Functional Safety in Systems of Road Vehicles

Jan Jacobson, Christian Grante (Viktoria Institute) et al.
Functional Safety in Systems of Road Vehicles

Jan Jacobson, Christian Grante (Viktoria Institute) et al.
Abstract

Architectures for communication between road vehicles and road infrastructure are under development. The new applications made possible by advanced communication create new opportunities and new safety challenges. The functional safety aspects so far considered for single vehicles have to be considered also for cooperative systems of road vehicles. The report is the result of a study identifying needs and giving examples of some models which can be applied.

Key words: cooperative systems, functional safety, communication, road vehicle

SP Sveriges Tekniska Forskningsinstitut
SP Technical Research Institute of Sweden

SP Report 2010:07
ISBN 978-91-86319-43-4
ISSN 0284-5172
Borås 2010
# Contents

**Abstract** 4

**Contents** 5

**Preface** 7

**Summary** 8

1 **Introduction** 9

2 **Functional Safety** 11
   2.1 Approaches for functional safety 11
   2.2 Standards for functional safety 11
   2.3 Risk and hazard classification 13
   2.4 How to develop safe and reliable control systems 14

3 **Cooperative architectures** 17
   3.1 Architectural Types 17
   3.1.1 Ad hoc architecture 17
   3.1.2 Centralized architecture 18
   3.1.3 Hybrid architecture 19
   3.2 Summary 20

4 **Applications of cooperative systems** 22
   4.1 Example A: Platooning 22
   4.2 Example B, Road maintenance 23
   4.3 Example C, Intersection 24
   4.4 Example D, Traffic accident 25

5 **Functional safety challenges in cooperative systems** 27
   5.1 Design using ad hoc architecture 27
   5.2 Design using hybrid architecture 29
   5.3 Design using centralized architecture 30
   5.4 Implications regarding the examples and architectures 32
   5.5 Functional safety implications in cooperative systems 33
   5.5.1 Decision-making process 33
   5.5.2 Local or remote decisions and information 34
   5.6 Architecture for cooperative systems 35

6 **Future work** 37

Annex A **References** 39
   A.1 Platooning 39
   A.2 Standards 39
   A.3 Functional safety 40

Annex B **Terminology** 41
   B.1 **System** 41
   B.2 **Function** 41
   B.3 Safety 41
   B.4 Risk 41
   B.5 **Scenario** 42
   B.7 Traffic situation 42
<table>
<thead>
<tr>
<th>B.8</th>
<th>Cooperative systems</th>
</tr>
</thead>
</table>

**Annex C  Project proposals**

<table>
<thead>
<tr>
<th>C.1</th>
<th>Risk assessment</th>
<th>44</th>
</tr>
</thead>
<tbody>
<tr>
<td>C.2</td>
<td>Functional Safety in Open Cooperative Systems</td>
<td>45</td>
</tr>
<tr>
<td>C.3</td>
<td>Techniques and Methods</td>
<td>46</td>
</tr>
<tr>
<td>C.4</td>
<td>Improved safety and traffic efficiency in road maintenance site</td>
<td>47</td>
</tr>
<tr>
<td>C.5</td>
<td>Safe control of cooperative vehicles in roundabouts</td>
<td>48</td>
</tr>
</tbody>
</table>
Preface

Functional safety is one of the competence areas of SAFER, the Vehicle and Traffic Safety Centre at Chalmers. Functional safety in cooperative systems of road vehicles has been identified by SAFER and its industrial partners as a potential research topic. Communication between vehicles and between vehicles and the road infrastructure has been in focus for several large European research initiatives. Functional safety of individual road vehicles is addressed both by international standardisation and by the automotive manufacturers. Research has not yet thoroughly considered the functional safety aspects for systems of road vehicles.

SP Technical Research Institute of Sweden and the Victoria Institute have carried out this study of the topic of functional safety and systems of road vehicles. This report is based on a series of workshops and with contributions from the following authors:

Carl Bergenhem, SP
Christian Grante, Viktoria
Anders Hjalmarsson, Viktoria
Jan Jacobson, SP
Mikael Lind, Viktoria
Josef Nilsson, SP
Stefan Pettersson, Viktoria
Fredrik Svahn, Viktoria
Rickard Svenningsson, SP
Jonny Vinter, SP

The prestudy has been financed by RISE Research Institutes of Sweden.
Summary

Communication between vehicles and between vehicles and the road infrastructure will soon be common. Safety can be increased by for example instant information about road conditions or exchange of information when a crash is imminent. New vehicle functions may, however, introduce new risks if not carefully designed. There are always risks for human mistakes in specifications. Embedded electronics and software may fail in an unexpected way. This makes it necessary to consider also the functional safety of the cooperative systems.

Functional safety can be defined as “...the absence of unreasonable risk due to hazards caused by malfunctioning behaviour of electric/electronic systems” for road vehicles. Examples of new functions with functional safety requirements are platooning, intersection guidance and warning systems at road maintenance and accidents. There is now a need to consider functional safety also for systems of road vehicles. The dependability of the cooperative systems has to be demonstrated.

The architecture of a cooperative system will have significant influence on system functionality. This report describes three architecture types: ad hoc architecture, centralized architecture and hybrid architecture.

The techniques and measures applied for individual vehicles will not suffice for systems of road vehicles. New models will have to be developed. The report proposes future work to develop methodology for functional safety in systems of road vehicles.
1 Introduction

Wireless communication capabilities will soon exist in all new road vehicles. Exchange of information between vehicles and between a vehicle and the infrastructure will make new functions possible. Safety can be increased by for example instant information about road conditions or exchange of information when a crash is imminent. Travel can be made more efficient by speed adaptation and route selection based on the traffic situation. The environment will benefit from smoother traffic with less congestion.

It is easy to find examples of applications where the benefits of cooperative systems have to be balanced against the potential new risks. Road trains (“platooning”) of vehicles will give benefit to efficiency and to the environment, but must not allow failures of a single vehicle to endanger safety of all vehicles in a road train. Warning systems at traffic accidents and at road maintenance will save lives, but must not give false alarms. Cooperative systems in intersections might allow smooth traffic without the need of traffic lights, but the requirements for the reliability of the signalling system will be high.

Several research projects have demonstrated the possibilities of vehicles communication both on national and European level. The SAFESPOT project [http://www.safespot.eu.org] is working to design cooperative systems for road safety based on vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communication. SAFESPOT will prevent road accidents by developing a “Safety Margin Assistant” to detect in advance potentially dangerous situations and extend, in space and time, drivers’ awareness of the surrounding environment.

The COOPERS project [http://www.coopers-ip.eu] focuses on the development of innovative telematics applications on the road infrastructure with the long term goal of a “Co-operative Traffic Management” between vehicle and infrastructure, to reduce the gap of the development of telematics applications between car industry and infrastructure operators.

One of the objectives of the CVIS project [http://www.cvisproject.org/] is to create a unified technical solution allowing all vehicles and infrastructure elements to communicate with each other in a continuous and transparent way using a variety of media and with enhanced localisation.

The GST project [http://www.gstforum.org/] is creating an open and standardized end-to-end architecture for automotive telematics services. The purpose of GST is to create an environment in which innovative telematics services can be developed and delivered cost-effectively and hence to increase the range of economic telematics services available to manufacturers and consumers.

![Figure 1. Functions and functional safety are both necessary in cooperative systems](image-url)
The prime concern when introducing new automotive technology is to show that the technical concepts are sound and cost-efficient. There must be a user acceptance and the intended benefits must be demonstrated. The safety aspect is also to be considered. New vehicle functions may introduce new risks if not carefully designed. There is always the possibility that mistakes are introduced in the specification due to human error. Embedded electronics and software may fail in an unexpected way. This makes it necessary to consider also the functional safety of the cooperative systems. (Figure 1.)

Functional safety is addressed for a system, e.g. a car, a truck, an industrial robot or a medical device. A system comprises of a set of elements, at least sensor, controller, and actuator, in relation to each other in accordance with a design. But a system can be regarded at different levels. A vehicle is considered as a system, but the elements of the vehicle may also be systems in themselves. Examples are the engine control system, the airbag system, the entertainment system and the seatbelt system of each passenger. An element of a system can be another system at the same time. A cooperative system of road vehicles contains several individual vehicles.

Functional safety has so far been considered for individual road vehicles. With increasing communication between vehicles and between vehicles and the infrastructure, there is now a need to consider functional safety also for systems of road vehicles. The dependability of the cooperative systems has to be demonstrated.

An example a safety considerations for cooperative systems is if vehicle actions should be allowed to be requested by other vehicles or by the infrastructure. There is now general acceptance that a vehicle is allowed to brake autonomously if the driver does not react to an un-avoidable accident. The vehicle itself can be allowed to take actions if appropriate actions from the driver are missing. However, the consequences can be questioned if actions to control individual vehicles are requested by the infrastructure.

Models to handle functional safety in cooperative systems are necessary. State-of-the-art is to handle functional safety for individual vehicles. There is a need to develop models and techniques for cooperative systems in order to

- identify hazards
- assess risks
- develop safety goals
- choose architectures
- choose techniques and measures for management of fault
- validate the functional safety of cooperative systems

This report is divided into six chapters. The first chapter provides an introduction to the subject of functional safety in systems of road vehicles. The second chapter explains functional safety and some basic safety concepts. Architectures for cooperative systems are given in chapter 3, and four examples of applications are described in chapter 4.

Chapter 5 of this report drafts some models for handling of functional safety in cooperative systems. This leads to the proposed future research listed in chapter 6.
2 Functional Safety

2.1 Approaches for functional safety

Compliance with end-user expectations is a central aspect in the design of machines, vehicles and control systems. However, an increasing use of Programmable Electronic Systems (PES) has increased the complexity and thereby made it harder to develop such systems in a safe and reliable way. Both hardware and software may behave unexpectedly and eventually trigger system failures. This has increased the focus on functional safety.

Functional safety is one part of the overall safety of a product. The risks addressed by “safety” are the risks for harm to persons or to the environment. Harm to property and financial assets is often regarded as “security”. Functional safety can be defined as “... the absence of unreasonable risk due to hazards caused by malfunctioning behaviour of electric/electronic systems” for road vehicles according to the draft international standard ISO 26262 [26262]. Similar definitions exist for other products. System safety is a wider concept than functional safety. There are aspects such as fire safety, electrical safety, chemical safety and mechanical safety which are not included in the concept of functional safety. But all these aspects contribute to the overall system safety.

Functional safety can be approached with a qualitative or quantitative perspective. With a qualitative approach the system behaviour at fault is used as a measure to indicate the safety level. A requirement for single fault tolerance is often stated for a safety-related function. An example of such a design basis is the hydraulic dual-circuit brake system of a road vehicle. A single fault may damage one of the brake circuits, but reduced braking capability is kept through the remaining redundant brake circuit. The qualitative approach is not always sufficient to describe Programmable Electronic Systems.

A quantitative approach for functional safety is becoming wide-spread in many industries. This probability-based approach aims to describe the probability of dangerous failure. The probability can either be expressed as failure per hour or failure on demand. An example of the quantitative approach is when a car manufacturer calculates the probability of air-bag failure to be sufficiently low for the expected life cycle of the car. Adequate hardware reliability data will be required as input for the calculations. Obtaining adequate data is the main challenge to succeed with the quantitative approach.

State-of-the-art frameworks for functional safety address both the product and the process by which it has been developed. It is not enough to study only the properties of the product since faults can be introduced all through the life cycle. The functional safety may be well described by the design documentation, but an improper maintenance procedure may increase the risks of failure. An overall safety lifecycle is often specified. (Figure 2.)

2.2 Standards for functional safety

There are several international standards addressing functional safety. Different industrial sectors have found the need to describe functional safety in the way most suitable for their products.

The international standard IEC 61508 [61508] is a basic safety publication covering the functional safety of electrical, electronic and programmable electronic safety-related systems. A major objective of the standard is to facilitate the development of application sector international standards. The standard will also enable the development of
electrical/electronic/programmable electronic safety-related systems where application sector international standards may not exist.

The intention is that the generic IEC 61508 should be possible to adapt to different industries and to different development management systems. However some issues have been raised:

- The overall safety lifecycle of IEC 61508 assumes installation of the item at the customer site to proceed the overall safety validation. This is not the case for mass-market products such as road vehicles. The safety of a road vehicle is validated before the start of production.
- IEC 61508 considers safety functions often to be distinct from the control functions. However, control functions and safety functions of automotive systems are usually inseparable.
- The techniques and measures suggested by IEC 61508 are not always suitable for automotive development.
- Subcontracting is not addressed by IEC 61508.

A draft international standard ISO 26262 [26262] for functional safety in road vehicles was published in 2009. It is further developed in collaboration with international standardisation bodies to make a sector-specific standard for cars. ISO 26262 is intended to be applied to safety-related systems that include one or more E/E systems and that are installed in series production passenger cars with a max gross weight up to 3,5 t.

The draft standard ISO 26262 addresses possible hazards caused by malfunctioning behaviour of E/E safety-related systems including interaction of these systems. An example of malfunction is if an obstacle detection system gives an alarm even if an obstacle is not present. It does not address hazards as electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy, and similar hazards.

The ISO 26262 draft provides an automotive safety lifecycle, an automotive specific risk-based approach for determining risk classes (Automotive safety Integrity levels, ASILs) and requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety being achieved.

The ASIL is one of four levels to specify the necessary requirements of the item or the element and safety measures for avoiding an unreasonable residual risk. ASIL D represents the most stringent and ASIL A the least stringent level.

The safety lifecycle specified (Figure 2) starts with the definition of the item and ends with the decommissioning. The basic idea of the safety lifecycle is to consider functional safety aspects all through the life of the vehicle.
2.3 Risk and hazard classification

The development of safety-related E/E systems typically involves a risk analysis to identify and classify hazards associated with the systems. The draft version of ISO 26262 contains normative parts on how to execute the analysis. As reported above there are some limitations to the standard that can complicate an application to cooperative systems. One of the issues concerns the potential consequences of hazards. As the standard only addresses hazards in single vehicles it does not directly apply to cooperative systems where hazards can affect a fleet of cars with potential consequences for several persons. As a result it is not clear if the classification scheme used in ISO 26262 where ASIL D is the highest safety integrity level is enough (it might be necessary to extend with a higher level for the most critical cooperative systems).

An alternative classification schema is given by MISRA in Guidelines for Safety Analysis of Vehicle Based Programmable Systems [MISRA GSA]. These guidelines address safety in single and multiple vehicles and unlike ISO 26262 it is not limited to passengers cars but also applies to busses where hazards can have catastrophic consequences for several persons. This suggests that the MISRA guidelines can be more suitable than those of ISO 26262 for analysing cooperative systems.

The safety analysis of cooperative applications focuses on the procedure described in the ISO 26262 and MISRA guidelines. An Automotive Safety Integrity Level (ASIL) shall be determined for each hazardous event using the estimation parameters severity (S), probability of exposure (E) and controllability (C).

The severity parameter is a measure of the extent of harm to an individual in a specific situation. It can be classified as no injuries, light and moderate injuries, severe and life-threatening injuries (survival probable), life-threatening injuries (survival uncertain) or fatal injuries.
The probability of exposure of each operational situation shall be estimated. The probability of exposure shall be described as incredible, very low probability, low probability, medium probability or high probability.

Controllability describes avoidance of the specified harm or damage through the timely reactions of the persons involved. The potential for controllability shall be assigned to controllable in general, simply controllable, normally controllable or difficult to control (uncontrollable).

Cooperative systems in the "inform driver" and "warn driver" categories (Table 5.1) share some properties which become clear when considering severity and controllability. The first observation is that the potential severity associated with these systems is limited but not negligible. Presenting erroneous information to the driver will in most cases only be considered a nuisance factor but can trigger driver reactions with severe consequences. Another observation concerns controllability where it can be concluded that it should be relatively easy for the driver to ignore incorrect information and control the vehicle without it. This reasoning however, is based on the fact that erroneous information can trigger unsafe driver behaviour and cause an accident.

Cooperative systems may also control "hard intervention" and "extreme intervention" applications which apply direct control to critical vehicle systems. The severity associated with faults in these applications is often high. An example is a malfunctioning platooning system which can cause multiple collisions in high speed driving. These cooperative applications also share relatively similar levels of controllability. They automatically or autonomously control vehicle systems such as brakes and powertrain drivers. The applications must actively override the systems to prevent accidents when malfunctions occur.

An aspect of cooperative systems that is not mentioned in either ISO 26262 or the MISRA guidelines is that safety-related decisions can be taken in central nodes. If a fault occurs in such a system it becomes extremely important to contain it since it can propagate to all connected vehicles.

2.4 How to develop safe and reliable control systems

Safe and reliable control systems are developed by applying techniques and measures to avoid systematic failures during different phases of the overall life cycle and to control failures during operation. It will be important to consider the functional safety aspects all through the development work.

The first step is to define the item to consider [26262]. An item is the system or array of systems or the function for which functional safety is addressed. All requirements must be specified. The purpose and the functionality of the item must be decided. But also non-functional requirements (e.g. environmental requirements) and legal requirements shall be available. If there are any already known safety requirements they should also be included in the item definition. Such requirements may be based on behaviour of similar items or assumptions on what behaviour is expected from the item.

The next step will be to perform a hazard analysis and a risk assessment. All operating situations in which incorrect behaviour of an item is able to trigger hazards must be described. The hazards of the item shall then be determined systematically, and the consequences of hazardous events shall be identified. The hazards may then be classified

14
by estimating the potential severity, the probability of exposure and the controllability. (Figure 3.) Low risks mean that no requirement in accordance with ISO 26262 is necessary. Quality Management (QM) is regarded as sufficient.

The top level safety requirements for the item are called safety goals. A safety goal shall be determined for each hazardous event evaluated in the hazard analysis. The existence of several safety goals for one item is possible. One safety goal can be related to several hazardous events. The ASIL determined for the hazardous event shall be assigned to the corresponding safety goal. The safety goals together with their attributes (ASIL, safe state, if applicable) shall be specified. (Figure 4.)
The development of a functional safety concept starts from the safety goals to derive the functional safety requirements. The safety requirements are then allocated to the provisional architectural elements of the item. As an alternative, external risk reduction measures can be applied to obtain the required functional safety. An external measure is separate and distinct from the item that reduces or mitigates the risks resulting from the item.

The safety requirements can then be used as input for hardware and software development. A high ASIL will require the application of very efficient techniques and methods for development. Development at a lower ASIL may be satisfactory using techniques and measures with moderate efficiency.
3 Cooperative architectures

The architecture of a cooperative system will have significant influence on system functionality. In addition, the architecture will define the safety integrity level of the system as a whole and in its different parts.

With the objective to illustrate how different architectural approaches impact functional safety in cooperative systems of road vehicles we have identified three distinctly different architectures types. These are:

- Ad hoc architecture
- Centralized architecture
- Hybrid architecture

These architectures are centred on three key properties considered of particular importance when designing robust and reliable cooperative systems.

First, the architecture tends to define the type of information flowing across a system. It can be designed to support raw sensor data or aggregated data, reflecting system level properties. The latter requires an “intelligent infrastructure” processing raw data from fixed and mobile sensors.

Second, the architecture defines how communication is made across the distributed system of vehicles and mobile units. It may be designed for local communication, where mobile units are interconnected through vehicle-to-vehicle links. As an alternative, infrastructure-based solutions may significantly extend the range, in practice allowing for global communication.

Third, the architecture outlines the logic behind decision-making in the system. An intelligent infrastructure may be designed for centralized decision-making, where an “intelligent infrastructure” caters for the holistic perspective. In contrast, decentralized approaches assign decision-making to remote clients.

3.1 Architectural Types

3.1.1 Ad hoc architecture

An ad hoc architecture (Figure 5) does not have any elements that can be classified as infrastructure. Instead, the system is made of ubiquitous computing platforms hosted by various mobile units, automatically connecting to each other when possible and appropriate. Mobile units include various vehicles, pedestrians, road workers, etc. Consequently, a vehicle system based on an ad hoc architecture employs

- local communication, meaning that it does not rely on an infrastructure for connectivity
- the remote units make system level meaning of raw sensor data transmitted from other vehicles in the system
- decision-making at the level of individual vehicles
Automatic Identification System (AIS) is an example of an ad hoc architecture. AIS is a transponder-based architecture, where vessels and aircrafts continuously broadcast vehicle position, without knowing the receiver and without terrestrial infrastructure. Through this ad hoc concept any vehicle is guaranteed to have an accurate position of its closest neighbours, equipped with transponders. One of the main purposes of AIS is to support collision avoidance functionality. Since transmitted messages have no explicit target, decision-making is made locally, at the receiving unit.

3.1.2 Centralized architecture

In a centralized architecture the clients, made up of various mobile units, are exceptionally thin. (Figure 6.) Essentially, these mobile units feed an infrastructure with remote data and execute actions commanded by the infrastructure, orders. One of the key purposes with this solution is to make the mobile units cheap and simple to manufacture and support over time. Consequently, a vehicle system based on a centralized architecture

- relies on an infrastructure for global connectivity,
- compiles system level meaning by centralized aggregation of both vehicle data and infrastructure information,
- decision-making is centralized, made at the infrastructure level.

The centralized architecture does not provide the actors with any information. All decisions are taken centrally and only orders are communicated to the actors.
Automated Guided Vehicle Systems (AGV) is an example of a centralized architecture used today. It is increasingly common in many industrial settings to use automatically guided vehicles in goods handling and logistics. These unmanned vehicles often co-exist with manual vehicles and personnel working in the warehouses alongside the vehicles. For navigation, these vehicles rely on a fixed infrastructure (e.g. scanning lasers and reflectors) resolving vehicle position in relation to a fixed reference frame. The fleet of AGVs is guided by an off-board AGV control system, handling ordering, traffic control, and surveillance of vehicles.

3.1.3 Hybrid architecture

A hybrid architecture combines centralized and decentralized (ad hoc) architectural approaches (Figure 7). First, it recognizes that an infrastructure can play a key role in communication, data collection (fixed sensors and general information, such as weather), data aggregation (processing raw data, such as traffic flow) and routing of information (all clients do not need all information). Second, it recognizes that applications and services may change over time, vary across car brands, and make an important element in business models. As a consequence it assigns decision-making capability to the client side – the cars. Third, the centralized data aggregation opens up for relatively thin clients, easy to produce at acceptable cost. On-board computers simply do not have to be designed to process large amounts of raw data. In summary, the hybrid architecture

- relies on an infrastructure for global connectivity
- aggregates information in the infrastructure
- allocates decision-making to the client side.

In the hybrid architecture information is filtered and aggregated so that each actor receives the information that is viewed as critical to him or her. In this particular example we have chosen to see that infrastructure as local not connected to big infrastructural optimization sources but designed to cover a local area, such as a road maintenance site, intersection or accident. Advisory decision is made centrally but each actor takes its own decision based on both the cooperative information and recommendations but also in many cases individually collected information e.g. from onboard sensors.

Traffic Information Channel (TMC) is a hybrid architecture in use. RDS-TMC is today’s backbone in the production and diffusion of traffic information. It makes use of a public (and sometimes private) infrastructure to measure traffic flow (speed and density). Another infrastructure – FM radio networks – is responsible for
communication with the vehicles. Finally, a navigation system may propose alternative routes, making a basis for manual decision-making by the driver.

**Instrument Landing System (ILS)** is yet another example of a hybrid architecture that is currently in use. The ILS is made of a fixed infrastructure combined with an on-board autopilot, used to guide an airplane during the landing phase. It functions by transmitting radio signals from at least two fixed positions at the runway, modulated at different frequencies. Measuring the difference between the signals, a client-side receiver can estimate its position in relation to an ideal glidepath. Thereby lateral and vertical guidance is provided during landing.

### 3.2 Summary

As illustrated, the three studied architectures hold different properties of importance to functional safety aspects of a cooperative road vehicle system. Table 1 summarizes the implications of the properties. Table 2 compares the three architectures to the three identified key properties and outlines the key advantages of each.

<table>
<thead>
<tr>
<th>Table 1 Practical implications of the three key properties</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Property</strong></td>
</tr>
<tr>
<td>---------------</td>
</tr>
<tr>
<td>Information</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Communication</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Decision-Making</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Table 2 Key properties in selected architectures

<table>
<thead>
<tr>
<th>Architecture</th>
<th>Information</th>
<th>Communication</th>
<th>Decision-Making</th>
<th>Key Advantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad hoc</td>
<td>Raw. Information flowing in the cooperative system is essentially manifested as raw data, locally produced in distributed vehicles.</td>
<td>Local. Mobile units are interconnected through local, vehicle-to-vehicle communication.</td>
<td>Distributed. Mobile units take decisions autonomously on the basis of local and remote information.</td>
<td>The ad hoc architecture allows for time critical applications (local com.), multiplicity in services (raw data) and quick adaptation to contextual change (local decision-making).</td>
</tr>
<tr>
<td>Centralized</td>
<td>Aggregated. Information from mobile and fixed sensors is aggregated by an infrastructure to reflect system level properties</td>
<td>Global. Mobile units are interconnected through a fixed infrastructure.</td>
<td>Centralized. Mobile units act on centralized decisions, made at an infrastructural level.</td>
<td>The centralized architecture opens up for optimal control of cooperative systems (centralized decision-making) with thin and inexpensive clients (centralized decision-making and aggregated data).</td>
</tr>
<tr>
<td>Hybrid</td>
<td>Aggregated. Information from mobile and fixed sensors is aggregated by an infrastructure to reflect system level properties</td>
<td>Global. Mobile units are interconnected through a fixed infrastructure.</td>
<td>Distributed. Mobile units take decisions autonomously on the basis of local and remote information.</td>
<td>The hybrid architecture allows for vendor specific solutions (distributed decision-making), yet with system-level reasoning (aggregated information and global communication). In addition, it enables efficient roll-out options, with end-user value at limited adoption (rich and varied infrastructural data and local decision-making).</td>
</tr>
</tbody>
</table>

We have argued that the nature of communication, information, and decision-making are central aspects when designing architecture for safety critical cooperative systems. Figure 8 places each architecture in a three dimensional property space, reflecting these aspects. This illustration is primarily to regard as a cognitive tool, supporting the elaboration of architectural concepts in cooperative systems.

Figure 8. The selected architectures in a property space.
4 Applications of cooperative systems

Cooperative infrastructures for road vehicles may be used for many different functions that benefit the cooperative and functions that benefit the individual vehicles. This chapter describes four different application areas where cooperative systems would make new functions possible. The application scenarios are vehicle platooning, road maintenance, intersection (system of road crossings) and traffic accident. These applications have been selected as they are fundamentally different in structure, planning, investments and duration. The differences challenge the cooperative systems and their functional safety from different perspectives.

The design of the particular function for the application depends on which cooperative architecture that is implemented. The cooperative architectures are described in Chapter 3, Cooperative Architectures. A possible functionality is given by applying an architecture on an application scenario and the functional safety challenges.

4.1 Example A: Platooning

Platooning is a concept which is also referred to as road-trains. A platoon is defined as a number of vehicles that are travelling together and electronically connected via wireless communication. A platoon consists of a lead which can be either a vehicle or the infrastructure and one or more following vehicles. The following vehicles of a platoon are controlled autonomously, i.e. without driver involvement in longitudinal movement or even without driver involvement in both lateral and longitudinal movement. This allows the drivers to undertake other activities that would normally be prohibited for reasons of safety; for example, legally operate a phone. The foreseen benefits of platooning are cleaner environment, increased safety, improved “driver comfort” and reduced congestion.

The platooning concept improves traffic efficiency. The car will travel extremely close and thus take up far less road space. All the vehicles in a platoon will also accelerate and decelerate at the same time, preventing “shock waves” that travel through the traffic flow and cause congestions. The road usage can also to some extent be planned in to give possibilities of not only better use in the special dimension or the road system but also in time. There are also studies that show a fuel consumption reduction of up to 30%.

Figure 9 shows a platooning situation. There is a truck that leads the platoon which consists of five following vehicles. These followers are automatically controlled and the drivers can relax and perform simple tasks. One vehicle has just left the platoon and has taken the motorway exit. The driver of the vehicle leaving the platoon is given manual control as soon as the situation is deemed as safe.

Platooning, as defined here, implies a new type of “vehicle” on public roads. This will create new situations such as interaction with other road users. New potential risks will be introduced. A failure of a single vehicle must not endanger the safety of other vehicles of the platoon. Techniques for functional safety should assure that faults will not spread among the vehicles. Risks in new traffic scenarios such as entering the platoon, leaving the platoon or dissolving the platoon must be assessed.

The following vehicles in a platoon are automatically controlled. This driver has little or no control over the vehicle except to request a “leave” or “emergency leave” from the platoon. When accessing the risk associated with a safety-related function, the driver
controllability will be very low or impossible since the vehicle is automatically controlled during platooning.

The platoon itself creates an obstacle due to its external dimensions since the platoon may contain several vehicles. An example is a situation where other vehicles cannot exit a motorway because a platoon is blocking it.

![Figure 9. Platooning (copied from www.sartre-project.eu)](image)

4.2 Example B, Road maintenance

The road maintenance application scenario (Figure 10) has several possible functionalities. The aim is to significantly reduce the number of accidents, which are common with severe consequences for the vulnerable road workers. Another aim is to improve traffic efficiency in relation to road maintenance work by use of cooperative systems.

Road maintenance can be viewed as an environment that is changing over time, but with control. The changes are planned and an infrastructure updated with relatively high precision can be made. However, there are often unprotected road workers close to high speed traffic and road maintenance machinery who do not travel in orderly manner as normal vehicles do. There is a risk for road workers to be hit by passing vehicles. There is a risk for passing vehicles to crash into the maintenance machinery.

The cooperative functionalities should warn both road workers, road maintaining vehicles and traffic vehicles for hazardous situations or even autonomously prevent them from happening. It could also optimise the traffic flow to prevent congestions which often appear in relation to road maintaining sites.

Road maintenance and building of roads are by nature temporary. It is therefore not realistic that large permanent investments are made. The introduction of an automatic warning system would reduce risks. The risk of the road workers being hit by passing vehicles can be reduced by alerting the workers if a vehicle approaches at high speed. The risk of a vehicle running into the road work signs or the temporary protective structures can be reduced by alerting the driver when approaching the road maintenance site.

New cooperative functions will reduce the risk of accidents and save lives of both motorists and road workers. But the warnings given must be reliable. The road worker must be able to trust that he will be warned if an approaching vehicle causes a threat to
him. Both motorists and drivers expect the system giving proper warnings. But they will also expect the number of false alarms to be kept low. A high frequency of false alarms will lead to the fact that warnings are ignored. Reliability will be essential to achieve functional safety. The driver will still have the task to observe hazardous situations.

Figure 10. Road maintenance (copied from http://vagvakt.se/tma.vagvakt.php)

4.3 Example C, Intersection

Intersections are critical parts in the infrastructure where severe accidents take place. Today’s onboard sensors in vehicles are relatively effective to avoid rear end collisions but they have very small possibilities in handling objects coming from the side. A cooperative system has obvious advantages in these cases since it is not limited to the narrow field of view that the onboard sensors have. Intersections are thus an application scenario suitable for cooperative systems with high possible benefit in terms of safety.

Considering traffic efficiency, intersections have a high impact. In a city it is often the intersections or rather system of intersections that determines the traffic flow. (Figure 11.) The intersections create disturbance in the traffic flow causing shock waves that travels back and forth in the flow, both before and after the intersections. The shock waves are the reason that speed varies in dense traffic, creating congestion of cars that move and stand still and then move again. Intersections thus have a high impact on traffic flow and traffic efficiency in e.g. a city.

A way of improving the situation in intersections with crossing roads is to implement overpasses or even ring roads. Overpasses and ring roads are associated with relatively high investments in the infrastructure. An alternative could be an “intelligent” intersection through cooperative systems or even an intelligent system of intersections that can optimize the traffic flow. A cooperative intersection system could thus improve
safety and efficiency with a relatively small investment. Intersections do not change over time and are therefore suitable for permanent infrastructural investments.

The cooperative system is expected to provide smooth traffic through the intersection without the need for stopping. Speed adoption and directions for which lane to choose will reduce congestion. New risks will be created when vehicles pass through an intersection without traffic light, only guided by the cooperative system. A failure of the cooperative system will be similar to a conventional traffic light signalling “green” in both directions. The risk of false signalling must be kept acceptably low. The requirements for functional safety imply that the cooperative system should be trusted by the motorists at a similar level as a traffic light.

Figure 11. Intersection (copied from http://www.gcdc.net/)

4.4 Example D, Traffic accident

A traffic accident is obviously not planned. (Figure 12.) It is hazardous even for those not involved since it has a high probability of causing additional accidents. An accident scenario is thus a hazardous situation. It may cause a new accident involving the rescue vehicles and personnel. Congestion often appears in addition to the hazards caused by the accident.

The aim of cooperative functionality would be to improve safety by preventing new collisions and to rapidly start controlling the traffic flow.

There are obvious challenges in cooperative functionality that improves traffic accident sites since an accident is a random and no planned event. The cooperative system
- needs to detect an accident and prevent additional accidents
- should support the rescue of those involved by making the accident site available for fire-men, ambulances, etc
- should identify the demographics of the accident site although lack of map or plan of the traffic accident environment
- should optimise the traffic flow, both by using the possibilities at the site and alternative routes where the area of the accident can be avoided
- are required to distribute traffic between alternative routes to prevent congestion and optimise traffic flow past the accident.

![Traffic accident](image)

Figure 12. Traffic accident

The warnings issued by the cooperative system must be reliable. Warnings must be given when an accident occurs. Otherwise a false sense of safety will be created for the motorists. Functional safety also requires that the frequency of false warnings will be at a sufficiently low level.
5 Functional safety challenges in cooperative systems

This chapter challenges current state-of-the-art for functional safety analysis, by evaluating the different examples described in chapter 4, which are implemented by using the different architectures described in chapter 3. The aim has been to evaluate if current processes, methods and tools for functional safety analysis are sufficient in handling automotive cooperative systems.

The example scenarios (Platooning, Accidents, Road maintenances and Intersections) have been chosen. They have different properties in the sense that they occur with different planning horizons and the possibility of building a fix infrastructure to address a specific situation is different. The benefits and drawbacks of the architectures are therefore not the same for the different application scenarios. Some application scenarios can make use of the architectural advantages and avoid the drawbacks and vice versa. The design space for different scenarios implemented on different architectures is huge. The areas that are discussed in this chapter can be described by Figure 13, where all application scenarios are discussed from each architectural perspective (chapters 3.1 to 3.3) and where each application scenario is implemented in each architecture, discussing the advantages and drawbacks as well as the functional safety challenges.

The main difference between the application scenarios is the frequency of change of the site boundaries. A site boundary is defined as a change of the physical infrastructure or of the traffic roles. The application scenarios created in this manner ought to cover a diversity of application scenarios in the design space. This means that they are far from covering the whole space but gives many different challenges that can be used to test the functional safety aspects of the cooperative systems.

![Figure 13. Map between application scenario changes property and architecture type.](image)

5.1 Design using ad hoc architecture

Each road user is broadcasting its ID, position, speed and acceleration vector. It is assumed that the majority of vehicles do this. It can be systems built-in in the vehicles or
nomadic devices. Each actor receives the information being broadcasted, filters out information of interest, evaluates it and acts on it.

In Example A, Platooning, it is essential for each vehicle following the lead vehicle to receive the information of the surrounding vehicles in order to position itself in the right manner according to the vehicle ahead. The vehicle can use its own sensors but due to the fast dynamics the cooperative information is necessary to provide early intentions and information from all vehicles ahead. Each vehicle is regarded as its own system. The platoon is regarded as a system of systems since the vehicles are interacting to achieve the common goal: platooning.

In Example B, Road maintenance, each road-worker, road maintenance vehicle and road blocking device are broadcasting ID, their position, speed and acceleration vector. It is assumed that a great number of the vehicle passing by is doing the same and listening to the broadcasted data. Each actor can estimate the potential threat each vehicle or road maintaining device is posing and act accordingly.

For Example C, Intersection, all road users broadcast information about themselves and are listening to others. This is an effective way of knowing that someone is approaching from e.g. the side. However, without knowing the traffic rules of the intersection (which we do not in ad hoc architecture) we can only avoid accidents in low speed and mitigate those in high speed. There are small possibilities of improving efficiency with ad hoc architecture since each vehicle decides its own actions. Another consequence of ad hoc architecture that limits efficiency improvements is that decisions are made based on information from a small circle area around each vehicle.

In Example D, Traffic accident, ad hoc architecture is efficient since it is instantly in place. It may prevent additional accidents by quickly providing the vehicles in the vicinity with the information of e.g. road blockage ahead. It could even give warnings for congestion, in case many vehicles transmit that they are standing still at the same position and that estimation is made by the approaching vehicle. It will however be difficult to lead the passing traffic in a smart way unless combined with the traditional traffic reporting system.

The ad hoc architecture in Example A is providing all necessary information, at least for a platoon in which the longitudinal dimension is automatically controlled. Since the communication is moving with the vehicles the ad hoc architecture has clear advantages. The effectiveness of the function depends on the distance to the vehicle in front, the smaller the better. Unfortunately it is the opposite for the integrity of the cooperative information necessary for this function. With a large distance the fallback may be an onboard sensor. Lateral support may be possible but may also require some infrastructural support.

Examples B, C and D may be utilised for warnings and autonomous collision avoidance using the best practice functional safety techniques for the design in the vehicles. The system implementing these functions will have the complete filtering, functionality, threat estimation and decision making in the vehicle. The problem lies in the integrity of the information received. The receiver can in some cases verify the information with own sensors, but this will not be the case for the majority of the situations and not at all possible for nomadic devices or vehicle lacking suitable on-board sensors.

The conclusion may be derived that it will be essential not only to communicate the ID, position, speed and acceleration vectors but also the integrity of the information. The integrity information will tell the receiver how certain the sender is that the information is
correct. The receiver can then make his own decision on e.g. safety distance; if the information can be used to warn or even to autonomously brake and steer away?

The question arising is thus “How should the integrity classification of ad hoc information be made?”. Efficiency aspects as platooning controlled slots in the infrastructure, guidance through road maintenance, accidents and optimization of intersection systems are not possible. The main benefit is that the functionality is present as soon as two interacting actors are equipped with the ad-hoc cooperative system.

Additional to that the safety integrity information needs to be present it may also need to be of a higher integrity level than the traditional onboard information. Functional safety standards e.g. ISO/DIS 26262 [26262] regard the vehicle as the highest abstraction level and do not consider platoons or coordinated vehicles. Therefore the standard is unsuitable for developing a platooning system.

The highest integrity level in ISO 26262 is ASIL D. In general terms this level is applied to functions which realise safety goals that can imply loss of life for one or few persons, e.g. occupants of one car, in the event of an accident. In contrast, an accident with cooperative functions that involves many vehicles can imply the loss of life for several persons.

5.2 Design using hybrid architecture

The difference in Hybrid architecture compared to ad hoc is that the information can be controlled by a central unit. Each road user is still broadcasting its ID, position, speed and acceleration vector. The difference is that they are broadcasting it to a cellular device. The cellular device can add and filter data, giving a higher level of aggregated information with both information and advisory decisions. The communication can also be aimed to one or several road users.

The road users, as in the ad hoc architecture, make their own decisions but relying on filtered and processed information received from a cellular unit. It is possible to determine and send recommendations of safe and efficient actions to connected road users.

Platooning would be implemented in the same manner as in the ad hoc architecture, with a lead vehicle but communicating via a network. The advantage would be that the amount of information could probably be limited to one set of moment parameters for the platoon and a recommendation of position, speed, acceleration and even distance to each individual vehicle. The information quality would probably be improved. The difficulty is that the function is continually running, since no disruptions are allowed. This would imply huge challenges in handing over platoons between different cellular units. Complete road coverage must also be granted. One advantage is that the car does not require synchronised functions to do platooning together.

The hybrid architecture used in the road maintenance application scenario would make it possible for the road users to get information about the road maintenance site before entering the site. A map of the site can be communicated additional to the actors that pose a threat or is threatened by the own vehicle. Road maintainers and their equipment may also communicate much more detailed information to the infrastructure unit that can process it in order to give the road users an even better picture of the site.

Recommendation of speed, lane, etc, could be given in order to improve efficiency as well as safety. Only the users in need of the information will be provided with it. For
example those who travel in the direction in which the road is being maintained would be
given the information but not those who travel in the opposite direction. Another
advantage is that only a vehicle currently heading into a critical situation with a road
maintainer is given information to avoid a hazardous situation but not the vehicles ahead
and behind. The functionality could even be extended by for instance recommendation
signs, warning lights and sounds in the infrastructure to also inform road users not
equipped with functionality for cooperative systems.

Regarding the intersection example, the hybrid architecture provides the ability of
supplying information about the traffic rules and a map of the intersection. This ability
improves the potential for safety significantly, compared to ad hoc architecture. The
decisions in the vehicle will be based on the threat posed by the other road users, and on
the knowledge of how the own vehicle and the other vehicles should and probably will
act. In a system of intersections it is possible to optimise traffic flow if some of the
crossings are equipped with e.g. controllable traffic lights.

Applying the hybrid architecture at an accident site could give some advantage in
guidance of vehicles passing the accident site. It is however tricky since it is an
unplanned event. In traffic accidents that take a long time to clear, it is possible that
information could be added to the system by e.g. the police. It is questionable how much
it would improve situations compared to ad hoc architecture complemented with
traditional traffic information.

As can be seen in the examples above the hybrid architecture has clear advantages,
especially regarding planned traffic environments compared to the ad hoc. The functional
safety for the particular actions taken by the users could be handled in the same manner
as in ad hoc architecture. As in ad hoc architecture it is important to have an integrity
level of the information being broadcasted. The cellular unit will be responsible for the
safety integrity of this information. This is another challenge compared to ad hoc
architecture. The cellular unit affects many vehicles implying that it has the potential of
causing more severe hazardous situations than the ad hoc architecture.

Currently, there is a lack of processes and methods in the evaluation and design of the
cellular unit, its functions and processing mechanisms. Another obvious safety challenge
is the filtering. Filtering provides many advantages, with the aimed information making
better use of available capacity and improving e.g. delays. It also gives the possibility to
improve the integrity and confidentiality of the information. However, processes and
tools for granting the integrity of the filtering is yet to be developed. How can it be
proven that the essential information is not filtered away and how can it be proven that
nonsense information is filtered away? Processes, methods and tools need to be
developed in order to design and guarantee the integrity of the information in such
systems.

5.3 Design using centralized architecture

The centralized architecture has the ability of providing improved safety and efficiency
for road traffic. It takes central decisions and sends out orders to each road user. It clearly
gives better opportunities to improve the traffic efficiency optimisation using dynamic
systems where for instance “virtual” traffic lights can be placed for short periods of time,
by e.g. a road maintenance site, without making changes in the physical layout. We
believe that almost a 100% penetration of the system in vehicles is necessary to achieve
the functional safety benefits and thus make an implementation possible. Although a
penetration of about a quarter of the vehicles would improve traffic efficiency, since with
such a penetration ratio it is possible to affect the pace of the community of vehicles. For
efficiency that e.g. allows more dense traffic, almost 100% penetration is essential. This also applies to most safety benefits since decisions need to be taken for all parties involved in a hazardous situation with close interaction in order to guarantee a better and not worse outcome of interferences. The obvious penetration problem of getting the system in all vehicles can be solved by keeping vehicles without the system separated, e.g. in separate areas or lanes.

Compared to ad hoc and hybrid architectures the decision making process is centralised in the centralized architecture. Instead of making threat assessments and safety related decisions in the vehicle it is made in the central unit.

Using a centralized architecture for platooning has the advantage that only thin clients are needed. It would be possible to gain efficiency benefits since the platoons could be planned and their passing of traffic bottlenecks could be optimized. The technical challenge of the centralized system for platooning is however huge. It requires total vehicle control for the central unit, insignificant delay, and high safety integrity.

Centralized architecture also has benefits when applied to the road maintenance application. If all vehicles support this architecture the traffic can be guided in smart manners as a road maintenance site evolves without changing the physical infrastructure. The vehicles can in each moment be guided to achieve optimal traffic efficiency. The ability to avoid accidents by planning the traffic flow dynamically will probably have a positive effect on reducing the number of accidents. The safety integrity is also vital. Possibly, the travel direction of lanes could be changed frequently in order to optimize flow. A failure in the system could then have devastating effects.

Intersections are generally fixed infrastructure devices that do not change. With the ability of centralized architecture, traffic flow through a city can be made highly efficient and the number of accidents could be reduced significantly. The speed of many vehicles can be planned so that they do not even have to stop in crossings but can “float” through in planned slots.

The ability to make use of centralized architecture in the traffic accident application scenario is less obvious. It could e.g. be beneficial for the police to control a traffic accident site. Algorithms that can handle such stochastic events are not impossible but complex. It is questionable if centralized architecture could be used to quickly take control of a traffic accident site, automatic algorithms is probably a must. There would not only be safety consequences of a failure but also traffic congestion.

Functional safety with centralized architecture will be less complex for the vehicle. Only low level functional safety for the actuators and their control is essential, as in today’s vehicles. The safety integrity of the communication and central decision unit is however a huge challenge. The communication does not need to be delivered with safety integrity information since the actors in the system do not take their own decisions. However, integrity of the orders given to the actors need to be in level with the actions that should be taken. This also relate to the probability with which it is delivered. The integrity of the decisions will affect many users in a complex system putting hard functional safety requirements on the system, requirements that we currently do not have methods and tools to handle. If active safety applications were to be considered on a Centralized architecture the technical and functional safety challenges to accomplish the short delay and the high integrity of the orders would be significant.

If the scene is changing, as in the case of a traffic accident and to some extent at a road maintenance site, it is necessary to take measures to see to that the map used by the system is in accordance with reality. It will be critical to the functional safety. Also
methods to assure that permanent sites, such as a road crossing, are secured need to be developed.

Another obvious problem is to handle entering and departure from a controlled zone that has centralized architecture into hybrid, ad hoc or even none cooperative architecture. In the centralized architecture the driver is not in charge and thus not responsible. An HMI that in a safe manner allows for handing over the responsibility from driver to central control and vice versa is essential. The handling of the traffic efficiency control is probably easier to implement since the time delay is less important than in the safety related applications that take autonomous actions. Still functional safety is not available for these applications. It will still be extremely important that the messages arrive, but not with a high time precision.

5.4 Implications regarding the examples and architectures

The development of an intelligent infrastructure is most likely a gradual implementation. The different architectures have different advantages. Ad hoc architecture is the easiest to start implementing, since it only requires implementation in vehicles. It has obvious applications when it comes to safety, near each vehicle or actor, if the functional safety through information integrity can be guaranteed. It can especially help in random scenarios like traffic accidents, where it is possible that the other presented architectures add little extra value. Ad hoc architecture can also provide the same functionality to sites where a cellular system is not operational.

Our mobile phones are already operating on a cellular network, a network that could make hybrid architecture rapid and easy to build up. No use of the ad hoc architecture at all however, demands a very good coverage by cellular units. It gives opportunities for recommendations regarding traffic efficiency and higher detail for better safety systems where both map and traffic rules can be considered. It is also possible to filter disturbing information. From a functional safety perspective, the hybrid architecture is a bigger challenge than the ad hoc architecture. The cellular units, their filters, and functions need to be evaluated in some manner. It is also vital to consider functional safety integrity of the communicated information. There are safety concerns, especially if floating car data should be used. It will be difficult to support the data traffic and also the interrupts that will be inevitable. The functional safety needs to consider these aspects.

The centralized architecture is the easiest implementation from a functional perspective of the end user. Order comes what to do and when to do it. This architecture ought to provide the best opportunities for optimal traffic flow. Many accidents could also be avoided with a better traffic optimisation. It will, however, provide an extreme functional safety challenge at the central control since the decision has been moved from the vehicles to the infrastructure. New processes, methods and tools need to be developed in order to accomplish functional safety in such systems. The accomplishment of functional safety for active cooperative safety functions in the system is a tremendous challenge.

A combination of the different architectures is probably the best way of building a cooperative infrastructure. For the active safety close to vehicles and actors, the ad hoc architecture is good, it works without cellular support. It could however be possible to have the benefits of the ad hoc architecture in the hybrid architecture, but it requires very good cellular coverage. A probable solution is hybrid architecture combined with centralized architecture where the traffic efficiency is controlled in a centralized architecture manner. The cooperative safety is provided through hybrid architecture, maybe combined with ad hoc architecture. It gives the advantage of the different
architectures but without the tricky functional safety problem with cooperative safety functions in centralized architecture. With this conclusion it is important to develop functional safety measures that can support different architectures and the possible combinations of them. The party or country that develops methods to handle the functional safety for a cooperative system will have the opportunity to lead the development. Today, there does not seem to exist a mature way of dealing with these challenges. This fact will most likely change when the challenges become more widely recognised.

5.5 Functional safety implications in cooperative systems

This chapter discusses why cooperative systems require new and different processes to cope with the functional safety aspects. The best practice for functional safety processes for development of in-built systems in road vehicles of today does not provide the support needed.

A functional safety process for cooperative systems needs, additionally to address that:

- guidance for selection of cooperative architecture with respect to functional safety is needed.
- consequences are considered to be trivial in today’s road vehicles in that only one vehicle is affected. In cooperative systems more advanced methods are necessary in order to determine consequences which are much more complex.
- frequency of failure is significantly more complex than in road vehicle of today systems, requiring more advanced methods for its estimation.
- controllability notion needs to be expended not only considering what the own driver can do but also the other actors in the system in order to avoid a consequence.
- in some manner is it necessary to address the fact that the performance of the communication channels may vary.
- robustness for any type of cooperative system architectures is a requirement.

Some of these aspects are elaborated on in the sections below.

5.5.1 Decision-making process

A critical part of the applications is the decision-making process that decides on its actions. Thus, this sub chapter presents an analysis for some of the issues relating to decision-making. The interaction between decision-making processes, drivers, sensors and basic vehicle functions such as acceleration and braking is included in the analysis is also discussed.

There have been many suggestions of applications to realize when vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communication channels are available in vehicles. Some examples are vehicle platooning (chapter 4.1), intersections (chapter 4.2), road maintenance (chapter 4.3), traffic accident (chapter 4.4), road side information [CVIS], and route guidance [CVIS]. The authority that these applications have over the control of the individual vehicles varies. In a platoon it is necessary for the application to fully control the speed of each vehicle, thus having a high degree of authority of control. On the other hand we have the route guidance systems which only give suggestions on optimal routes to the driver and let him decide the appropriate control action. Table 5.1 presents this relation between application and level of control authority over the vehicle. The grouping of applications is based on the following categories:
- Driver information – provides information to the driver in normal driving
- Driver warning – presents warnings to the driver in critical situations
- Soft intervention – controls vehicle speed and/or heading direction in normal driving and can not override driver commands
- Hard intervention – limits the driver’s ability to control vehicle speed and/or heading direction and takes over control
- Extreme intervention – disables driver commands and takes control over vehicle speed and/or heading direction

The level of authority is divided into discrete levels ranging from low to high.
- High – allowed to control highly safety-critical functions of the vehicle including steering
- Medium – allowed to control safety-critical functions within strict boundaries
- Low – not allowed to control any safety-critical functions but can advice the driver on appropriate action

<table>
<thead>
<tr>
<th>Level of authority</th>
<th>Inform driver Ex: Informative messages</th>
<th>Warn driver Ex: Warning messages</th>
<th>Soft intervention Ex: Speed limitation</th>
<th>Hard intervention Ex: Emergency braking</th>
<th>Extreme intervention Ex: Autonomous steering</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A consequence of the systems in the groups "hard intervention" and "extreme intervention" is that the driver has little or no control over the vehicle. The platooning system is one example where the driver lets go of both steering and speed control. Since these systems are designed to lower fuel consumption by minimizing air drag, the vehicles in the road train have to drive close to each other. In such a driving constellation most drivers are not expected to be able to handle the vehicle safely. Driver interaction is therefore limited to a few request commands, such as "leave" or "emergency leave". For such systems it is important to remember the Vienna Convention which states that drivers should always be in control of the vehicle [Vision zero international].

### 5.5.2 Local or remote decisions and information

Local and remote decisions are based on local or remote information. Local information is defined as information from sensors connected to the ego vehicle (vehicle A) such as camera, radar, GPS hardware, etc. Remote information is defined as information from sensors outside ego vehicle (other vehicles (V2V), cellular units (V2I), etc.). Table 5.2 elaborates features and risks encountered using combinations of local and remote information/decisions for a Collision Avoidance by Braking function.
Table 5.2 Collision Avoidance by Braking system controlled by the ego vehicle (denoted as vehicle A) or from the environment (other vehicle or a cellular unit).

<table>
<thead>
<tr>
<th></th>
<th>Local decision</th>
<th>Remote decision</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Local information</strong></td>
<td><strong>Scenario:</strong> Vehicle A detects obstacle and decides to brake.</td>
<td><strong>Scenario:</strong> Vehicle A detects obstacle and informs environment, which controls the brakes of vehicle A.</td>
</tr>
<tr>
<td></td>
<td><strong>Feature:</strong> Fast activation of brakes, state-of-the-art today</td>
<td><strong>Feature:</strong> Several vehicles can be controlled simultaneously to prevent an accident.</td>
</tr>
<tr>
<td></td>
<td><strong>Risk:</strong> Additional safety information from the environment is ignored</td>
<td><strong>Risk:</strong> It will take longer time to activate the brakes.</td>
</tr>
<tr>
<td><strong>Remote information</strong></td>
<td><strong>Scenario:</strong> Environment informs vehicle A about obstacle and vehicle A is ready to brake.</td>
<td><strong>Scenario:</strong> Environment informs Vehicle A about obstacle and controls the brakes of vehicle A.</td>
</tr>
<tr>
<td></td>
<td><strong>Feature:</strong> Detection of obstacles outside the field of view of vehicle A</td>
<td><strong>Feature:</strong> Detection of obstacles outside the field of view of vehicle A</td>
</tr>
<tr>
<td></td>
<td><strong>Risk:</strong> Information may not be secure</td>
<td><strong>Risk:</strong> Information and decision may not be secure. It will take longer time to activate the brakes.</td>
</tr>
</tbody>
</table>

The use of several sensors to achieve a more accurate or dependable result is known as sensor fusion. Sensor fusion takes advantages of a number of sensors to e.g. detect erroneous (or deliberately corrupted) sensor values by comparing them. In the same manner, the use of both local and remote information (sensor values) will probably lead to a more safe and secure cooperative system.

### 5.6 Architecture for cooperative systems

Figure 14 shows a view of a feed-back control system. The decision block in the middle (the controller), takes sensor values as input (the left block) to be able to actuate the controlled system (the right block). The controlled object can be a single road vehicle or systems of road vehicles. Actuation in this context is the execution of a function, e.g. an adaptive cruise control system. Observe that the left block in Figure 14 is seen from a single vehicle where e.g. local information is values from sensors within the vehicle. Also note that several vehicles can be actuated simultaneously. Thus, a single erroneous actuation of the decision block can lead to an unexpected behaviour for several road vehicles.
Figure 14. Different locations of sensors, functions (actuators) and type of decisions
6 Future work

As seen in chapter 5 it is necessary to address the new challenges that cooperative road vehicle systems put upon functional safety. A large part of the challenge has to do with that these systems are more complex. They require suitable methods for handling the high complexity in estimation of e.g. consequences, frequencies of failures, errors and fault propagation, controllability, detection and robustness. We believe that a smart way of handling such complexity is to use model-based safety methods and analysis.

Another problem is that many people are connected in cooperative systems, where each decision may be taken by different parties. Where in such a system a decision is taken significantly affects the functional safety as discussed in this report. Methods need to be developed in order to design the architectures for cooperative systems that give the best possible functionality and also fulfil the functional safety requirements.

A large difference with cooperative systems, compared to the embedded automotive systems of today, is that many have different service providers that act together in the same system. Road vehicle manufacturers, institutions and vendors will provide different functionalities based on a common information and decision flow. A question that needs attention is how safety integrity should be addressed in such open systems.

We suggest that the following research questions are addressed with projects in order to start building a framework for functional safety in cooperative systems:

- Risk assessment
  - to further develop current risk assessment methods to also cover cooperative systems. More specifically this involves;
    - determine how faults that affect several vehicles shall be analysed,
    - develop a method for estimating the Controllability parameter when cooperative systems limit the driver’s ability control the vehicle,
    - determine if risk assessment can be improved by a model-based approach.

- Functional Safety in Open Cooperative Systems
  - At a general level, the objective of this project proposal is to outline technology management principles for open cooperative systems of road vehicles. More precisely, it aims for an improved understanding of how design, roll-out, diffusion, and acceptance of technology influence functional safety in such systems. The project will deliver:
    - A stakeholder analysis identifying key actors and their respective incentives in open cooperative systems.
    - Business scenarios illustrating opportunities for the different stakeholders.
    - Reference architectures used to evaluate different functional safety aspects towards identified business scenarios.
    - Governance strategies and mechanisms demonstrating how stakeholders can exploit technology to reach business goals with acceptable functional safety.
Techniques and Methods

This work package will develop techniques and methods for developing and realising cooperative systems. Assuring functional safety in such a system is a major challenge. The work will use the relevant and currently available standards as a base: IEC 61508, MISRA guidelines and ISO WD 26262.

An example of approach is to augment 26262 with a further level of severity (for multiple deaths), a guideline for assessing controllability in a cooperative system and an additional ASIL-level with further requirements.

Safe control of cooperative vehicles in roundabouts

One drawback with roundabouts is that vehicles need to decrease speed which may lead to traffic congestions. The aim of this demonstration project is to implement a centralized architecture (chapter 3) for one roundabout which controls the flow of traffic by automatically adjusting the speed for each approaching vehicle.

Improved safety and traffic efficiency in road maintenance site

Investigate the possibilities and functionality of using cooperative systems to improve the traffic safety environment at road maintenance sites and demonstrate possible implementations. Investigate the possibility through a cooperative system to improve the traffic flow pass a road maintenance site and demonstrate one possible implementation.

Field Operational Study for functional safety base line

Collecting naturalistic driving data to develop a baseline of what is an acceptable risk for a cooperative system.

Descriptions of the proposed research projects are provided in annex C.
Annex A  References

A.1  Platooning

[CVIS] The European research Project CVIS
www.cvisproject.org/en/cvis_subprojects/applications/

[SafeSpot] The European research project SafeSpot
www.safespot-eu.org/applications.html

[SARTRE] The European research project SARTRE (Safe Road Trains for the Environment)
www.sartre-project.eu

[VAS] The Swedish national research project VAS (Vehicle Alert System)
http://ceres.hh.se/egroupware/sitemgr/sitemgr-site/?page_name=Safety

A.2  Standards

Standards are protected by copyright and can be obtained from ISO (www.iso.ch), IEC (www.iec.ch) or by national standardisation organisations (e.g. www.sis.se).

ISO 26262-3 Functional Safety – Road Vehicles. Part 3: Concept phase
ISO 26262-7 Functional Safety – Road Vehicles. Part 7: Production and operation
ISO 26262-8 Functional Safety – Road Vehicles. Part 8: Supporting processes
ISO 26262-10 Functional Safety – Road Vehicles. Part 10: Guideline (informative)


A.3 Functional safety

[MISRA GSA].
Guidelines for Safety Analysis of Vehicle Based Programmable Systems
MISRA, The Motor Industry Software Reliability Association
Annex B Terminology

B.1 System

The concept of system can be defined in many ways. Without being too formal, a system will be used to characterize an object, or a collection of objects, whose properties are desirable to study. With such a broad definition, most things in our environment are systems. There are natural and man-made (designed) systems; the latter is of interest e.g. from an (automotive) engineering point of view.

Systems have boundaries which defines which objects are inside and outside the system; objects outside the system defines the environment. In general, there might be inputs to and outputs from systems. As an example for control systems, inputs can be divided into control inputs and disturbances, where the former can be manipulated as desired (within certain limits) whilst the latter cannot. Outputs, which can be interpreted as the response of the system applying the inputs, are defined by the designer of the system depending on the purpose of the system under study. Most often in engineering systems, inputs are related to sensor measurements.

A subsystem is a set of objects or elements, which is a system itself, and a part of a larger system.

B.2 Function

The meaning of the term function depends on the area in which the word is used. In engineering, a function is frequently interpreted as a specific process, action or task that a system is designed to perform. Examples in the automotive industry are the brake system, which should decelerate the vehicle when activated (usually by using the brake pedal but there are also other possibilities like manually control of the exhaust brake), or the climate system which for instance adjusts the temperature inside the vehicle cab.

Functions can be combined together defining new functions. For instance, a cruise controller consists e.g. of the accelerator functionality (i.e. the possibility to inject more fuel accelerating the vehicle) in combination with sensor measurements of the vehicle speed and a speed controller accessing the accelerator functionality.

B.3 Safety

The term safety is used to describe many different properties. Generally, and popularly, safety means a relatively high degree of freedom from harm. In mechanical and civil engineering, which were the first to face design with expressed concern for safety, the term safety often refers to knowledge of strength of materials, fatigue, etc. However, in automotive industry, we are concerned with product and system/functional safety.

B.4 Risk

System safety most often uses the notion of risk. This is a widely used approach in the chemical, nuclear, railway and aerospace industries can be seen in almost all safety standards developed in the transportation sector.

A product, system or safety function is generally considered to be safe if the level of risk is reasonable. Risk is a combination of the consequence (the impact of the event) and the
likelihood/frequency (how often the event occur) of unplanned undesirable events and it is common to formally define the risk as

\[
\text{risk} = \sum_{i=1}^{n} \text{frequency}(i) \times \text{consequence}(i)
\]

where \(\text{frequency}(i)\) and \(\text{consequence}(i)\) is the frequency and consequence respectively associated with event (several events can occur).

There is always a maximum frequency that can be tolerated even if the consequence is, for all practical purpose, negligible. Likewise there is a maximum consequence that can be tolerated even if the frequency is, for all practical purpose, negligible.

For a specific event, the risk \(\text{risk}(i)\) is acceptable if it is lower (or equal to) than a specified value, say \(r(i)\) and unacceptable if higher that this value. Taking the logarithms of the risk equation above for event (and rearranging the terms), leads to that \(\text{risk}(i)\) is acceptable if

\[
\log(\text{consequence}(i)) \leq \log(r(i)) - \log(\text{frequency}(i))
\]

otherwise unacceptable. In a log-log scale, the border between the acceptable and unacceptable region is a straight line, see the figure below.

**B.5 Scenario**

A **scenario** (from Italian, that which is pinned to the scenery) is a synthetic description of an event or series of actions and events. Scenario development is used in policy planning, organizational development and generally, when organizations wish to test strategies against uncertain future developments.

Scenarios are widely used by organizations of all types to understand different ways that future events might unfold. **Scenario planning** or **scenario analysis** is a complex business process related to **futures studies**.

In transportations, one scenario could result in platoons with the purpose to increase the vehicle throughput, or road intersection supervisors planning the traffic through the intersection.

**B.7 Traffic situation**

A **traffic situation** is the state of the traffic at a certain time.

**B.8 Cooperative systems**

A cooperative system is defined to be multiple dynamic entities (or systems) that share information or tasks to accomplish a common, though perhaps not singular, objective. Examples of cooperative control systems might include: robots operating within a manufacturing cell, unmanned aircraft in search and rescue operations or military surveillance and attack missions, arrays of micro satellites that form distributed large aperture radar, employees operating within an organization, and software agents. The term entity is most often associated with vehicles capable of physical motion such as robots, automobiles, ships, and aircraft, but the definition extends to any entity concept.
that exhibits a time dependant behavior. Critical to cooperation is communication, which may be accomplished through active message passing or by passive observation. We assume that cooperation is being used to accomplish some common purpose that may be greater than the purpose of each individual, but we recognize that the individual may have other objectives as well, perhaps due to being a member of other caucuses. This implies that cooperation may assume hierarchical forms as well. The decision-making processes (control) are typically thought to be distributed or decentralized to some degree. For if not, a cooperative system could always be modeled as a single entity. The level of cooperation may be indicated by the amount of information exchanged between entities.

In transportation, a reasonable scenario is that the numbers of cooperative systems will most likely increase in the future. Both platooning and road intersection supervisors are examples of complex cooperative systems.
Annex C  Project proposals

C.1 Risk assessment

Background
Risk assessment is a key phase in the development process of safety-related automotive electronics. A state-of-the-art development process starts with a conceptual definition of the system and continues with a hazard identification phase. All operating situations in which the incorrect behaviour of the system is able to trigger hazards must be described. The list of hazards that is produced in the hazard identification phase serves as input to risk assessment. By classification of all the hazards it is possible to assign an overall risk class to the system that corresponds to the highest risk. Subsequent phases in the development process are then chosen in accordance with the overall risk class to ensure sufficient and acceptable level of safety.

The draft international standard ISO 26262 provides an automotive safety lifecycle and an automotive specific risk-based approach for determining risk classes (i.e. Automotive Safety Integrity Levels, ASILs). Procedures for systematically determining hazards of the item are described together with the identification of consequences of hazardous events. The Automotive Safety Integrity Level (ASIL) is determined for each hazardous event by combining the estimation parameters severity (S), probability of exposure (E) and controllability (C). The severity parameter is a measure of the extent of harm to a person in a specific situation. Exposure includes the likelihood that a situation is hazardous if it coincides with a system malfunction. Controllability describes avoidance of the specified harm or damage through the timely reactions of the persons involved.

Applying the described risk assessment procedure to cooperative systems poses some problems. The following issues have been identified:

- Current methods for risk assessment are designed for single vehicles. As cooperative systems include at least two vehicles it is not clear how to apply the methods (e.g. maximum severity corresponds to life-threatening or fatal injuries to one or a few persons).
- A cooperative system in a vehicle can potentially limit driver commands in order to receive and actuate control commands (e.g. steering or acceleration commands) from other vehicles or infrastructural nodes. How this affects the estimation of the controllability parameter is not described in current methods for risk assessment.

Objective
The overall objective is to further develop current risk assessment methods to also cover cooperative systems. More specifically this involves to:

- determine how faults that affect several vehicles shall be analysed
- develop a method for estimating the Controllability parameter when cooperative systems limit the driver’s ability to control the vehicle
- determine if risk assessment can be improved by a model-based approach.

Methodology
An initial phase of the project shall perform a survey of cooperative systems to obtain a correct view of the possible malfunctions and hazards that are not covered by traditional risk assessment. Further work will follow an interactive process where theoretical work is mixed with application to use cases.
C.2 Functional Safety in Open Cooperative Systems

Background
Cooperative systems of road vehicles are of increasing interest for automakers, national road administrations, and end-users. These systems allow for a holistic perspective where the interconnection of mobile units is expected to deliver superior solutions to everyday traffic problems. A key challenge in the design of cooperative systems is to create an ability to act on the basis of dynamic and uncoordinated resources. The setup of actors (vehicles, pedestrians, fixed infrastructural elements, etc) may change over time and the technology is often under the control of different stakeholders (automakers, road administrations, public authorities, etc). As a consequence, cooperative systems require radically new architectural solutions, recognizing an open system perspective. However, such open architectures tend to break up the traditional approach to failure mode analysis. It is simply not possible to take low level errors to system level consequences when the system setup is dynamic and its parts are essentially unknown.

Objective
At a general level, the objective of this project proposal is to outline technology management principles for open cooperative systems of road vehicles. More precisely, it aims for an improved understanding of how design, roll-out, diffusion, and acceptance of technology influence functional safety in such systems. The project will deliver:

- A stakeholder analysis identifying key actors and their respective incentives in open cooperative systems.
- Business scenarios illustrating opportunities for the different stakeholders.
- Reference architectures used to evaluate different functional safety aspects towards identified business scenarios.
- Governance strategies and mechanisms demonstrating how stakeholders can exploit technology to reach business goals with acceptable functional safety.

Methodology
This initiative will be set up as a four step design science research project (Hevner et al. 2004; Gregor and Jones 2007). With this approach we draw particular attention to guidelines and implications for the design of cooperative systems. As part of this overall research method we intend to use stakeholder theory (Donaldson and Preston 1995) to analyze actors, incentives, and business models. Finally, our studies of the interplay between stakeholders and technology will follow normal practice in case study research (Eisenhardt 1989; Yin 2009).
C.3 Techniques and Methods

Background
The functional safety standard ISO/DIS 26262 regards the vehicle as the highest abstraction level and does not consider a coordinated system of vehicles, such as platoons.

The Automotive Safety Integrity Level (ASIL) specifies the item's or element's necessary requirements and safety measures for avoiding an unreasonable residual risk [26262]. The ASIL is found by assessing the severity, exposure and controllability of risk. The highest integrity level in 26262 is ASIL D. In general terms this level is applied to functions which realise safety goals that can imply loss of life for one or few persons, e.g. occupants of one car, in the event of an accident. In contrast, a failure in a coordinated system of vehicles can imply loss of life for several persons.

Controllability is a factor in assessing the ASIL. It is defined as the probability of the driver to handle the situation. The definition of controllability implies that the driver has manual control over the vehicle and that the vehicle is not influenced or controlled by external systems. In the case of cooperative systems there may be some degree of external influence to the vehicle.

Due to the three main flaws described above, the draft standard is unsuitable for developing coordinated systems.

Two examples of coordinated systems are given:
1) A platoon of vehicles aims to drive with a smallest safe gap between vehicles. Current projects such as SARTRE indicate that several vehicles will be involved. In the event of an accident all these vehicles may be affected. Vehicles that participate in platooning will be automatically controlled. Hence the driver controllability is reduced or even removed.

2) Traffic intersections and crossings are controlled by traffic-lights and other devices to coordinate the traffic for efficiency. In the very largest intersections in Europe there can be as many as 400 vehicles inside the intersection area. A malfunction of the control devices is e.g. green traffic lights in both directions. This situation can imply an accident where a large number of vehicles is involved.

Objective
This work package will develop techniques and methods for developing and realising cooperative systems. Assuring functional safety in such system is a major challenge that is addressed here. The work will use the relevant and currently available standards as a base: IEC 61508, MISRA guidelines and 26262.

An example of approach is to augment 26262 with a further level of severity (for multiple deaths), a guideline for assessing controllability in a cooperative system and an additional ASIL-level with further requirements.

Methodology
This project proposal is performed after the risk assessment proposal. The risk assessment will investigate and propose new methods to assess and analyse functional safety related risks in cooperative systems. Related and relevant standards will be studied. Techniques and methods will be recommended for developing cooperative systems.
C.4 Improved safety and traffic efficiency in road maintenance site

Background
Road maintenance sites are one of the most dangerous working environments. Each year there is a large number of injuries and even deaths among road workers.

The traffic sites also pose a disturbance in traffic. The road maintenance sites create bottlenecks causing congestions.

Objective
Investigate the possibilities and functionality of using cooperative systems to improve the traffic safety environment at road maintenance sites and demonstrate possible implementations.

Investigate the possibility through a cooperative system to improve the traffic flow passing a road maintenance site and demonstrate one possible implementation.

Methodology
Workshops would be used for creating ideas of different concepts. Selection methodology would be used to select the concept with highest potential. The concepts would then be designed using best practices design methods according to the functional safety requirements. The design would then be demonstrated in a demonstrator situation.
C.5 Safe control of cooperative vehicles in roundabouts

Background
Junctions with traffic lights or stop signs have the most serious accidents. Head-on collisions, left-turn collisions and right-angle collisions are examples that may lead to severe accidents since such crashes will probably have a high angle of impact. Roundabouts reduce those types of crashes since vehicles travel in the same direction and at low speed. Research shows that roundabouts are safer than both traditional junctions and traffic circles ([http://www.iihs.org/sr/pdfs/sr3505.pdf](http://www.iihs.org/sr/pdfs/sr3505.pdf)). Roundabouts can probably be made even safer with the use of cooperative systems with high functional safety.

Objective
One drawback with roundabouts is that vehicles need to decrease speed which may lead to traffic congestions. The aim of this demonstration project is to implement a centralized architecture (chapter 3) for one roundabout which controls the flow of traffic by automatically adjusting the speed for each approaching vehicle.

Methodology

Virtual demonstrator (project phase I)
A roundabout traffic scenario and the corresponding safety aspect may first be simulated to find an algorithm for controlling the individual speed of vehicles which maximizes the throughput of the roundabout, in a safe manner. There are commercial simulation tools available such as the PreScan tool ([http://www.tno.nl/](http://www.tno.nl/)) which is used e.g. in the Grand Cooperative Driving Challenge initiative ([http://www.gcdc.net/](http://www.gcdc.net/)). The project may also need to develop methods, models and tools for evaluating functional safety aspects.

Physical demonstrator (project phase II)
The ad hoc architecture (chapter 3) uses only V2V communication and is not feasible for implementing a cooperative roundabout function since vehicles make their own decisions based on local or remote information. Two vehicles can at the same time take identical decisions, to e.g. decrease the speed and try to enter the roundabout directly after the other vehicle, which may result in a deadlock situation. The same holds for hybrid architecture since the decisions are made by the vehicles.

Centralized architecture is more suitable if e.g. a central unit, placed inside the roundabout, is making all the decisions based on information from the surrounding (weather condition, pedestrians, etc.) and the approaching vehicles. By using the ideas behind sensor fusion, the central unit can use different sensors (information from different vehicles and the environment) to improve the quality of the decisions and to improve dependability by comparing information from several sensors where one or more sensors may be erroneous or have degraded performance.
SP Technical Research Institute of Sweden develops and transfers technology for improving competitiveness and quality in industry, and for safety, conservation of resources and good environment in society as a whole. With Sweden’s widest and most sophisticated range of equipment and expertise for technical investigation, measurement, testing and certification, we perform research and development in close liaison with universities, institutes of technology and international partners.

SP is a EU-notified body and accredited test laboratory. Our headquarters are in Borås, in the west part of Sweden.

SP consists of eight technology units and six subsidiary companies. Three of the companies, CBI, Silso and JTI are each 60% owned by SP and 40% by their respective industries.