rapidly expanding area used throughout different industries and approaches range from simplistic univariate tracking to complex multivariate machine learning methods. However, to fully mimic the senses of a professional test driver is way beyond scope of the ETAVEP-project. The project focuses on a limited list of primarily safety relevant mechanical faults and wear which influence the dynamic behaviour of the vehicle frame/body, i.e., how dynamical mechanical forces from the road surface propagate through the suspension/chassis and into the frame/body of the vehicle. In a conventional test setting, the test driver will monitor both these vibrations and structure borne noise through her sensory system. With this background the ambition was to develop an *on-board monitoring system for vehicle faults focusing mechanical faults and wear that may detect faults as well as (or better than) an experienced test driver***.** In particular, investigate if statistical models of expanded non-parametric transmissibility estimates (Johnson & Adams, 2002) using Local Rational Models (LRM) (McKelvey & Guérin, Non-parametric frequency response estimation using a local rational model. IFAC Proceedings Volumes, 45(16), 49-54., 2012) with a general sensor setup could provide a sufficiently robust and accurate performance in this capacity.

General approach

In order to gradually build up knowledge a logical plan with increasing complexity was established, see Figure 6 The workflow is divided into two subsequent phases; first the offline phase and followed by the online phase. The offline phase is defined as the case when data creation, storage, analyses and vehicle status judgment can be performed separately and with no in-vehicle near real time requirements. The online phase is the scenario when near real time status monitoring is performed in-vehicle and is in full communication with a traffic control system or unit.

For the offline phase the initial analysis included the case of virtually generated road load data using state-of-the-art Computer Aided Engineering (CAE) models, tools and digitally scanned road profiles. Training data is established from a fault free virtual vehicle model aka baseline configuration after which different faults are introduced and the performance of the algorithm is assessed. The unique feature of testing and adjusting the algorithm in this environment is that it is deterministic. This is assumed to be the simplest case to study on a complete vehicle level as influence of noise and scatter in the data are not present. The second part of the offline phase is to introduce actual measured data on a physical full vehicle. Again, the setup is offline in the sense that the data (both baseline configuration and with injected faults) is acquired and stored first and later the data is used to analyze the performance of the algorithm and sensors sets and positions. Naturally, it is worthwhile to mimic an online scenario in the offline case by splitting the measured time data series into small consecutive portions/time windows and streaming those to the algorithm. This is done to assure that the entire process is likely to work in the online phase. The second part of the offline phase, a physical vehicle with and without faults, was divided into two cases; the slightly more controlled case with a vehicle excited by a hydraulic shake rig and the more demanding and sought case of a vehicle driving on events at a proving ground. A principal difference to the CAE case is that noise and scatter in the measured data will influence the performance of the algorithm. The offline phase is completed when types, placement and number of sensors have been assessed, the code containing the algorithm is optimized and the status monitoring results are sufficiently robust. In the online phase, measurements are performed in real time in a physical vehicle at the proving ground and an in-vehicle measurement system streams data to the algorithm which performs real time assessment (typical once every one second) of the vehicle status. This status is communicated over-the-air to the traffic control as described in Figure 20.

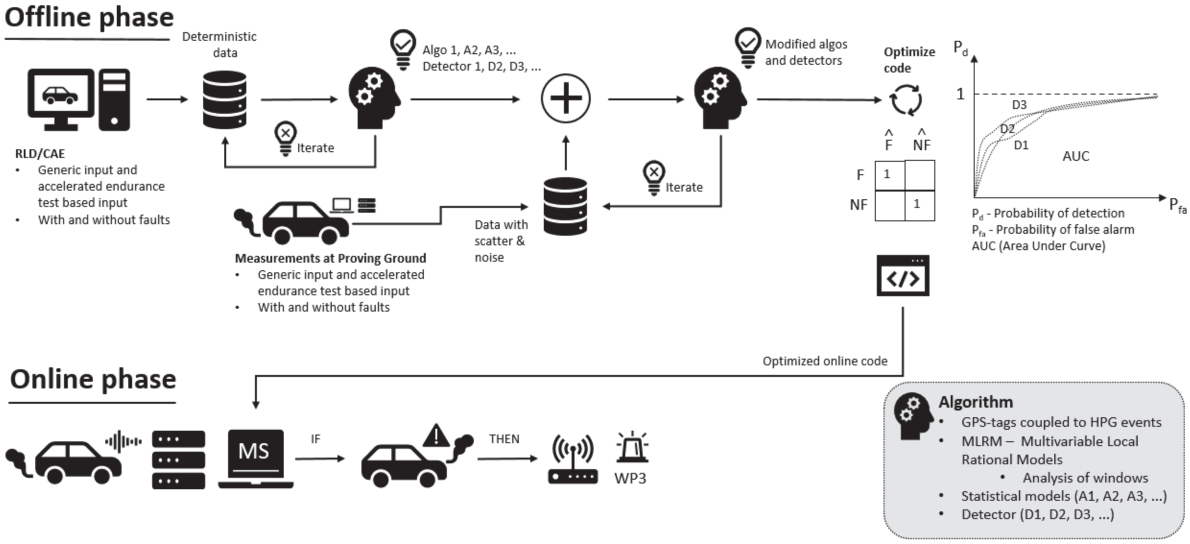


Figure 6 Overview of logical plan with increasing complexity

Overview of the algorithm

The theoretical details of algorithm that was developed within the ETAVEP-project has been published as an academic paper by (McKelvey, McKelvey & Nordberg, 2021). In addition, a thesis on Master level covering the development and evaluation of the algorithm is also a result of the project (McKelvey, 2022).

To perform early detections before a full fault, the vehicle needs to be instrumented with sensors at strategic locations in order to capture and track the overall dynamic behavior of the vehicle. A method was developed following (Johnson & Adams, 2002) which incorporates transfer path analysis through a non-parametric approach to transmissibility estimation. For ETAVEP the recent LRM (McKelvey & Guérin, 2012) which in an efficient manner circumvents the spectral leakage that normally degrades classical non-parametric empirical transfer function estimates was used. Since the problem at hand is multivariate, the LRM method was extended to the multivariate case along the lines of (Voorhoeve, et al., 2018).

An overview of the algorithm is presented in Figure 7, Figure 8 and Figure 9. The sensor data (simulated or measured) is grouped as inputs and outputs. For a certain window size, the data is transformed into the frequency domain using the Fourier transform under the assumption that the dynamic system (complete vehicle) is a linear quasi-stationary dynamic system. A non-parametric estimation of the MIMO (Multi-Input Multi-Output) frequency response function estimate matrix is established via an LRM based divisor product. These multidimensional data points, the Frequency Response Matrix (FRM), form a base constituent in the algorithm, see Figure 7. The LRM based divisor product can be replaced by any other suitable approach such as ARX (Auto-Regressive eXogenous input) or EFTFE (Empirical Transfer Function Estimate). These two other methods to establish the frequency response function matrix data points were also included in this study as comparison. Due to non-evitable mismatch between the measured signals and the modelling assumptions, the estimated FRM from each window of data will vary slightly over time even if the mechanical structure is unchanged. This variation is due to non-linear effects and that the sensors used only partially capture all excitations acting on the vehicle. To take this variation into account when designing the detector, we build a statistical model which describes the FRM data and estimate the parameters of it using training data from a fault free vehicle, see Figure 8. After this baseline model is established, the system can be switched to the monitoring or detection mode as illustrated in see Figure 9. In the monitoring mode each new window of sensor data generates new FRM data which is then contrasted against the baseline model. The statistical distance between the model and the FRM data, called a T-statistic, indicates how far away the present FRM data is to the baseline model. A mechanical fault which changes the transfer path dynamics captured by the sensor setup will make this distance increase and a fault situation can be called if the value is above some threshold.

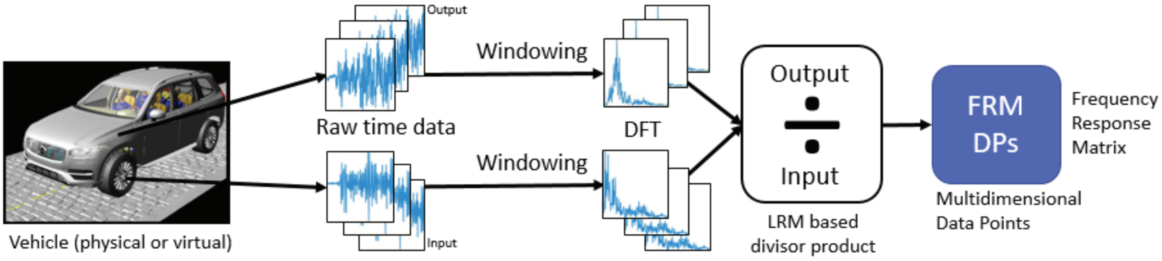


Figure 7 Creation of multidimensional frequency response matrix data points

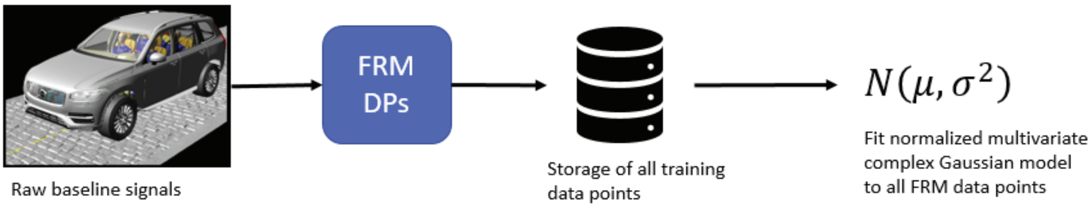


Figure 8 Training on baseline vehicle configuration (no fault) to create a statistical model

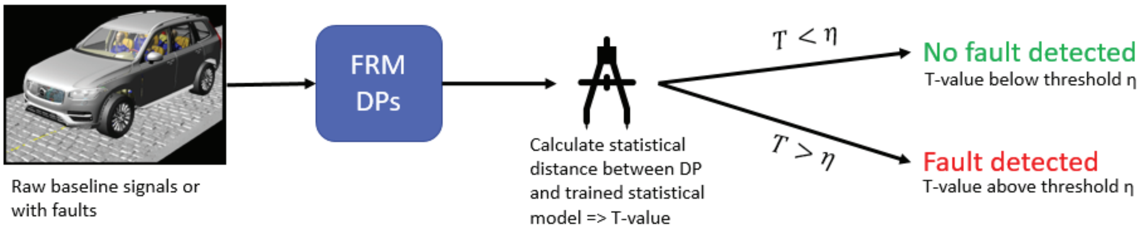


Figure 9 In monitoring mode a detector measures the statistical distance to the statistical model via a T statistic and determines if a fault is present or not depending on the T-value versus a predetermined threshold

.

The actual vehicle dynamic behavior from significant road excitation is typical non-linear but here assumed to be suitably well approximated by a linear quasi-stationary dynamic system. This implies that a trained model as in Figure 8 is dependent on the road excitation. Hence each principally different road excitation situation will need to be modelled and trained separately. This is considered a minor issue in a proving ground scenario as there are multiple methods to accurately keep track of the position of the vehicle and associated proving ground road situations e.g; Belgian pavé, washboard, etc.
From the estimated FRM data it is during the monitoring phase possible to generate several test-statistics. Each test-statistic is generated by calculating it from a subset of the output sensors. This gives the possibility to understand which sensor subset sets deviate most from the baseline and can be used for fault localization.

Selection of hyper parameters

To successfully use the monitoring algorithm presented above some hyper parameters need to be selected to suit the application at hand. Firstly, the sensor setup needs to be decided in terms of number of sensor locations and grouping of the signals into inputs and outputs to support the overall idea of tracking the transfer path properties. The sampling frequency of the sensor signals need to be large enough to cover the range of dynamic responses which are expected to be important. Based on the vehicle properties, we have used the frequency range between 4 and 100 Hz for analysis. This imply that a sampling frequency of at least 200 Hz would be needed. In the tests conducted we have used 500 Hz (heavy vehicle) and 1 kHz (light vehicle) as sampling frequencies. The method uses block-based processing and hence is based on analysing a window of sensor samples. The selection of the window size is fundamental trade-off between the delay to a fault detection and sensitivity to disturbances and measurement noise. A large window will give a longer detection delay but lower sensitivity to the disturbances. The LRM method has the possibility provide non-parametric estimate of the FRM at any frequency (lower than half the sampling frequency). In this work we have used 20 frequencies equidistantly placed between 4 and 100 Hz. Computational complexity increases (linearly) with the number of frequency points. The number of points should be selected large enough to reasonably model the frequency response function in the selected frequency window. Finally, the LRM method has a local model order hyper parameter and a local window size parameter. The evaluation performed in this project has shown that the results is not very sensitive to the selection of these parameters (McKelvey et.al., 2021). For the LRM method we have used local model order 3 and local window size 30.

Sensor setup strategy

It is neither practical nor economically viable to have a dedicated sensor for each potential mechanical failure mode that a test vehicle may experience. Therefore, a general sensor setup that is easily mounted and that can capture important failure modes is desired. It is important that input sensors are placed where the externally exciting forces enter the vehicle. The output sensors should be placed such that the force path from the input to the output covers the mechanical structures which are aimed to be monitored. To be able to detect a fault it must be observable in the sensor signals.

Experimental evaluation

The method presented above was evaluated on data from several experimental campaigns ranging from multibody simulations, shake rig tests to data collected from vehicles at Hällered Proving Ground.

Multibody simulation

The vehicle simulation model used in the experiments was developed by Volvo Cars and is a state-of-the-art multi-body system, with 2000 degrees of freedom and generates signals with a sampling rate of 1kHz. The simulation used a model of the Volvo XC90, complete with bushings, springs, dampers, etc. The road surface used in the simulations is a 3D-scan of a section of Belgian pavé at the Hällered Proving Ground in Sweden.

Six symmetrically placed points are chosen in the front of the vehicle. For each point, accelerations in the vehicle's longitudinal and lateral direction are extracted from the model. The two front wheel centers are taken as input points since the road surface conditions are impractical to measure and use. Hence, there are four input signals and eight output signals that represent a possible instrumentation of a real test vehicle. The sensor setup results in a FRM of size eight by four that is evaluated at 26 frequency points between four and 100 Hz. The analysis window size is selected to 8192 which corresponds to eight seconds measurement time (McKelvey et.al., 2021).

In the simulations the following faults have been generated:

- Loose ball-joint on the front- left suspension knuckle
- 25%, 50% and 75% degradation of the front lower control arm rear bushing.

A baseline model was established from a simulation with the unchanged model. The graph in Figure 10 illustrates the monitoring results for loose ball case. The results clearly illustrate that the sensor setup easily catch the loose ball joint fault. Similarly, the fault due to degradation of the control arm bushing was identified with expected correlation.

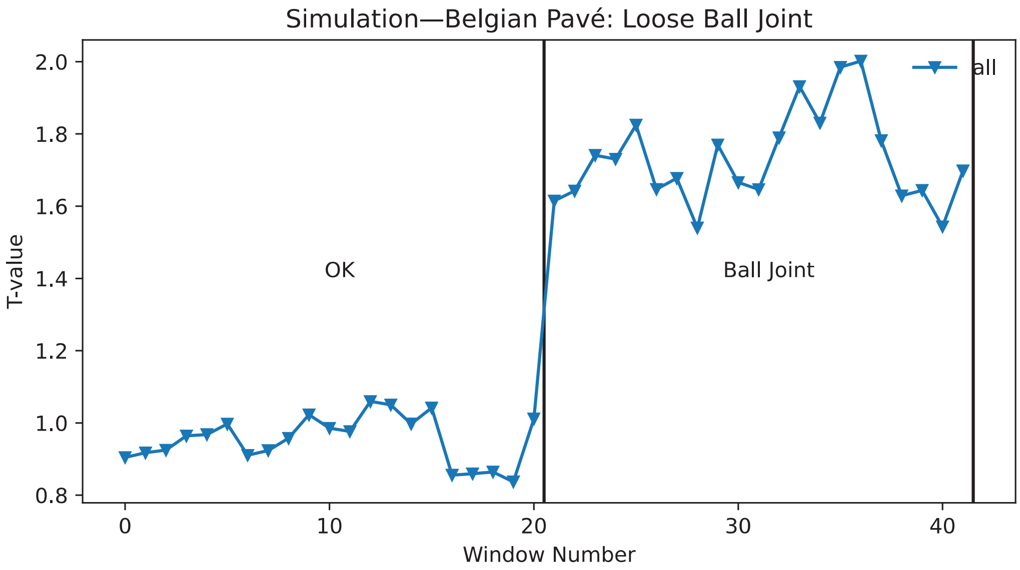


Figure 10 T-value plot for two test segments placed back-to-back. Left section (OK.1): fault free case. Right section (F.1): Loose ball-joint fault. Analysis window size 8192 samples (~8 seconds)

Shake rig test case

For this test set up Volvo Cars life cycle test lab was used with a Volvo XC90 test car exited driven by a 3D-Belgian Pavé road load surface. Six measurement segments were extracted from the complete test cycle, each segment around 23 seconds long. Three measurements were taken early in the longevity test, and three were taken after one of the front suspension towers failed. There were four accelerometers, measuring acceleration in the horizontal direction, mounted in the four corners of the vehicle frame. These four signals were used as output signals in the model. The acceleration, in the horizontal direction, at the center of the four wheels were used as the input signals. Two of the early measurements extracted with the front suspension intact were used as training data. The third segment with the front suspension intact became the fault-free validation data set. The three measurements with the failure of the front suspension were all used as validation data. The sample rate is 512 Hz, and the analysis window size is 4096 which corresponds to 8 seconds. As in the Multibody simulation test with this test case the algorithm was also able to successfully identify the fault.

Heavy vehicle at Hällered Proving Ground

A Volvo FH heavy vehicle was instrumented with triaxial accelerometers with two sensors on the back of the cabin, two sensors on the frame just in front of the rear cabin mounts, two sensors on the frame over the front axle and two sensors on the front axle as shown by the green arrows in Figure 11.

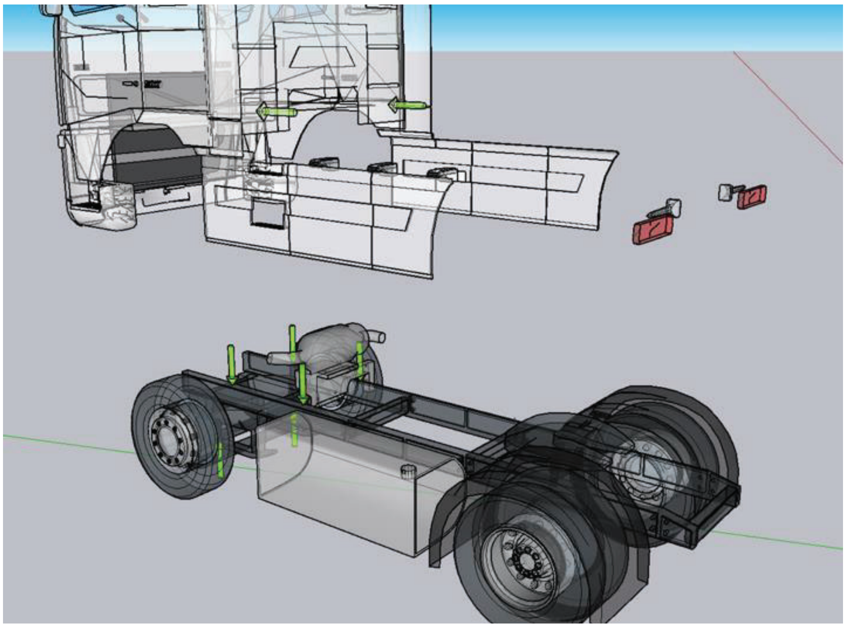


Figure 11 Sensor position according to green arrows

Two separate induced faults were evaluated. The first generated by loosening the right lateral shock absorber for the cabin and the second induced fault was generated by loosening the top mount of the left shock absorber. None of the faults where possible for the driver to feel or notice.

Tests and results

The tests were carried out at Hällered Proving Ground on different road surfaces (e.g., Belgian pavé, patched asphalt and washboard). Accelerometer data was collected from test drives without the induced faults and with the induced faults. For each road surface an initial test drive was conducted to collect training data to establish the statistical baseline model.

Figure 12, illustrates the monitoring results from three test drives on the Belgian pavé road surface. The left part in the graph corresponds to the initial fault free test drive. The middle section is a test drive with fault one (loose right lateral shock absorber for cabin) is induced and the righthand side is a test drive when the vehicle has been restored to a fault free condition. Four different T-statistics corresponding to different sensor sets are shown. The sensor sets used for the different T-statistics are:

- all – All sensors
- left – Sensors located at the left in the vehicle
- right- Sensors located at the right in the vehicle
- cab – Sensors located at the cab

The fault is not visible in the T-statistics, and we can conclude that the sensor setup and the analysis methodology is not sensitive to this fault. The test driver could not notice this fault either when driving.

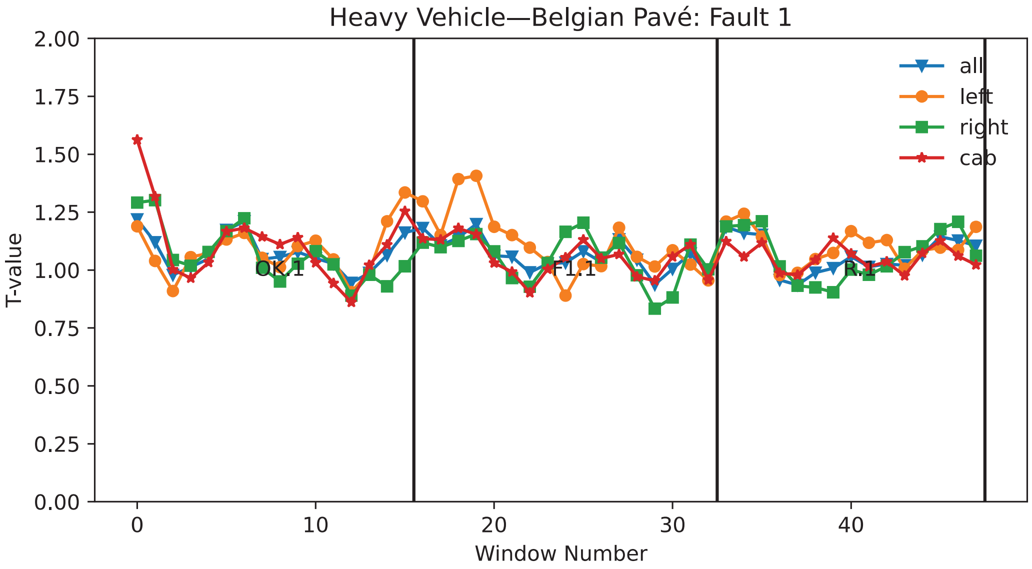


Figure 12 T-value plot for three test drives placed back-to-back. Left section (OK.1): fault free case. Middle section (F.1): Fault 1. Right section (R.1): Vehicle restored to fault free state. Analysis window size 4096 samples (~8 seconds).

Figure 13 illustrates the monitoring results from four test drives on the Belgian pavé road surface for induced fault 2. The left part in the graph corresponds to the initial fault free test drive. The two middle sections are two test drives with fault 2 (loose top mount of the left shock absorber) induced and the righthand side is a test drive when the vehicle has been restored to a fault free condition. The fault is clearly in the T-statistics except for the Left subset of sensors. The test driver could not notice fault 2 when driving the vehicle. The analysis window size was here 4096 samples corresponding to approximately 8 seconds. To illustrate the influence of the window size Figure 14Figure 13 show the results when the window size is 1024, i.e., approximately 2 seconds. A shorter window will reduce the detection delay but leads to a higher variance in the T-statistic as expected.

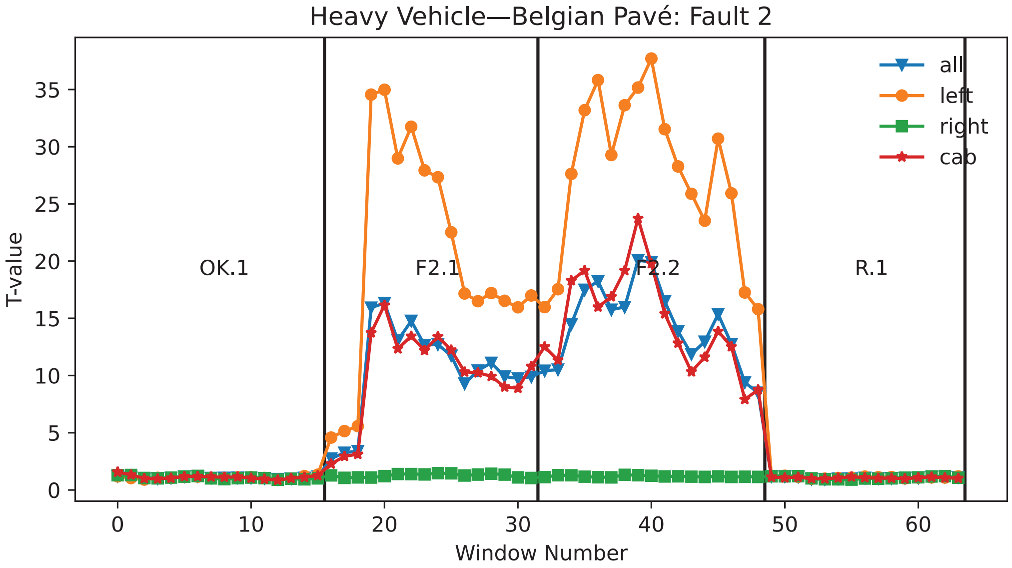


Figure 13 T-value plot for three test drives placed back-to-back. Left section: fault free case. Middle section (F.2.1 and F:2.2): Fault 2. Right section: Vehicle restored to fault free state. Analysis window size 4096 samples (~8 seconds)

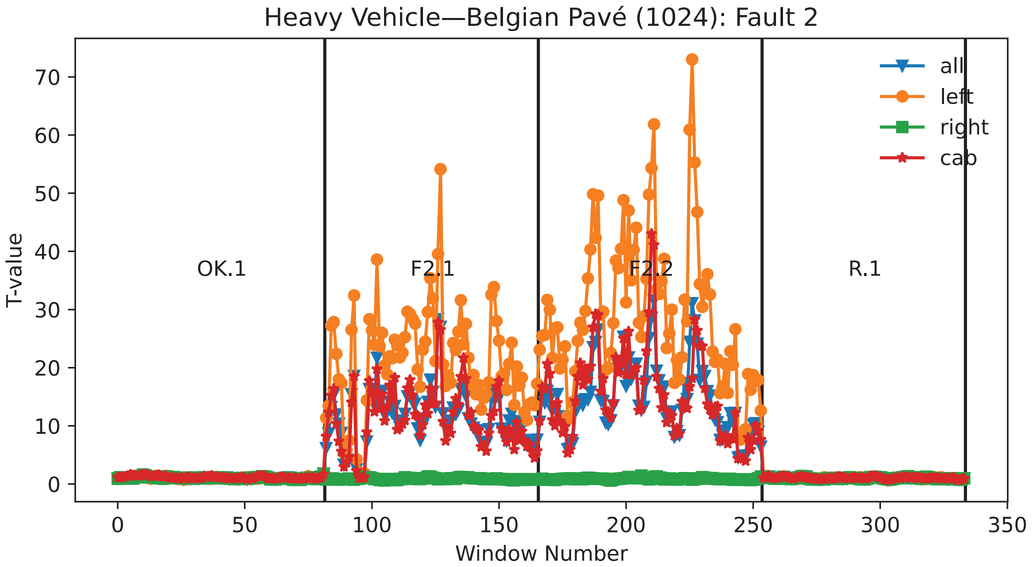


Figure 14 T-value plot for three test drives placed back-to-back. Left section: fault free case. Middle section (F.2.1 and F:2.2): Fault 2. Right section: Vehicle restored to fault free state. Analysis window size 1024 samples (~2 seconds)

Light vehicle tests at Hällered Proving Ground

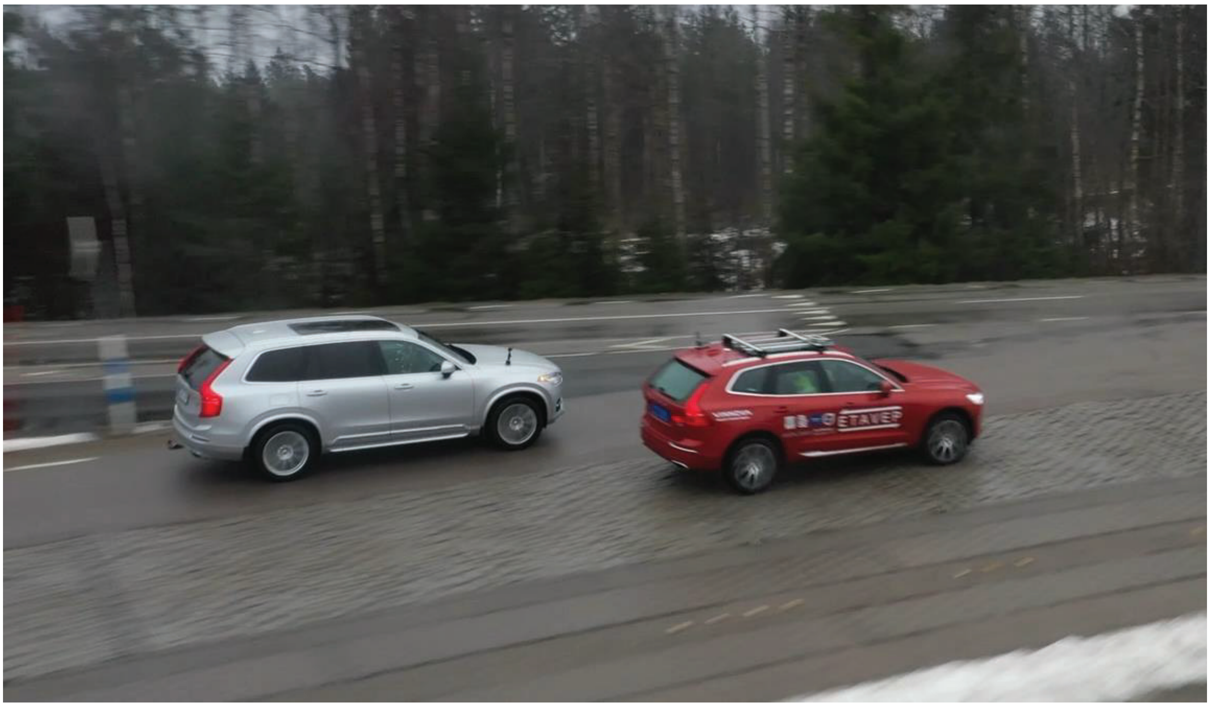


Figure 15 ETAVEP Volvo XC60 driving on the Belgian Pavé track at Volvo Cars Hällered Proving Ground.

Two tests were carried out at Volvo Cars Hällered Proving Ground. In the first test measurements were collected with and without faults injected on different road surfaces. In the second test the online monitoring implementation was validated by injecting a fault during driving. The car used at the proving ground was the ETAVEP Volvo XC60 test car which has air suspension, see Figure 15.

Sensor setup - light vehicle

Triaxial accelerometers at the following places on the instrumented test car were used for the evaluation:

- Left and right top mount (2)
- Driver seat rail (1)
- Global body accelerations measured inside arm rest area (1)
- Front left and right damper fork (only z-axis) (2)
- Right front side of subframe, middle rear part of subframe, left front side of subframe (3)

The following faults are generated during first vehicle test:

- (Top Mount) Top-Mount screws (both left and right side) loosened 180 degrees.
- (Torque Bar) Upper engine torque rod screw loosened 180 degrees, to simulate deviation on the engine movement
- (pt3) - Drilled holes on the lower control arm bushing (Pt.3) to simulate wear on the bushing
- (pt4) Drilled holes on the lower control arm bushing (Pt.4) to simulate wear on the bushing.

The injected faults were judged by the test drivers to be barely noticeable during driving.

During the second vehicle test the aim was to evaluate the online implementation and detect an oncoming failure during driving. Modification have been made to the car to be able to inject a fault that could occur during testing. The front left air suspension was modified so the air could be emptied with the wanted characterization to inject both a gradually rising fault and abruptly arisen fault. The air in the suspension can be easily reestablished by closing a valve to reconnect the compressor air flow to the suspension. The failure was hard to detect for an experienced test driver even if the driver was the one to inject the failure. Hardest to detect was when a gradient fault was injected.

Tests and results

The tests were carried out at Hällered Proving Ground on different road surfaces (e.g., Belgian pavé, patched asphalt and washboard). Accelerometer data was collected from test drives without the induced faults and with the induced faults. For each road surface an initial test drive was conducted to collect training data to establish the statistical baseline model.

Figure 16 illustrates the monitoring results from the test drive on the Belgian pavé road surface for the first injected fault (Top Mount). Three different T-statistics corresponding to different sensor sets are shown. The sensor sets used for the different T-statistics are:

- all – All sensors
- subframe – Sensors located at the subframe
- lhs- Sensors located at the left side of the vehicle

All four faults injected were visible in the T-statistics where the weakest signature was obtained for fault pt4.

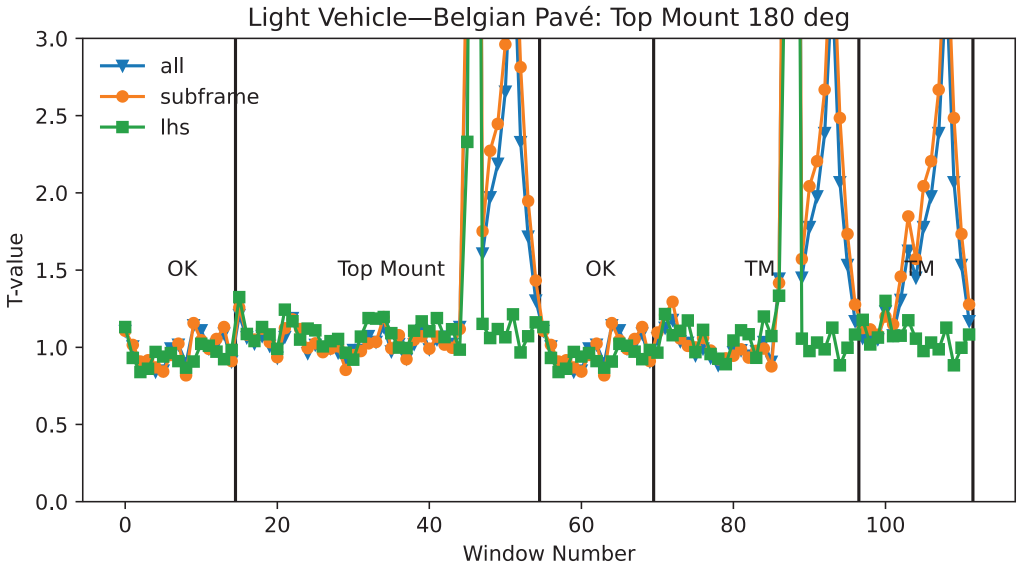


Figure 16 T-value plot for five test drives placed back-to-back. OK: fault free case. Top Mount and TM: Top Mount Fault. Analysis window size 4096 samples (~4 seconds).

The second test was conducted with the aim to validate the online capability of the monitoring/analysis system. Here the air suspension fault was introduced and removed during driving. Either the fault was introduced gradually or abruptly. The test drives were conducted both on the Belgian pave road surface and on regular asphalt. Three different T-statistics corresponding to different sensor sets are shown. The sensor sets used for the different T-statistics are:

- all – All sensors
- lhs – Sensors located at the left side of the vehicle
- damper-fork – front left and right damper fork (z-axis)

The result for Belgian pave with both gradual and abrupt injection of the fault is shown in Figure 17 and the result for regular asphalt with a gradual fault injection is shown in Figure 18 The faults are clearly seen in the T-statistics where the damper-fork sensor selection seems to have the highest sensitivity.

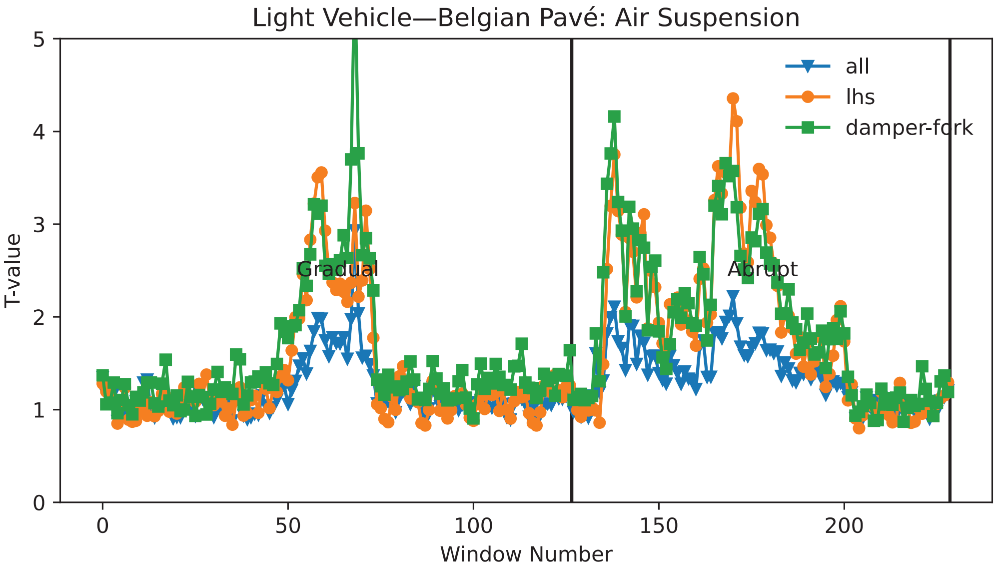


Figure 17 T-value plot for test drive on Belgian Pavé. Gradual: Air suspension fault gradually introduced. Abrupt: Air suspension fault abruptly introduced. Analysis window size 4096 samples (~4 seconds).

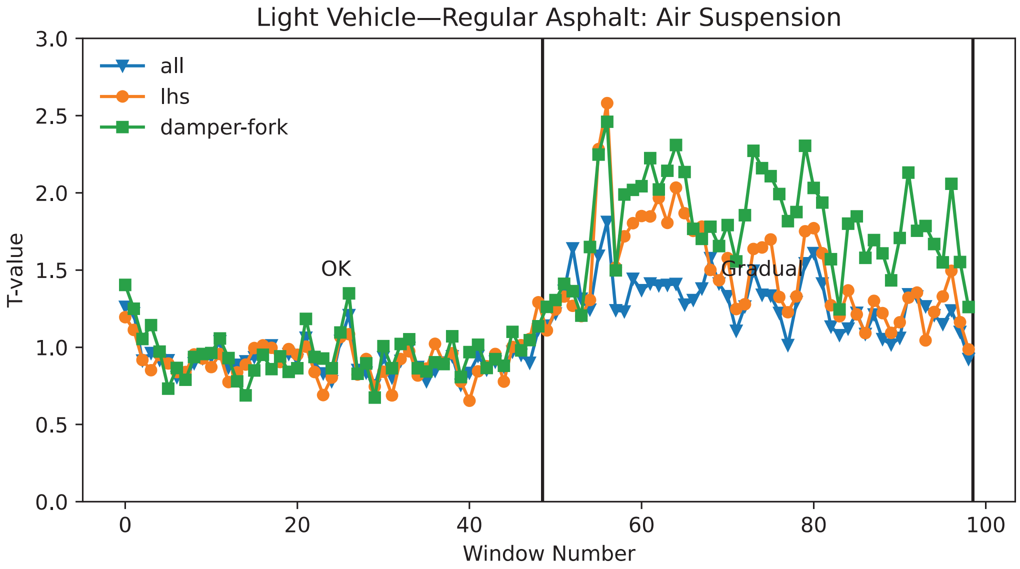


Figure 18 T-value plot for test drive on regular asphalt. Gradual: Air suspension fault gradually introduced. Abrupt: Air suspension fault abruptly introduced. Analysis window size 4096 samples (~4 seconds).

Data streaming solution in-vehicle

The online monitoring functionality was realized with an analysis computer connected to DeweSoft measurement system with shared disk connected via onboard ethernet network. The measurement system produces a measurement file every second and store it on disk. The analysis computer reads the files from the measurement computer disk via an ethernet connection and analyses each file as they appear and determines the current status, see Figure 19 below. The data processing is done in Python. In principle there is no need for two computers (measurement and analysis). The chosen setup was done for practical reasons. In a more production like implementation the data acquisition would directly be integrated in the analysis computer and thereby remove the need for disk-based file I/O.

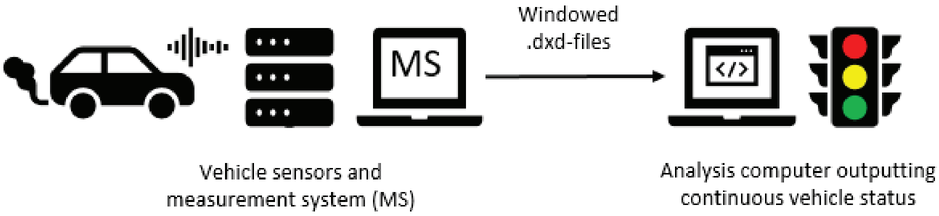


Figure 19 Principal setup of measurement system, measurement computer and analysis computer.

Communication interface and signalling specification between vehicle and traffic control

The vehicle monitor functionality connects and continuously transmits status signals via the vehicle network connected to traffic control, see Figure 20. The status message is a simple string containing a time stamp and a three-level status integer with the following interpretation: no fault, major fault – brake vehicle immediately, minor fault - check issue at next vehicle workshop inspection).

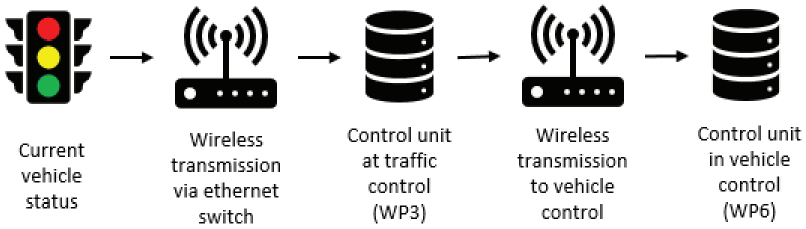


Figure 20 Principal overview of how e.g., a stop signal from the analysis computer is transmitted to Vehicle Control

Conclusions

The experimental tests have shown that the presented methodology is a viable alternative to monitor the structural integrity of a test vehicle. The method is based on analyzing the signals from accelerometers placed at strategic places on the vehicle. A multivariate transfer path analysis approach is employed which is based on dividing the signals into an input group and an output group. From these signals multi-input multi-output frequency response matrices are estimated at a set of frequencies. By comparing these matrices with a statistical model derived from training data from a baseline case structural changes can be detected. The method is data driven and make no model assumptions beyond the linear transfer path analysis and the estimation of the frequency response matrices use the non-parametric LRM technique. The method has very few hyper parameters that need to be selected and the result is rather robust against the specific choice. Almost all faults tested were detected by the algorithm. In the tested cases measurement windows in the range from 1 to 8 seconds is enough to clearly see the effect of the fault. The transfer path model is assumed linear which is not the case for any physical object. This implies that the nominal baseline models are dependent on the excitation. Hence, it is required to have road surface dependent baseline models. The required computations are modest and real-time processing was achieved with a low-cost laptop computer. The possibility to create sensor subgroups to generate several T-statistics open for the possibility use their behavior as fault-fingerprint and be able to not only detect the existence of a fault but also point to the location of it. The consensus from the test drivers was that all faults tested were very hard to detect for the test driver while driving. During the online test with gradually leaking air suspension, it was clear that the algorithm picked up the error before the driver and passenger in the car.

6.4 Vehicle Control

Today highly trained test drivers guarantee to stop the vehicle if the safety is compromised (e.g., faults in the vehicle, obstructions on the test track or given stop signal from the traffic controller). The vehicle is stopped as a safety precaution, while reducing the speed the severity of the potential accident is reduced. Therefore, it is essential for the test driver to be reactive to reduce the speed as fast as possible.

As self-driven vehicles might lack controls or space for test driver, there is a need to substitute the stop capability which test drivers provide. Ideally the substitution would be a robotic replica of the test driver. Creating a robotic replica of the test driver is a huge undertaking and extremely complex hence ETAVEP has focused on the stop capability. Giving, the research question *"How to take emergency control over an autonomous vehicle at risk?"*. If a risk materializes in any of the monitoring systems, how does one make sure that the autonomous vehicle can be brought to a safe stop?

General approach

To build a foundation several adjacent existing solutions (e.g., autonomous mining, aircraft and agriculture) were examined. None of the evaluated solutions were applicable for direct implementation in ETAVEP. To further strengthen the foundation to be able to answer the research questions automotive related safety standards and legal regulations were assessed. With the congregated knowledge concepts were drafted. Draft concepts were assessed and derived into a final concept with applicable standards, regulations and common practice applied.

The implementation of the final concept was divided into two parts, software/electronic and mechanical. The software and electronic includes brake-by-wire, logic, communication and power supply. The mechanical includes an external controlled mechanical brake system.

To ensure that the implementation can take emergency control over an autonomous vehicle at risk a comprehensive test suite was developed and executed to verify the function, to ultimately answer the research question.

How to take control over a self-driven vehicle at risk?

A vehicle under risk is defined in ETAVEP as when there is a possibility of collision (e.g., with a vehicle, pedestrian or infrastructure). An accident could result in severe consequences, both economical- and human harm. The preferred solution is a system to completely remove the possibility of an accident to occur, and in the unlikely event of an accident, reduce the speed as much as possible. This concludes that the system is a robust and provides low latency. To gain robustness two separate brake systems were used to ensure redundancy. One utilizes the vehicles brake-by-wire system, the other using a hardware external fallback brake. To maintain low latency, an internal network architecture with state-of-the-art equipment was used. The architecture was separated into a high priority and a low priority segment. The high priority segment was the essential components needed to bring the vehicle to a stop, such as brake functionality, power supply, communication, and computing logic. The low priority segment was non-necessary components for carrying out the stop, such as steering and throttle control, see Figure 21.

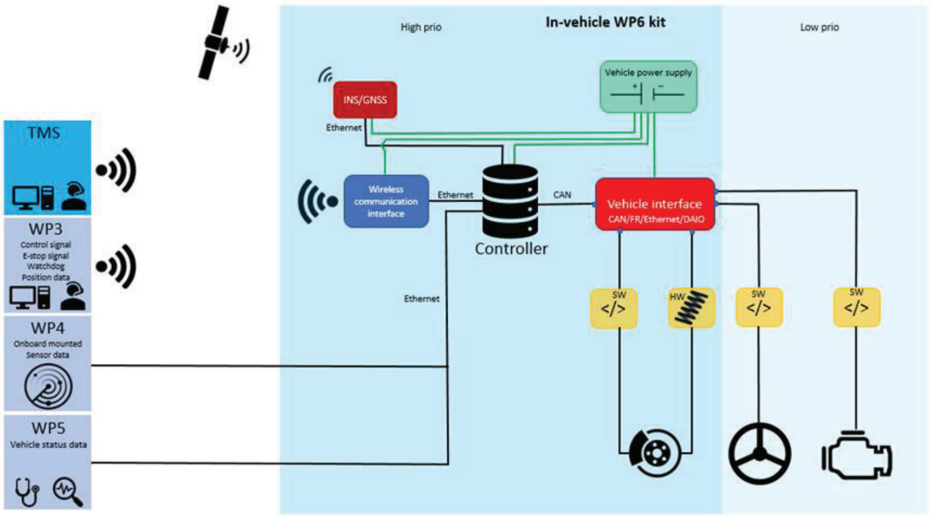


Figure 21 Architecture with high and low prioritized segments

The software emergency robot interface uses the internal brake-by-wire capabilities to command the vehicle to a stop. To achieve this, it requires connection to the vehicles internal buses to manipulate the signals transmitted in between nodes that controls the deceleration of the vehicle. It is mandatory to ensure exclusive rights to override any message from the vehicle to gain deceleration control. The solution acts as a bypass when there is no stop request, which allows the test to be conducted without interference from the system.

The hardware emergency robot utilizing external actuators is independent of the software emergency robot, this generates a redundant system, having two parallel systems. Since autonomous vehicles in the future most likely will not have any conventional brake pedals like most today's vehicles, there was a need to prove that an external fallback system could be working in future cars without conventional brake pedals. The design is using a spring-loaded lever that sets pressure on a hydraulic braking system if triggered by e.g., an emergency stop signal, loss of communication or power failure. It is made of a brake master cylinder and a brake-booster connected to the internal hydraulic valve stack block, see Figure 22 and Figure 23. This setup will not influence the vehicles internal brake system while not active.

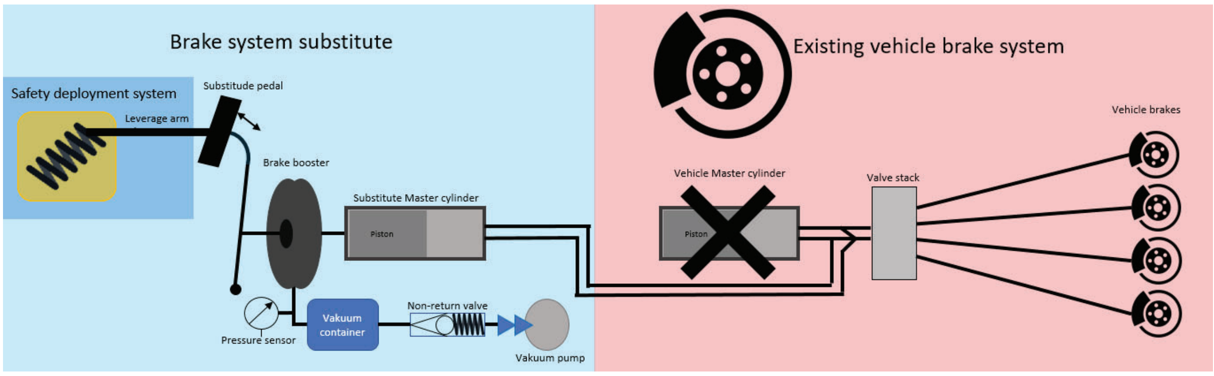


Figure 22 Drawing of the implementation of the hardware fallback interface.

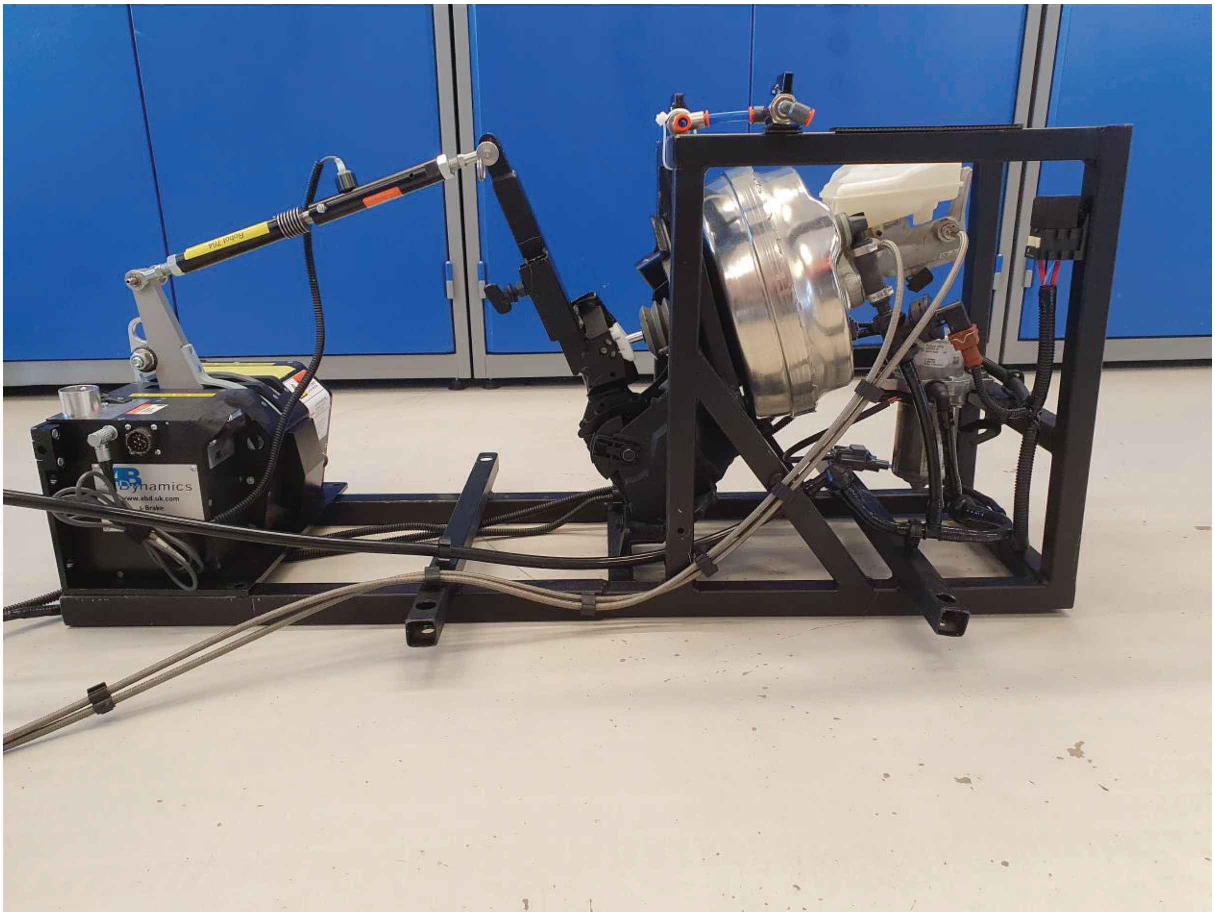


Figure 23 The hardware fall back interface

The normal state of the system is “always braked” which means that the vehicle is only allowed to move if the system is fully functional and not in emergency stop mode.

To mitigate consciences of power failure, the system was complemented with Uninterruptable Power Supply (UPS) enabling the system to remain operative while the vehicle systems fail. Although if the UPS would fail the Hardware emergency robot will brake.

Safety principles

Since safety on the test track is the corner stone in the operation of test tracks, well-established safety principles must be implemented to guarantee safety. As automotive have well founded safety principles (International Organization for Standardization, 2018), (International Organization for Standardization, 2013) that regulates and advises on system design, it is mandatory to follow these. Regulations regarding machinery obliges that an assembly with moving parts needs to obey directives (Arbetsmiljöverket, 2008) (International Organization for Standardization, 2015). Emergency stop functions principles are defined in (International Organization for Standardization, 2015), which implies certain conditions an emergency stop must fulfill. The system’ communication is based on recommendations reported in (International Electrotechnical Commission, 2016)Each standard and regulation applied to the system can be studied further in Figure 24.

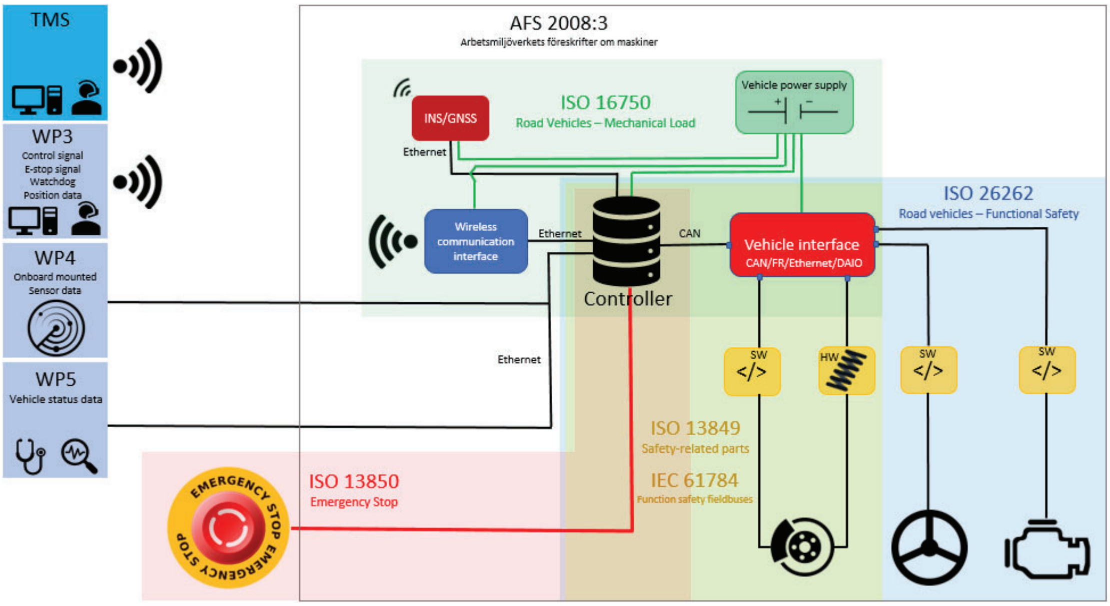


Figure 24 Architecture with corresponding standards

Verification and validation

To verify the functionality of the system a checklist needs to be run through each time the system starts before a self-driven vehicle can enter mixed traffic. The test suite is applicable on all types of self-driven vehicles and guarantees that essential safety measures is satisfied. The fundamentals of the checklist can be studied in Figure 25.

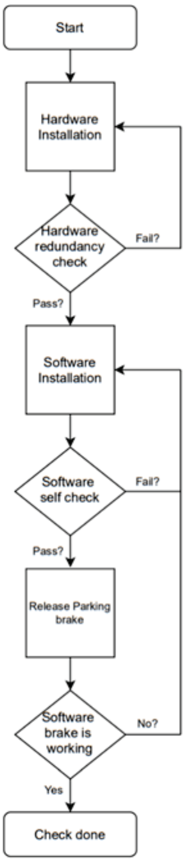


Figure 25 General Flow chart of checking the status of the system

During the project the system has been tested extensively. Both the software and hardware systems have been tested by acceptance, functional and robustness testing. In total 15 test scenarios have been tested such as communication loss, vehicle failure and stop signal. The testing has shown that the system is reliable and responsive, for all the different test cases. The system works as intended and is able to bring the vehicle to a stop.

Best practice

The best practice from now on referenced as the ETAVEP solution is describing the best way to take control over a vehicle during risk.

To ensure robustness redundancy is required; therefore, two standalone systems are used to brake the vehicle. Ideally two different system setups, the ETAVEP solution is to use a software and hardware based independent system. The software based requires connection to the vehicles internal buses to manipulate the signals transmitted to the nodes that control the deceleration of the vehicle. This requires in-depth software knowledge of how the vehicles internal system is constructed and functioning. There is mandatory to ensure that the software-based system always has exclusive right to conduct a stop. The normal condition of this system must be always braked, and only released when everything else is working as intended and not in emergency stop mode.

The hardware-based system must be independent of the vehicle's internal software. The normal condition of this system must be always braked, and only released when everything else is working as intended and not in emergency stop mode. The system must be installed with knowledge of the existing brake system in the vehicle.

The design of both systems needs to be mobile and easy to install in the vehicle to reduce human error. The installation instructions need to be clear leaving no room for interpretation. The design must withstand high stress and vibrations levels that could occur during test. The communication needs to be robust and provide low latency.

The practice of decision making used in ETVAEP is whether to stop the car or not. The decision making is carried out globally on the traffic management server and within vehicle control if internal faults occur.

The documentation provided should be comprehensive for the whole system. It’s important that the user can understand the full system. Every time the systems starts safety checks need to be carried out. A checklist is described to ensure that everything work as intended. The personnel that will use the equipment need to have a proper education on how the system works. This is recommended to be done with safety training both theoretically and practically before using the system.

Conclusions

ETAVEP has proven due to extensive testing that it’s possible to implement a stop using both a software and a hardware interface proven in the proof-of-Concept. The implementation was also shown on the Scandinavian Conference on System and Software Safety 2021. As the testing has shown it is important to have an action plan when a fault occurs. For example, if a power-shortage occurs there must be a solution to stop the vehicle, this is solved by the “normally stopped” approach (e.g., the hardware system).

It is important to have mandatory education of the personnel that will use the system. The system needs to run through a mandatory health check before each startup to be able to operate. Since this is a safety critical system, misuse can cause fatal accidents. During the project the ability to steer away from dangerous situations were considered but decided not to be implemented due to complexity of making sure to cause a more dangerous situation after the steering intervention.

The next step is to take the concept into a product development phase.

6.5 Monitoring of Surroundings

Today the monitoring of the test tracks relies on the test drivers driving at the specific track. They can easily discover any other vehicle, human, animal or object at the test surface and avoid a collision. Since autonomous vehicles do not have any drivers something else needs to work as the eyes at the tracks and therefore a local monitoring system needs to be applied. This is important since the vehicles at a proving ground are under development and do not have fully functional systems. The main purpose is, of course, to prevent any accidents where an autonomous vehicle hit another vehicle, human or object. Also, to detect vehicles, authorized or unauthorized, entering the test area. Consequently, the goal for this part of the project is to answer the research question “Which local monitoring principles need to be applied?”.

General approach

The chosen monitoring system that was used can be seen in Figure 26.

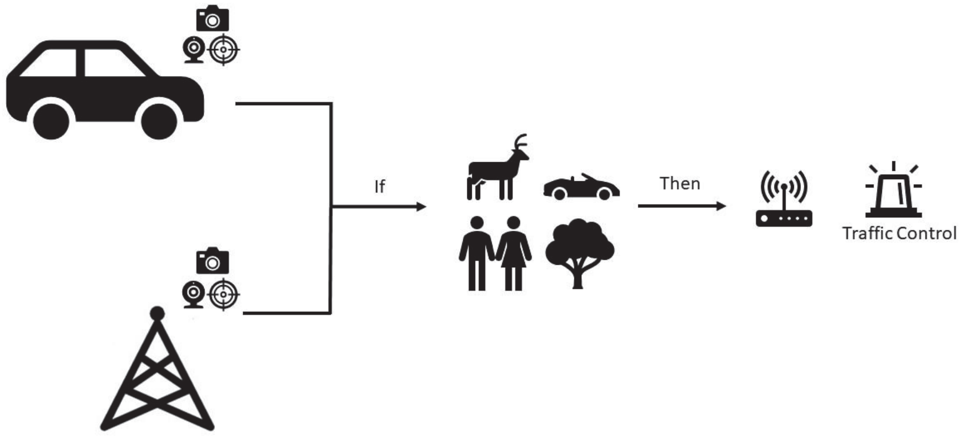


Figure 26 General approach of the monitoring system

The concept that was decided to use was to monitor the test tracks by using stationary and/or vehicle mounted sensors and send any detections to the traffic control.
To find out which sensors are best suitable to use the first step was to perform an evaluation of different type of sensors and the number of sensors was limited to four; lidar, radar, camera and ultrasonic. It was also evaluated if stationary or vehicle mounted sensors were the most suitable to use for each requirement.
After decided which sensors to use some iteration between developing the software to be able to detect and track different object and performing tests at the test track was done. Started with basic test, for example field of view and range, and then focused on tests based on the use cases. Both stationary and vehicle mounted sensors were used during the testing.
The last important part was to define the communication with the traffic control to be able to send the information from the sensors. Finally, several days of testing was carried out to verify both the ability to detect and track and the ability to send the information to the traffic control.

Evaluation of the different types of sensors

The first step was to investigate and gather information about different sensors. The research was wide enough to cover different solutions to guarantee eligibility between them. The sensors were then assessed on the basis of different criteria and the information was summarized and complied in a table. The criteria were based on what functions are necessary for monitoring in the most common conditions. Due to the geographical placement of the test tracks in this project it was important that the monitoring worked in both bad weathers, e.g. heavy rain, and in darkness.

Table 2 Evaluation of the sensors against basic performance aspects

Performance aspect	Radar	Lidar	Camera	Ultrasonic
Object detection	Good	Good	Fair	Poor
Object classification	Poor	Fair	Good	Poor
Distance estimation	Good	Good	Fair	Fair
Edge detection	Poor	Good	Good	Poor
Lane tracking	Poor	Good	Good	Poor
Visibility range	Good	Fair	Fair	Poor
All weather performance	Good	Fair	Poor	Fair
Dark or low illumination performance	Good	Good	Fair	Good

The Table 2 showed the different sensors' strength and weaknesses. Due to poor performance, it was decided that the ultrasonic sensor should not be further investigated.

The table showed that no one of the sensors can handle the monitoring by itself if a good performance in all aspects is required. A combination of radar and camera could be enough to cover all the performance aspects. Another possibility is to use radar and lidar, if fair object classification is enough. At the test track object classification might not be necessary. It could be enough that the sensors detect an object and the vehicle receives a stop signal without knowing what kind of object. In that case the camera can be excluded since lidar can handle edge and lane detection as good as the camera.

The most cost efficient is to only use two different sensors. Although, in this project all three types were used and tested to further investigate which is the best combinations.

Evaluation of the sensors against the use cases

The purpose of this task was to evaluate and determine if the three types of sensors radar, lidar and camera reach the requirements based on the use cases produced in the project and therefore are suitable to use.

All the use cases were compiled in a document and the three different sensors were assessed against each use case. It was three levels of assessment based on the same colors as the previous table. Red = cannot reach the requirement, yellow = unsure if the requirement can be reached and green = can reach the requirement. It was also decided however a stationary, a vehicle-mounted or a mix setup was preferred in each use case. See example in Table 3.

Table 3 Example of the evaluation against the use cases

	Stationary/ Vehicle mounted	Radar	Camera	Lidar
Regulated intersections				
Detect and report if there are any vehicles in the intersection/roundabout or not	Stationary	🟩	🟩	🟩
Detect and report if there are any pedestrians in the intersection/roundabout or not	Stationary	🟨	🟩	🟩
Define a zone around vehicles where pedestrians can be in danger	Stationary	🟩	🟥	🟩

Stationary installation of the sensors
Most important for the stationary mounting is to always ensure good vision over the area. Therefore, the sensors are preferably mounted in an elevated position. Also, for good performance it is important that the sensors do not move, e.g., due to vibrations or other movements from the attachment point. During this project a light weight and elevation adjustable tripod with three anchorage points to ensure a stable setup was used for stationary mounted lidar and radar.

Camera
The camera used in this project was an Axis Q1615-LE Mk III, see Figure 27.

Figure 27 Axis Q1615-LE Mk III

For the camera the *you only look once* v5s6 object detector was chosen as it manages good detection performance with a processing time of 35-40 ms per frame on a laptop Graphics Processing Unit, GPU.

One task was to convert the information from pixel coordinates to latitude and longitude coordinates. The solution for the project was to estimate object depth using prior knowledge of the object height. By using the relationship between the actual object height, and the pixel height, the depth of the object could be computed. The method has a few drawbacks. It assumes that the pixel height corresponds to object height, which is only true if the camera is looking straight at the object without any roll. This could be solved using semantic segmentation and a pose estimator, which would transform the perspective of individual objects in the image. Another assumption is that objects are rigid. This is true for cars, but not for humans. If someone would bend or sit in the image, the bounding box would become smaller, and the method would produce a depth estimate much further away than what is true.

Lidar

The lidar used in this project is a H2 prototype from Luminar Inc. The lidar determines range to object with a laser measuring time of flight to calculate the distance to the object. This generates a point cloud representation of the surrounding, see Figure 28.

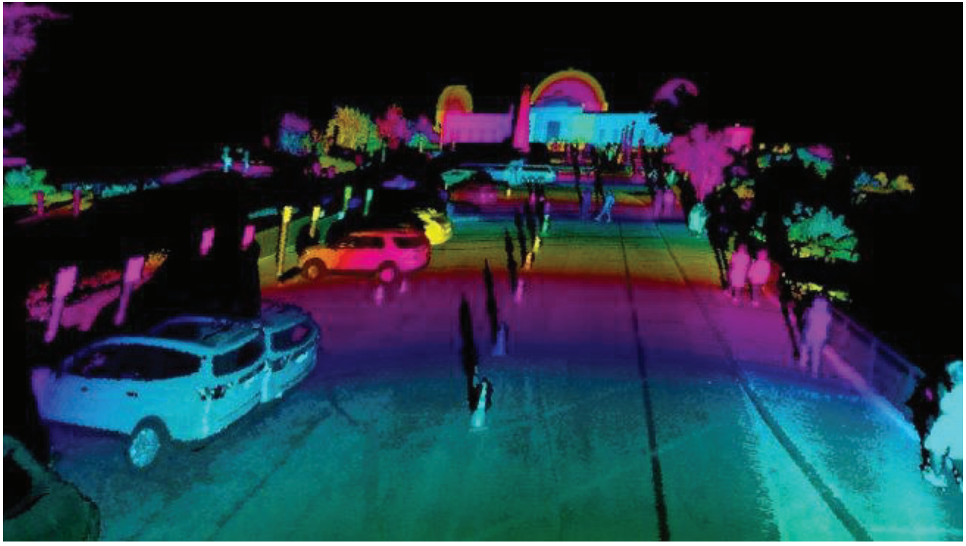


Figure 28 Example of a point cloud generated by a lidar.

The point cloud needs to be processed to extract adequate data. To detect objects of interest for example vehicles, pedestrians and other obstacles there was imperative to filter the point cloud so the position of the objects of interest could be found. This was done in two steps.

The first was to rationalize the point cloud into two different states, drivable ground and non-drivable ground. This was done by an algorithm called Random sample consensus (RANSAC). This algorithm tries to divide the point cloud into two states with an iterative method to estimate parameters of a mathematical model from a set of the point cloud. The second step was to cluster the points considered non-drivable to determine position of the objects. To cluster the non-drivable points an algorithm called Density-based spatial clustering of applications with noise (DBSCAN) was used. The tracking algorithm uses a Kalman-filter and tracks the clustered object from the DBSCAN. The algorithm also filters tracks considered false. It can track unlimited number of objects. The lidar transmits object data to traffic control in a polygon shape to represent the area covered by the object.

Radar

The radar used in this project is a Saferadar Lannik 2. The radar sensor measures (radial) velocity inherently. In fact, detecting (relative) velocities is what the radar does best. This is due to how the waveforms and signal processing works by sending a burst of linear chirps and transforms it to measurement (using the Fourier transform).

The role of the tracker is to increase the target location accuracy (main purpose of Kalman filter), to filter out false alarms generated by the background and to separate closely spaced targets by assigning measurements to the correct track.

The whole signal processing chain used for the radar is shown in Figure 29. It started with reading the raw data from the FPGA (Field-Programmable Gate Array) and ended with transmitting tracks to the traffic control.

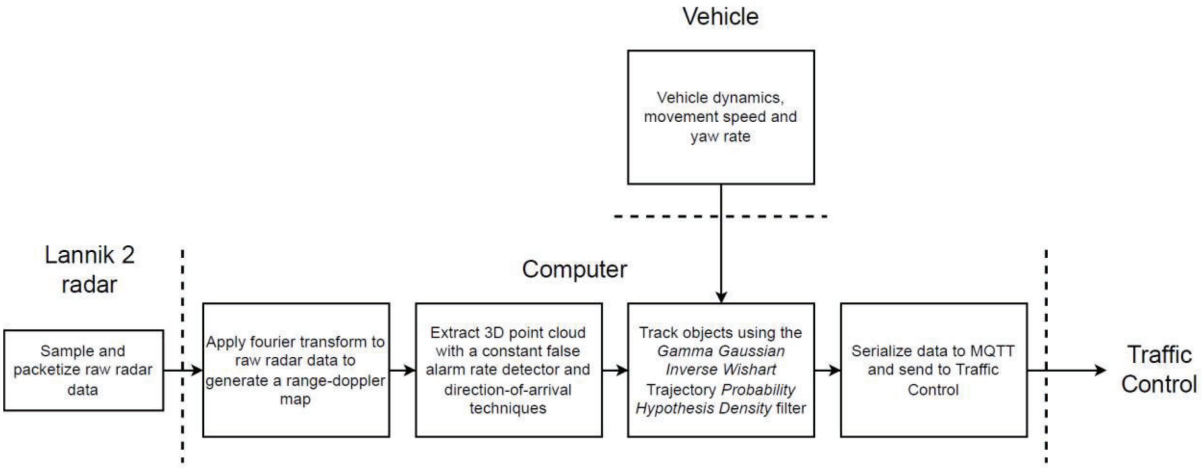


Figure 29 Radar signal processing chain. In case we have vehicle mount some input from the dynamics is needed

Vehicle mounted installations of the sensors

The mounting position was determined by different factors, it needs to give a sufficient overview of the surroundings of the car and yet to be able to detect objects in the very near surroundings of the car. After performing a high-frequency structure simulation, HFSS, of five different mounting positions for the radar it was decided to place the radar at a rig attached at the roof rack of the vehicle together with the lidar, see Figure 30. The simulation showed the hood, windshield or roof were not affecting if the radar was placed in these positions.

Figure 30 Vehicle mounted radar and lidar

For vehicle mounted radar the radar requires some input from the vehicle dynamics, especially for the tracking. Adapting the signal processing and tracking to a vehicle mounted setup takes some work but is doable. There are work left in the tracker to solve the moving platform adaption, for example choose the coordinate system.

Verification and validation tests

To be able to reach all the requirements there was four essential tasks the sensors need to manage:

- Detect pedestrians, moving as well as stationary, more than 3 seconds before collision.
- Detect vehicles, moving as well as stationary, more than 3 seconds before collision.
- Detect stationary objects, e.g., tree branches or a forgotten ladder at the track.
- Detect and distinguish between multiple objects at the same time.

Due to limitations in time and economy it was impossible to test all the different variations of scenarios produced by the project and therefore a test plan was made. The plan focused on the main scenarios and found six different tasks. The assessment was that if the sensors reached the requirements in Table 4 the system could handle all the common events at a test track.

Table 4 Test Plan

Test number	**Type of test**	**Requirement**
1	Field of view	Detect objects at a distance over 66 m.
2	Speed	Detect objects driving at a speed up to 80 km/h.
3	Regulated intersection	Detect multiple humans and vehicles.
4	Slower vehicle	Detect slower moving vehicle in front, >3 sec to collision, including stationary vehicles.
5	Lane change/Cut in	Detect multiple vehicles in adjacent lanes.
6	Overtaking	Detect an oncoming vehicle, >3 sec to collision.
7	Oncoming vehicle in the same lane	Detect an oncoming vehicle, >3 sec to collision.
8	Obscured situations	Detects objects that are hidden for the vehicle, due to e.g. curves or crest.

After confirming that the sensors could reach the basic requirements, field of view and speed, the testing of more specific scenarios began. Several different variations from test number 3-7 were performed during a number of test days at AstaZero test track.

Another important thing to test was the communication with the traffic control, therefore several test days were performed together with the traffic control and also with the emergency stop. During these days focus was to test the whole chain from detection, send data to the traffic control and send stop signal to the car. Here we used a platform with a pedestrian target.

No testing in heavy rain, fog or other hard weather conditions was done. The days for testing had to be planned at least a couple of weeks in advance and therefore it was not possible to plan after the weather.

A number of different variations of the use cases were tested to verify that the sensor system was suitable for monitoring. The testing could proceed over a day without any interruptions due to malfunctioning sensors. Although, to verify that the sensors are capable for the task over time some reliability testing during several days needs to be done but was excluded in the project. Since AstaZero is an independent test track with many different customers it was not possible to monitor a track over several days due to secrecy.

Results from the Verification and Validation tests

The sensors could detect, track and distinguish multiple objects and was able to detect both stationary and moving vehicles and pedestrians. As a result, they can handle oncoming, overtaking and slower moving vehicles.
Also, the communication to the traffic control was working.

Camera:

- Detection range of pedestrians is 60 meters.
- Detection range of cars is roughly 70 meters.
- The horizontal field of view is variable, 40-102 degrees.
- The vertical field of view is variable, 22-58 degrees.

Lidar:

- Detection range of pedestrians is roughly 75 meters.
- Detection range of cars is roughly 230 meters.
- The lidar is operating at 10Hz.
- The field of view is ± 60°.

Radar:

- Detection range of pedestrians is 60 meters.
- Detection range of cars is roughly 180 meters.
- The radar is operating at 15 Hz.
- Field of view is plus/minus 60 degrees in azimuth and plus/minus 30 degrees in elevation.
- The operation frequency is 76-77 GHz (and optionally 77-81 GHz).

Conclusions

In the project it had to be supposed that no sensor fusion was necessary. However, in a production system it is required. It is important to increase the accuracy of positioning on part of the sensors, to prevent situations where a vehicle with safety zone reacts to a sensor detection of the vehicle itself and to increase the accuracy of object classification if it is necessary.

The results showed that there are pros and cons of both stationary and vehicle mounted sensors. It could be easy to believe the best solution is to cover the tracks with stationary sensors for a complete monitor system. This is of course an option, and the advantages are that the sensors are always mounted at stable rigs and the sensors do not need any position data from a GNSS-device. On the other hand, this solution would require hundreds of sensors which produce a huge amount of data. It would be comprehensive, and unnecessary, to handle all the data since most would be without interest because no self-driven vehicle drives at the specific place at the time.

The most significant advantage of vehicle mounted sensors is that they only collect detections of interest, the ones in the vehicle’s path. The biggest drawback is the risk that the monitor sensors interfere the vehicles sensors, especially for the radar if they use the same frequency. Vehicle mounted sensors come with limitations in where the vehicle can be allowed to be driven. If only using vehicle mounted sensors it is impossible to handle obscured situations like curves or obscured intersections. Therefore, a mix of both vehicle mounted and stationary sensors is the best alternative.

6.6 Traffic Control

To maintain safety when multiple vehicles are out on the proving ground, traffic coordination is highly essential. Therefore, this part of the project focused on building a prototype (proof-of-concept) program for keeping the dedicated test area safe.
To simplify – one can say that the complete goal and task for Traffic Control was to collect as much information as possible from and about the test track. Using this information to ensure safety by sending control signals to all controllable vehicles. See Figure 31.

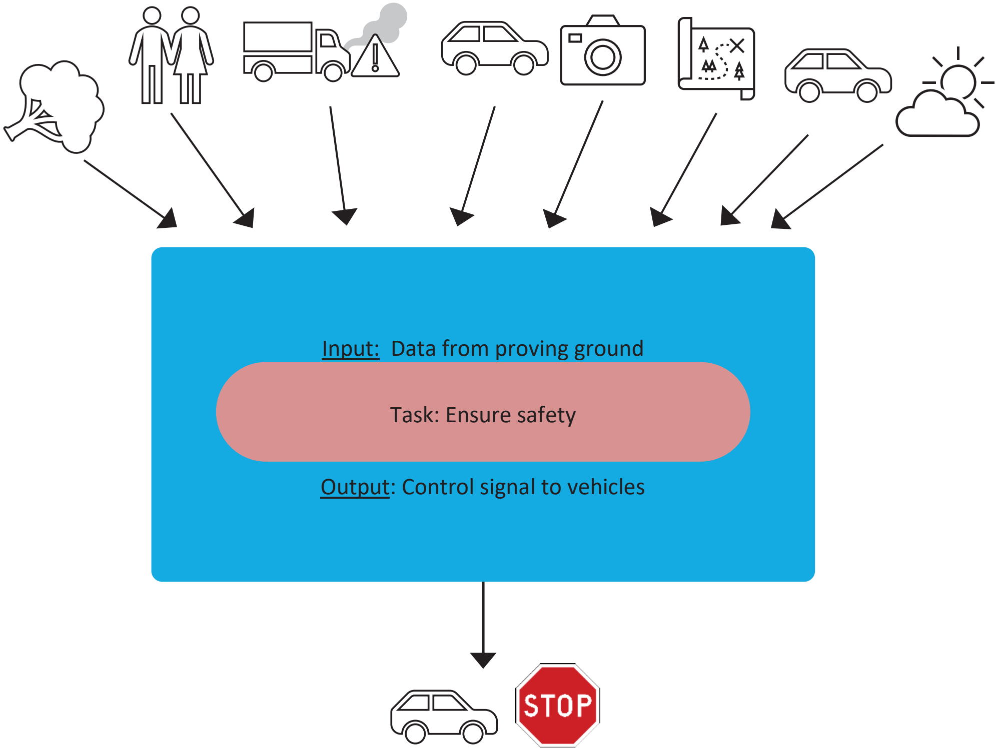


Figure 31 Traffic Control task

General approach

To provide a safe testing environment of self-driven vehicles, the first step was to benchmark potential state-of-the-art systems in similar applications. The results from the benchmark investigation gave important information about how to look at traffic control systems and evaluate what is available already.

Additional to the benchmark, a thorough use cases and risk assessment investigation was made about how to understand the test track rules and environment, by collecting relevant information on the test track, other vehicles, pedestrians and other objects. With the provided information and collected data which then had to be handled sufficiently, a relevant evaluation should be made. In case of an identified unsafe situation, the self-driven vehicle had to be stopped in a controlled way.

It must be ensured from these both activities that the self-driven vehicle will be possible to stop before running into an unsafe situation. Therefore, a dynamic traffic control system had to be developed during the project that sufficiently could collect all the relevant information needed. Based on this information an adequate decision had to be made when to send a stop request and make sure the vehicle is safely halted before any unsafe situation occurs.

It was not obvious what exactly an unsafe situation is, and how to detect one automatically. For the traffic control system, the control algorithm of an observed self-driven vehicle is a black box and it might behave erratically (prototype). This problem is aggravated by the fact that numerous objects need to be observed, which means that detecting unsafe situations needs to happen under performance constrains. Eventually, the situation cannot be resolved by steering the self-driven vehicle, but an emergency brake request is the only possible action. In order to deal with these challenges, a conservative approach was taken, called *safety zone*, that calculates an area in front of the vehicle in which no other objects may be. This area is then periodically checked in order to detect unsafe situations. Both calculation and detection can be parameterized to allow different degrees of risks of collisions for different test scenarios. Further ways to reduce the inherent conservative results by programmatically translating traffic rules are sketched as *driving corridors*.

Benchmarking of state-of-the-art related applications

A benchmark was initially performed of closely related systems, among others automated port and mining environments, available at the time for the review. Any updates of the systems or new systems developed during the project has not been taken into consideration.
Often when looking into systems used for self-driven vehicles, they are developed for a specific vehicle, specific traffic situation or operational design domain.
This study shows that there is no “one fits all” solution, but rather a variety of systems designed for their respective environment.

System description and design

The ETAVEP system consists of several parts, described in the previous sections of this report, that all communicates with the Traffic control. The system layout can be seen in the Figure 32.

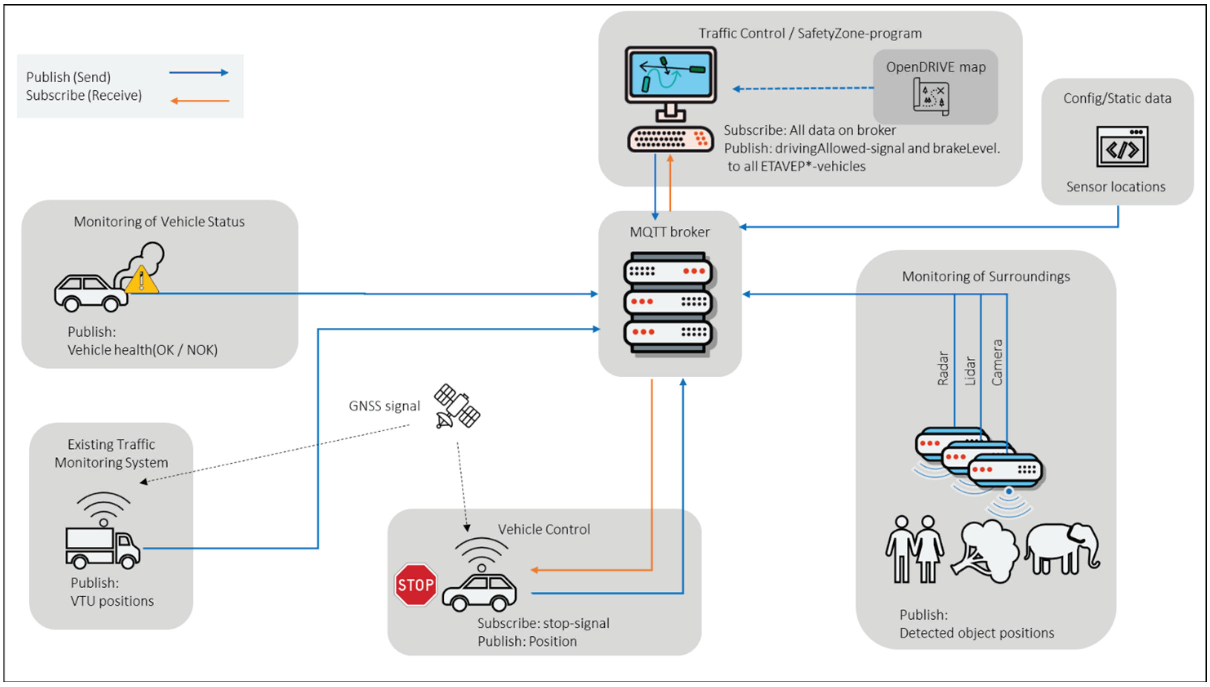


Figure 32 System Overview

In the following sections each part of the system will be described further and how all the sub-systems are interacting in the traffic control system.

Design and evaluation of the Safety Zone Concept

The *safety zone* is an area around moving objects in which no other objects shall be present, see Figure 33. The safety zone concept enables to build a surveillance system with a supervisor that ensures that the self-driven vehicles do not deviate from their respective allowed routes (from a situation-specific safety perspective). A concept is presented how to calculate such dynamic safety zones based on basic vehicle dynamics, available measurement data and other relevant information.

While the safety zone provides a strong basis for safety in a mixed testing environment, including self- and human driven vehicles. The safety zone alone might be too conservative in this case, and further research is proposed on a concept called driving corridors.

The requirements from the risk assessment performed in the ETAVEP project are used as input and have been integrated in the design of the safety zone concept.

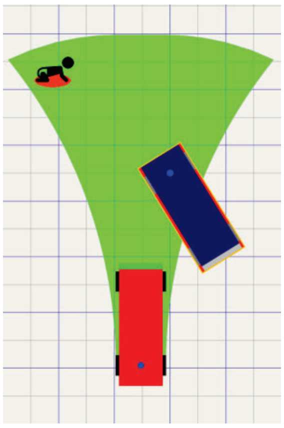


Figure 33 Safety Zone

Assumptions and restrictions for the safety zone concept

To design and evaluate a safety zone concept, it is necessary to make assumptions and restrictions. A schematic overview of the data flow between the ETAVEP sub-systems is shown in Figure 34. The indicated data describes minimum information that is sent. Usually, more information is available on a test track, and this will improve the performance of the system further.

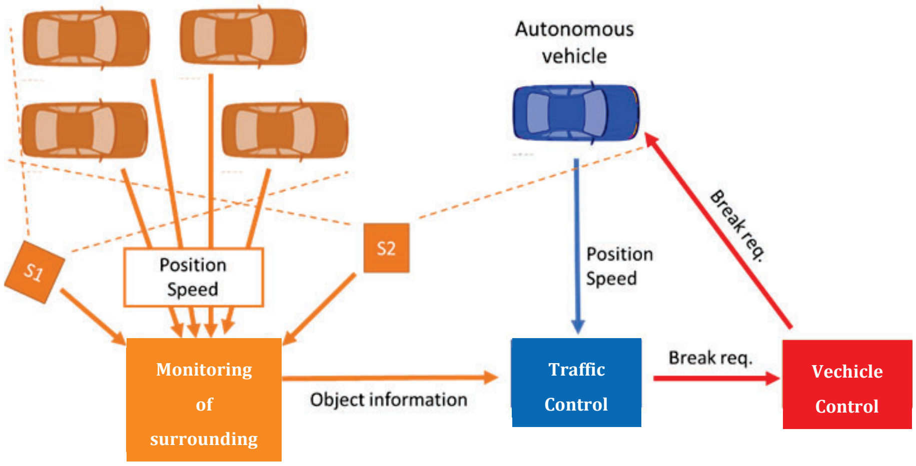


Figure 34 Schematic overview of data flow from a Safety Zone perspective

a) The self-driven vehicles are equipped with RTK GNSS (Real Time Kinematic Global Navigation Satellite System) and their position data has high precision in the range of a few centimeters and an update rate of 10 Hz or more. Uncertainty in positions and velocities must be included in safety zones calculation for the self-driven vehicles.

b) Sensor data from different sensors on the test track is collected by the monitoring of surroundings. It also receives position information from GNSS receivers in other vehicles and moving objects on the test track, but possibly with higher uncertainty and delays that need to be accounted for.

c) The assumption is that all vehicles may be modelled as point masses but with the additional geometry of the vehicles included. Ackermann steering geometry (linkage arrangement used in virtually any car-like vehicle) is assumed, and a simplified bicycle model is used to calculate possible paths.

Information organization – layer concept

A data layer model for test scenario description was proposed by the German PEGASUS project (PEGASUS, et al., 2019) (Weber, et al., 2019).

For the safety zone concept in ETAVEP, a layer concept was applied as well. However, the concept was simplified to the ETAVEP project's specific needs with a test track layer (Layer 1) and an object information layer (Layer 2) used as detailed in the following.

Layer 1: Test track information

The availability of accurate test track information is required for ETAVEP, as the project shall monitor how objects move on the tracks. This information has been further divided in two sub layers:

A. Static test track information like road boundaries, speed limits, road surfaces.

B. Dynamic test track information like state of traffic signals, temporary geofences, driving directions in case it can be changed.

Layer 2: Object information

Layer 2 contains information about all movable objects on the test track, regardless of whether it is moving during the test. The safety zone concept focuses on self-driven vehicles however safety zones for all moving objects could be evaluated to increase overall test track safety.

Again, the information has been further divided in two sub layers:

A. Static object information like object type, dimensions, acceleration and steering capabilities.

B. Dynamic object information like current velocity, acceleration, position (incl. confidence), average communication delays.

How the object information is represented exactly is not constrained by the safety zone concept. It does, however, make sense to take relevant standards like (International Organization for Standardization, n.d.), OpenDRIVE or OpenSCENARIO as a reference.

Proposed safety zone concept

The fundamental idea of the safety zone concept was to calculate an area around each self-driven vehicle that was used to periodically check whether an action needs to be taken by the traffic surveillance to avoid critical situations. These checks depend on the same test track information that was used to allow the traffic surveillance to determine whether a self-driven vehicle behaves as expected on a high level, e.g., whether it follows the road within its lane. To achieve this, a proper model for calculating safety zones around objects and checking their relation to surrounding objects was defined. Further, accurate track information was needed to adapt the safety zone to specific situations like oncoming traffic. This is stepwise addressed in the following.

Safety zones for moving objects

First, a single moving object was considered. In this case, the aim of the safety zone was to determine the area which the object could reach, before stopped, in an emergency brake situation, given the current state (Object layer information). I.e. the safety zone is the hazardous area to be in when the moving object behaves erratically (e.g., malfunctioning self-driven vehicle) and needs to be stopped.

Safety zone definition

The following helper function determines the point to which a vehicle moves after driving a given distance d with a current turning radius of r:

$$\mathrm{driveAndTurn}(d, r) = \left(|r| \cdot \sin\left(\frac{d}{|r|}\right), r \cdot \left(1 - \cos\left(\frac{d}{|r|}\right)\right)\right)$$

Given the moving objects width w, distance between rear axle and front end d_{front}, braking distance d_{b} and the minimum turn radius r_{min}, define the safety zone as the shape that originates in the middle of the vehicle's rear axle and is enclosed by the union of the following sets of points:

Left side:

$$\left\{(x,y) \in \mathbb{R}^2 \mid (x,y) = \left(x, y' + \frac{w}{2}\right) \wedge (x,y') \in \mathrm{driveAndTurn}(d, r_{\min}), \forall d \in [0, d_{\mathrm{b}} + d_{\mathrm{front}}]\right\}$$

Right side:

$$\left\{(x,y) \in \mathbb{R}^2 \mid (x,y) = \left(x, y' - \frac{w}{2}\right) \wedge (x,y') \in \mathrm{driveAndTurn}(d, -r_{\min}), \forall d \in [0, d_{\mathrm{b}} + d_{\mathrm{front}}]\right\}$$

Front:

$$\{(x,y) \in \mathbb{R}^2 \mid \ (x,y) \ \in \mathrm{driveAndTurn}(d_{\mathrm{b}} + d_{\mathrm{front}}, r), \forall r \in [-r_{\min}, r_{\min}]\}$$

Rear:

$$\left\{(x,y) \in \mathbb{R}^2 \mid x = 0, y \in \left[-\frac{w}{2}, \frac{w}{2}\right]\right\}$$

Figure 35 gives a visual representation of how the safety zone was calculated.

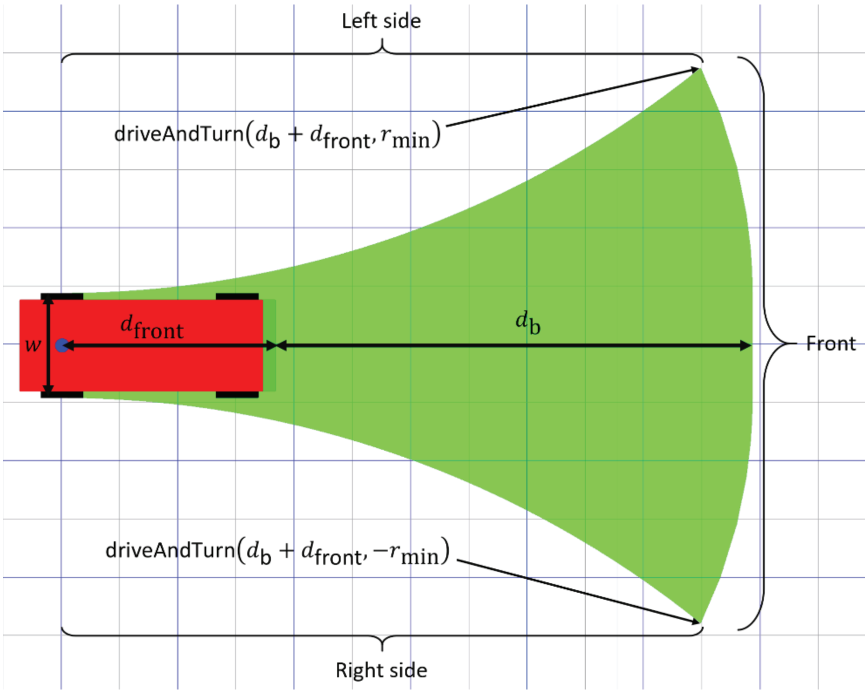


Figure 35 Visualization of safety zone calculation

Obtaining accurate values for d_{b} and $r_{\min}$ requires calculating the vehicle's dynamics for the current state. To keep the computational costs low, a simplified dynamic model is described here.

Vehicle dynamic model

In order to obtain input values for the safety zone, modelling the brake distance and the turning radius is needed. In general, more accurate models for these parameters will improve the accuracy of the safety zone and make it less conservative but at the cost of complexity, and thus, at the cost of computation time

Braking distance

The braking distance of a moving vehicle depends on numerous parameters (Jacobson, 2020), e.g., the current speed, braking capability, road surface type, tires, weather, etc. Depending on the information in test track and object information layer as well as computing resources available, the braking distance can be modelled more or less precise.

One simple estimate of the braking distance can be obtained, e.g., using the "Three Seconds Rule". It is an aid for drivers to estimate a suitable distance to the vehicle driving in front. It states that after the next three seconds, the vehicle should be behind the point the vehicle in front is right now, and can be expressed in this simple equation:

$$d_{\mathrm{b}} = 3 \cdot v, \text{where } v \text{ is the current speed}$$

Using this rule, the only information required about the observed vehicle is the current speed and computation costs are negligible. However, it can be quite conservative since it is not using the relative speed in relation to surrounding objects.

A more accurate, but still simplified model is described in the following. It takes potential delays t_d like network latencies or system delays in the vehicle (once the brake request arrived) into account. After t_d, the vehicle is assumed to brake with the maximum deceleration (= minimum acceleration) a_min known from object information layer.

During t_d, the vehicle might accelerate and because the object information layer is subject to the same delay (at least network latencies), the worst-case acceleration needs to be assumed, i.e., maximum acceleration. Given the current vehicle speed v_curr, the speed after t_d is therefore:

$$v_\mathrm{d} = v_\mathrm{curr} + a_\mathrm{max} \cdot t_\mathrm{d}$$

The distance driven after t_d is:

$$d_\mathrm{d} = v_\mathrm{curr} \cdot t_\mathrm{d} + \frac{a_\mathrm{max} \cdot t_\mathrm{d}^2}{2}$$

After t_d, maximum deceleration is assumed, the point in time t_stop at which the vehicle stops is:

$$v_\mathrm{d} + a_\mathrm{min} \cdot (t_\mathrm{stop} - t_\mathrm{d}) = 0 \Rightarrow t_\mathrm{stop} = t_\mathrm{d} - \frac{v_\mathrm{d}}{a_\mathrm{min}}$$

Finally, the total distance required is:

$$d_\mathrm{stop} = d_\mathrm{d} + v_\mathrm{d} \cdot (t_\mathrm{stop} - t_\mathrm{d}) + \frac{a_\mathrm{min} \cdot (t_\mathrm{stop} - t_\mathrm{d})^2}{2} = v_\mathrm{curr} \cdot t_\mathrm{d} + \frac{a_\mathrm{max} \cdot t_\mathrm{d}^2}{2} - \frac{(v_\mathrm{curr} + a_\mathrm{max} \cdot t_\mathrm{d})^2}{2 \cdot a_\mathrm{min}}$$

For experiments in the project, fixed values were used for $a_\mathrm{min}, a_\mathrm{max}$ and t_d. Note that $a_\mathrm{min} < 0$ and $a_\mathrm{max} > 0$. A graph showing calculated speed and distance vs. time using this model is shown in Figure 36. More accurate models for these parameters will improve the accuracy of the safety zone. Delays that should be considered in estimating t_d are, e.g., network, detection and position estimation delays.

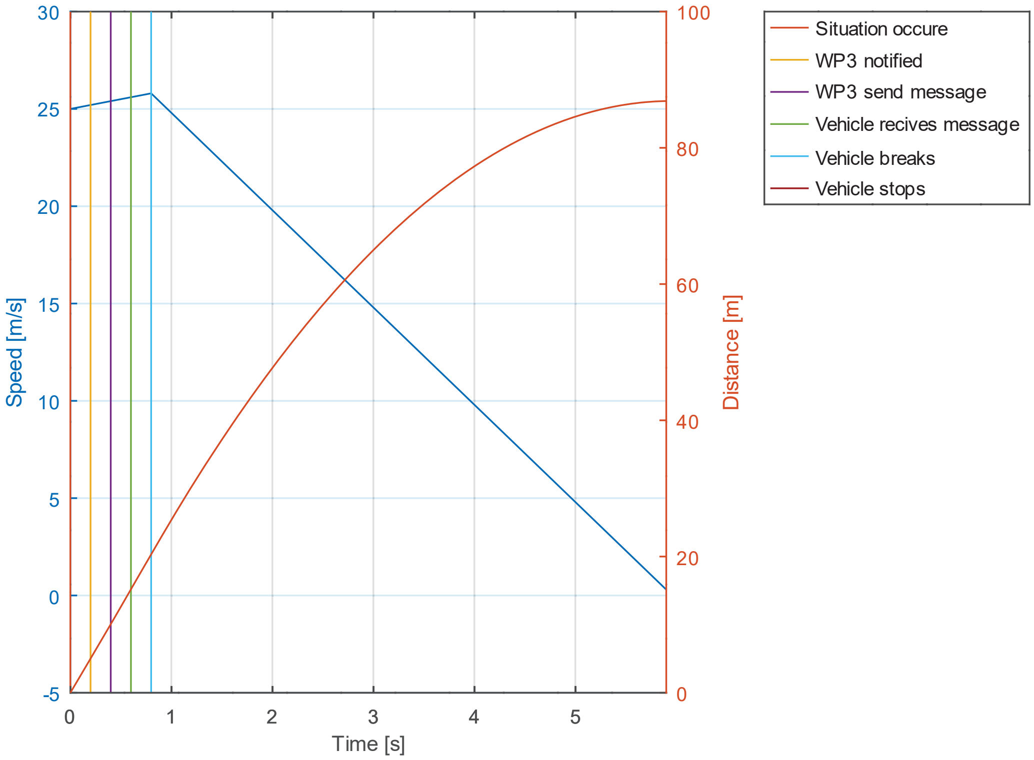


Figure 36 Calculated vehicle speed and driven distance vs.time

Turning radius

The minimum turning radius is a parameter for the safety zone calculation that determines the width of the safety zone. At low speeds, the limiting factor for a smaller turn radius is the steering of the vehicle. In this case, the bicycle kinematic model (Jacobson, 2020) is utilized with the rear axle as the reference point to determine the minimum turn radius $r_{\text{min}}^{\text{steer}}$:

$$r_{\text{min}}^{\text{steer}} = \frac{d_{\text{axle}}}{\tan(\theta_{\text{max}})}$$

Where d_{axle} is the distance between front and rear axle and θ_{max} is the maximum steering angle.

At higher speeds, the *side friction* factor f_{sf}, i.e., the friction between the vehicle's tires and the road surface, determines the minimum turn radius. f_{sf} depends on many parameters, mainly vehicle speed (higher speeds lead to lower values). Lower values of f_{sf} translate into smaller turn radiuses and, thus, a bigger safety zone. At best, f_{sf} is available as object information layer, a conservative constant value (usually around 0.2 for passenger cars) (Jacobson, 2020) can be used, but it is desirable to determine different values for different road surfaces and weather conditions. Then, the minimum turn radius based on f_{sf} is modelled as:

$$r_{\text{min}}^{\text{sf}} = \frac{v_{\text{curr}}^2}{f_{\text{sf}} \cdot g}$$

Where g is the earth's gravitational force. Finally, the minimum turn radius is modelled as:

$$r_{\text{min}} = \max\left\{r_{\text{min}}^{\text{steer}}, r_{\text{min}}^{\text{sf}}\right\}$$

Relative safety zones

The introduced safety zone definition does not depend on information about other objects. Essentially, every object that enters the safety zone is therefore considered stationary, even when it is moving in the same direction, see Figure 37.

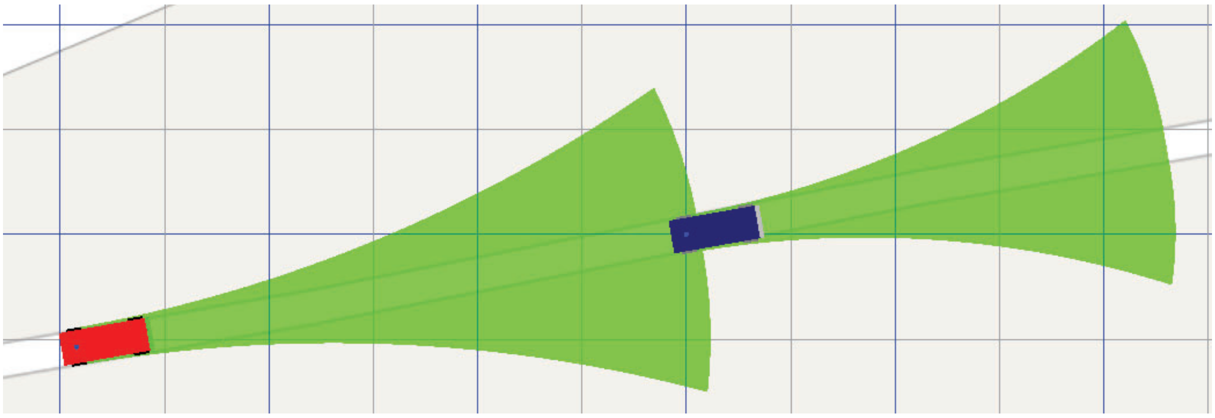


Figure 37 Vehicles following each other (independent safety zone)

To be less conservative and allow vehicles to drive closer without compromising safety, it was needed to determine whether the "other" vehicle is in proximity of the self-driven vehicle is actually driving in the same direction, then it was possible to calculate safe distance between the vehicles. First, the current velocity vectors $\vec{v}_{\text{ego}}$ and $\vec{v}_{\text{other}}$ of the self-driven vehicle and other vehicle are used to determine whether the vehicles are driving in the same direction, i.e., when their relative angle is less than 45°:

$$\frac{\vec{v}_{\text{ego}}}{\left\|\vec{v}_{\text{ego}}\right\|} \cdot \frac{\vec{v}_{\text{other}}}{\left\|\vec{v}_{\text{other}}\right\|} > \cos 45°$$

If this is the case, the safe distance is calculated as following (Shalev-Shwartz, Shammah, & Shashua, 2018):

$$d_{\text{rel}} = \max\left\{\left(\left\|\vec{v}_{\text{ego}}\right\| \cdot t_d + \frac{1}{2} a_{\text{max,ego}} \cdot t_d^2 - \frac{\left(\left\|\vec{v}_{\text{ego}}\right\| + t_d \cdot a_{\text{max,ego}}\right)^2}{2 \cdot a_{\text{min,ego}}} + \frac{\left\|\vec{v}_{\text{other}}\right\|^2}{2 \cdot a_{\text{min,other}}}\right), 0\right\}$$

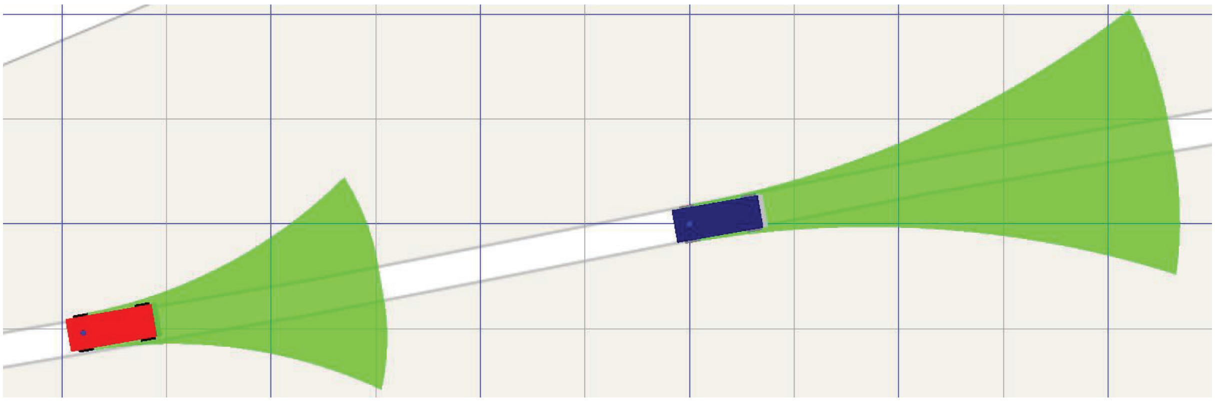


Figure 38 Vehicles following each other (same parameters as previous figure, but using relative safety zone)

Using d_{rel} and r_{min}, a safety zone for the self-driven vehicle can be calculated that is less conservative when following another vehicle and the required parameters are available as object information layer as shown in Figure 38**Error! Reference source not found.**. To reduce computational cost, it should only be considered for vehicles within a certain distance, e.g., vehicles that are close to the safety zone.

Driving corridors to make the safety zone less conservative

The planning algorithm of the vehicle is treated as a black box, consequently, all possible movements of the vehicle until it can reach a stop need to be considered. Therefore, the safety zone is conservative and will in certain circumstances be larger than needed.

The test track data information layer must include information about the lanes and their driving directions. This is important to check whether a vehicle deviates from its path, but even for the safety zone to be less conservative. Consider the example where oncoming traffic meets each other in separate traffic lanes, see Figure 39. The vehicles will end up in each other's safety zone and an undesired emergency stop will be requested. If the vehicles are trusted to stay within their respective lanes, it is possible to restrict the safety zone to the traffic lane, as shown in Figure 40, and avoid this problem.

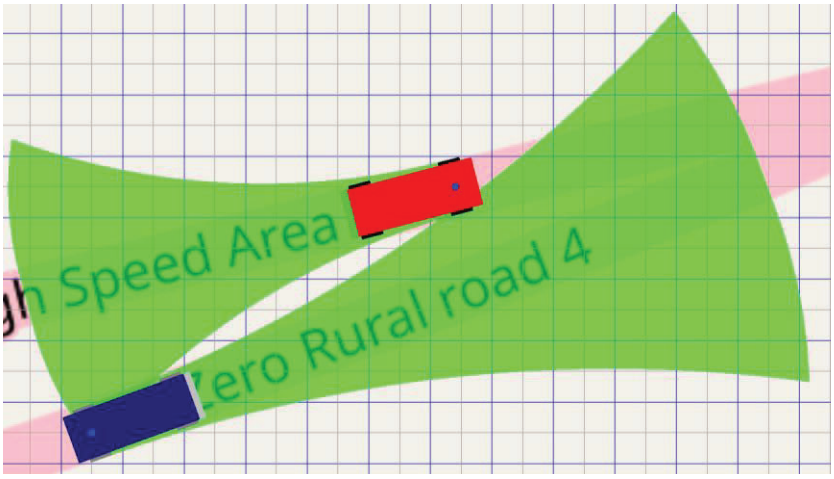


Figure 39 Two vehicles meeting each other on separate lanes (diverging into separate roads)

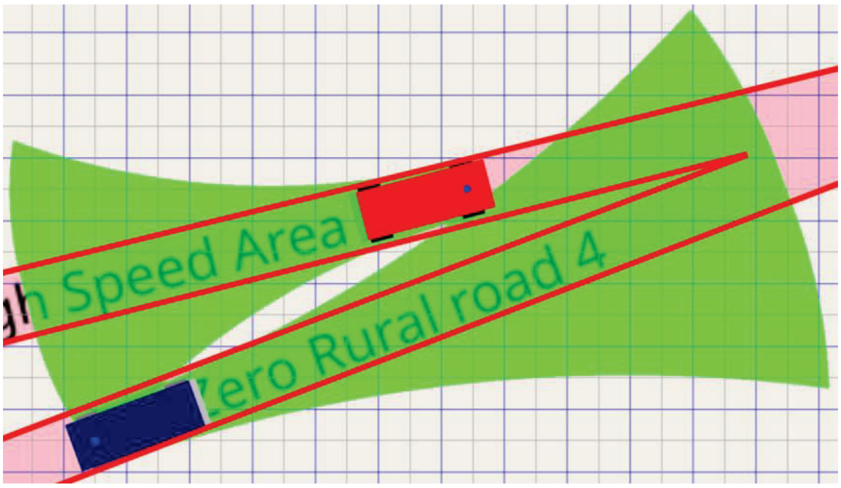


Figure 40 Two vehicles meeting each other as in the previous figure, but safety zone is only applied to their respective lanes

Driving in intersections are other challenging traffic situations that would need to be taken into consideration.

Designing a surveillance system that handles all possible intersections is a challenge that is outside of the scope of ETAVEP. Verification and validation of such a system would be even more challenging.

Retrieve data from existing monitoring system

All existing vehicles at the proving ground must be equipped with a *Vehicle Tracker Unit*, VTU that reports its position with a low update frequency (~1Hz) that is used by the existing *Traffic Monitoring System*, TMS.
This data is retrieved, and then republished onto the MQTT-broker according to Figure 41 below:

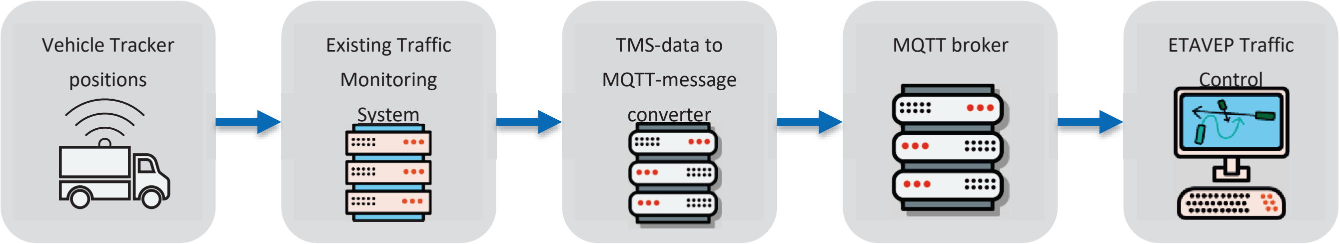


Figure 41 VTU to ETAVEP-signal logics

The Safety Zone program subscribes to the VTU-data and the tracker positions are displayed in the program as small red dots, see Figure 42. If any of these trackers is inside the safety-zone, it will result in sending a *drivingAllowed*-signal set to false (i.e. “brake”).

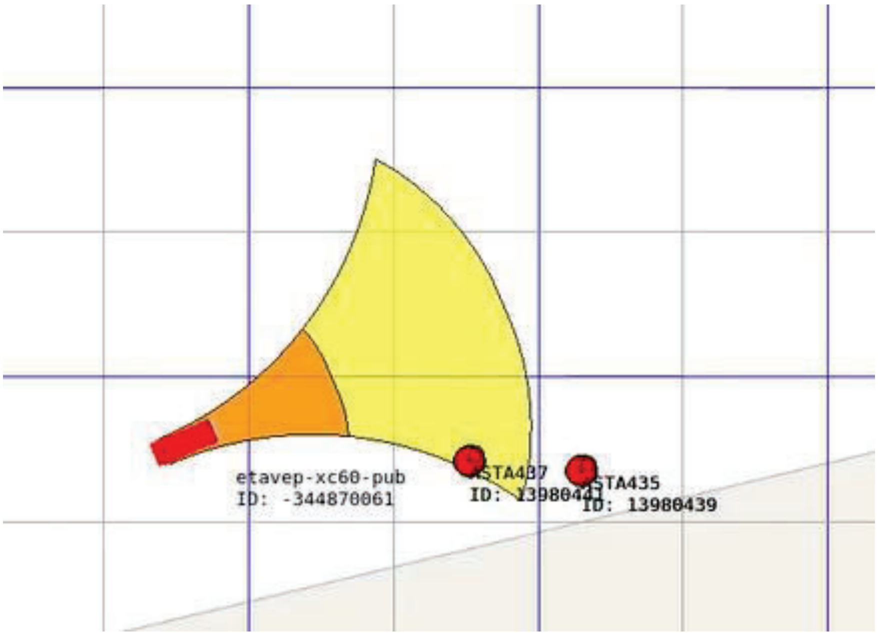


Figure 42 VTU device detected inside Safety Zone

Due to the low update frequency of the Vehicle Tracker Units, an enlarged tracker position is calculated based on the reported tracker velocity, see Figure 43.

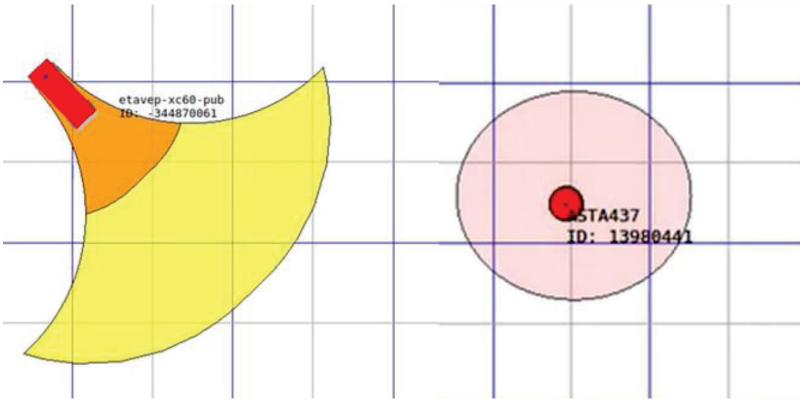


Figure 43 VTU with uncertainty circle in pink

Integration towards the sensors monitoring the surroundings.

Sensors were integrated in the traffic control program and represented by *Field of View*, FOV, circle sectors. The sensors' actual FOV is retrieved from the corresponding MQTT topic, but for proof-of-concept purposes set to a fixed assumed value of 120 degrees, see Figure 44.

The sensors report data in their local coordinate system meaning that the traffic control program had to make necessary transformations on the data to place them in a global coordinate system.

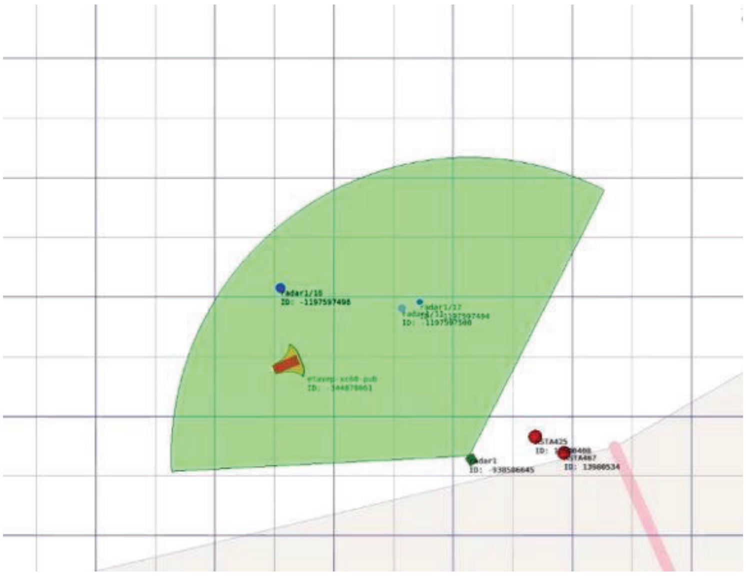


Figure 44 Sensor Field of View representation

Figure 45 shows a sensor detection overlapping with a safety zone (in contrast to Figure 44), meaning that the drivingAllowed signal is false here. Furthermore, two sensors are here detecting the same object. The two sensor detections are treated as separate objects by the program.

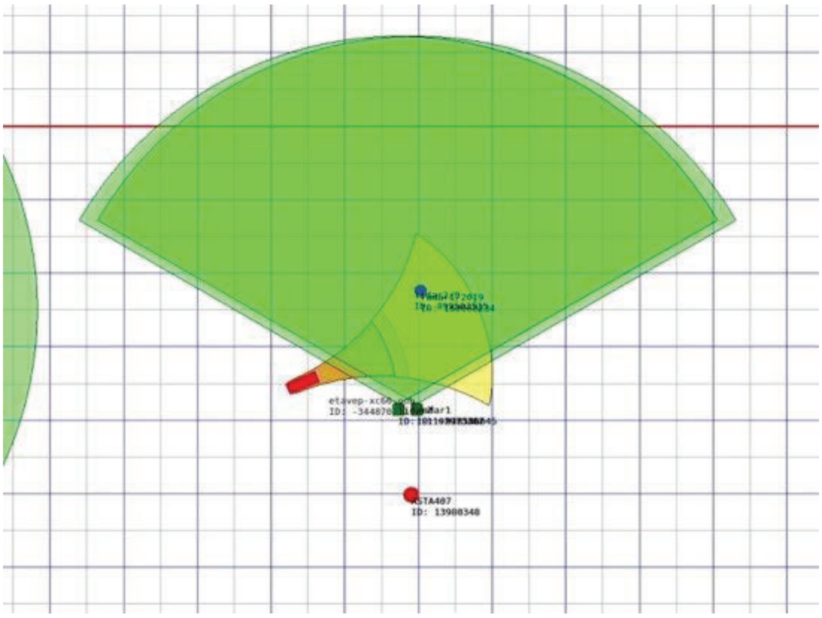


Figure 45 Sensor overlapping with safety zone

Communication setup

Communication is essential for the Traffic Control to work, and therefore it was decided to use a communication method that is reliable, easy-to-use and industry established, yet scalable. Hence, the MQTT (Message Queuing Telemetry Transport) messaging transport protocol. This protocol is used in m2m-applications (machine-to-machine) and in the IoT-context (Internet-of-Things).

The traffic control system applies a MQTT protocol for making information available between all parts. MQTT is based on a publish/subscription protocol where all clients in the system can *publish* and *subscribe* to *topics*, which enables the exchange of data. The information is published to a broker using a topic which then a client can subscribe to. Whenever a message is published on a topic, all clients subscribed to that topic will get a message with that information. This creates a scalable setup as none of the clients need to know the entire network setup, and only subscribe/publish to topics relevant to itself.

The system depicted in the figure uses a single MQTT broker, which all involved entities including the traffic control server are connected to. A client can be of type;

- Publish-only.
  Such as the external sensors or any vehicle that cannot be controlled.
- Publish + Subscribe.
  The normal case for a vehicle in the project
- Subscribe-only.
  Typically, a map display or an actuator of any type.

There are two MQTT brokers available in ETAVEP, see Figure 46. One physically and logically located at AstaZero and one available from any internet connection.

The AstaZero MQTT broker can only be accessed from the AstaZero networks, but the public broker can be accessed from anywhere.

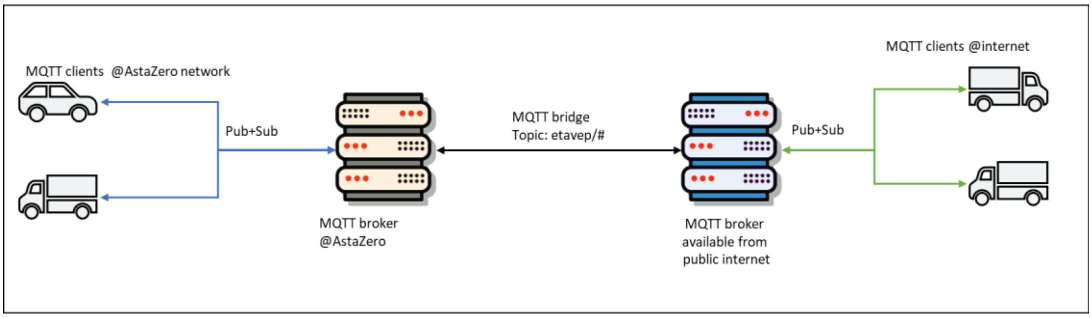


Figure 46 MQTT broker bridging

MQTT topics

The MQTT broker was physically located at AstaZero and the ETAVEP-project was using a unique ETAVEP-MQTT-topic not to be mixed with other data that might be transported through the broker.

SafetyZone-program

The software was developed using C++ and Qt 5.12 (graphical display toolkit) allowing the software to be compiled to most operating systems without much difficulty.

Based on the message information communicated via the MQTT broker the software construct a representation of the conditions on the test track. The software generates a drivingAllowed message with a frequency of 100 Hz, together with a time stamp which can be utilized as heartbeat information for safety, and the receiving vehicles should determine whether to brake based on the status of the signal.
The drivingAllowed status can be aggregated by several different stopping reasons and currently the stopping reasons implemented are whether an object is inside a given vehicle's safety zone or if that car is outside a lane as defined by an OpenDRIVE map.

Implementation of safety zones

The safety zone was generated according to the method described above using Qt's graphics library, as are the objects detected by "Monitoring of surroundings" task. When there is an overlap of a safety zone and another dynamic graphic element (e.g. Figure 45), the situation is determined unsafe, and a stop signal is sent. The check on whether a detection of an object lies within any vehicle's safety zone is performed at a frequency of 100 Hz.

Depending on the distance from the self-driven vehicle to an object, when it is detected, a brake level parameter inside the drivingAllowed message might be included. This part of the message is a percentual value which can be used by the receiving car to apply the brakes with the same ratio as specified in the value, which goes from 0% to 100%, and was calculated using a linear interpolation using the distance between the car and the detected object. As this distance decreases, the brake level percentage increases.

Implementation of how to detect vehicle path deviation

Given a GPS coordinate of a car, an OpenDRIVE file, i.e. a scanned map of the test track, can be used to determine if the point is within or outside of a specific lane. This was further enhanced by knowing the size, i.e. outer boundaries, of the vehicle, which can then be used to more accurately determine if a vehicle has deviated from a lane.

The heading of the vehicle was not considered for the check using OpenDRIVE, meaning that the lane check will allow cars driving in the wrong direction if they are within a lane.

This check was performed with a frequency of 100 Hz and done in parallel to the SafetyZone check.

Vehicle Control integration – safety stop information.

Finally, when all information has been aggregated and evaluated, communication with the vehicle has to be accomplished and, in case of an unsafe situation, a stop command has to be sent to the self-driven vehicle. For receiving a signal to stop the physical movement of a vehicle a dedicated hardware, Object Monitor Gateway (OMG), see Figure 47 and software Object Monitor Gateway Control (OMGC) was used and installed in the vehicle.

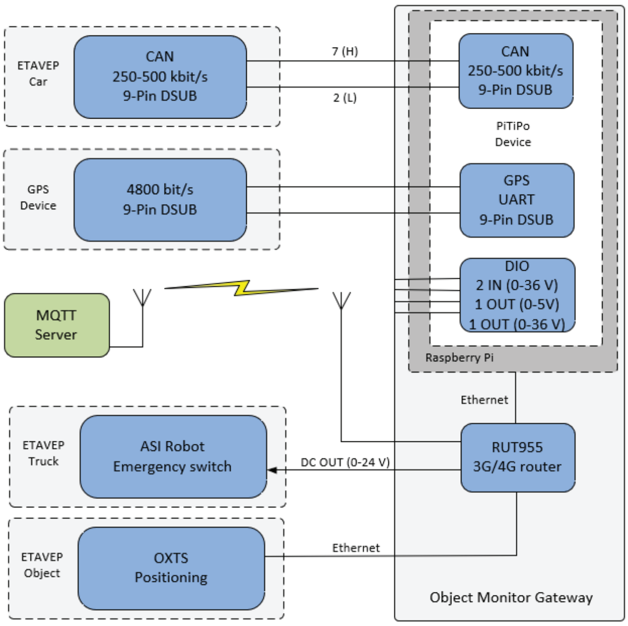


Figure 47 OMG and OMGC system

The OMGC unit is listening for the drivingAllowed status from the MQTT-broker and will generate either a CAN-frame or a DC OUT signal depending on the receiving system in the vehicle. See Figure 47, and when the drivingAllowed status is set to false this signal will trigger a brake of the vehicle.

Driving corridors

A concept to solve translation of traffic rules into logical information for use in the safety zone concept was subject to future research and sketched here as *driving corridors.* The main aim was to use information about the test track from track information layer to define driving corridors in which a vehicle is allowed to drive. The aim is that by ensuring that a vehicle remains within its corridor, it can be ensured that the vehicle follows the traffic rules. This does not only include lateral motions, but also longitudinal, e.g., checking whether self-driven cars slowdown in time for stopping at intersections when expected. Dynamically updating driving corridors according to the information of the track information layer (e.g., based on state of traffic lights) is out of scope and left for future work. Concerning the safety zone, driving corridors are important to make it less conservative and allow situations that are potentially challenging but desired, e.g., meeting at intersections or test cases for automatic emergency braking systems. 6 common cases are highlighted to illustrate the concept how driving corridors are used to determine priorities in intersections according to traffic rules from track information layer. See Figure 48 a-f.

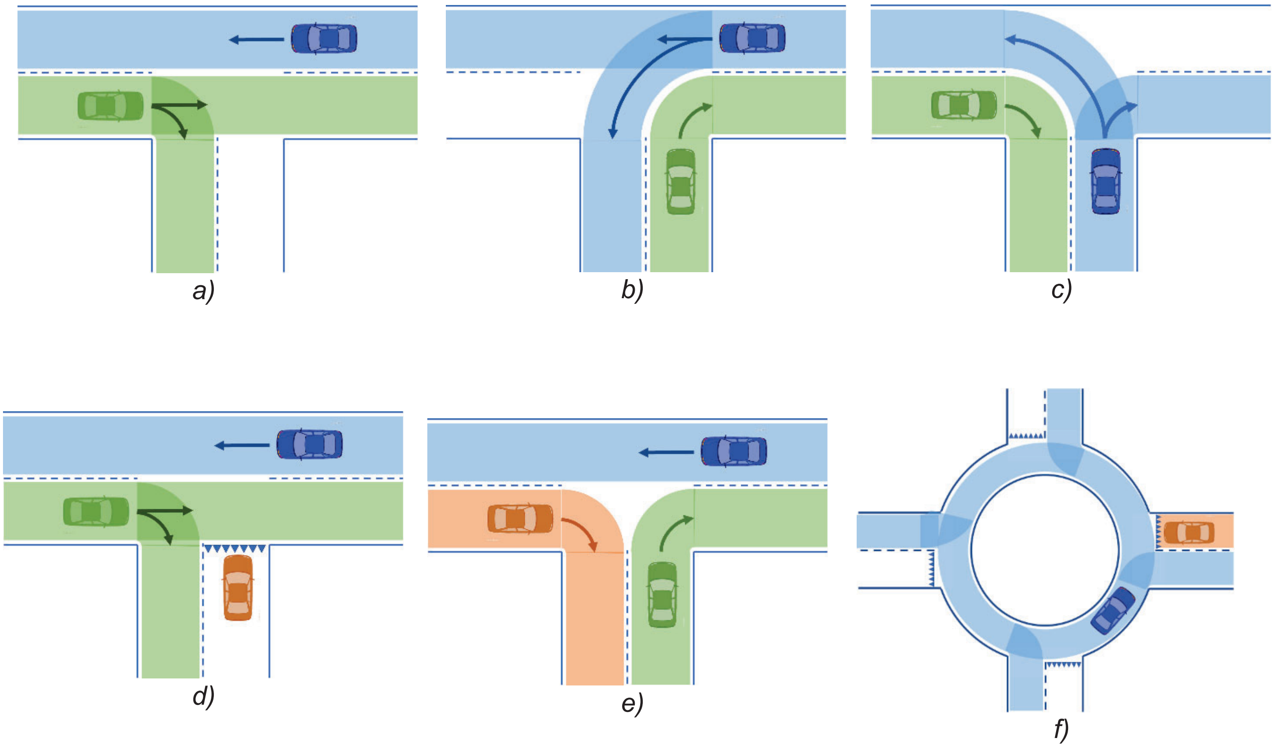


Figure 48 Examples of traffic situations in T-cross (1) to e) and roundabout (f)). The examples are further explained in the text

Figure 48 shows how different situations in a T-cross intersection including a special type of intersection, a roundabout, to illustrate how driving corridors can be used to make the safety zone-based traffic surveillance aware of traffic rules. At no time should driving corridors of different cars overlap. An overlap would create ambiguous situations and it would mean that the priority of the different participants cannot be decided based on applied traffic rules. In all cases, each vehicle should only apply its safety zone to its own driving corridor.
In summary, the safety zone concept presented is a solid basis for safe as well as effective testing of self-driven vehicles on existing proving grounds. The concept of driving corridors was proposed to be investigated further to make the solution of safety zone-based traffic surveillance less conservative and allow more effective testing.

Conclusions

The safety zone concept was well suited as a conservative outer bound on vehicle movement on areas where all such movement is also physically possible. With regards to stationary or slowly moving objects on open areas it is difficult to imagine a better solution. It captures the physically possible vehicle movements to the sides within a predefined horizon. The concept will be further refined in product development projects to reduce its interference on testing before being applied in a production setting. In this work, it will be necessary to test the system well, using a large amount of data to motivate the safety it provides.

Within the scope of ensuring presence of other traffic participants in a safety zone, causing a stop signal to be transmitted, the system shows adequate performance. The project demonstrations have shown that, in case there is an object in the safety zone, the vehicle has made a complete stop before any collision occurred. The same results have been demonstrated when any object has been detected by the surrounding sensors in the FOV circle sectors.

The scaling of the algorithm with multiple vehicles needs further investigation if the solution is to be implemented with only a single supervisory machine (in contrast to having dedicated on-board hardware for handling a single safety zone).

For areas where expected movement is more well defined (such as on a normal road with one lane on either side), the safety zone alone is overly conservative. While it is certainly true that even human drivers on a normal road could swerve into oncoming traffic, as captured by the safety zone, it is not likely. To formally guarantee the safety on such roads, physical barriers would be necessary everywhere, which is not feasible. In the same way that such barriers are not present on all roads, a certain level of risk must be tolerated also for testing but certainly based on maturity level of the test object. For further research there is a need to investigate what is described as driving corridors, representing the expected behavior of vehicles according to traffic rules. Intersecting the corridors with the safety zone would provide a less conservative basis for stopping a vehicle, which could be an acceptable middle ground between minimizing risk and enabling testing of vehicles. Again, the maturity level of the test object must be considered.

Due to the complexity of designing a system which monitors the adherence to traffic rules, these situations were excluded from the scope of this project in favor of the situations which could be handled by a strict system dynamic based monitoring and analysis of vehicle movement.

The MQTT based communication structure was well suited for the presented application due to the loose coupling it requires of, and enforces on, the participants. For example, replacing one sensor for another does not affect the implementation of other parts of the system.

Control of vehicles is limited to braking which is well motivated from a safety standpoint (lowering system energy). It is necessary that the control is implemented as a heartbeat with timestamps to counteract failure of the system to ensure safety due to e.g., network interruptions or long algorithm delays when several vehicles are present.

6.7 Proving Ground Design and Way of Working

Based on the initial work around risk assessments it stood clear to the project that one aspect of the system was missing. To perform testing of self-driven vehicles on test tracks, a number of supporting enablers also need to be put in place. Many of the risks had to be addressed to proving ground design and way of working.

The project investigated supporting enablers, to understand which of them needed to be addressed for making testing possible. Examples of such enablers are where human interactions should take place and how to design the test environment for safe operation. A number of workshops where experts covering different competence areas and experience participated created a fruitful environment for addressing the issues. The findings from the workshops were summarized and reviewed. As a result, checklists, guides, definitions and even proposals of how to improve the design of the proving ground have been delivered. It was decided to ignore technical limitations within the proof-of-concept and instead focus on an overall proving ground perspective. The reason for this was to make the result feasible to the proving grounds during and directly after the project. It was categorized into track definitions, personnel, vehicle, test preparations and emergency preparedness.

Track definitions

To use a test track for self-driven or mixed testing there are a lot of aspects to consider due to the actual track usage. The project has analyzed tracks from a general point of view but also more concise by analyzing the tracks High Speed Area at AstaZero and Durability Track at Hällered Proving Ground as examples, see Figure 49 and Figure 50. The outcome is presented in a checklist, see Table 5. Examples of aspects to consider:

- Definition of actual test area, it could be a geofenced part of track as well.
- Designating of official entrance and exit. Need to regulate other access roads.
- Speed regulations
- Locations for safe stops
- Locations where oncoming, overtaking and lane change is convenient/not convenient
- Need of one-way

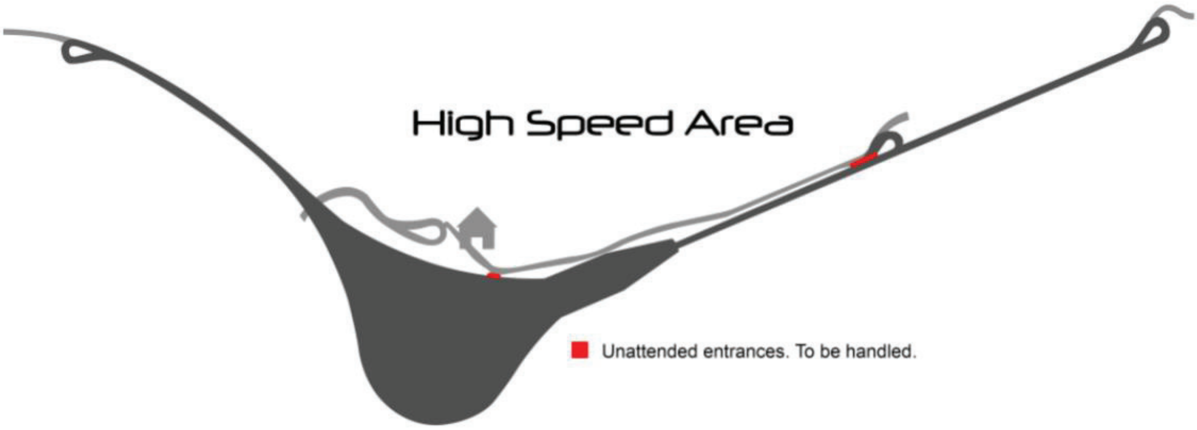


Figure 49 Unofficial access roads marked red on High Speed Area, AstaZero

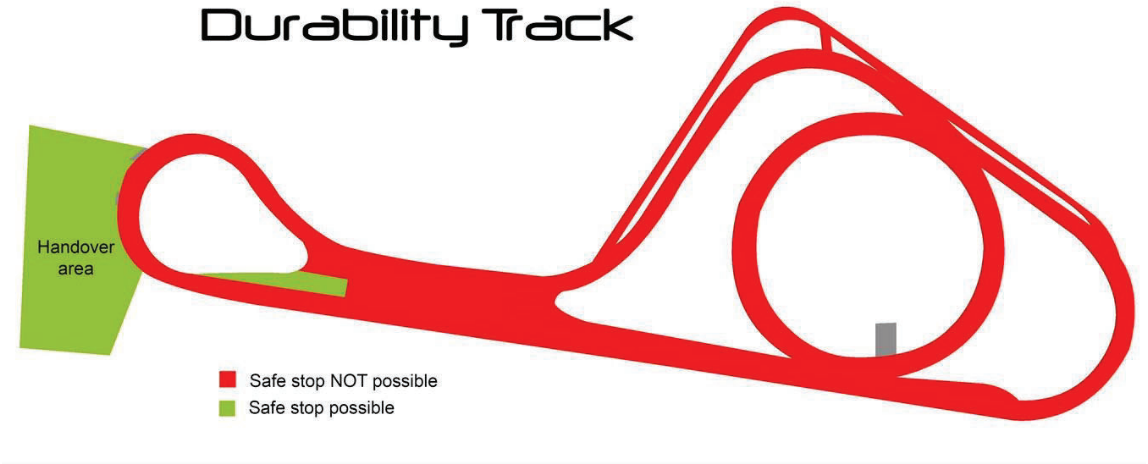


Figure 50 Safe stop concept at Durability Track, Hällered Proving ground

Personnel
It is of most importance that roles and responsibilities are clearly stated and communicated within the team. In the project clear role definitions have been made to further support structure and training for future personnel. Note, different organizations might have different point of view due to these roles. The communication of responsibilities and authorities is always crucial to maintain safety.

The term *Test Driver* is defined to be the person who is responsible for the control and safety of the vehicle under test even when the vehicle is operating in an autonomous mode. The test driver is situated in the vehicle, but not necessary in the driver's seat, during testing and is able to override autonomous operation of the vehicle at any time.

The *operator* oversees testing of a self-driven vehicle without necessarily being seated in the vehicle. In this case it is expected that a 'remote driver' would still be able to override autonomous operation of the vehicle at any time. The operator has the same responsibility as a test driver. The operator could have responsibility over more than one vehicle.

What training and permission needed for the roles will be the outcome from risk analysis on each test.

The project has investigated the responsibilities of the test driver and operator and found that the obligations are equal for both roles. Some examples follow:

- It is the responsibility of the test driver/operator to take full manual control if they feel the vehicle is maneuvering unsafely or in contravention of the prevailing road traffic regulation.
- The test driver/operator should remain alert and ready to intervene if necessary, and under no circumstances allow themselves to become distracted from the task of monitoring.
- Due to increased risk of fatigue and distraction, test driver/operator are required to take a reasonable break whenever doing extended continuous driving, regardless of whether driving is automated or fully manual. The risk assessment shall consider any such driving time limitations.
- If a fault in the vehicle occurs, the test driver/operator is responsible to communicate the type of fault to personnel in handover area or rescue patrol.

Vehicle Responsible is responsible for ensuring that the vehicle is properly equipped, in good condition and safe to send out onto the track.

Test Team Manager is defined to be the line manager who is directly accountable for the test driver/operator and who has the legal work environment responsibility over his/her employees. The test team manager should hold a full knowledge of the planned test activities and be experienced in the vehicle testing and risk assessment.

Vehicle

Changing vehicle mode to/from self-driven

When looking into the process of shifting a vehicle from manual to self-driven mode (and vice versa) visualization, physical location and work procedure was considered.

A visual indication of a self-driven vehicle is needed for traffic manager and the traffic management system. Preferable the self-driven vehicle has an AD icon on the overview screen. It is of outmost importance for the traffic manager to know who the operator responsible of the vehicle is, in case of communication requests.

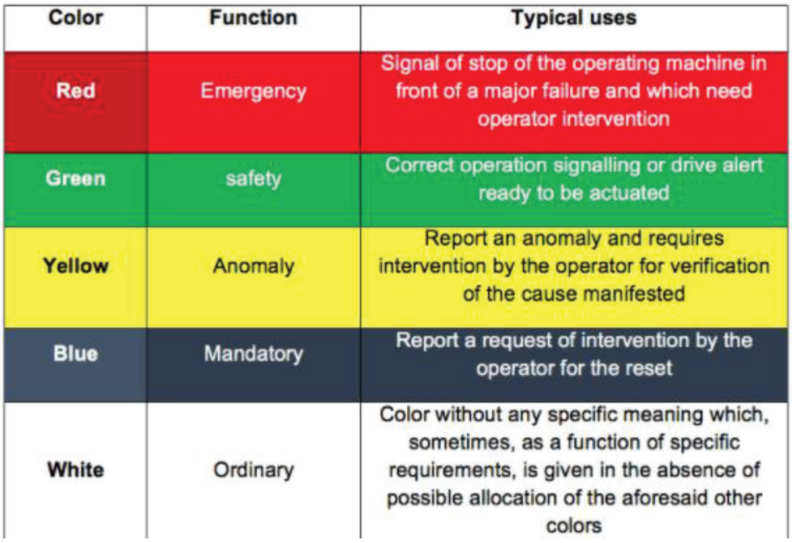
Figure 51 The design of the sign is agreed by a work group within European Proving Ground Safety Association in 2019

For other testers on the test track, magnetic signs can be useful as indication, see Figure 51. The sign should be used on self-driven vehicles with no safety driver, visual from all angles. The signs also need to be reflective to be visual in the dark. A vehicle with a safety driver onboard is to be consider as a manual driven vehicle (no sign). If the vehicle is to be various due to safety driver onboard or not the traffic manager needs to be informed when the sign is on and when it is off. The icon on the overview screen should be easy to change.

Figure 52 Examples of visualization of driving mode

The onboard safety driver must at any time know the mode of the vehicle. This can be done by a display or indicator lamp, see Figure 52.

A function that needs to be visualized outside the vehicle, is when it is in emergency stopped mode and considered safe to approach. There has been a lot of discussions about this visualization within the European Proving Ground Safety Association and it has been difficult to reach consensus due to color of lights, if they should flash. Figure 53 shows an example that the project finds distinct and hard to misunderstand. The project states that an indicator needs to be visual from 360 degrees of the vehicle, preferable on the roof of the vehicle if a car, a truck might need several indicators. It must show whether there is function or not. When designing this indicator standard (European Committee for Standardization, 2002) is recommended to use as a guideline as well as involving stakeholders. See Figure 53 for recommended colors. Note! The indicator procedure must be kept simple.



Color	Function	Typical uses
Red	Emergency	Signal of stop of the operating machine in front of a major failure and which need operator intervention
Green	safety	Correct operation signalling or drive alert ready to be actuated
Yellow	Anomaly	Report an anomaly and requires intervention by the operator for verification of the cause manifested
Blue	Mandatory	Report a request of intervention by the operator for the reset
White	Ordinary	Color without any specific meaning which, sometimes, as a function of specific requirements, is given in the absence of possible allocation of the aforesaid other colors

Figure 53 The color of the signal light towers, as defined in EN 60073 standard "Fundamentals and Safety for man-machine interface, marking and identification – Coding principles, indicators and actuators"

Figure 54 Warning sign

It is also important to inform people that are indirectly affected by the testing. Signs stating that self-driven vehicle testing can be carried out must be provided at the entrance to the test track, see example of sign in Figure 54.

The possibility to change between manual and self-driven mode differ from track to track. The proving ground management needs to make an assessment on each track. The project considers the change to, or from self-driven mode must be made while the vehicle is standing still. If the change is made during driving it must be a driver onboard. Then the vehicle can be considered as a manual driven.

For a track like the Durability Track a designated and fenced area for safety check and handover is needed, see Figure 55 An ordinary parking would not be safe enough. A handover area is not necessary if the usage of the test track is exclusively or if the track is designed in a way that allow each vehicle a lot of space (like High Speed Area). A defined handover zone could be needed in some tests.

Figure 55 Proposed design of handover area

In Figure 56 the procedure for a driverless vehicle that enters the handover area (referred to as HOA in the figure) and test track is presented. The project has also defined the steps for exiting the track. When the flow-charts were produced, the Durability Track was the model, but the outlines could be used for a total proving ground or a set of tracks, possibly with a modification of the design.

It is up to each proving ground to decide on regulations of the handover area and how to inform and educate people involved. Examples of regulations could be:

- To enter the handover area, you need a special safety training
- Never walk right in front or behind a vehicle
- Walking speed

It is likely that a handover area is camera monitored.

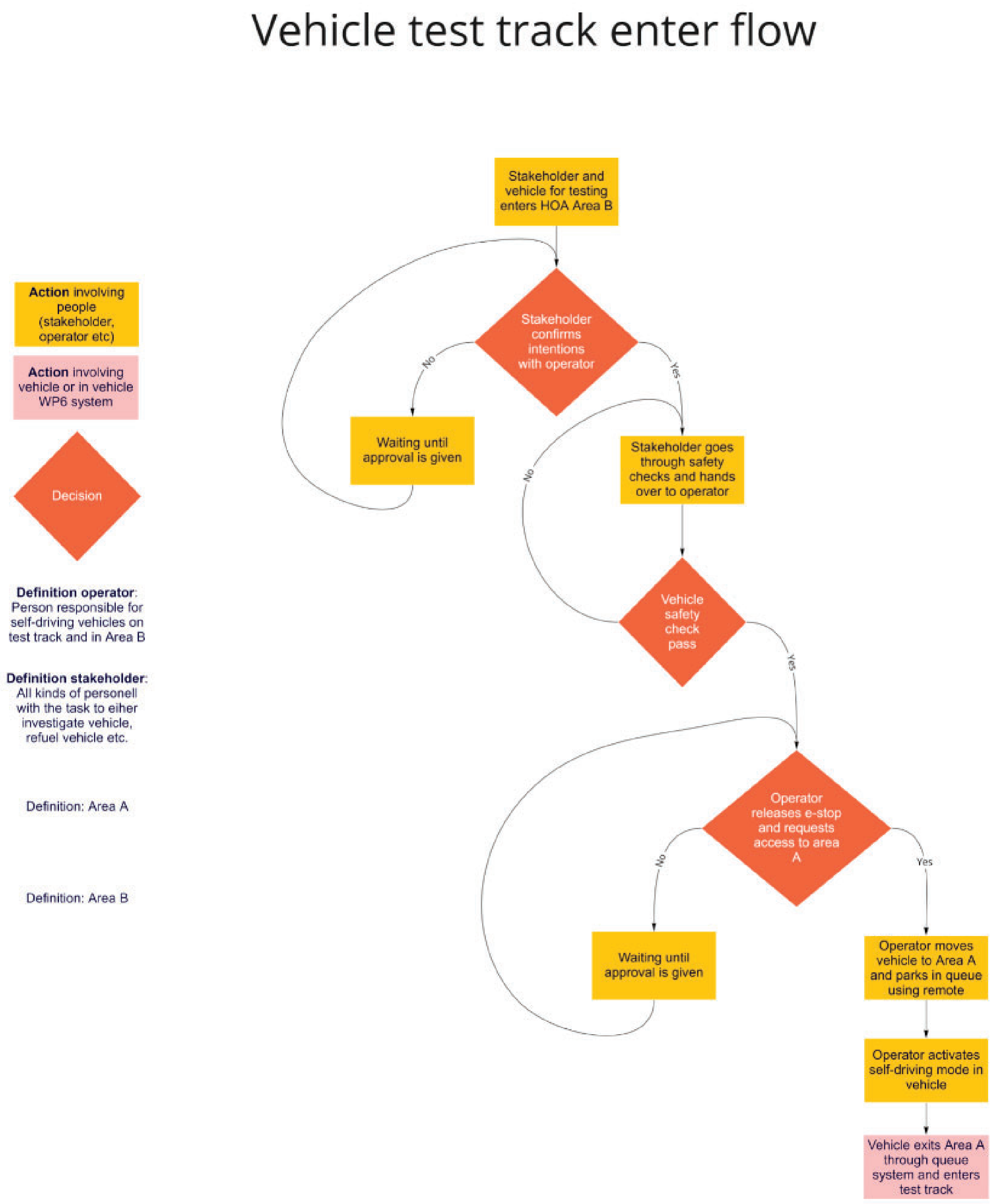


Figure 56 Flow chart showing vehicle entering test track

Vehicle inspection

For the safety of the test track to be secured and to make sure to find obvious faults in the vehicles, inspections need to be carried out before tests and on a regular basis. The project has looked into inspections and routines necessary and how the same routines could possibly differ between manually driven vehicles and self-driven vehicles.

For today's testing with skilled test drivers, it is established that test vehicle inspections vary due to the nature of test and vehicle. The type and length of test has a direct connection to whatever extent vehicle inspections are carried out with. The project finds the current vehicle inspection procedures, efficient and can be kept as recommendations with some amendments.

For the intended proof-of-concept, it is of absolute importance that a vehicle can be brought to a safe stop whenever a critical situation is given. For that there is numerous safety checks that needs to take place to ensure that the system is in fact capable to do so, as described in 0 Vehicle control. Additionally, a vehicle related part of the safety check should be added and carried out ahead of a self-driven vehicle is launched on the test track. The additional vehicle safety check part should include, but not necessarily limited to the basic roadworthiness check’s such as tire, brakes and steering system.

There might be faults introduced to the vehicle during updates, both hardware and software related, that is not recognized with the current inspection recommendations. Normally skilled test drivers should recognize these kinds of malfunctions. Even if the safety solutions implemented in ETAVEP will bring a malfunctioning vehicle to a safe stop, it is primarily considered to be a safety fallback system rather than a system designed for continuous operation which would also decrease efficiency on the test track. Also, it is of high importance for stakeholders that vehicles are tested in the correct vehicle status to gain relevant results. How an additional check due to updates should be designed depends on what kind of update or change has been done to the vehicle but could include software read-out, actual measurement on the vehicle, close monitoring of vehicle data during initial testing or whatever is found relevant from case to case.

Optional to the vehicle safety checks, possible additions should be investigated. It is recommended that the type of test, vehicle type as well as current risk assessment should be used as foundation when optional vehicle safety check is chosen.

Remote control

In certain situations, a remote-controlled movement of vehicle is needed. Remote control could be performed either from a remote location or it could be performed walking next to the vehicle, carrying the necessary controls. Remote driving could be used for transporting vehicles from workshop to test track, in handover area or when the self-driven functionality is not working. Remote Control is defined as open loop control of vehicles steering, throttle and brake capacity with the highest achievable speed allowed of 7 kph.

When remote control takes place, it is of great importance that it is executed in a safe manner. The project has investigated the enablers for safe operation and propose following: It should be done by trained operator. The speed should be limited to <7 kph. Further on the remote driving should only take place in areas approved for the purpose or in special cases after approval from traffic manager. An operator should not remote control more than one vehicle at a time. The operator needs to have 360-degree visual view of vehicle surroundings and if controlling from a remote location, a map position view of vehicle’s current position that includes other vehicles and relevant infrastructure.

Test preparations

Risk assessment of test with self-driven vehicles

The risk assessment (also referred as risk analysis) is a fundamental tool for the proving grounds, with or without self-driven vehicles operating on the tracks. The project has analyzed the risk assessment procedure to find what differs analyzes of self-driven tests from todays' test. The project has leaned against the outcome from risk analysis at many points during the work.

Success factors for risk analysis of self-driven tests:
- The risk assessment work needs to be specific, realistic and solution-oriented
- More extensive risk assessment should be split into several occasions
- Frequently follow-up of the assessments
- Involve different areas of expertise
- The risk assessment procedure needs to be improved and built on continuously as self-driven vehicles become more common on test tracks. In the future shared knowledges and experiences provide a solid foundation in risk assessment work with self-driven vehicles.

Examples of where output from risk assessment are required. When deciding
- extensiveness and frequency of vehicle safety check
- level of drivers' proficiency including training and license for new type of test
- work procedures for operators due to fatigue, boredom, breaks, duration of work shift
- number of vehicles allowed on test track
- speed regulations for a test type and/or specific test track

Test track regulations and processes

A proving ground normally has a setup of regulations and processes to maintain safety on the tracks. When starting up self-driven or/and mixed testing these rules need to be considered due to the new conditions that self-driven vehicles bring. Each track, set of vehicles and test might need special safety measures. This could be adjusted vehicle safety checks, extra training for test drivers, procedures to enter a test area, additional information in the check in procedure and so on. The project has observed existing rules of a proving ground and suggested amendments due to self-driven vehicle tests. Some examples are

- A sign or lamp indicating that the vehicle is in self-driven mode is required
- One shall never drive to close or aggressive towards a self-driven vehicle
- All remote driving of self-driven vehicles out and back from the test tracks shall be approved by traffic manager
- When driving self-driven vehicles remotely, you must only handle one vehicle at a time
- Pedestrians/manual vehicles should pay attention to self-driven vehicles and not go/drive out in front. Common traffic rules apply but self-driven vehicles take precedence over pedestrians.
- Signs that self-driven testing can be carried out must be provided at the entrance to the respective track

Information before test start - Booking and check-in

Before taking a self-driven vehicle into test it needs to be ensured that a risk assessment is conducted, that staff has the proper education and experience to handle the test and that the test is reasonable due to number of vehicles, maneuvers and speed. Further it also needs to be stated whether the vehicle is driven with or without safety driver, how the vehicle is transported to the actual test track and that the test is placed on a suitable test track or in a geofenced zone. The team around a self-driven vehicle needs to be appropriately staffed to be able to consider safety aspects and backup person for critical steps must be appointed and present.

At the check-in, the test team announces the roles they have so that the test track staff and traffic manager are aware of this. It is important that the traffic manager can communicate with the right persons e.g test leader or safety driver. That this is announced each time by the test team at check-in is an assurance that nothing has changed, and that misunderstanding can be avoided. If the roles changes during the test the test leader should be responsible to inform the traffic manager immediately.

If a vehicle is to be changed from manned to unmanned (or the opposite) during the day, the test team must notify the traffic management. Traffic management always has the right to approve or reject these changes for safety reasons.

Emergency preparedness

The project has investigated the emergency preparedness of a proving ground. This can be divided into systemic preparedness and remedial preparedness. The systemic is about what happen if the system loses contact or power. The remedial is more about how to handle an emergency stopped vehicle due to rescue operations.

In summary it is important for the proving ground to have clear routines and that staff is prepared to handle the situations that might occur. What differs from manually driven vehicles is mostly the aspect of how to safely approach an self-driven vehicle that has stopped.

When it comes to the ETAVEP-system, instructions for systemic emergency preparedness covering a large number of potential emergencies that could occur i.e., total power failure, loss of contact to vehicles, accidents etc. have been established by the project. Examples can be seen in Figure 57.

Power failure of proving ground

The traffic manager communicates to everyone in the proving ground that there is a power outage and requests all testing to be stopped and wait for further information. If there is a longer power outage, the traffic manager must decide how the test teams safely can leave the track. A power backup with batteries is required.

Loses or inadequate contact with individual vehicle

If traffic control loses contact with an individual vehicle, the traffic controller contacts the operator and announces that they must end the test and drive slowly to the first safe stop and wait until the fault has been rectified. If the traffic manager deems that all testing needs to be stopped for safety reasons, the traffic manager must do so.

Figure 57 Examples of systemically emergency preparedness instructions

Conclusions

Self-driven and mixed testing raises a lot of questions due to the interface between (wo)man and machine and the proving ground design. The project has successfully analyzed the need and delivered a specific checklist, instructions, definitions and design proposals. It is always the actual test, vehicle and track that decide safety measures needed. The risk analysis is together with the outcome from ETAVEP a fundamental tool. When all result was compiled, it was summarized in a checklist, see Table 5. This checklist can be used when to take a track into use for self-driven or mixed testing. It could be a brand-new test track, but it could also be an existing track that is to be used in a new way. The checklist will be used to support construction and implementation of new test tracks at AstaZero and Hällered Proving ground.

The routines developed by the project are now ready to be used in testing and further development by the partners within ETAVEP. Much of the result is already put in use like the risk assessment, the vehicle inspection and the procedure that regulates how the test team communicate whether there is a safety driver onboard or not. The icon that indicates self-driven vehicle in the traffic manager interface is used on daily basis.

Table 5 Before taking test track with self-driven testing into use

✓	**Checkpoints**	**Notes**
	Test track defined. Where are the edges? Need of geofence?	
	Vehicle type defined (Is other traffic allowed in the test area?)	
	Maximum number of vehicles defined	
	Official entrance and exit defined. Are there any other or unofficial entrances/exits?	
	Speed limits defined	
	Zones for safe stop defined	
	Zones for one way traffic defined. Need of regulation to change driving direction?	
	Zones for oncoming/not oncoming defined	
	Zones for overtaking/not overtaking defined. Actions for minimizing need of overtaking?	
Yes/No	Are there situations where an operator needs to make decision? Eg entrance, crossing, certain moment…	
	Need of stationery and/or vehicle mounted supervision defined	
	Roles and responsibilities within the test team defined and communicated	
	Procedure for changing self-driven/manual mode established. 1. Visualization 2. Location 3. How is it done?	
	Procedure for vehicle inspection established	
	Procedure for check of safety system (ETAVEP system) established	
	Procedures for remote driving established. Where? How? Who?	
	Risk assessment conducted for vehicle, track and test	
Yes/No Yes/No Yes/No	Existing proving ground regulations enough? Any additional safety measurements needed? Communicated within the test team?	
Yes/No Yes/No Yes/No	Any special check-in procedure? Is the vehicle likely to change between manned/unmanned? Any additional safety measurements needed?	
	Emergency procedure established. Accident, system failure…	
	Procedure to safely approach an emergency stopped vehicle established	

6.8 Summary

By merging the different project parts, defined as a layer-based framework, see Figure 58, to form the proof-of-concept, the project has shown that it is possible to enable self-driven vehicles to operate in a mixed traffic environment at existing proving grounds in a safe way.

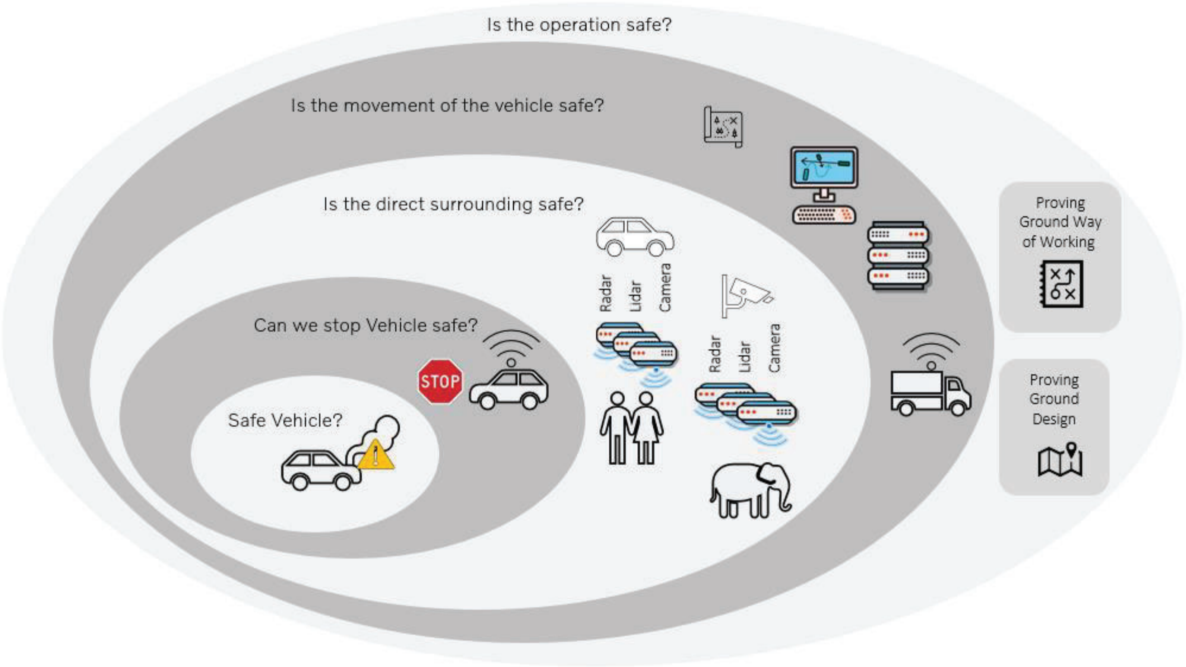


Figure 58 Layer-based framework of how to enable safe operation

It is important to understand the system by having the right training, information and procedures. The findings showed that slight adjustments can lead to unforeseen events. To verify the condition of the vehicle an algorithm have been developed to detect non-trivial mechanical faults, using a non-parametric Local Rational Model algorithm. The algorithm was able to differentiate if the vehicle had any faults through verification at the proving ground with actual faults injected. The vehicle stop functionality was ensured by using two standalone brake systems to guarantee stop functionality at all times, and complete redundancy for faults like power failure and communication loss for a vehicle under risk. Extensive testing of the vehicle stop functionality proves that the system is both reliable and responsive. To be able to distinguish pedestrians, vehicles or other objects in proximity to the self-driven vehicle, external sensors were integrated to guarantee a safe environment. The sensors were tested at the proving grounds with both vehicle mounted and stationary mounted sensors to ensure sufficient detection capability. The traffic control utilizes the safety zone concept showing the potential to make sure safety is not compromised. This have been tested at the proving ground by multiple scenarios. If there are vehicle faults or objects in close proximity to the vehicle the traffic control sends a stop signal. To ensure the operation stay safe, guidance and routines concerning proving ground design and way of working needs to be adjusted and promptly followed.

7 Dissemination and Publication

7.1 Dissemination of Knowledge and Results

The dissemination of knowledge has been done by publication in two scientific journals and three Conferences. The ETAVEP is an associated project to SAFER. Furthermore, the project has had several meetings during its duration by coordinator and partners during to internal and external audience, at which it has generated great interest, among others with SAE. During the project two demonstrations have been hosted.

How are the project results planned to be used and disseminated?	Mark with X	Comment
Increase knowledge in the field	X	ETAVEP has largely increase the knowledge level of how self-driven vehicles can be tested on proving grounds as its whole not only for mixed traffic.
Be passed on to other advanced technological development projects	X	The work within ETAVEP has not yet be passed onto new projects but there are several areas considered
Be passed on to product development projects	X	Sub-systems of ETAVEP are planned to be implemented in the industry of testing vehicles.
Introduced on the market		
Used in investigations / regulatory / licensing / political decisions		

The project hosted workshop: Safety for Testing self-driven Vehicles at Existing Proving Grounds at the 9th Scandinavian Conference on System & Software Safety (SCSSS) on the 24th of November in Gothenburg

7.2 Publications

McKelvey, T., McKelvey, D., & Nordberg, P. (2021). A Multivariate Local Rational Modeling Approach for Detection of Structural Changes in Test Vehicles. *IFAC-PapersOnLine*, *54*(7), 79-84.

Sjudin, J., Marcusson, M., Svensson, L., & Hammarstrand, L. (2021, November). Extended object tracking using sets of trajectories with a PHD filter. In *2021 IEEE 24th International Conference on Information Fusion (FUSION)* (pp. 1-8). IEEE.

Hjelm, H. (2020). Object free area estimation using a LiDAR sensor in rough terrain, Department of Electrical Engineering Chalmers University of Technology

McKelvey, D., 2022 (submitted), Detection and monitoring of mechanical faults in vehicles using multivariate—frequency domain—transfer function estimates, Department of Electrical Engineering Chalmers University of Technology

Krantz, S., & Östberg, P. (2021). Lidar rörelsedistorsionsfiltrering Punktmolnsfiltreringssytem för bilar i realtid, Department of Electrical Engineering Chalmers University of Technology

8 Conclusions and Future Research

The ETAVEP project has presented a proof-of-concept that showed it is possible to integrate self-driven vehicle testing into existing proving ground environments. The proof-of-concept covers vehicle speed up to 80 kph and is independent of vehicle types, maturity, road type and weather (excluding snow). The project has been able to answer four of the five research questions. The fifth, "*What is a sufficient set of test cases for validating concepts that have been developed to address 1-4?*" Was not answered fully in the project. The question showed to be far too vast to be fitted into the project, but the question was partly answered as the project was able to verify the concepts using the outcome from the risk assessments done.

Further the project has shown that more research needs to be made within the area to enhance performance, robustness, safety and reliability. Future topics covering:

- How to validate a supervision system of self-driven vehicles combined with human driven vehicles?
- How can virtual geofencing be done and what reliability level is needed to be able to say the system is safe?
- How can traffic rules be translated into context dependent and supervised sections of the road in which the vehicle is allowed to move?
- How to detect abnormal behavior of a vehicle from "anonyme vehicle data" to prevent accidents?
- Can centralized track fusion in traffic control improve the robustness and reliability?

The project has been an essential key for Swedish industry to launch self-driven vehicles without risking safety. It contributes to the "Zero Vision" target and increase the Swedish capacity for research and innovation. ETAVEP has not only advanced the development of autonomous testing environments but has also allowed the partners to remain at the forefront in this field.

9 Contributing Partners and Contacts

The project partners were AstaZero, Chalmers University of Technology, RISE, SafeRadar Research, Volvo Cars and Volvo Group.

Organization	Contact Person
AstaZero	Jenny Viklund
Chalmers	Tomas McKelvey
RISE	Marvin Damschen
SafeRadar Research	Johan Degerman
Volvo Cars	Arvid Pearson
Volvo Group	Romain Klein

The Project was run as an associated project within SAFER, Vehicle and Traffic Safety Centre at Chalmers.

10 References

Arbetsmiljöverket. (2008). *Arbetsmiljöverkets förskrifter om maskiner (2008:3).*

European Committee for Standardization. (2002). *Basic and safety principles for man-machine interface, marking and identification - Coding principles for indication devices and actuators (IEC Standard No. 60073:2002).*

International Electrotechnical Commission. (2016). Industrial communications network – Functional safety fieldbuses (IEC Standard No. 61784-3-13:2016).

International Organization for Standardization. (2013). *Road vehicles – Environmental conditions and testing for electrical and electronic equipment - Mechanical loads (ISO Standard No. ISO16750-3:2013).*

International Organization for Standardization. (2015). *Safety of machinery — Emergency stop function — Principles for design (ISO Standard No. ISO 13850:2015).*

International Organization for Standardization. (2015). *Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design (ISO Standard No. 13849-1:2015).*

International Organization for Standardization. (2018). *Road vehicles — Functional safety (ISO Standard No. 26262:2018).*

International Organization for Standardization. (n.d.). *Road vehicles — Test object monitoring and control for active safety and automated/autonomous vehicle testing — Functional requirements, specifications and communication protocol (ISO Standard No. ISO/AWI TS 22133).* Retrieved April 12, 2021, from ISO/AWI TS 22133.

Jacobson, B. (2020). *Vehicle Dynamics Compendium.*

Johnson, T. J., & Adams, D. E. (2002). *Transmissibility as a differential indicator of structural damage. J. Vib. Acoust., 124(4), 634-641.*

McKelvey, D. (2022). *Detection and monitoring of mechanical faults in vehicles using multivariate—frequency domain—transfer function estimates, Master Thesis, Department of Electrical Engineering Chalmers University of Technology and University.*

McKelvey, T., & Guérin, G. (2012). *Non-parametric frequency response estimation using a local rational model. IFAC Proceedings Volumes, 45(16), 49-54.*

McKelvey, T., McKelvey, D., & & Nordberg, P. (2021). *A Multivariate Local Rational Modeling Approach for Detection of Structural Changes in Test Vehicles. IFAC-PapersOnLine, 54(7), 79-84.*

PEGASUS, Mazzega, J., Lipinski, D., Eberle, U., Schittenhelm, H., & Wachenfeld, W. (2019, May 14). *PEGASUS METHOD.*

SAE International. (2014). *Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems, s.l.: SAE International.*

Shalev-Shwartz, S., Shammah, S., & Shashua, A. (2018). On a Formal Model of Safe and Scalable Self-driving Cars. *ArXiv170806374*. Retrieved from http://arxiv.org/abs/1708.06374

Weber, H., Bock, J., Klimke, J., Roesener, C., Hiller, J., Krajewski, R., . . . Eckstein, L. (den 12 June 2019). A Framework for Definition of Logical Scenarios for Safety Assurance of

Automated Driving. *Traffic Injury Prevention, 20*(sup1), S65-S70. doi:10.1080/15389588.2019.1630827

Viklund, J. (2019). *Prestudy - Safety self driving vehicles (SAE level 4/5) at AstaZero.* Retrieved March 10, 2022, from https://www.vinnova.se/en/p/prestudy---safety-self-driving-vehicles-sae-level-45-at-astazero/

Voorhoeve, R. v. (2018). *Non-parametric identification of multivariable systems: A local rational modeling approach with application to a vibration isolation benchmark. Mechanical Systems and Signal Processing, 105, 129-152.*

11 Appendix

11.1 Appendix: Use cases broken down into scenarios

Regulated intersection (gates, give way, stop, traffic light)

- T-intersection with obligation to give way, max speed 30, 50 or 80 kph
- Four-way intersection, right of way and give way, max speed 30, 50 or 80 kph
- Roundabout, four connections, max speed 30 kph
- Pedestrian crossing

Non-regulated intersection (any angle)

- High Speed Area, not under test
- Vehicles approaching from unofficial roads

Elevated roads

- Elevated roads, up to 80 kph

Following lane including curves and slopes

- Catching up, vehicle in front brakes
- Catching up, constant speed
- Catching up, stationary object
- Catching up, accelerating
- Single vehicle drives in lane
- Vehicle drives at the same speed as vehicle in front

Lane change/merge (up to 4 lanes)

- Cut in scenario, faster vehicle in the right lane
- Cut in scenario, slower vehicle in the right lane
- Cut in scenario, both vehicles at the same speed
- Cut out scenario
- Lane merge of two lanes, no one with obligation to give way
- Cut in, dual lanes
- Lane change, single vehicle

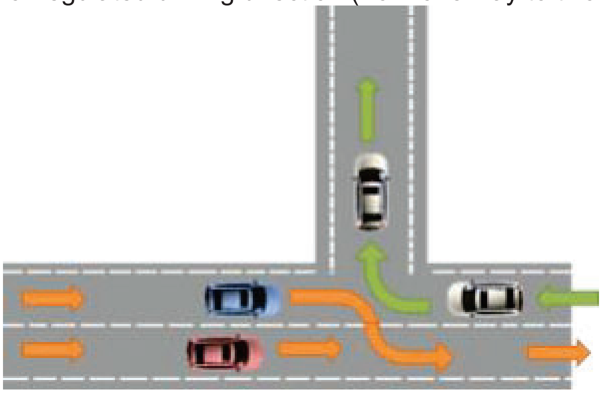
Overtaking (up to 4 lanes)

- Overtaking, using the oncoming lane
- Overtaking of stationary object, using the oncoming lane
- Overtaking in separate lanes, no lane change involved
- Overtaking of slow-moving vehicle. Slow-moving vehicle occupies more than one lane

Oncoming

- Oncoming, straight forward, 30, 50 or 80 kph
- Oncoming, curve, 30, 50 or 80 kph
- Oncoming of vehicle that occupies more than its own lane, 30 kph
- Oncoming of vehicles on a road where there is not space enough to meet, max 30 kph.

Change of regulated driving direction (from one way to two way)



Change of driving direction (from forward to reverse)

- From forward to reverse, no vehicle behind
- From forward to reverse, with vehicle behind
- From reverse to forward, no vehicle in front
- From reverse to forward, with vehicle in front

Test area collaboration

- Share the same test track with geographical separation
- Share the same test track, drive alternately (e.g., slots)
- Share the same test track, ad hoc usage

Special events

- Special tracks like “Figure of Eight”
- How to hand over a self-driving vehicle to maintenance staff, e.g., low fuel status
- Self-driving vehicle get an unexpected stop on track and needs to be towed away
- Complementary risk aspects from a current risk assessment made by AB Volvo