Final report:
Electrical architecture in future hybrid vehicles[1] (AFFE)

Project within Fordonsutveckling
Author
Date 2012-10-15
Dnr 2009-01439

[1] El-arkitektur för framtida elhybridfordon

Content

1 Executive summary

The automotive industry is facing a shift from traditional combustion engines to more efficient, long lasting and environment friendly solutions.

Parallel hybrid vehicles have already been introduced. However, the low efficiency of the mechanical drive line and its embedded limitations still make those system limited. The full potential may only be reached with a series hybrid solution, which allows for minimal mechanical losses and optimal energy efficiency.

A series hybrid vehicle based on electric hub (wheel end) motors will need “drive by wire” solutions, exchanging the mechanical transmission with power cables, electronics and software. The design and architecture of this control system is a challenge and bottleneck for the whole automotive industry.

The objective of the project is to present a realistic control system architecture for series hybrid road vehicles with wheel end electrical motors including “drive-by-wire” solutions. The architecture must fulfilling safety requirement as well as all functional requirements needed for the integration of various vehicle subsystems and drive line components. The result shall include guidelines, principles and solutions as well as proof of concept for the design and system integration. Besides fulfilling safety and cost efficiency requirements the control system shall be scalable and able to adapt to various platform configurations.

The intention is to adapt the activities of the project to the functional safety standard ISO 26262, which is expected to become an important standard for the automotive industry as e.g. more “x-by-wire” functions are introduced.

The project cover a total budget of 11 MSEK, based on a support from VINNOVA of 50% included.

Parties in the project are:

- AB Volvo: Project leader and responsible for the application. Producer of commercial vehicles with extensive knowledge of architecture development for multi segment usage. Has delivered electric hybrid vehicles such as busses, garbage trucks, etc.
- BAE System Hägglunds: Military vehicle producer with special knowledge in electric transmission and special vehicle integration.

- Mecel AB: System and software supplier within the automotive industry with extensive knowledge in in-vehicle communication, software architecture, system development and development processes.

The automotive industry is challenged to find sustainable solutions to environmental and energy requirements. The vehicle platforms of the future must incorporate energy efficient systems solutions to be able to extensively lower our dependency on oil as source of energy. It has been made clear that the application of electrical drivelines combined with electrical energy stores (e.g. batteries) will help reach these goals. This has also been emphasised by the Globaliseringsrådet in their report "*Gör sverige till ett elbilens pionjärland*". ("*Make Sweden the pioneer country of electric cars*")

Traditional gearboxes and mechanical transmissions introduce significant energy losses. By substituting these for electromechanical machines controlled by software and electronics the energy losses as well as vehicle driveline weight can be reduced leading to environmental advantages.
This can only be achieved with the application of drive-by-wire solutions, which has been used in aviation and maritime applications for a long period of time. Current technology and safety assurance methodologies suggest that there are great opportunities for full scale application of drive-by-wire solutions also for the road vehicles of the future.

A carefully designed systems architecture will be required to be able to manufacture safe, effective and competitive solutions from the currently available technology and components. The architecture must support the configurations needed to fulfil the safety requirements of the vehicles and drivelines of the future. It will be a decisive challenge to define such architecture, and to secure technology, knowledge and methods for the realisation of these drivelines and related functions.

In this project the aim has been to present a realistic control system architecture for a series hybrid road vehicle with 4 electric wheel motors including "drive-by-wire" solutions. The architecture has been designed in order to fulfil safety requirements as well as functional requirements needed for the integration of various vehicle subsystems and drive line components.

The results include guidelines, principles and solutions as well as proof of concept for the design and system integration. Besides fulfilling safety requirements the system is scalable and able to adapt to various platform configurations.

2 Background

Traditional gearboxes and mechanical transitions for propulsion of vehicles imply significant energy losses. By replacing these with electromechanical systems controlled by electronics and software, energy losses are reduced and significant vehicle weight savings can be made, thus contributing to the environmental benefits.

In order to achieve this, the use of so-called Drive-by-Wire solutions is required. These solutions have since long time been used in control systems for e.g. aircrafts and sea vessels. Technology and quality assured work methods suggest a great potential for this type of technology also for future road vehicles.

To be able to produce safe, competitive and efficient solutions in an economically way based on the components and technologies which are currently under development, a well thought out architecture is required. The architecture must support a structure that meets the safety requirements for future vehicles and powertrains. It is a major challenge to define such architectures and assure the technology, expertise and methodology needed in order to realize the electric powertrains and related functions.

With transmission systems based on electric drive and serial hybrid solutions where e.g. electric wheel motors are used, the degrees of freedom regarding which functionally that can be achieved increases compared to a traditional mechanical drive train. The energy-consuming gear stages in the mechanical transmission are replaced by electric power distribution controlled by electronics and software. The electric drive motors also act as generators so that the braking energy can be used later during acceleration. Individual control of the wheel drive allows for improvements in accessibility, performance, directional stability, and more. Used in a correct way such a system can not only be more energy efficient but also provide enhanced user experience, safety and comfort.

The degrees of freedom in the system set very high demands on reliability and safety. Failure of the control system can lead to serious consequences if it is not designed in an intelligent way. The control system integrating the parts has to meet new levels of safety and robustness requirements compared with similar systems. One may compare with a parallel hybrid electric vehicle, which is based on a combination of both conventional and electric drive line, and is not entirely dependent on the "new" system introduced. Here the proven conventional technology remains as a "fall-back" solution if failure should occur. Parallel Hybrid vehicles have less potential in terms of functionality, flexibility and energy efficiency compared with serial hybrid vehicles.

For series hybrid solutions, which are the focus here, there are tougher requirements in terms of availability and safety on the electronics and software implementing the functionality of the systems.

All different levels of the system, from sensors, electronics, communication, operating system and application software, must be designed for a safe system. This means that systems development, design and test activities are carried out such that overall quality is ensured at the proper level. It is all about how to utilize and integrate the correct technologies as well as applying appropriate methods and work processes.

As mentioned above, the drive-by-wire solutions have already established themselves in other forms of transport systems such as aircraft, ships, etc. Both technology and methodology is available to introduce this type of solutions in the automotive industry.

Instead, the challenge is to design architecture and systems solutions for safe and reliable control systems for future series hybrid vehicles with sufficient flexibility, scalability and growth potential in order to meet the market expectations.

The project partners have approached the problem area on their own through research and development activities, both internally and in external collaboration, and accumulated their own experiences, such that they are complementing each other.

Volvo has since many years a leading role as a supplier of commercial vehicles and has had successes with the parallel hybrid solutions for e.g. buses, garbage trucks, etc.

BAE System Hägglunds has extensive experience in the development of series hybrid solutions such as e.g. the SEP, and long experience of other advanced system solutions for automotive systems, where safety-critical aspects are central. Hägglunds has participated in external R & D projects, for instance in the Green Car programme with a focus on electrical machinery and vehicle dynamics specifically for series hybrid vehicles. Internally, the recent process development to include the ISO 26262 standard has been conducted, where Hägglunds also have been actively involved in the standardization work.

Mecel AB has extensive experience in system development within the automotive industry. Mecel was present when the first generation of distributed communication systems (CAN-based) were developed in the early 90's and has since then become a global player, supplying both products and expertise in the field. Mecel is well positioned to take the "In-vehicle Communication" to the next generation system (drive-by-wire solution). Among other things, Mecel has both expertise and proprietary tools based on AUTOSAR, the standard software platform chosen by the automotive industry, and also ISO 26262 , the standard approach to create safe system solutions, and finally, the model-based tool chains that are necessary to cost-effectively build the system for this project. Mecel has also, as a supplier to the automotive industry, the necessary knowledge to industrialize solutions into cost effective products.

Volvo and Hägglunds both design and build vehicles for various industries, and Mecel has for years been engaged by both Volvo and Hägglunds. The different business focus

and expertise complement each other and an interaction between the different domains (military and commercial vehicles), has been a "win-win" situation that will strengthen the Swedish automotive industry.

Volvo and Hägglunds use their market knowledge to formulate system requirements. Mecel has experience with methods and tools for modeling functionality and build executable models. All three partners have contributed to the choice of technology for realizing a bench system.

3 Objective

A series hybrid vehicle based on electric hub (wheel end) motors will need “drive-by-wire” solutions, exchanging the mechanical transmission with power cables, electronics and software. The design and architecture of this control system is a challenge and bottleneck for the whole automotive industry.

The objective of the project has been to present a realistic control system architecture for series hybrid road vehicles with wheel end electric motors including “drive-by-wire” solutions. The architecture fulfils safety requirements as well as functional requirements needed for the integration of various vehicle subsystems and drive line components. The results include guidelines, principles and solutions as well as proof of concept for the design and system integration. Besides fulfilling safety and cost efficiency requirements the system is scalable and able to adapt to various platform configurations.

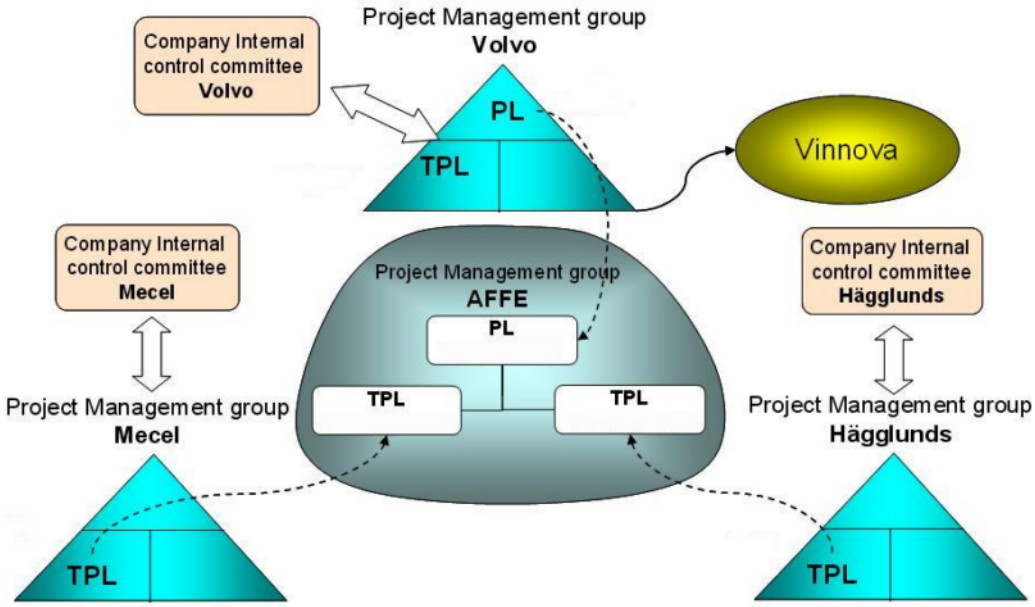
The strategy has been to use existing standards and technologies in the project. This involved adapting the activities of the project to the functional safety standard ISO 26262, implementing the software architecture using the AUTOSAR standard and realising a bench system using industry standard hardware and communications solutions to validate the solution. Also, the tool chain was based on an industry standard set of development tools by Mathworks to support a model-based development approach.

4 Project realization

This section describes the organization and execution of the project.

4.1 Organization, management and communication

The project organisation has on "the top" a project management group with 3 persons formally selected as representatives from each company part. The formal members of the steering management group and responsibilities etc. is defined in the document "Projektavtal AFFE.



Project Management Group:
Project Leader (Coordinator): Stefan Nord, Volvo AB
Technical Project Leader: Carl-Michael Wagner, Volvo 3P
Technical Project Leader: Peter Lööf, Mecel AB
Technical Project Leader: Tom Sundelin, BAE Systems Hägglunds AB

Each partner are free to define a control committee to support and guide there group of project members to fulfil the progress and result fulfilment in accordance with their goals and strategy to participate in the project.

4.1.1 Communication

Regular telephone conferences together with LiveMeeting have been held throughout the project from 2009 to 2012:

Year	No meetings
2009	5
2010	35
2011	7(*)
2012	12

(*) During 2011 the number of meetings were relatively low compared with 2010 and the basic reason was problems with the allocation of resources, first at Volvo and then later also at Mecel. The large amount of meetings during 2010 was that the there was a lot of planning work during that year. In addition to this, a number of physical meetings have also been held:

Date	Location	Description
2010-06-15	BAE Systems, Stockholm	Project planning workshop
2010-08-23	BAE Systems, Stockholm	Project Meeting
2010-09-15	BAE Systems, Stockholm	Kick Off
2010-10-06	BAE Systems, Stockholm	Project Meeting
2010-12-14	BAE Systems, Stockholm	Project Meeting
2011-02-02	Mecel, Gothenburg	Kick Off
2011-06-21	BAE Systems, Örnsköldsvik	Project Meeting
2011-10-26	BAE Systems, Stockholm	Project Meeting
2011-12-15	BAE Systems, Stockholm	Project Meeting
2012-03-15	Volvo, Gothenburg	Project Meeting
2012-08-22	Volvo, Gothenburg	AFFE Seminar
2012-08-28	BAE Systems, Örnsköldsvik	AFFE Seminar

4.2 Methods and tools

4.2.1 General tools and standards

Initial in the project it was obvious that the ISO26262 was a useful standard. However this standard is only covering parts of the development and is supposed to be integrated with a general based development process. After evaluations of alternatives the project selected "Volvo System Engineering Guideline" as a general structure to follow and upon this apply the ISO 26262. Tools used for project documentation and planning have been "Teamplace" supported by Volvo. When the project participants have a long distance to travel for "physical" project meetings the use of Net meetings and telephone meetings have been frequently used. This have reduced travel cost, travel hours and have made communication between the project parts effective.

For making specifications and presentations standard Microsoft tolls have been used such as word, power point, Visio, MS-project etc.

For the model building, simulation and test, Math works products have been used such as Simulink and Simscape. The architecture and structure of the software have built on the use of AUTOSAR standard. CAN and FlexRay standards have been selected as candidates for the communication in the target system.

Summary of main tools used in the project:

- System engineering:
  - Volvos System Engineering Guideline
  - ISO 26262
- Architecture /design and simulation:
  - AUTOSAR
  - FlexRay
  - CAN
  - Mathworks tools
- Project management/documentation:
  - LiveMeeting
  - TeamPlace
  - MS Office standard tools

4.2.2 Methods for system definition

To define a common system definition for a future truck and its internal structure can be a challenge when the view can differ from each project part and individual project participants.

In the ”state of the art” work situation analyses have been made in a number of relevant areas to evaluate trends, tools and products to be used for the system definition and architecture work. See Figure 1

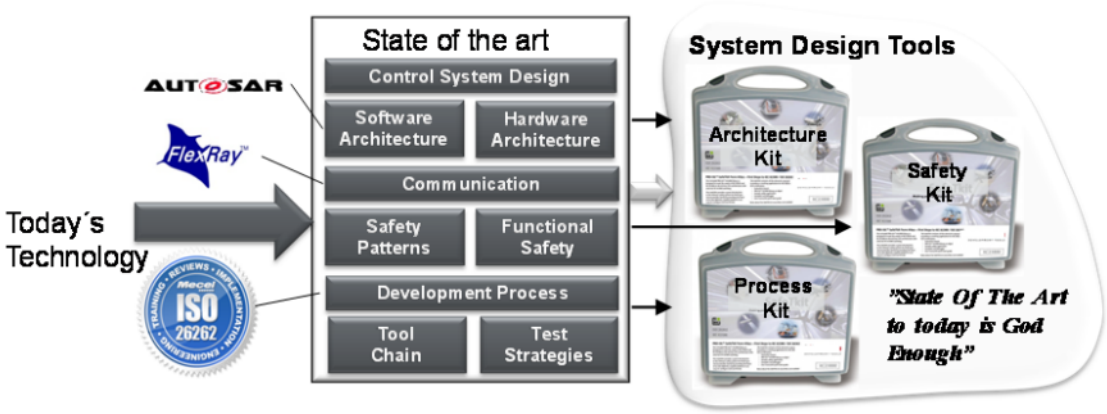


Figure 1. The “state of the art” work delivered input of “tools”-boxes supporting the system design of the future Vehicle platform in general and the control system in specific in the project.

In the “State of the Art” work package evaluations and motivations for the selection of different technologies was made.

The statement “State of the art – is good enough” was established in the project. When looking into the design of a product to be placed on the market in 10 to 15 years we should not speculate in using coming, not well-known solutions to much. Instead the idea was to find new but matured usable technologies that likely will be established and used during the next 10 years instead of speculating to using more immature newcomers of technologies. AUTOSAR, FlexRay and the ISO26262 were evaluated and selected parts during this work package.

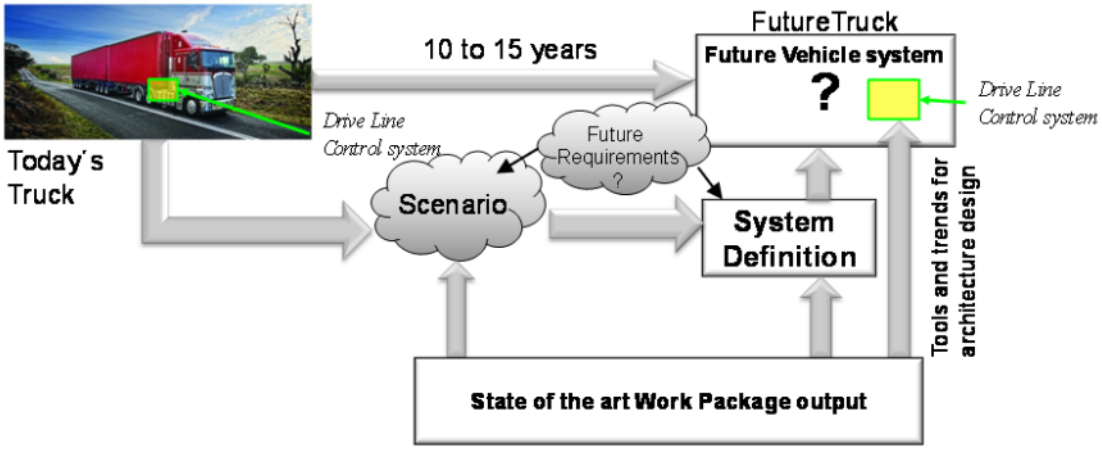


Figure 2. The output from the "State of the art"-work was used as input to a scenario description of how series hybrid system could evolve. This was in the next step used to make the system definition of the future Vehicle and also effecting the definition of the control system.

The output from the "state of the art work" was used making scenarios and system definitions defining the future Vehicle systems in general. A typical 4 wheel drive smaller Truck was selected as a target system to simplify the process to define and design the control system. See Figure 3. Even if the goal was to make a general control system usable for different kind of Vehicle platforms, there was a need to simplify the picture in the first step with a clear defined target system.

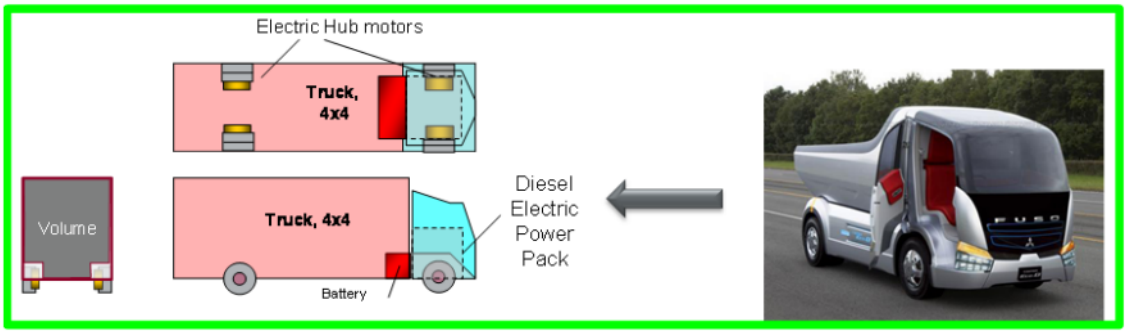


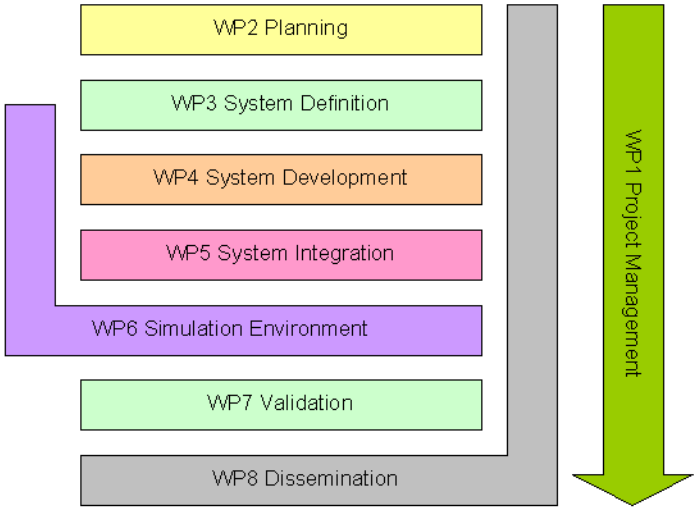
Figure 3. A typical Truck with four wheel serial hybrid drive was selected as a target system.

4.3 Work packages and execution

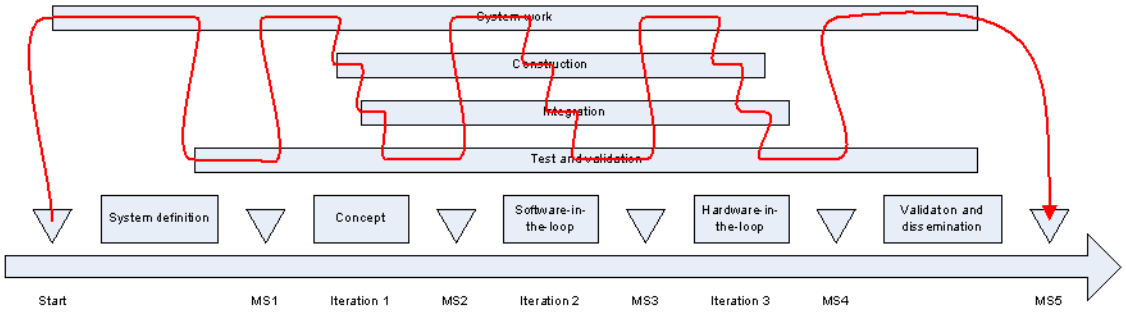
The eight work packages carried out in the project is outlined below.

Work Package	Duration (month)	Activities	Results/deliverables
WP 1: Management	Project	Administration, Project meeting organisation, Follow up	Status reports, presentations
WP 2: Planning	2	Decide work process (including model strategy), Plan phase 1, Develop a terminology glossary	Project plan, Glossary, Project Process description
WP 3A: State of the art	1	Mapping of research area, Technologies and Standards identification, Communication technology, Test/verification strategy	Reports with recommended technologies, standards and best practises
WP 3B: System Definition	2	Need/Requirement analysis form Vehicle functions, Project Delimitations, Communication technology, Design decision, Test and verification strategy (functions), Outline a preliminary architecture	Requirements specification, Concepts decision, Architecture description Validation strategy
WP 4: System development	4	Functional development, Requirements Evaluation/Elicitation, EE architecture Topologies (signal and Power distr.), Definition of Safety concepts, Automotive safety case, Definition of Interfaces (to interacting vehicle functions/systems), Processes and tools, Adapt a auto-generated Tool-chain	Detailed Architecture description, Design descriptions, Safety concepts, Safety cases, Models, Interface descriptions, Defined Tool-chain
WP 5: Integration	2	Integration approach and testing, Functional Integration	Executable system
WP 6: Simulation environment	4	Test environment and verification strategy, Implement and configure a sw-platform, Model in the loop development, Develop test and simulation environment, Integrate and verify a completed test bench	Test bench integrated with the simulation environment
WP 7: Validation	3	Test and verification, model in the loop, Test and Verification in Test bench, Safety validation	Proof of concept, Test reports, Safety report,
WP 8: Dissemination	1	VINNOVA Presentation, Define presentation (ppt) material, Write Report, Plan phase 2	Final report and presentation

The work package structure and their internal relationship are outlined below:



The development in the project was planned with a first system definition work package, then three major, iterative, steps; concept, software-in-the-loop and hardware-in-the-loop, and lastly validation and dissemination work packages.



4.4 Challenges and experiences

The toughest challenge has been the resource situation, first at Volvo as Volvo 3P could not contribute with the amount of resources initially planned. The main reason has been highly prioritized product development projects. This led to lost momentum in the beginning of the project. This situation also made it hard for the other partners to secure resources as the project was not up to speed. The resource situation at Volvo was improved and during the spring of 2011 Volvo had manned up the project with resources from Volvo Technology. During the autumn of 2011, Mecel had to pause their activities due to prioritization of other projects. This gave however Volvo some time to catch up with some lost time. Also BAE Systems had some minor resource issues from time to time. The distributed nature of the project was initially a concern. But the use of a combination of physical meetings and teleconferencing using e.g. MS Live Meeting and application sharing has shown to be very effective in combination with a common project area in Volvo's TeamPlace environment.

5 Results and deliverables

5.1 State of the art

The State of the art analysis was a part of WP3A and was intended to serve as a foundation for the further development work within the project by mapping the research area and proposing suitable technologies, methods, tools and processes.

5.1.1 Software Architecture

This State of the Art, SoA, study with regards to Software Architecture for the AFFE project is concluding the research efforts of finding out which are the probable SoA technologies for making software in 2015 that would be applicable for creating safety related software for distributed vehicle dynamic control functions.
The study has investigated a number of different possibilities for the software layers. It is proven by the software industry that layered and modular software architecture with well-defined interfaces is the most efficient way to distribute development over location and time. With this approach it is not possible to gain the speed and size efficiency that can be reached by a highly integrated and monolithic software but on the other hand it is easier to locate problems and solve issues.
Based on the thesis that a SW architecture shall be layered the conclusion is: An automotive SoA ECU will probably contain AUTOSAR 4.x or higher. The ECU will on SW-C level contain components created in one or more model based development environments, i.e. Simulink for control loops and Enterprise Architect for UML models. Furthermore will they contain software written in C and possibly C++ based on the Embedded STL. Possibly will, for the embedded development, new concepts as i.e. functional programming become industry standard as well.
The recommendation from this study is that AFFE will be built on an AUTOSAR platform version 4.x and also implementing the concepts of; model based programming by using Simulink, imperative programming by using C and OO programming by the use of C++ where each concept is applicable. AFFE should also if possible try to implement a SW-C in a functional language. (Fritzson, AFFE 015 State of the Art Software Architecture, 2010)

5.1.2 Communication

This SoA study is concluding the research efforts of finding out which are the probable state of the art technologies for in vehicle communication in 2015 that would be applicable for transmitting safety related information for distributed vehicle dynamic control functions.
The study indicates that there are several possible base technologies readily available for x-by-wire. Aerospace as well as industrial application has mature x-by-wire concepts that are in production. These concepts are however not ready to use for the automotive

applications that want to do x-by-wire. Aerospace protocols are produced by the fact that few units are produced at a high cost it is therefore better to use commercial-of-the-shelf hardware at a higher cost than spending development time on producing highly specialized solutions. This argumentation can also be applied for the military branch of road vehicles where the number of produced units is low compared to development time.
For the protocols implemented for industrial applications the argument is that the protocols are highly optimized for automation use with profiles and a set structure of interoperability, it is not likely that the automotive industry will try to reform an industrial protocol and adapt it for automotive use. Industrial applications are, at most times, stationary installations with larger distances between communication nodes. Altogether this makes field buses less likely to rise as an accepted technology.
Based on the arguments above together with the analysis described in the full report (Fritzson, AFFE 016 State of the Art Communication, 2010) the possible technologies for future use are FlexRay and an automotive specified Ethernet solution possibly based on AVB or TTEthernet technology. At this point in time TTP is not accepted by automotive and it is not reasonable to expect that to change shortly.
The conclusion is that for current studies in the AFFE project FlexRay should be used as the main communication protocol for closed loop regulation. It is probably wise to give some attention to the development of TTEthernet and AVB related protocols. Since they have the properties needed and attention by the automotive industry they might be SoA in a near future. (AFFE 016 State of the Art Communication)

5.1.3 Tool chain

The tool chain SoA investigation for AFFE is an effort to find out which type of tools that will be the automotive industry SoA in 2015. The investigation is made with regards to development of the closed loop and safety related part of the electrical architecture for electrical hybrid vehicles.
In AFFE the aim should be to use commodity tools as much as possible since these tools are the ones that are available at the participating companies, it is however necessary to evaluate these tools with regards to safety requirements. The cutting edge of the tool development within the automotive industry is currently aimed at ISO 26262 and AUTOSAR. These focus areas together with tools that can reduce the manual work necessary for validation and verification; there is currently no industry standard on how to write requirements that can be automatically tested by tools. Additional efforts should possibly be spent to find and possibly contribute to tools within these areas. (AFFE 017 State of the Art Tool Chain)

5.1.4 Hardware Architecture

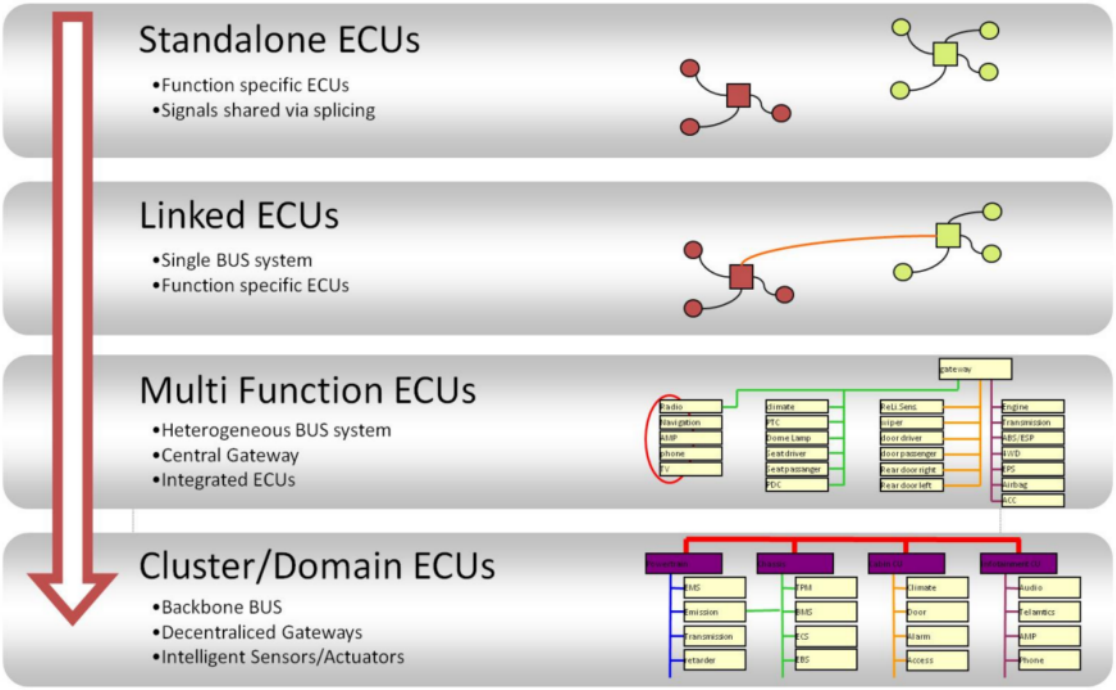
This part of the SoA explores trends and requirements for the hardware architecture. Non-safety critical application currently remains single-processor unit with simple hardware watchdog and directly coupled actuators and sensors. Safety critical hardware components are considered by being very dependable and therefore need to support fault

tolerance, error detection and error handling. Redundancy is the traditional approach for improving hardware dependability.

Severity index based on Volvo Safety related ECUs (application specific) this is linked then to the EMC requirements. ECU's are early characterized by (critical characteristics):

1. A danger that can lead to personal injury
2. A failure in operation
3. A disturbance in operation

The Picture below shows the Automotive Network Topology Evolution.



Important aspects for the future automotive hardware architecture:

- Well defined and standardized interfaces
- Flexibility
- Complex Gateway with high performance (multi-core controllers) and specific networking
- Reduced number of ECUs
- Simple error detection and error handling
- Reduced wiring
- Software standardization (AUTOSAR)

The integration of Safety Critical features into the EE network architecture that today consists of a distributed electronic architecture composed by several Electronic Control Units (ECUs) with distributed functionality will put up new prerequisites. Such as

- a fault tolerant design with error detection and error handling
- a more complex communication system
- a dependable power supply network

and yet it needs to be

- cost effective
- flexible
- scalable
- higher speed and accurate information exchange
- Standardised

Space and cost reduction are high priorities for automobile applications, there is a demand for improved circuit reliability with the minimum amount of hardware addition. According ISO26262-5 hardware development shall at least include the following safety related requirements:

Hardware safety requirements

- shall control external failures of the hardware (i.e. failure occurring outside of the limits of the hardware)
- shall control internal failures of the hardware item, with their relevant attributes such as timing and detection abilities of a watchdog
- shall have monitoring methods committed to indicate internal or external failures to the driver (e.g. watchdog with driver warning),
- shall avoid and control systematic failures (e.g. safety critical timings in normal mode of operation).

5.1.5 Safety Patterns

A good method for architecture conception is to use structure components from a library of experienced and well tested components. In literature these components are called styles or architectural pattern. The libraries define the pros and cons of each component and its possible imbrication with other ones.
Design pattern includes several blocks and their interfaces. It describes the whole subsystem providing the safety functionality. Around a main design pattern idea, small dissimilarities generate variants. This causes a huge number of design patterns.

This SoA study presents a list of design patterns corresponding to safety issues that can be applied in automotive electronic architecture. For each pattern, the description of the

structure is précised with its pros and cons, with the implementation strategy and with a concrete application.
To facilitate the selection of the better architecture solution regarding a need, these patterns are compared in a clear representation. The axes of comparison are the different properties of a system and its creation project constraints.
This SoA study would not have been complete without relating to standard norm. A parallel is made between the library of safety patterns defined here and the recommendation of the norm ISO 26262.

5.1.6 Development Process

This SoA study is based on the topic: What processes are currently used to develop automotive safety functions?
More such functions are expected to be developed, and the upcoming ISO 26262 standard is also expected to have an impact on the processes being used. When defining or selecting a development process several aspects need to be considered, here we focus on the following:

- The actual activities needed to produce the desired output
- The control gates for managing the project
- The way to organize development in iterations
- System development processes versus software development processes
- Compliance with functional safety standards
- System safety

There exist several standards and published processes to rely on, but there is no known single process that is covering all aspects needed. Some efforts to create a complete and integrated process remain. In practice it is usually not a good strategy to take an existing development process and tell an organization to start using that process. It is necessary to start from processes existing in the organization and gradually adapt those to be compliant with the standards.

According to this SoA study there are a lot of processes defined to some level of detail that could be useful for developing automotive products including safety functions. However, there is really no complete process that you can take off-the-shelf and apply as it is. You need to integrate and adapt these existing processes. More importantly, even if there was such a complete and finished process, it would in practice not be possible to enforce it on an organization. It is in practice necessary to start from existing processes in the organization and gradually improve and adapt the processes to incorporate more capabilities, e.g. compliance with functional safety standards.

For an individual AE project, where there is more freedom to choose a process other that the normal process used in the organization, other processes could be tried out. It is probably still wise to start from existing processes that people are familiar with and then

add missing aspects from e.g. ISO 26262. If other processes are tried out, there should preferably be someone with previous experience from this process that can support or lead the project.

The problem of choosing a process already used in the organization of a company is that it is considered to be a company secret and nothing that the company is willing to spread outside to other companies. For this project it was a major obstacle, but was solved by using a generic process defined by Volvo: Systems Engineering Handbook.

5.1.7 Functional Safety

In the AFFE project we interpret 'functional safety' as defined in the ISO 26262 standard:

> *Functional safety: absence of unreasonable risk due to hazards caused by malfunctioning behavior of electrical/electronic systems.*

An investigation of the state of the art in the field of functional safety was performed and documented in an early phase of the AFFE project. Several standards, guidelines and research projects were overviewed and are briefly listed below.

ISO 26262 is a standard for functional safety of road vehicles. The standard is based on a safety lifecycle encompassing the definition, development, verification, validation, production, maintenance and decommissioning of an automotive electrical/electronic system. It sets requirements on what to do, how to do it and how to document the results of these activities. For the AFFE project, we consider ISO 26262 to be the most relevant standard related to functional safety. The motivation for this selection is that ISO 26262 covers the full scope of functional safety while being specifically concerned with automotive electronic/electrical systems. Furthermore, it represents the current view of functional safety shared by major automotive manufacturers and suppliers throughout the world.

IEC 61508 is a standard for "Functional safety of electrical/electronic/
programmable electronic safety-related systems". It is generally considered to be the fundamental standard for development of safety-critical systems, at least for those industrial domains for which no other domain-specific functional safety standard exists. However, since the ISO 26262 is based on the IEC 61508 and is adapted to the automotive industry's specific needs and ways of working, we do not consider IEC 61508 to be particularly relevant to the AFFE work except as a reference for understanding the background of ISO 26262.

The United Nations Economic Commission for Europe has produced a set of vehicle design regulations. Annex 18 of ECE-R13H for brake systems and Annex 6 of ECE-R79 for steering systems are concerned with "Special Requirements to be Applied to the

Safety Aspects of Complex Electronic Vehicle Control Systems". These annexes define requirements for documentation, fault strategy and verification.
These UN standards are specifically concerned with steering and braking and may therefore not seem particularly relevant for hybrid propulsion. However, the functional safety issues covered in these annexes are general and could be applied to any application. But more importantly, their requirements related to functional safety are in principle covered by for example ISO 26262. Therefore we do not consider these standards as particularly important for the AFFE project.

The MISRA C and C++ guidelines contain rules for the source code in these programming languages, in order to reduce the possibility of programming error and to avoid programming constructs that are ambiguous or otherwise known to cause problems. MISRA C has been adopted and used across a wide variety of industries and applications including the rail, aerospace, military and medical sectors. Furthermore, a significant number of tools are available that support enforcing the MISRA C rules.

EASIS (Electronic Architecture and Systems Engineering for Integrated Safety Systems) was an EU-funded research project in 2004-2006. The project addressed hardware and software architecture issues as well as systems engineering methodology.
One work package of EASIS was concerned with dependability issues and actually focused on functional safety. In this work, a dependability activity framework was defined and guidelines for a number of dependability-related development activities were created.

CESAR (Cost-efficient methods and processes for safety relevant embedded systems) was a European ARTEMIS project during 2009-2011, focusing on requirements engineering, component-based engineering and associated development tool support. With respect to the AFFE project, the automotive-specific subproject (SP 5) and its relation with other CESAR subprojects has some relevance for AFFE.

5.1.8 Test Strategies

In the document ref (Abrahamsson, 2010) aspects concerning test strategies and it´s relation with the ISO26262 are presented and discussed. A summery is presented in the followings:

Some important goals for the test work are to:

- find problems* in the electronics and software as early as possible in the development process.
- assure the quality of the embedded system.
- continuously validate the hardware and software functionality.

The test strategy is dependent on the development strategy that has to be adapted to what kind of system to develop and test. For more complex products an Iterative development process is preferable even if the process is described in a V-model.

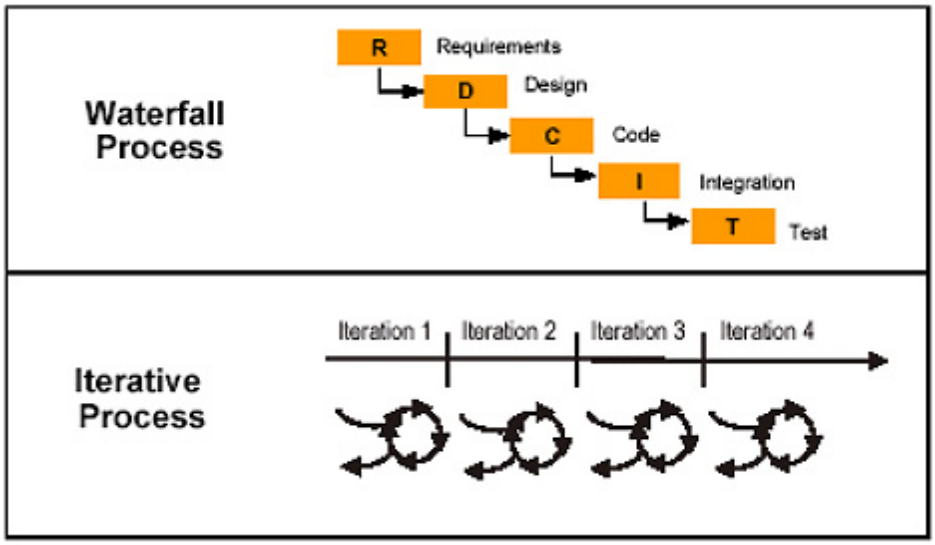


Figure 4 Waterfall model is normally suitable for non- complex system development and an Iterative development process more suitable för a more complex system development.

Development of a hybrid driveline is complex; often the requirements change during the process and it is an immature product. Therefore it is suitable to use an iterative development process hence the testing is iterative.

One important strategy is to divide the test in different levels. Examples of levels are:

- Vehicle integration and testing
- Sub-System integration and testing
- HW/SW integration and testing
- Component testing (both software and hardware)

The use of the ISO26262 standard supports the test activities in a good way. The project have analyzed this and tried to follow this standard during evaluation in the work.

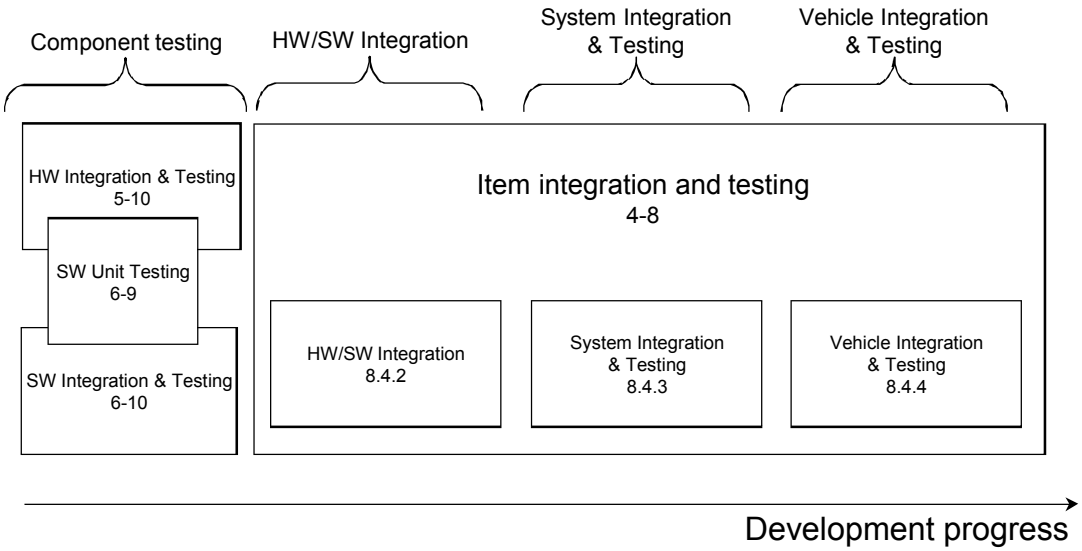


Figure 5. In the picture references is made to different parts of the ISDO26262 standard, giving guidelines for different levels of testing.

5.1.9 Control Design

This SoA study is concluding the research efforts of finding out which are the upcoming technologies for vehicles control systems. It aims to give an overview of the control and regulation techniques developed for hybrid vehicles, with focus on the control systems for serial hybrid and find out which control architecture and algorithms will be SoA in 2015. Nevertheless, one shall be aware that even if the control strategy makes the performance of the whole system, we have to be aware that the hardware configuration dictates to some extent which control strategies make sense. So, the conclusions of this study may not apply to all hybrid vehicles hardware architectures.
Before determining a suitable control system architecture, one shall wonder what are the main objectives, and whatever the hardware architecture, the key goals for a hybrid vehicle remains the same. They are: Maximum fuel economy, Minimum emissions, Maximize operating range, Minimum system cost, and Good driving performance. With this SoA, we have been able to determine that, considering the key goals, to succeed in the realization of a relevant control system and provide a smart, efficient and reliable control strategy, 3 main areas have to be focused on. Those three domains are Vehicle motion control, Energy management, and Functional Safety.
Many kinds of controllers can be used on hybrid vehicles, and to control systems in general, depending on the function and the objectives. Those controllers can be classified in 4 main families depending on their structure: Deterministic rule-based controllers,

Fuzzy rule based methods, Global optimization, Real-time optimization. The main characteristics of each type of controller have been presented in the appropriate chapter, and those descriptions will help us to choose the most suitable type of algorithm for our system. Nevertheless, the control system architecture can vary a lot and is more dependent on the appreciation of the designers than conventional rules, but for one type of problem some tendencies can be highlighted and the same type of controller algorithm, part of one of the four aforesaid families, is often used.

According to the articles published, for a serial-hybrid powertrain with in-wheel motors as it is described in the AFFE project, the recommendations for state-of-the-art control system algorithms could be to use: deterministic rule-based controller for the high-level functions of the vehicle motion control (driveline supervision), fuzzy rule based methods for the low-level functions of the vehicle motion control (torque repartition, close wheels control), and real time optimization strategy for energy management. Finally, the choices of the strategies for safety management will be dependent on the balance between risk and available resources for each risk.

5.2 System Scope Definition

As a part of the WP3 in the AFFE project there is a task to investigate what type of development process can be used to develop a system such as the system in scope of the AFFE project. Since the resources in the project does not allow creation of a completely new development process nor maybe not needed since existing processes might be fully feasible. It was therefore decided to try to use the so called Volvo Engineering Guideline, SEG, consisting of the following main parts:

- System Scope Definition
- System Development
- Sub-system development
- Component development
- System integration

In the project we try to apply the System Scope Definition part of the SEG on the AFFE system resulting in this document: (AFFE 026 System Scope Definition). The entire SEG is a Volvo internal document but can be made available for the other project partners in the frame of the AFFE project. As described in the SoA investigation of development process for safety relevant applications (see chapter 5.1.6), when defining or selecting a development process several aspects need to be considered:

- **The actual activities needed to produce the desired output**
  The SEG well define activities and its input and outputs.
- **The control gates for managing the project**
  The SEG does not define project related gates explicitly but due to its nature it can easily be used to find points in the process where gates are naturally placed.
- **The way to organize development in iterations**
  The SEG is described with iterative activities i.e. an activity must in some cases be repeated when a certain input to an early activity has been produced by a later activity.
- **System development processes versus software development processes**
  The SEG covers the system development as well as the SW development activities.
- **Compliance with functional safety standards**
- **System safety**
  There is no explicit support for functional or system safety in the SEG so here is a potential need for revision to, if applicable, formally integrate the safety activities in the SEG.

The experience from this work trying to apply the SEG System Scope Definition is that it is a feasible process to use and that it gives a very good support to the engineer. However the SEG should be revised possibly leading to a revision regarding the functional safety issue since the Functional Safety standard ISO26262 has been released since the creation of the SEG.

5.3 Electrical & Electronic Architecture

In the project variants of different possible physical architectures are evaluated and described. In general one conclusion is that the hardware technology to day is not an obstacle for to support the qualities of a system to both fulfill functional requirements and safety requirements needed. Not even for a future serial hybrid Vehicle with individual separated HUB-motors. However there is not a single ideal, optimal architectural solution to find. This relates to the fact that besides safety and performance the architecture relates to a lot of non-functional requirements such as cost, production, knowledge etc. Those differ from company to company and there individual situation as well as it differs between different market and situation where the product (Vehicle) is used. Anyway the project have defined a generalized physical architecture to build on that have the quality to be modular and flexible to be expended both in size (number of wheels) and in level of redundancy. Below principle picture of this architecture is shown.

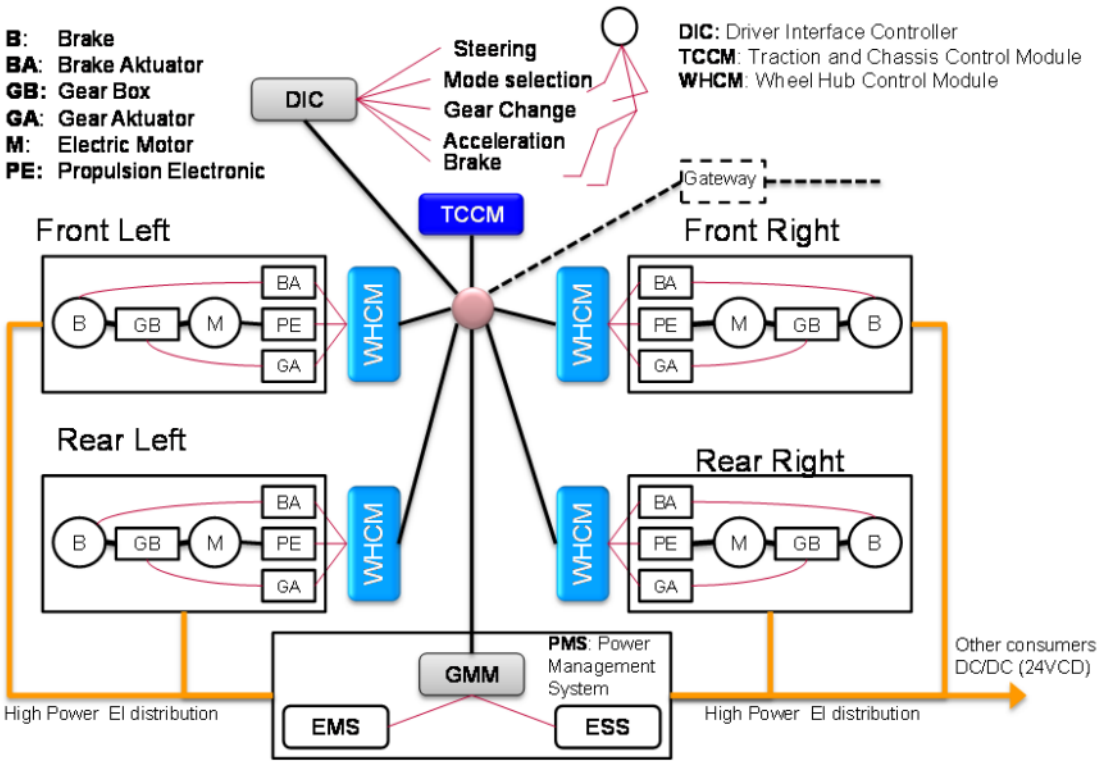


Figure 6 Different solutions to support safety requirements are evaluated in the project.

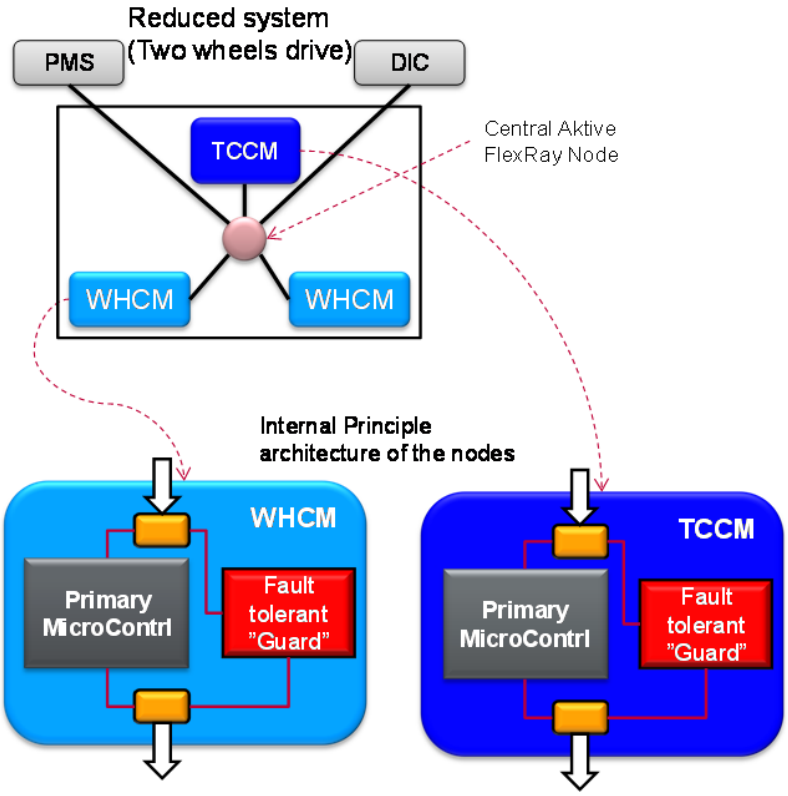


Figure 7. The use of multi core processors the probability for fault findings increases. By using the same principle design of the nodes investment in quality and reduction of price could be combined.

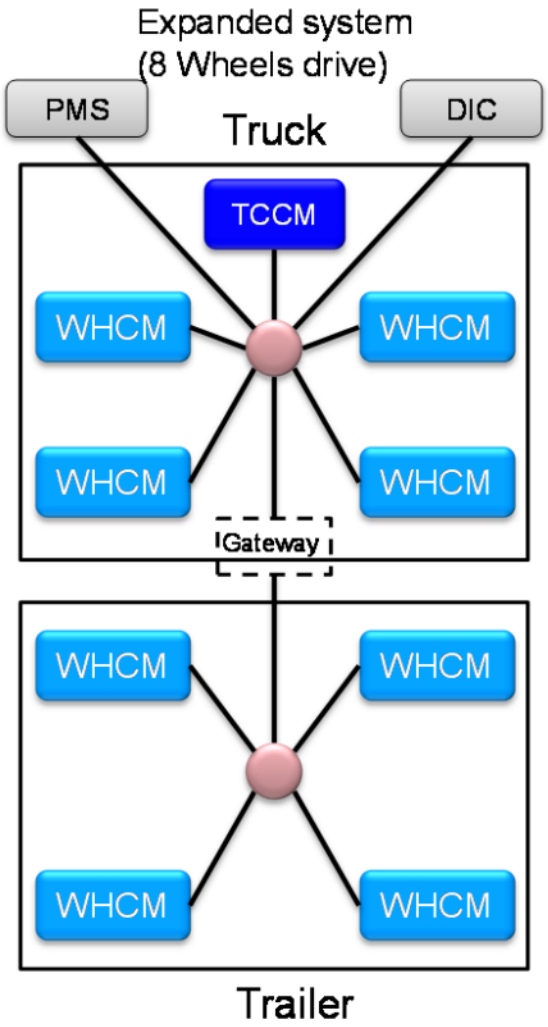


Figure 8. The use of FlexRay communication net could be expanded to cover also a trailer supporting the transmission with additional hub-motors. In the picture the network could be expanded with a redundant additional network that is supported by the FlexRay technology.

5.4 Control System Development

Based on the SoA study, following activities have been carried out during the project aimed control system developing.

5.4.1 Analysis – Desired Capabilities

Use (AFFE 026 System Scope Definition) document as an input following desired capabilities in the control system are determined. Detail description for each capability and system requirements can be found in above mentioned document.

- Motion Mode Control
  - Driving situation determination
- Transmission Power Control
  - Energy management system
- Vehicle Dynamics Configuration
- Motion Control
  - Driver wishes interpretation
  - Total moving torque determination
  - Final torque combination
- Brake Control
  - Retardation
  - Brake management system
- Steering Control
- Stability Control
  - Slip Control
  - Lateral acceleration controller
  - DYM/Yaw Controller
- Vehicle mode Control
  - Driver wishes interpretation
- Diagnostics
  - Functional safety management

5.4.2 Design - Electric Transmission Control Functional Architecture

Different versions of the architecture have been discussed. A satisfied final functional architecture is illustrated in Fig. 4. The desired capabilities listed in above section are mapped in the architecture.

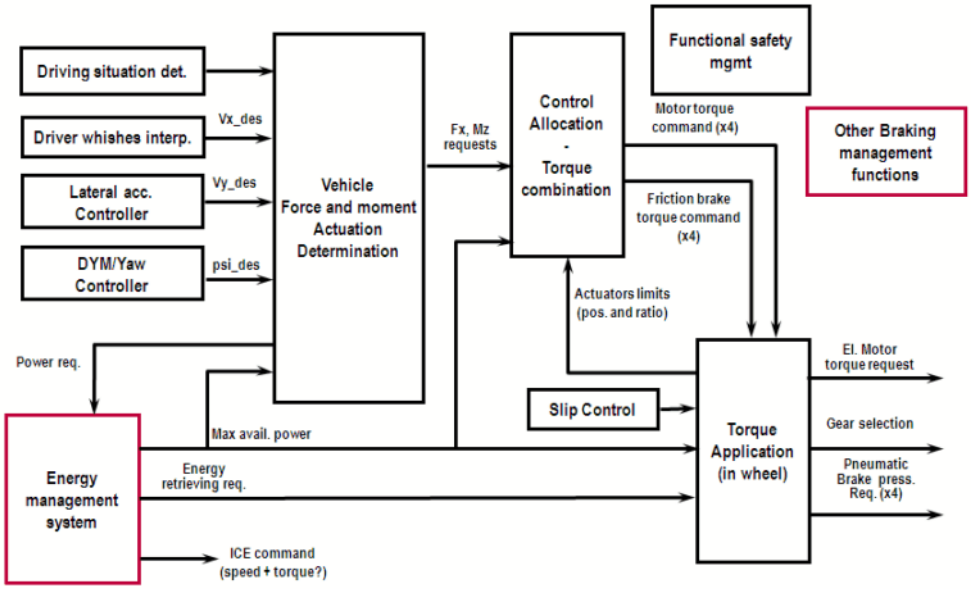


Figure 9 - Illustration of preliminary design for Electric Transmission Control Functional Architecture, final version (Red marked blocks are out of project scope)

5.4.3 Implementation - strategy

After we agreed on a satisfying global functional architecture, we had to evaluate what we could be able to implement within the time we had and determine where our priorities were. We finally came to the conclusion that the top priority was to design the propulsion and braking functions for the basics movements, so the most important functions for us were to be able to understand the driver request, create a torque request to each wheel from this, and send and apply those requests on the wheels. Then the second priority was to improve those basics movements' functionalities with for example yaw-rate control, or slip-control.

Then, as an option in our development, if time allowed it in our planning was to have a look at the functional safety requirements and fulfill at least one of them on the demonstrator. Unfortunately it appeared that we had no time for that due to several integration problems. So, no diagnostics have been implemented.

Finally, we decided not to development any energy management algorithms as well. The reason for not implementing energy management was simply because even if we talked about the system architecture in the project, we did not choose a precise energy storage

system, yet we would have needed such information to be able to manage correctly the available power.

So here is a schematic presentation of the implemented functions:

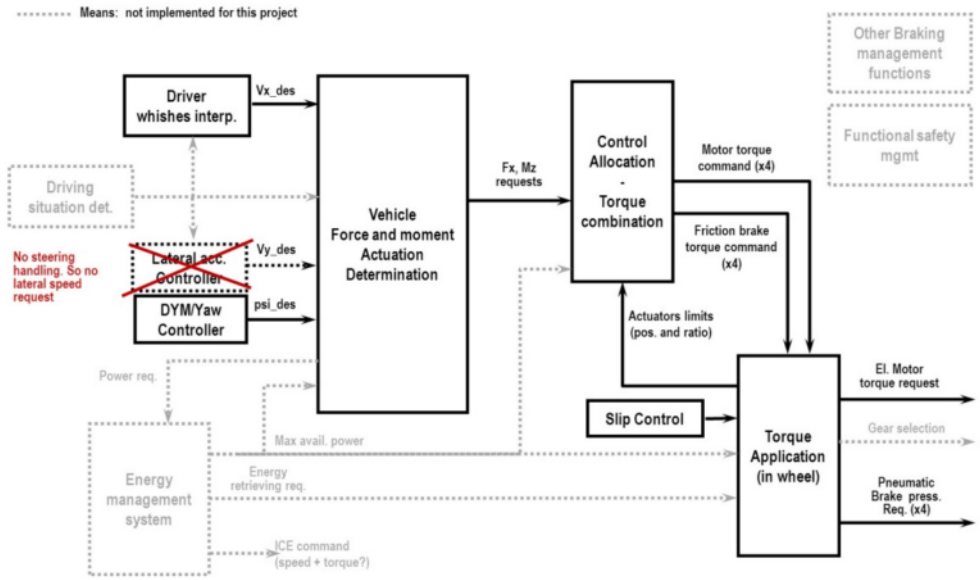


Figure 10 - AFFE Implemented functions

This functional architecture is distributed over 2 different function levels or ECUs according to the hardware architecture (Fig. 3) chosen in the project. I.e. one TCCM (Traction and Chassis Control Module), and one WHCM (Wheel Hub Control Module) in each wheel.

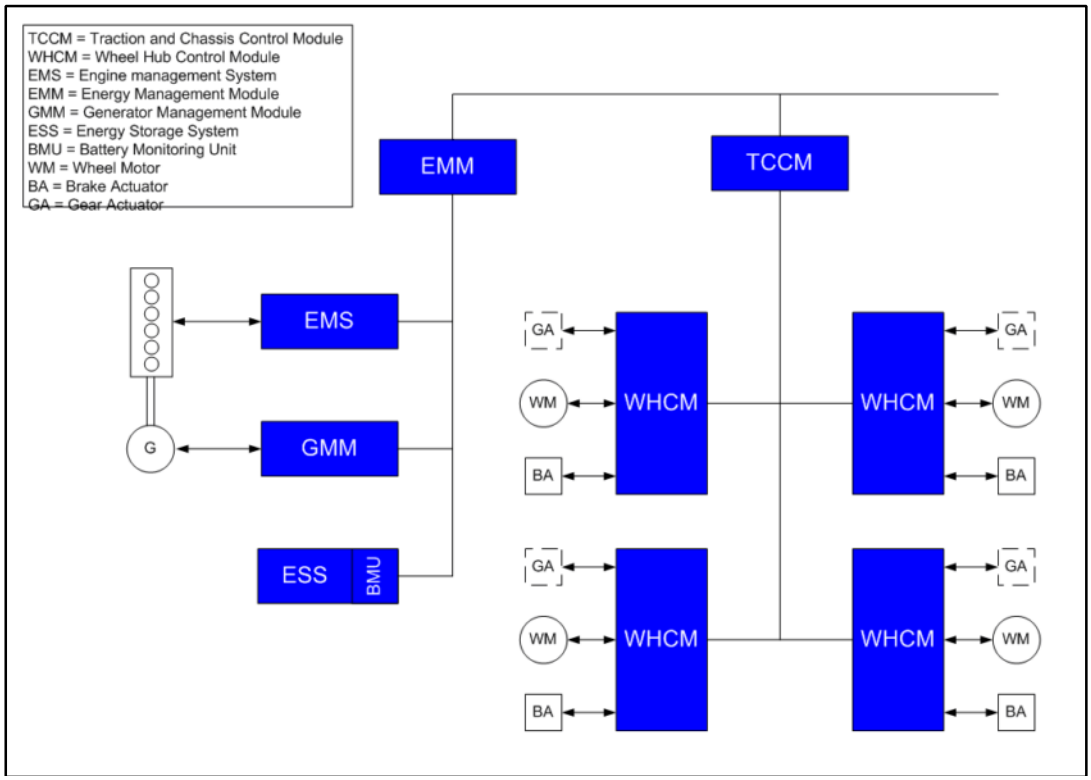


Figure 11 - AFFE Hardware architecture

A corresponding functional partitioning in control system is implemented. The first part is implemented in the TCCM and is a vehicle-level /node, including all the functions which should be run on a vehicle level such as: driver interpretation, path and vehicle dynamics control and control allocation. This part has been called “MainSystem”. The second part is implemented at the wheel level or the WHCM. In this unit, all the functions concerning close-control of the wheel actuators are implemented such as: Electric motor control, friction brakes control and slip control. This part has been named “WheelControl”.

With this architecture, the functions have been implemented as described in Figure 12.

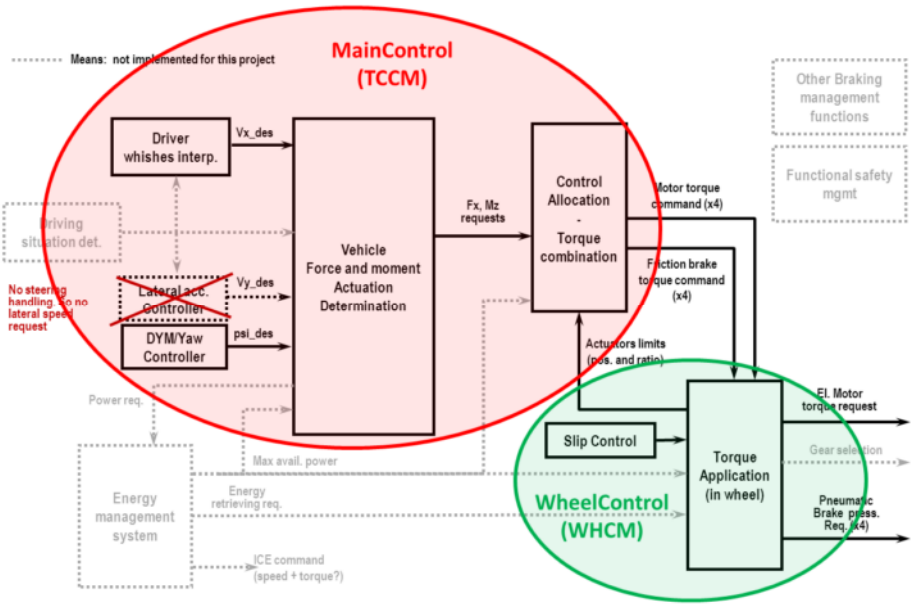


Figure 12 - AFFE functions repartition in functional components

5.4.4 Implementation - model

Various publications (references can be found in (AFFE 023 State of the art Control Design)) have been used as a base for the development of the control system model. The overall system model is illustrated in the Fig. 5.

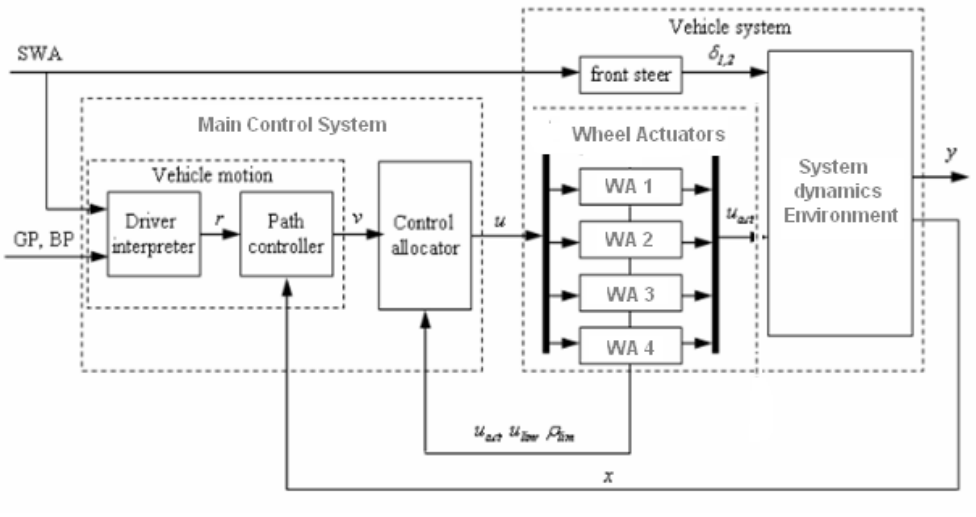


Figure 13 - Illustration of how Control system is. Used abbreviations in illustration: Steering Wheel Angle (SWA), Brake Pedal (BP), Gas Pedal (GP), Wheel Actuator (WA)

The vehicle motion controller calculates the desired path ‘r’ within the driver interpreter and then the path controller tries to keep the desired path by correcting the global forces and yaw torque through vector ‘v’. The correcting ‘v’ commands are then distributed by the control allocator onto the available motion actuators. There is a wheel controller in each motion actuator. It has two objectives. The first objective is to check that the commands computed by the Control Allocator are achievable and if necessary apply additional limitation, and also transform the request from the control allocator into actuator request if needed (i.e. translate actuator request into voltage or change unit). The second objective of the Wheel controller is to watch the wheel actuators (electric motor and friction brake in our case) and compute the actuators limits at every time step, to send them to the Control allocator for next calculations.

Detail implementation algorithm can be found in document (AFFE 032 Control System Development).

5.5 Functional Safety

The functional safety work was conducted in accordance with ISO26262. The scope was defined to include derivation of a Functional safety concept as defined in ISO26262-3. No focus was given on implementation aspects in HW and SW.

The used methodology is further elaborated in section 5.1.7.

5.5.1 Item definition and assumptions

Derivation of a preliminary architecture and a preliminary Functional description is a pre-requisite in ISO26262 to allow the safety analysis to start. This is defined as an Item Description in the standard. The safety work is therefore not formally a part of the initial design. A draft of the system must first be evolved.

The required information to make up an “Item Definition” is approximately what is specified in previous chapters 0 and 5.3. But since this is a research project aiming to derive a future architecture, that information was not available as input to the start of the safety work. Several architectures were evaluated for quite a long time. But we could not wait for a final decision on what architecture to use. So the safety work had to be done in parallel.

A good solution would have been to use two or three iterations, where the safety work would feed-back the results to another iteration of architectural and functional design. And changes in the design would have caused updates to the safety analysis. But the time span of this project did not allow more than one iteration.

Instead we had to make assumptions.

One of the assumptions we made was to exclude (friction) brake control from traction control. This assumption was later revalued by the project, but there was no time to update the safety analysis and derive a new functional safety concept.

We made assumptions on the size and type of vehicle and on some functionality that were not yet defined.

Another assumption was to use a simple star architecture with a centralized control node as described in the figure below. (Note that the nomenclature had not yet settled at this time. The names of the nodes were different compared to e.g. section 5.3.)

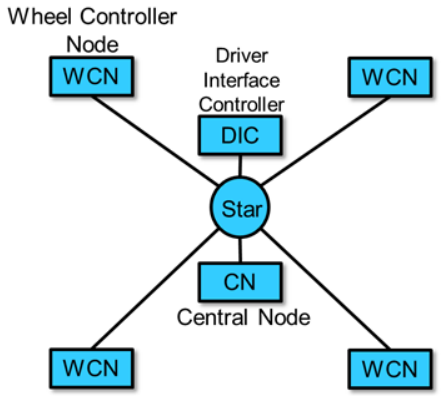


Figure 14 - Assumption of principal architecture

Overall, the assumptions were fairly correct – apart from excluding brake control. That would have changed or concept since we made an assumption of independent friction brakes with very few common mode failures to the traction control. It is highly likely that the criticality for some safety goals would have increased as a consequence.

5.5.2 Hazard Analysis and Risk assessment

The hazard analysis is based on perceivable failure modes of the traction function. In total 21 failure modes. They were derived from new analyses and experience from pervious projects. This work is fairly straight forward.

The next step is to evaluate each failure mode based on the intended use of the vehicle. Each failure mode were given an ASIL (criticality level) as defined by the method in ISO26262-3. This includes evaluating exposure to the driving situation, the controllability for the driver after the failure and the potential consequence if the failure leads to an accident.

A lot of effort was spent on the different cases. All assumptions regarding vehicle behavior and human interaction were logged.

The experience from this work is that it is necessary to involve several people from cross-functional disciplines to derive the ASIL classification. It is a subjective work were different people have different opinions. The cost could be very high if the classification is later reconsidered to be at a higher level. So it is necessary to carefully review the assumptions.

The standard does not give an absolute guidance to ASIL classification of different failures and there is currently no industry common interpretation. We expect to first see development of internal company guidelines, which may or may not spread between companies. It can be noted that the outcome of this project has already affected ASIL classification in other projects.

Seven Safety Goals were defined to counteract the failures. A safety goal is a high level requirement which inherits the highest ASIL of the corresponding failure modes.

- The vehicle shall prevent actuation of a propelling torque that exceeds a hazardous level on any individual wheel when there is no propulsion command from either the user or from an external system. (ASIL B)
- Asymmetric torque appliance during commanded forward speed shall not be allowed to the extent that the vehicle control can be jeopardized. (ASIL A)
- A propelling torque appliance that exceeds a hazardous level shall be prevented from being actuated if the user or another system commands retardation. (ASIL C)
- Asymmetric torque appliance during commanded electro dynamic brake shall not be allowed to the extent that the vehicle control can be jeopardized. (ASIL C)
- The vehicle shall prevent actuation of a retarding torque that exceeds a hazardous level on any individual wheel when there is no brake command from either the user or from an external system. (ASIL B)
- The vehicle shall at commanded braking prevent actuation of a retarding torque that exceeds the nominal value for any individual wheel. (ASIL A)
- The vehicle shall at speeds near standstill prevent actuation of a propelling torque on any individual wheel in the opposite direction than the one selected by the driver. (ASIL B)

Defining safety goals was a rather straightforward task. It is not controversial as the ASIL classification or as complex as deriving the functional safety concept.

The verification of the hazard analysis and risk assessment was done with formal verification. It would have been good to use simulations (or even prototyping) to verify some assumptions.

The detailed analysis is documented in (AFFE 025 Hazard Analysis)

5.5.3 Functional safety concept

A functional safety concept is mainly a set of requirements that describes the functionality required to achieve the Safety Goals. These requirements shall be allocated onto the preliminary architecture.

This part is in our opinion the most diffuse one in the ISO26262 standard. It gives very little guidance on what "level" and how the Functional Safety Requirements shall be formulated. A lot of time was spent trying different approaches.

We came up with a level that we felt satisfied about. One of the key factors is to define the safety requirements without using negating wording. I.e. avoid sentences that can be transformed into: "the component shall not fail". The method of the functional concept defined by this project could more or less be propagated as a "best practice".

Allocation of the requirements on the preliminary architecture in Figure 14 rendered the need for portioning the nodes into at least two parts. One partition supporting a higher criticality level and one intended for the "main function". An example is given in Figure 15. (This concept can also be seen in Figure 7).

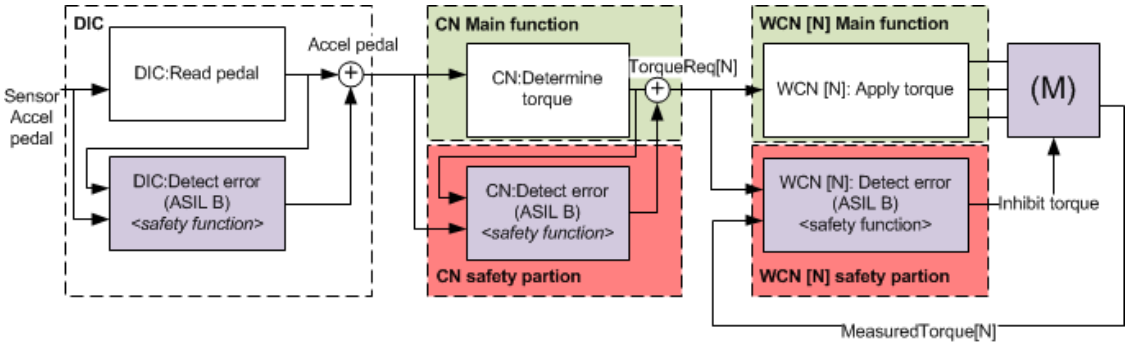


Figure 15 – Example of Functional Safety Concept allocation (Safety Goal 1)

One of the issues we evaluated was how to use functional redundancy when allocating the safety concept. Requirements at ASIL C and D level are commonly seen as cost drivers. Either you implement the requirements straightforward to a high NRE cost, or you add architecture requirements for redundancy to enable "ASIL-decomposition" by independent functions. Different opinions exist within project whether to use ASIL-decomposition at this stage. We have tested both approaches for the highest ASIL ranking Safety Goals. A lesson learned was that it is difficult to create complete redundancy with selected architecture. Some elements remain with requirements with high criticality (e.g., torque measurement).

Complete functional safety concepts were defined for five out of seven safety goals. The remaining two were considered so similar to others, that it would mostly be copy and paste work and not affect architecture.

The detailed functional safety concept is documented in (AFFE 029 Functional Safety Concept)

We only made one iteration to define requirements and architecture, more is required. The following iteration(s) should answer some issues we could not finish:

- We have made likely, but not verified, that the preliminary architecture defined in our assumption supports our functions.
- We have not evaluated if the safety functions counteract intended vehicle behavior.

5.6 Demonstrator development

5.6.1 Method development

5.6.1.1 MIL

The first step in our validation procedure was to test the reaction of the control system in a simulation environment. The model of the environment was provided by BAE and is described below.

The vehicle model consists of a mechanical model with 18 degrees of freedom, excluding the tyre model, shown schematically in Figure 16.

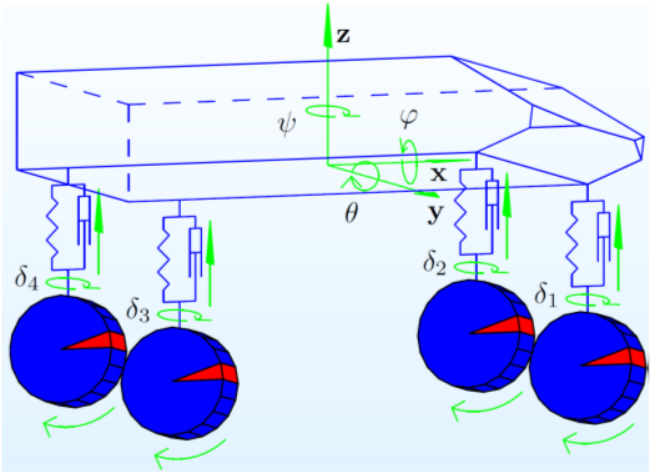


Figure 16 – Vehicle model with 18 degrees of freedom.

The tyre model used in this case is called the brush tyre model and is shown in Figure 17.

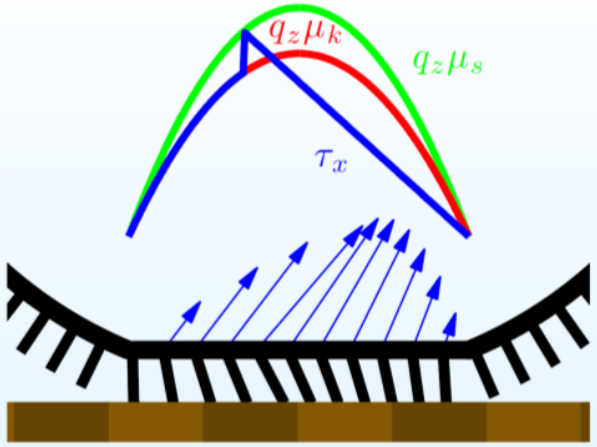


Figure 17 – Principle of the brush tyre model.

.

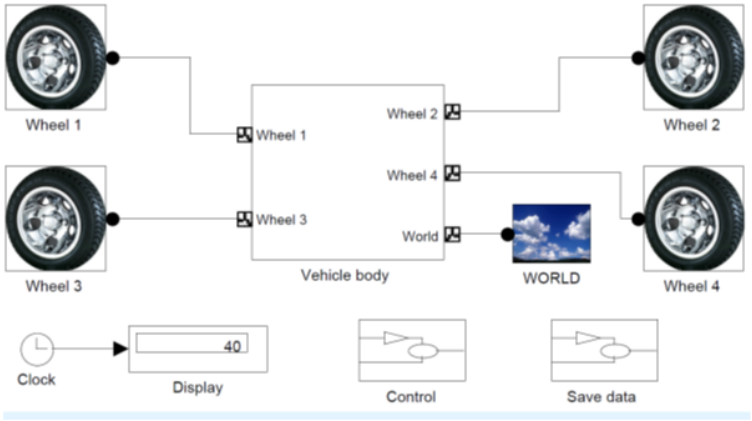


Figure 18 – Implementation of vehicle model in SimMechanics.

SimMechanics is utilised for implementing the vehicle model, see Figure 18. The main benefits of SimMechanics are that it

- handles 3D mechanical modelling
- is modular
- has bi-directional connections
- is completely integrated with Simulink; model implementations can use both SimMechanics and traditional Simulink blocks without performance penalties.

Some limitations that were encountered in this project are that it

- does not include a too extensive model library; e.g. tricky to implement the tyre model.
- only can handle a limited model complexity; e.g. the developed tyre model could not be combined with a friction brake disc model from the SimMechanics library within this project.

The following visualising methods have been evaluated:

- Matlab graphics
  - Frames are drawn by using conventional Matlab graphics tools and encoded into a video.
- SimMechanics mass moments of inertia
  - Made automatically; no graphics has to be provided.
  - Makes it easy to visually see if there are major modelling errors.
  - A bit slow.
- SimMechanics stl graphics animation
  - By providing stl files for the objects, SimMechanics can provide a geometrically correct animation.
  - Even slower
- Simulink3D animation
  - Beautiful animations
  - Slow
  - A bit buggy in the version used in this project.
- Blender 3D connected to the simulation through UDP/IP

- Beautiful off-line animations.
- Possible to animate with simplified graphics during the simulation, almost without performance penalty.
- Possible to run the animation on a different computer.
- Possible to interact with the simulation (e.g. like a game).

Since Blender 3D has the ability both to provide beautiful off-line animations, can provide on-line visualisations with negligible performance penalty and is reasonably easy to program in Python, it was utilised in this project.

Control System evaluation in MIL

The Control system and this environment model have been connected to each other in a common Simulink model and another block has been added to handle the inputs from the driver. The final MIL Simulink file (or test bench) looks as the figure below.

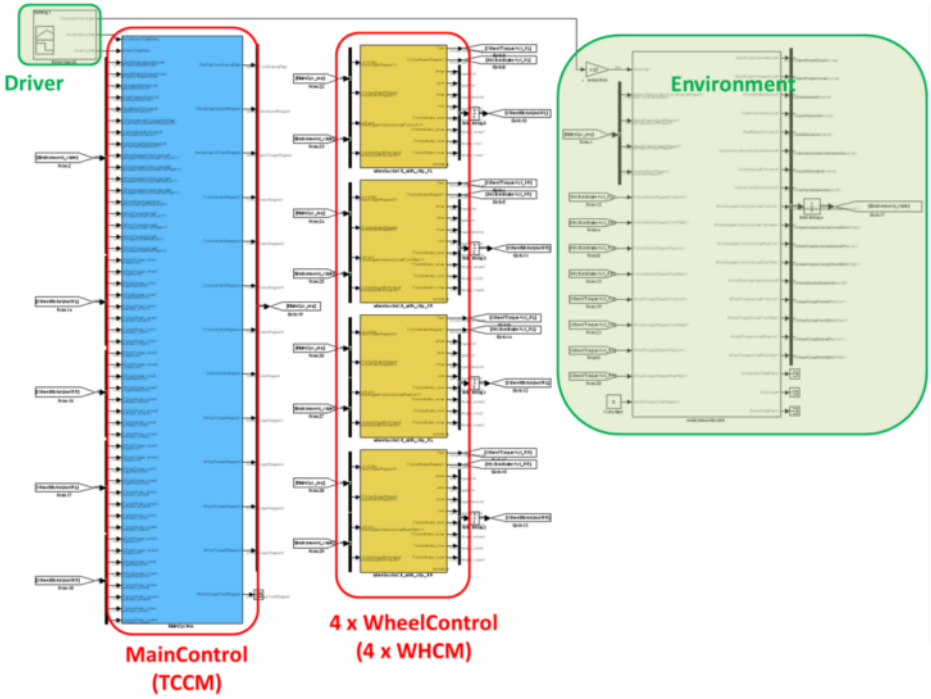


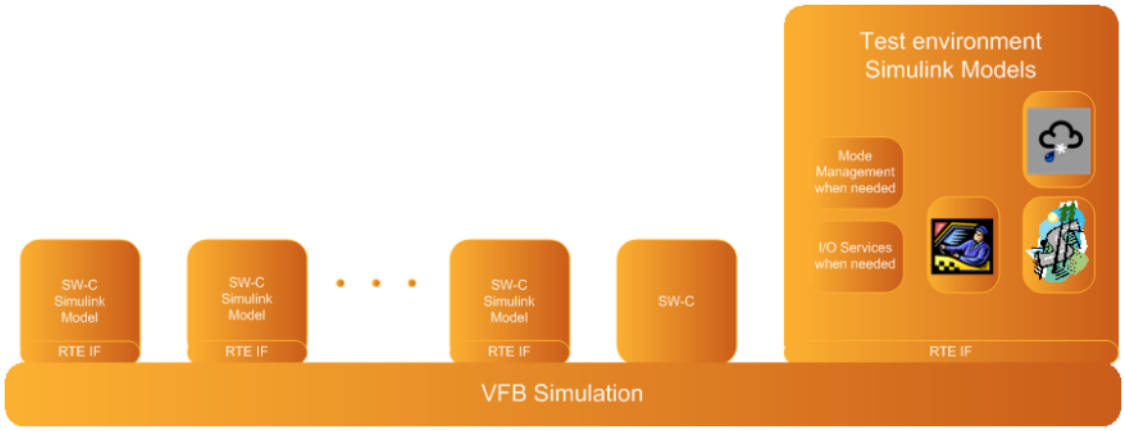
Figure 19 - AFFE functional components implementation on hardware

The MIL environment presented has been used along the whole control system development process together with specific test cases we had defined before. Those test cases to be used for verification of the software functionality in the AFFE demo function have been determined according to (AFFE 026 System Scope Definition) (and more specifically the chapter about Operation scenarios), and they are described in (AFFE 031 Test Case and Test Report). The test cases cover requirements on the AFFE demo function level.

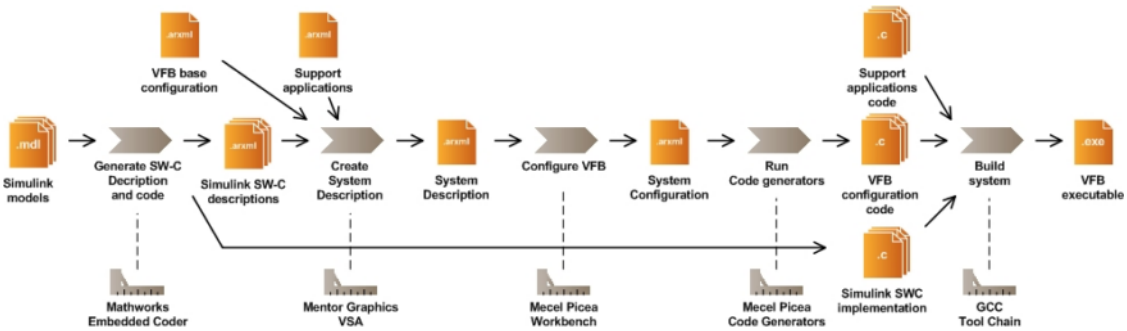
The tests cases cover basic vehicle motion such as acceleration, deceleration and turning situations. Another test case related to the vehicle stability has also been created to evaluate the improvement of vehicle stability thanks to the development of the control strategies. The entire test results have been documented and can be found along with test case descriptions in (AFFE 031 Test Case and Test Report).

5.6.1.2 SIL

The SIL development process introduces AUTOSAR 4.0 in a PC environment offering support for executing software components, SW-Cs, on a virtual functional bus, VFB. This offers support to test and validate a system on an AUTOSAR 4.0 platform in a PC environment at an early stage in the development process without any need for hardware. In SIL all communication between the different SW-Cs is performed by the VFB simulator, see the figure below, abstracting the communication buses.

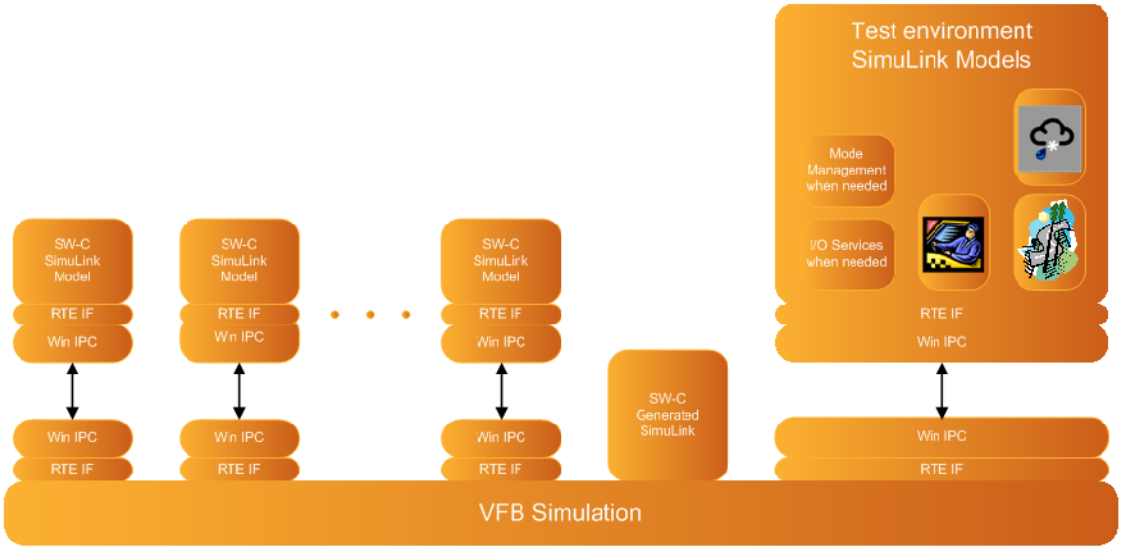


The SIL development process, as shown in the figure below, consists of five stages further described below.



- **Generate SW-C Description and code:** Generates SW-C descriptions as well as SW-C implementation code for each Simulink model created in the MIL development process.
- **Create System Description:** The SW-C descriptions and possible support applications are used together with an authoring tool, e.g. Picea Workbench, to connect the models to each other and will output a system description.
- **Configure VFB:** The system description works as input to a basic software configuration tool, e.g. Picea Workbench, where the AUTOSAR platform is configured, such as RTE and OS. The output of this stage is a system configuration file.
- **Run Code Generators:** The system configuration is used by multiple BSW code generators, e.g. Picea BWS Code Generator, to generate VFB configuration code.
- **Build System:** The VFB configuration code, the Simulink SW-Cs implementation code and possible support application code are compiled and linked together using for example the GCC tool chain to build an executable.

A shortcoming with the development process above is that in case errors are found in the models during simulation in the AUTOSAR environment these have to be corrected in the models, which in turn have to be code generated and integrated in the AUTOSAR environment. This can be a rather time consuming process. The avoid this time consuming process the SW-Cs are decoupled from the VFB and instead allowed to execute in their native environment, Simulink, as can be seen in the figure below. In VFB the SW-C is replaced with a pseudo SW-C which creates a connection to Simulink using an inter-process communication method to trigger the execution of a model. Any input and/or output data to and from the model are sent using the same connection. This design allows for increased debugging capabilities as the model can be debugged in its native graphical environment. It also allows for a faster debugging process as no code generation and no integration with the VFB simulator is required in the debugging process.

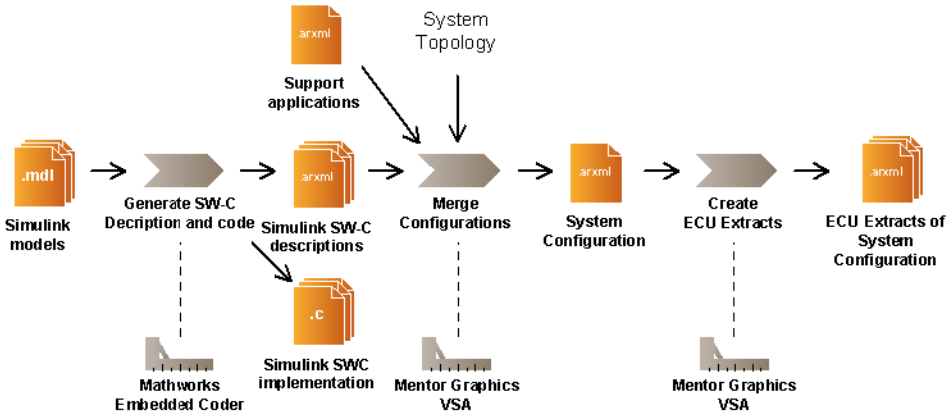


The idea of running the models natively in Simulink for increased debugging capabilities and to shorten the debugging process has been proven to work in a smaller system as part of a master thesis executed at Mecel, see section 5.7.2 for more details.
The real-time properties of the SIL cannot be guaranteed at all time. The reason is that the system executes on a non-real time platform, e.g. Windows.

5.6.1.3 HIL

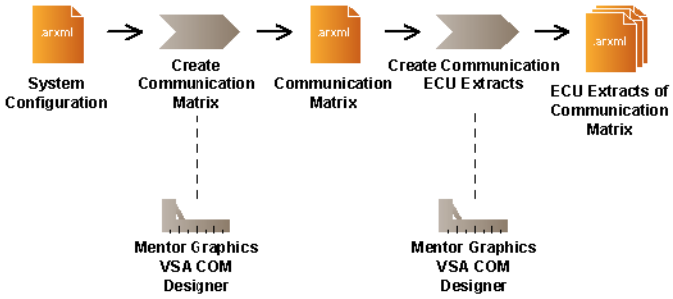
The HIL development process introduces AUTOSAR 4.0 on a target platform. This involves in contrast to the SIL process the introduction of system topology and communication buses. The HIL development process consist of three parts further described below.

The first part of the HIL development process, as shown in the figure below, deals with configuring the system level.



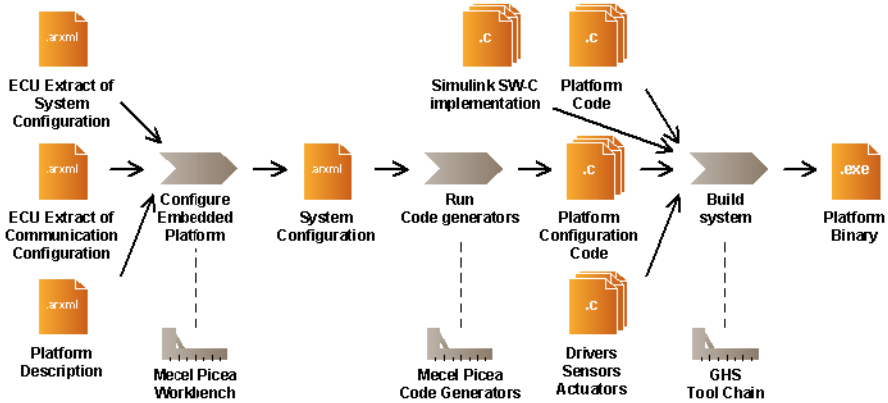
- **Generate SW-C Description and code:** Generates SW-C descriptions as well as SW-C implementation code for each Simulink model created in the MIL development process.
- **Merge Configurations:** The SW-C descriptions and possible support applications are used together with an authoring tool, e.g. Picea Workbench, to connect the models to each other as well as configuring the system topology and mapping the SW-Cs to ECUs, and will output a system configuration.
- **Create ECU extracts:** This stage involves creating an ECU extract of the system configuration for each ECU.

The second part of the HIL development process, shown in the figure below, deals with configuring the communication between the different SW-Cs on the different ECUs.



- **Create Communication Matrix:** With the system configuration from the process above as input this stage involves configuring the communication matrix between the different ECUs using a COM designer tool, e.g. Picea Workbench.
- **Create Communication ECU Extracts:** Given the communication matrix ECU extracts are created for each ECU.

The last part of the HIL development process, shown in the figure below, deals with configuration of the BSW modules at the embedded target.

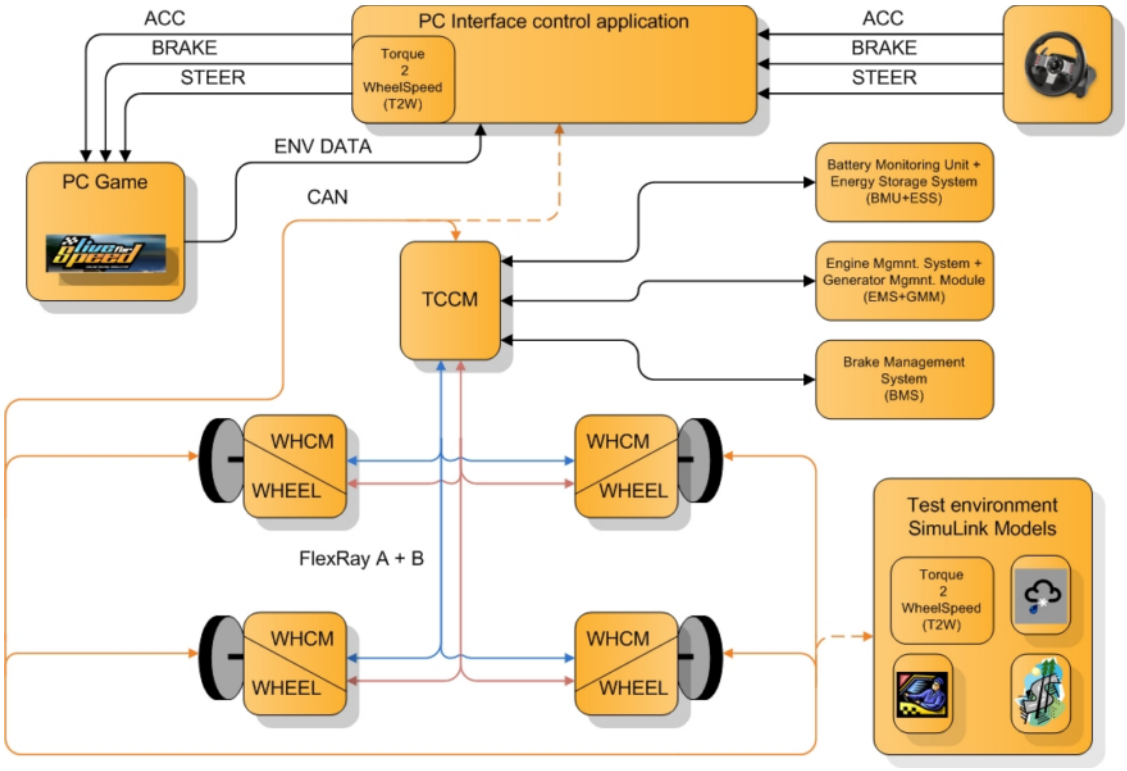


- **Configure Embedded Platform:** Given the ECU extracts from the previous processes and a platform description given by the target manufacturer this stage involves configuring the different parts of the target system such as OS, RTE, diagnostics, persistent memory etc. using a configuration tool, e.g. Picea Workbench. It also involves creation and configuration of drivers for the different sensors and actuators needed by the system. The stage will output a complete system configuration.
- **Run code generators:** The system configuration is used by multiple BSW code generators, e.g. Picea BSW Code Generators, to generate the platform configuration code.
- **Build system:** Using for example the Green Hills, GHS, tool chain the Simulink SW-C implementations, the platform code, the platform configuration code and code for drivers, sensors and actuators are compiled and linked together to build a platform binary.

The HIL development process can be combined with the SIL where some of the SW-Cs executes on target platform while some execute on the PC platform as a way to increase the flexibility.
The HIL development process more or less follows the AUTOSAR methodology which means there are a great support available through use of different AUTOSAR authoring and configuration tools. The AUTOSAR tool chain is as the standard itself under development, which can make the tool chain hard to master.

5.6.2 Demonstrator development

This section describes the intended architecture, see figure below, for the demonstrator system developed as a part of the project.

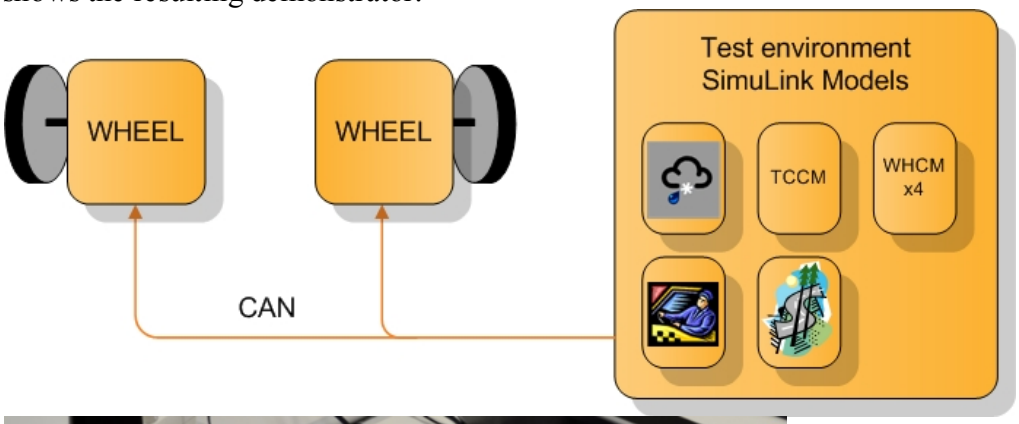


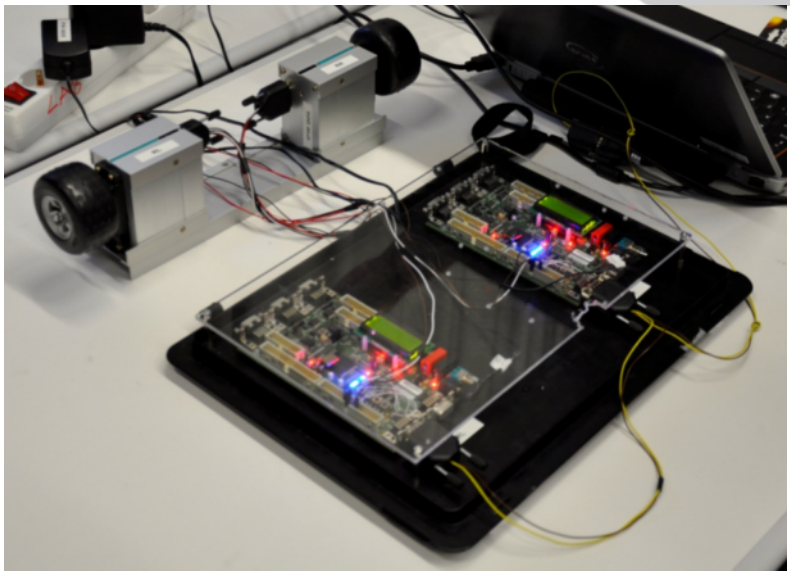
The control system consists of five ECUs each running AUTOSAR 4.0. The first ECU runs the TCCM model as a SW-C. The four other ECUs each run the WHCM model for one wheel as a SW-C and a wheel actuator SW-C to control the I/O to and from the wheel engine prototype. Two FlexRay channels are used for the communication between the different control system ECUs. The control system is connected to support systems to handle e.g. power management and brake management. These support systems communicate with the TCCM module and could either be implemented directly in the TCCM module or could be executed on a PC in the test environment.
The environment simulation and the input to the control system in the demonstrator can be generated in two different ways; either using Simulink models to simulate weather, road and driver input, or by using a PC game to generate the input.
The PC game environment provides a car simulator, Live for Speed, with a steering wheel, gas pedal and brake pedal to create input to the control system. The input from the steering wheel and the pedals are read by the PC interface control application, which in turn communicates with the control system over CAN to provide the user input. The actual values, such as wheel angular velocity of the physical wheels, are read from the control system by the PC interface control application and passed on to the car simulator

in the PC game. Any environmental data from the PC game are passed to the PC interface control application, which may pass it further to the control system.

5.6.3 Demonstrator results

The final demonstrator solution has due to time constraints been reduced to contain the test environment models and two wheel nodes, as can be seen in the first figure below. The control system models have been moved from the hardware units into the Simulink environment where they are executed together with the test environment models. The angular velocity for the wheels are extracted from the models and sent out on a CAN bus using shared memory. The angular velocity are read from the CAN bus by the two wheel nodes. Each wheel node includes a small wheel prototype engine and an ECU running AUTOSAR 4.0. A wheel actuator SW-C on each ECU is responsible for reading the angular velocity for that specific wheel from the CAN bus and to set the correct output signals to control the angular velocity of the wheel prototype. The photograph below shows the resulting demonstrator.





5.7 Master thesis

5.7.1 Methodology and design patterns for converting AUTOSAR Simulink models from SIL to HIL

Abstract: This project is a part of the Architecture For Future Electric-vehicles (AFFE) project. AFFE project is a research project funded by VINNOVA to bring out the next generation electric vehicles based on AUTomotive Open System Architecture (AUTOSAR). Modern vehicles are containing many electronic devices therefor the system complexity is also growing. Therefor this thesis project aims to find a methodology to develop software applications with instantiation possibility using Model-based Design environment, then do code generation and finally integrate into hardware without modifying the software applications configurations between different phases. For this purpose Simulink from Mathworks has been used as a Model Based Development tool for developing software applications, simulating and generating AUTOSAR compliant code. Mecel Picea Workbench has been used to make configuration for simulation in PC environment and hardware platform. The project ends with analysis of compatibility of different tools and configuration possibilities in different phases.
The outcome of this project shows that the AUTOSAR standard is young and therefore compliant tools have limitations. (Olsson & Pham, August 2011)

5.7.2 Connecting AUTOSAR VFB to Simulink Environment

Abstract: This thesis was conducted as a part of the Architecture For Future Electric-vehicles (AFFE) project. AFFE project is a research project funded by VINNOVA to bring out the next generation electric vehicles based on Automotive Open System Architecture (AUTOSAR).
The primary aim of the thesis is to analyze and demonstrate the possibility of connecting model-based design environments to the AUTOSAR Virtual Function Bus (VFB) to make the process of development of complex automotive systems easier. The tools chosen for this purpose were Mecel's Picea suite for the VFB implementation and Mathworks' Simulink as the model-based design environment.
The outcome of the project is that a scalable solution to connect the two disparate programs was created using two different Interprocess Communication (IPC) methods. (Mohan & Zügner, May 2012)

5.8 Delivery to FFI-goals

The FFI goals for the Vehicle Development program are subdivided in

- Vehicle Electrics and Electronics
- Embedded Systems and Software
- Material Science for more Efficient Vehicles
- Methods and Tools for Vehicle Development

The AFFE project concerns all but the third point. In the following chapters the goals of these sub areas will be compared with what has been achieved in AFFE.

5.8.1 Vehicle Electrics and Electronics

FFI-Goal: To raise the technical level of maturity to be able to industrialize results faster and increase customer value.

AFFE delivery: The technical level of maturity has been raised for a lot of technology areas within AFFE. E.g. results and experience from the use of ISO 26262 on a control system intended for commercial vehicles. Also results the work on developing different electrical architectures to be used for the control system contributes to this goal.

5.8.2 Embedded Systems and Software

FFI-Goal: To raise the technical level of maturity to be able to industrialize results faster and increase customer value.

AFFE delivery: The work on development of the software and also the results from the application of AUTOSAR 4.0 in this development contributes well to this goal.

5.8.3 Methods and Tools for Vehicle Development

FFI-Goal: Ensure that the Swedish automotive industry contributes and grants access to methods, tools and world-class expertise to enable rapid and effective development.

AFFE delivery: A lot of the tools used for SW development and simulation in AFFE have been tested to what is under development from the tool vendors, especially regarding their support for AUTOSAR 4.0. This will be of great use for the future development in the Swedish automotive industry, especially when the migration to AUTOSAR 4.0 starts.

5.9 Deliverables and Reports

A number of reports and deliverables have been produced within the project. All deliverables except for the Final Report are project internal and not public.

List of deliverables:

AFFE 006 Requirement process
AFFE 007 Buzz words
AFFE 008 Stakeholder list
AFFE 009 Requirements document
AFFE 011 System Architecture Description
AFFE 012 0ne third review requirements
AFFE 013 Glossary
AFFE 014 Hybrid vehicles
AFFE 015 State of the Art Software Architecture
AFFE 016 State of the Art Communication
AFFE 017 State of the Art Toolchain
AFFE 018 State of the Art Hardware Architecture
AFFE 019 State of the Art Safety Patterns
AFFE 020 State of the Art Development Process
AFFE 021 State of the Art Functional Safety
AFFE 022 State of the Art Test Strategies
AFFE 023 State of the Art Control Design
AFFE 025 Hazard Analysis
AFFE 026 System Scope Definition
AFFE 027 Functional Safety Concept ideas
AFFE 028 Safety-related topics discussed in Stockholm
AFFE 029 Functional Safety Concept
AFFE 030 Final Report
AFFE 031 TestCase_TestReport
AFFE 032 ControlSystemDevelopmentReport
Demonstrator Hardware
Control Model
Environment Model
Software in the loop rig
Hardware in the loop rig
AUTOSAR platform

6 Dissemination and publications

6.1 Knowledge and results dissemination

The project and the results have been presented at dedicated seminars within each partner's organization.

The AFFE project was described at the now annual conference "*Elektronik I Fordon*" held in Gothenburg. The AFFE project was presented as a part of the presentation made by Tom Sundelin from BAE Systems during two following conferences: April 8, 2011 and April 26, 2012 at the extended theme day of the conference.

At the end of the project, 2 AFFE final seminars were held, one at Volvo in Gothenburg in August 22, and one in at BAE Systems Hägglunds in Örnsköldsvik in August 28.

6.2 Publications

Olsson & Pham, *Methodology and design patterns for converting AUTOSAR Simulink models from SIL to HIL*. Chalmers University of Technology, Göteborg, August 2011. (Master thesis)

Mohan & Zügner *Connecting AUTOSAR VFB to Simulink Environment*. Chalmers University of Technology, Göteborg, May 2012. (Master thesis)

7 Conclusions and future research

7.1 Conclusions

The major task to investigate within the project has been to find a *"realistic solution"* for the control system of a future serial hybrid drive train, based on using "free wheel stations".

When minimizing the use of traditional mechanical parts in the transmission by the use of electric motors close to each driving wheel for the propulsion, the system will be highly dependent on the integrated electronics, software and power electronics that connect the whole system together. The total system and the propulsion of the Vehicle fully depend on those systems fulfilment of safety critical requirements and reliability requirements.

A lot of investments have been made on development and production of traditional driveline design for Vehicles that naturally holds back changes, that means new reinvestment and new risks. However we argue that knowledge and development culture are example of important things that also holds back an exchange of traditional mechanical drivelines with electric drivelines.

In the work package named "state of the art" within the project, we scanned the market on technologies, tools and processes supporting the development of the control system in focus. In general the work through the project and its results give the basis to make the conclusion that **technology of today is good enough to make this type of systems**. It means that the challenge to fulfil the right and good enough quality of such systems is not hold back by technology reasons. The challenges and bottlenecks preventing a full scale use of the kind of system we have been focusing on are mainly related other factors. This can be factors such as lack of application experiences using this kind of systems. It can also be lack of knowledge and practical experiences of using development processes, tools and standards supporting the development. The ISO 26262 represents one example of such a standard or "process tool".

Within the used expression *"realistic solution"* a reasonable system cost and life time cost, are some of the parameters counted in. The project has not got the conditions to; in detail investigate the cost parameters related to e.g. development, production and maintenance etc. of electric drivelines. The evaluation of those parameters have instead been based on experience and knowledge by the project member to find system design that gives reasonable challenges of time and new knowledge for making the development work, test and production. We also have assumed that by limiting the selection of technologies, components and design principles to a selection of well-established and reasonable mature ones, the system cost will be possible to hold to reasonable levels.

A general approach and idea have been to make the architecture "realistic" by integrating different type of redundancy and "fall back solution" to avoid getting a "to challenging"

ASIL Level. The idea is that an ASIL-D level is giving to high challenges to reach the right quality. ASIL-D will require an amount of test and evaluation work that will end up in unaccepted cost and lead time. The conclusion is that the ASIL-D level can't be accepted for the product in focus. ASIL-C must also be avoided if possible, but could be handled and accepted in a system if it is isolated to special components or represents a limited (minor) well defined part of a system. ASIL-B and ASIL-A are considered as reasonable accepted related to "cost", even if there always shall be a strive to lower the integrity level.

One general way to lower the safety integrity level is to add redundancy in the system functionality. Redundancy will give higher hardware cost and/or software development cost. Redundancy can increase maintenance cost and also lower the system reliability. However there should be an optimization to find optimum of the level of complexity of the system, the cost and ASIL level. Where this optimum is to be found depends on a lot of conditions that also not is technical related but have to do with, knowledge, experiences, capacity, processes etc. of the company, project and parties responsible and involved in the development process. Also the maintenance of the product has to be considered when selecting architecture and technology.

The project has presented a principle architectural solution with flexibility and degrees of freedom to be expanded to cover from 2 wheel drives to 8 or more driving wheels. Different redundancy levels could also be added to the presented system design with different levels of safety integrity levels and complexity. Properties such as modularity and flexibility have also been in focus for the presented architecture.

However a conclusion is that in practice there will not be a "one solution"-architecture that is optimal for this rather complex system we have had in focus, when the architecture have to be adopted to the situation defined by other parameters than related to pure technology. Instead modularity and flexibility are example of important needed properties of the system architecture, to support this adoption of the design in parallel with for example that confidence of use increases of components, technology, and processes. Those properties are also important for adaptations to change of requirements on the market and new demands from the user of the system. It will be too costly to make a completely new system architecture and design each time changes are needed. Instead an architecture and system platform has to be selected that are prepared for constant evolution of the system functionality. We think the principle solution presented by the project has those qualities.

Within this project we only had the time and resources to start and do some iterative loops, but evens so it is obvious how important model based development and the use of simulation technology are to ensure the quality, reduce time and make the development cost effective. To be competitive a development approach for control systems of more complex electric drivelines can't be without the use of this.

The development work of safety critical systems must be well managed and controlled. The ISO26262 supports this with guidelines and process stages etc., but this standard must be adopted to fit within an existent general development process. For example is it wise to find a way to use iteratively evolvement in the design process. Exactly how this shall be arranged is not especially supported by the ISO26262. In the project we have integrated ISO 26262 with parts of the "Systems Engineering Handbook" of Volvo to get a more complete development platform. A lesson learned on this is that the adaptation of existing system engineering processes to handle safety critical issues in new areas and the need of confidence in this, take time. This is also a challenge for actors on the market.

The challenge to increase the knowledge in the area of using electric transmission and its control systems are common in the branch. Increased collaboration on the market is needed. The infrastructure to fully support this is not established. Increased support from different authorities and communities, from national levels to supranational levels are needed from now and to foreseeable time to make a needed change possible closer in time. This is a necessity for the competiveness and business development for established and new actors on the market.

7.1.1 Summary of the conclusion

The following conclusions are made:

- Established technology to day is good enough to meet the qualities such as safety, performance, modularity, flexibility etc., for the system in focus.
- By limiting the selection of technologies, components and design principles to a selection of well-established and reasonable mature ones, the system cost will be possible to hold to reasonable levels.
- By fulfilling qualities of the system platform design and its architecture to be possible to reuse it for evolutionary functional increase and be adaptable for different applications, the cost could also be hold down.
- An iterative, model based development process where simulation technology in high degree are used, ensures the quality, reduce development time, reduces risks and make the development cost effective.
- ISO26262 have to be carefully integrated with a comprehensive general system engineering process to support projects and companies handling safety critical systems. This takes time and a lot of application to work in practice.
- There are a lot of non-technological related factors such as knowledge, experiences and processes etc. of companies, projects and parties responsible and involved in the development process that have to be developed and mature to break through with the use of new technology such as electric based drive trains for Vehicles.
- For the competiveness and business development of established and new actors on the market there are a necessity to increase the knowledge in the area of using electric transmission and its control systems. Increased support from authorities and communities, on national levels to supranational levels are needed for this development. This project is a god example of this.

7.2 Future Research

The purpose of this section is to provide a list of topics that can serve as input for decisions for future research and development. It can e.g. be work that was identified during the project as extensions but that had to be put aside for budget and/or resource reasons. It can also be topics that did not fall within the project scope but that will need further research and development in order to be able to develop the electric architecture of future hybrid vehicles.

- The development process described in SEG applied was not prepared for working according to ISO26262.
  There is a need for an update of the development process in order to support for the introduction of ISO26262 when developing commercial vehicles.
- More work will be needed on the electrical architecture in order to fully support all the functional requirements of future hybrid vehicles. As the project due to time and resource reasons had to narrow down the scope and the number of electrical architecture possibilities this leaves room for more future work within this topic.
- The maturity of the SW development tools needs to be increased regarding the support of AUTOSAR4.0. More work will be needed in the future within this area.

8 Glossary

AUTOSAR	AUTomotive Open System Architecture
AVB	Audio Video Bridging
BSW	Basic Software
CAN	Controller Area Network
COM	Communication module (AUTOSAR)
ECU	Electronic Control Unit
HIL	Hardware-in-the-Loop
IPC	Inter-Process Communication
MIL	Model-in-the-Loop
OO	Object-oriented
OS	Operating System
RTE	Run-Time Environment
SEG	System Engineering Guideline
SIL	Software-in-the-Loop
SoA	State of the Art
STL	Standard Template Library
SW-C	Software Component
TCCM	Traction and Chassis Control Module
TTP	Time-Triggered Protocol
UML	Unified Modeling Language
VFB	Virtual Functional Bus
WHCM	Wheel Hub Control Module

9 References

Abrahamsson, M. (2010). *AFFE 022 Test Strategies.* Örnsköldsvik.
Fritzson, M. (2010). *AFFE 015 State of the Art Software Architecture.* Göteborg.
Fritzson, M. (2010). *AFFE 016 State of the Art Communication.* Göteborg.
Fritzson, M. (2010). *AFFE 017 State of the Art Tool Chain.* Göteborg.
Mohan, N., & Zügner, H. (May 2012). *Connecting AUTOSAR VFB to Simulink Environment.* Göteborg: Chalmers University of Technology.
Näslund, P. (2011). *AFFE 025 Hazard Analysis.* Örnsköldsvik.
Näslund, P. (2012). *AFFE 029 Functional Safety Concept.* Göteborg.
Olsson, E., & Pham, D. (August 2011). *Methodology and design patterns for converting AUTOSAR Simulink models from SIL to HIL.* Göteborg: Chalmers University of Technology.
Soulier, N. (2011). *AFFE 023 State of the art Control Design.* Göteborg.
Soulier, N., & Yang, H. (2012). *AFFE 032 Control System Development.* Göteborg.
Söderqvist, T. (2012). *AFFE 026 System Scope Definition.* Göteborg.
Yang, H. (2012). *AFFE 031 Test Case and Test Report.* Göteborg.

10 Participating parties and contact person

Stefan Nord
stefan.nord@volvo.com
+46 31 322 2075

Lars Matsson
Lars.Matsson@mecel.se
+46 31 720 4552

Tom Sundelin
tom.sundelin@baesystems.se
+46 660 80818

FORDONSSTRATEGISK
FORSKNING OCH INNOVATION

Adress: FFI/VINNOVA, 101 58 STOCKHOLM
Besöksadress: VINNOVA, Mäster Samuelsgatan 56, 101 58 STOCKHOLM
Telefon: 08 - 473 30 00

www.vinnova.se/ffi