Collective research project Flanders' DRIVE II

Title of the project

Safety Integrity Levels in Automotive: from requirements towards a validated system

Acronym:

ASIL (Automotive Safety Integrity Level) - Functional Safety in Automotive

Summary project information

Motivation

In the last ten years, the automotive market has known a considerable growth in the share of electronics and embedded software in the finished product. Several reasons for this can be found:

- More comfort functions, e.g. adjustable air-conditioning, remote locking, etc.
- More active safety, e.g. ABS, ESP, smart cruise control, tire pressure monitors, etc.
- Lower consumption and better performance: electronic injection, hybrid powertrains, replacement of hydra mechanic parts by electronic ones for weight and gain in power, etc.
- Higher reliability: e.g. adaptive adjustment of the ignition at low and high temperatures, etc.
- Lower cost: mechanical parts can be more expensive.
- Flexibility in the configuration of the car

These elements are nevertheless closely connected, which means that a system approach is needed from the start. Reliability and safety are often linked. Another element is that, unlike hydro-mechanical solutions, an electronic solution with embedded software does not often gradually degrade. This means that a small error can immediately be fatal. This aspect is further enhanced by the exponential growth of the state space involved in the use of embedded software.

SIL levels

In 1998, the International Electro technical Commission (IEC) published the 61508 standard. Such a document contains requirements to minimize the failures in electronic systems. The standard gives several definitions of system integrity level or SIL. Applications and systems are classified by the probability of a dangerous failure arising per hour as follows:

Safety Integrity Level	Probability of dangerous failure per hour
SIL4	$>=10^{-9}$ to $< 10^{-8}$
SIL3	$>=10^{-8}$ to $< 10^{-7}$
SIL2	$>=10^{-7}$ to $< 10^{-6}$
SIL1	$>=10^{-6}$ to $< 10^{-5}$

Figure 1: High demand or continuous mode of operation

One FIT (failure in time) is equivalent to a dangerous failure per hour of $10^{-9.}$ Thus, a full system must work within a safety budget with devices where the total accumulation of FIT figures leads to

the SIL level characterization.

Determining the level of safety (SIL level) required in an application, is by no means an easy task. Clearly, the critical systems of an airplane require at least SIL3 compliance and in some cases SIL4. In a car, it is less obvious. There are examples such as steer-by-wire or brake-by-wire which clearly require a high level. There are several tools offered to analyze the required SIL level for a system and it is not the intent of this study to assign SIL requirements for different systems. Suffice it to say that there are safety critical systems in the car today which have to be considered.

This all requires:

- an advanced system approach,
- a systematic project approach,
- high quality demands in each phase of the project.

The advantages of this are that the total project can not only yield more reliable, safer, more efficient and cheaper systems but it can also make the product more competitive and may be developed with less effort. In a systematic approach, the cost of correction shifts to the starting phase. In that phase, corrections are often still conceptual, while corrections in the final phases can be very expensive and time consuming. Ultimately, this is what determines the competitive position of the company as a supplier.

The necessity of a higher reliability also starts to apply to consumer products. When a product breaks during the warranty period, it is often no longer economically repairable and the producer has no other choice than to replace it by a new product. Recent studies show percentages as high as 15%. The ecological and economical cost of low reliability is therefore very high. In the case of the automotive sector, the error can often not be reproduced or the cause cannot be found. In this domain as well, the economic cost can be very high. Solutions are needed for the short and the long term. In the short term, these solutions can be conceived within the current restrictions the sector imposes on itself. For the long term, other solutions can be found, less or not restricted by the sector, allowing for a more thorough and efficient approach.

This not only applies to the automotive but also to the off-highway sector. In the latter, the series are a lot smaller, with more product variants in small production runs and different components or subsystems from different and various suppliers have to be taken into account. Within the offhighway market, the same quality levels and robustness as in the vehicle industry are strived for but systems have to be developed with less people and less means. The evolution towards automotive standards produces a competitive advantage within the off-highway market.

The safety requirements start in the automotive sector, seep through slowly to the offhighway and eventually find a way to machine building. In this project proposal, we use the unique name “vehicle industry” because this is the main focus but the result can just as well apply to off-highway, machine building or related sectors in which embedded software is developed.

Remark: Experts Avionics and railways will give feedback and input to the processes and system architecture, but will NOT participate in assessment and tools development.

Motivating statements from the Flemish industry

During the preparation of the project we noted quite some statements about the urgency to have a SIL compliant methodology available:

“If we do not invest in building up this knowledge, we will lose crucial business opportunities to extend our growth or even to maintain our current position as preferred supplier for some of our customers.”

“If the partners in this project don’t join their knowledge and expertise and don’t go together the whole way in this project, none of them will reach their goal within 2 years by themselves. By then, foreign competitor companies will have taken a head start.”

“We are confronted with a lot of standards due to the different markets in off-highway. Every market has its own standard for safety, EMC, environmental conditions (temperature cycle, vibrations, shocks, …). Safety related standards are a part of that. We get lost in the huge amount of requirements, and we have to re-do this exercise several times, so a generic approach is really needed.”

“In our customer base of off-highway OEM’ers, there are more and more managers coming from the automotive industry. They are requiring the same procedures used in automotive as standard processes and related standards. We have to get used to those practices otherwise business will be lost.”

Project goal

The specific and measurable goal of this project is to provide each of the Flanders’ drive partners with the capability to execute projects in appliance to SIL (Safety Integrity Level). Because the partners, which have their business also in the off-higway (machinery) market, have to fulfill more and more new (safety) standards, the need for one generic method how to cope with the safety related standards is highly needed. The dream is to have in the future one generic safety standard based on the recommendations coming from this project.

Safety is the driving force for more reliability and a higher productivity in developing products that serve the Flemish automotive market. Especially the off-highway market demands the same safety, reliability and quality which have to be developed with less people. Therefore one clear method instead of many others is now needed.

Therefore the safety standard IEC61508, which is used as safety standard by the leading automotive (on-highway) companies like AUDI, BMW and Daimler, will be used as start point and other machinery safety standards and the Autosar standard will used as a reference. Also the upcoming requests of OEM and T1’s will be taken into account. In a second step the partners will be assessed on those standards to investigate their knowledge about safety processes, architectures and tools. Based on the information of the standards and present situation a “Flemish” innovative generic safety method including processes, architectures and tools will be created which can be used for other interested companies. Also a financial installation method will be set up so each partner is able to calculate the investment a certain SIL-Level requires and to provide guidance in the selection process and the decision making. The generic method will be tested by two case studies by the Flanders' DRIVE partners. The project closely cooperates with FMTC (Flanders’ MECHATRONICS Technology Centre). The deliverables that will be exchanged between the projects.

The project will considerably raise the competence and productivity of the participating Flemish partners and future users. This is needed because of the increasing demands for safety and security properties of the products and services they deliver. The underlying methodology (a box of tools, supporting a certain process, system architectures and technologies) is fairly generic and this justifies cooperation to reach these competences. An additional element is that none of the Flemish companies or the educational institutions really possesses this knowledge.

Therefore, it is primordial to acquire it for the Flanders’ DRIVE partners to remain competitive. It will also have a positive impact on making the partners more productive hereby reducing development costs and increasing the predictability of the development process. In a second step, this acquired know-how can be made available to a larger part of the Flemish industry through Flanders’ Drive as service centre.

Partners:

Altreonic, Dana Spicer Off-Highway, EIA Electronics, Flanders' DRIVE, PsiControl, Punch Powertrain, Triphase

Innovation objectives

In the 2nd quarter of 2006, Arthur D. Little Consulting investigated a request of Flanders' DRIVE in the "Car of the future". As a result of this study, the domains of "Light Weight Materials", "Active Safety" and "Clean Power Trains" were defined by Arthur D. Little as domains of importance for the Flemish automotive industry. These domains have been further elaborated into business cases which form the basis of Flanders' DRIVE II.
For this ASIL project, the business cases of the domains "Active Safety" and "Clean Powertrains" are of special interest because they deal with product development, where each product contains an important part of electronics, mostly with embedded SW included.
One example is the project ReVAS (Research Vehicle for Active Safety). In this collective project, knowledge and competences will be built up in several areas needed to intelligently integrate and explore new technologies and applications in the field of Active Safety and Vehicle Dynamics. The business cases in the last two domains fit in the framework of intelligent systems, involving automotive mechatronics, software, control, electronics , embedded systems and communication.
The development of these intelligent systems requires the stringent application of a process like the ASIL related activities described in this project. For that reason, we have defined a work package meeting the ASIL requirements for that Active Safety application. It is very important to be compliant with the standards currently demanded in the automotive industry. Related to intelligent systems, Flanders' DRIVE has implemented two TIS projects in the past, Oct 2004 until Feb 2008 during which, insights in the demands for technical support in the area of vehicle electronics have been collected.

The result, shown in figure 2, already indicates the necessity to make a further effort in the areas of IVN (In Vehicle Networks), embedded SW, integration, sensors and functional testing. Studies show that 90 % of the innovations within the automotive industry are based on vehicle electronics. 80 % of these innovations are software driven. The Flemish industry also states that embedded SW will grow in importance for their companies. Note that a fundamental part of an active safety system is the software. It takes care of the performance and safety of the system. This can only be the case when it is well integrated in the mechanics, electronics, computer hardware and communication bus.

Figure 3 shows the relatively strong growth in the importance of embedded SW for the Flemish companies that took part in the questionnaire. The importance in 2005 was set to 100. So the figure indicates a growth of 17% towards 2010.

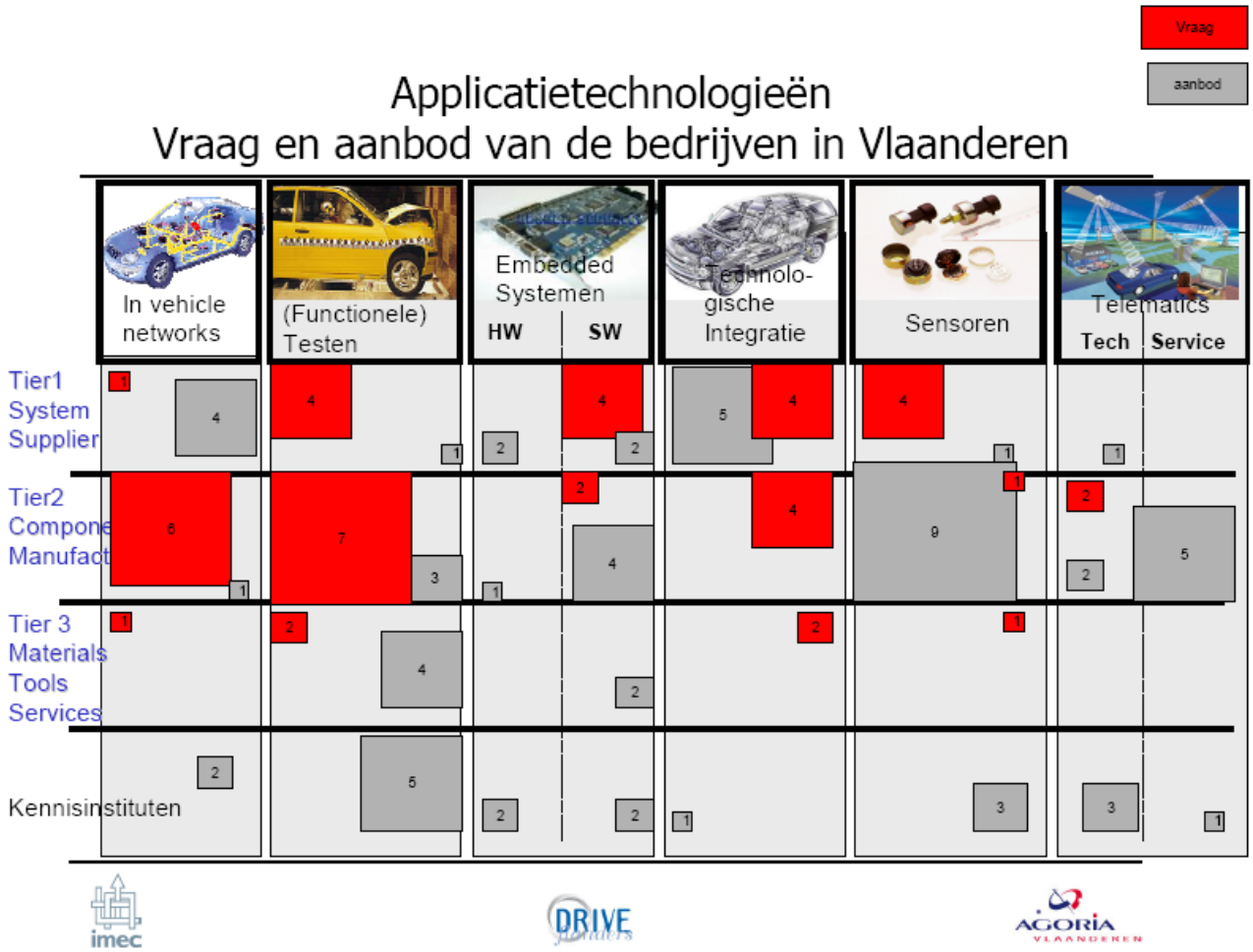


Figure 2: Automotive Technologies: supply (grey) and demand (red) of the Flemish automotive suppliers

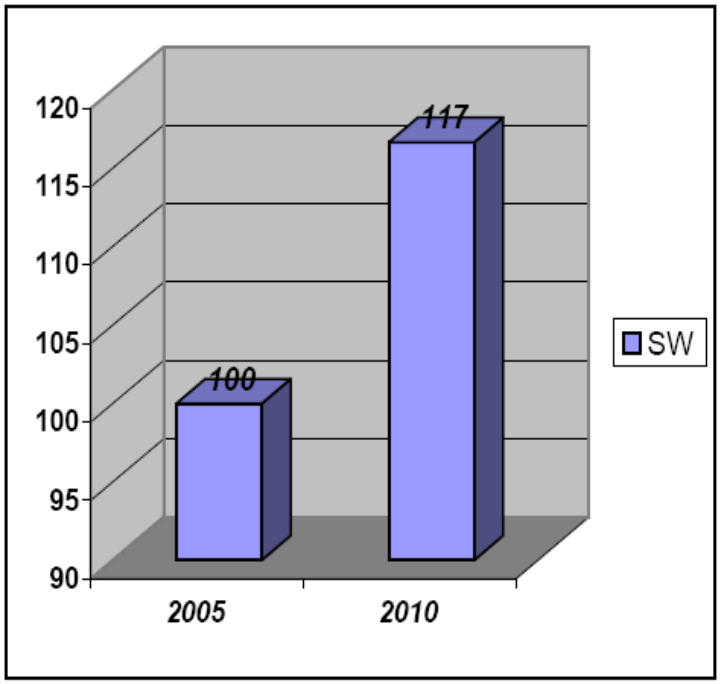


Figure 3: Growing importance of embedded SW within the Flemish automotive industry

At the same time, embedded SW is also one of the largest problem areas in automotive. More than 50% of the reliability problems are due to SW problems. The reason for this is the difficulty to test these, mostly stand alone systems, on their functionality. Note that these problems are not just software as such, but are also caused by integration issues and incompatibilities. Experience by the OEM an Tier1 has shown that the testing and debugging of the system and its software takes at least as much effort as developing it.
The study about the “car of the future” and the TIS projects reveal that there is an important need for some specific competences. Therefore, within the TIS projects, we have paid to the knowledge and competences available at the Flemish universities and technical universities. It is clear that there is a lot of competence available. It is also clear that there is a strong need for an intermediate level. This intermediate level will be played by Flanders’ DRIVE. Flanders' DRIVE will stimulate the industrial partners to use the available competences at the schools. On the other hand, this intermediate level will also express the demands for specific competences to the Flemish universities and technical universities.
In the past, within the previous TIS projects, seminars and workshops were organized where the research centers could recommend their available know-how and where the Flemish industry could stimulate the universities and technical universities to do applied research in the domains where they are active. Flanders’ DRIVE used also their industrial information to steer the research centers not only to disseminate the available know-how but also to build up new competences needed in automotive. Flanders’ DRIVE has supported and will further support TETRA projects in IVN (In vehicle Networks) like CAN, FlexRay, embedded SW, AUTOSAR and others.

However, it turned out that this was not enough and that there is a strong need for the Flemish automotive industry to have a centre available that not only builds up development process related competences but also does the necessary follow-up in this evolving area and keeps the Flemish automotive industry up to date.

Project objectives
In the ASIL project the following process competences will be mastered:

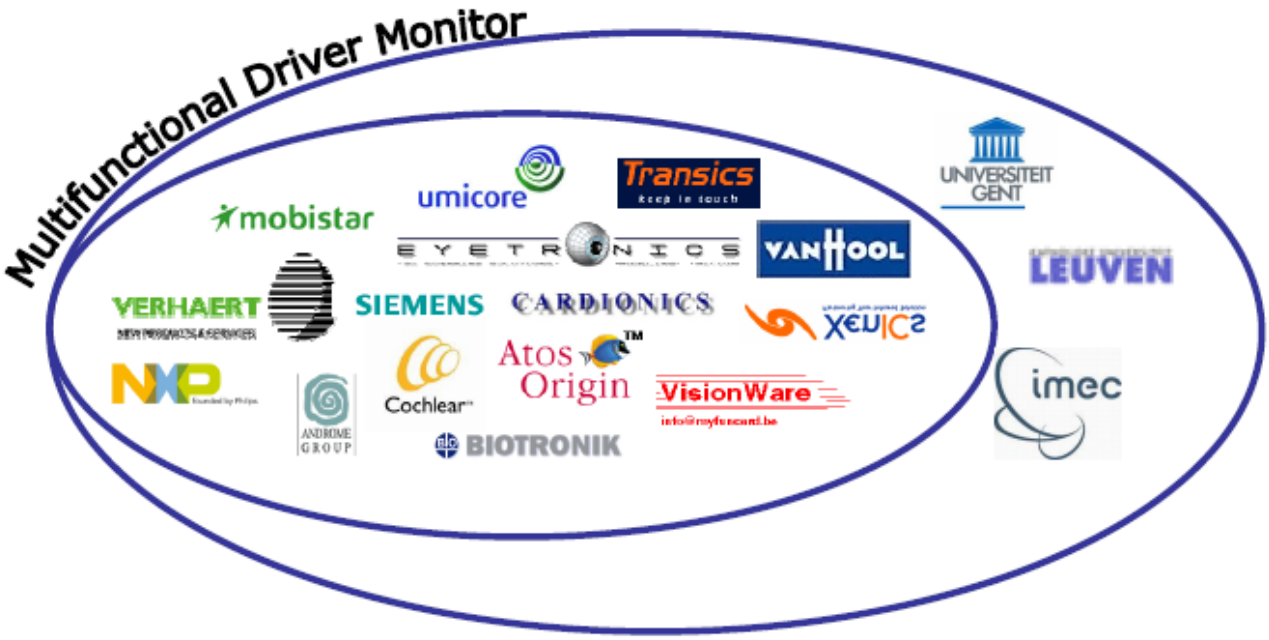
- Overview of the Safety Integrity standards in on- and off-highway
- ASIL compliancy knowledge
- Overview of processes and system architectures used
- Competence to evaluate system architectures
- Influence of SIL on Autosar
- Judgment on tools and technologies suited for ASIL

To achieve a successful design process, the following supporting competences need to be acquired and shared with the Flemish industry:

- Knowledge management
- Project Management
- Competence network with Universities and Technical Universities

Acquiring these competences is the main objective of this project. The transfer of the achieved results towards the participating companies will be accomplished by working on specific validation projects .

Expected results of the collective research project



The acquainted knowledge and competences will be used by the partners of Flanders' DRIVE. Every partner of Flanders' DRIVE, who develops or plans to develop intelligent automotive systems using components like controllers, sensors, actuators and others will sooner or later come into contact with the need to apply the ASIL process.

The specific and measurable goal of this project is to provide each of the Flanders' drive partners with the capability to execute projects according to the SIL (Safety Integrity Level) of the IEC61508 safety standard. The IEC 61508 defines 4 SIL levels, depending on the safety requirements of the end-system. SIL 4 is only needed for very demanding systems where active fault tolerance is a must and is considered outside the scope of the automotive sector. Nevertheless, the project will have prepared the framework to reach SIL4, should this become a requirement.

Contacts with the Flemish industry have often shown the shortage of design capabilities. Flanders' DRIVE will be able to support all development activities in the domain of Vehicle Dynamics. There will also be a spill-over to other domains within automotive or even to other sectors than automotive, i.e. machine construction, avionics or railway.

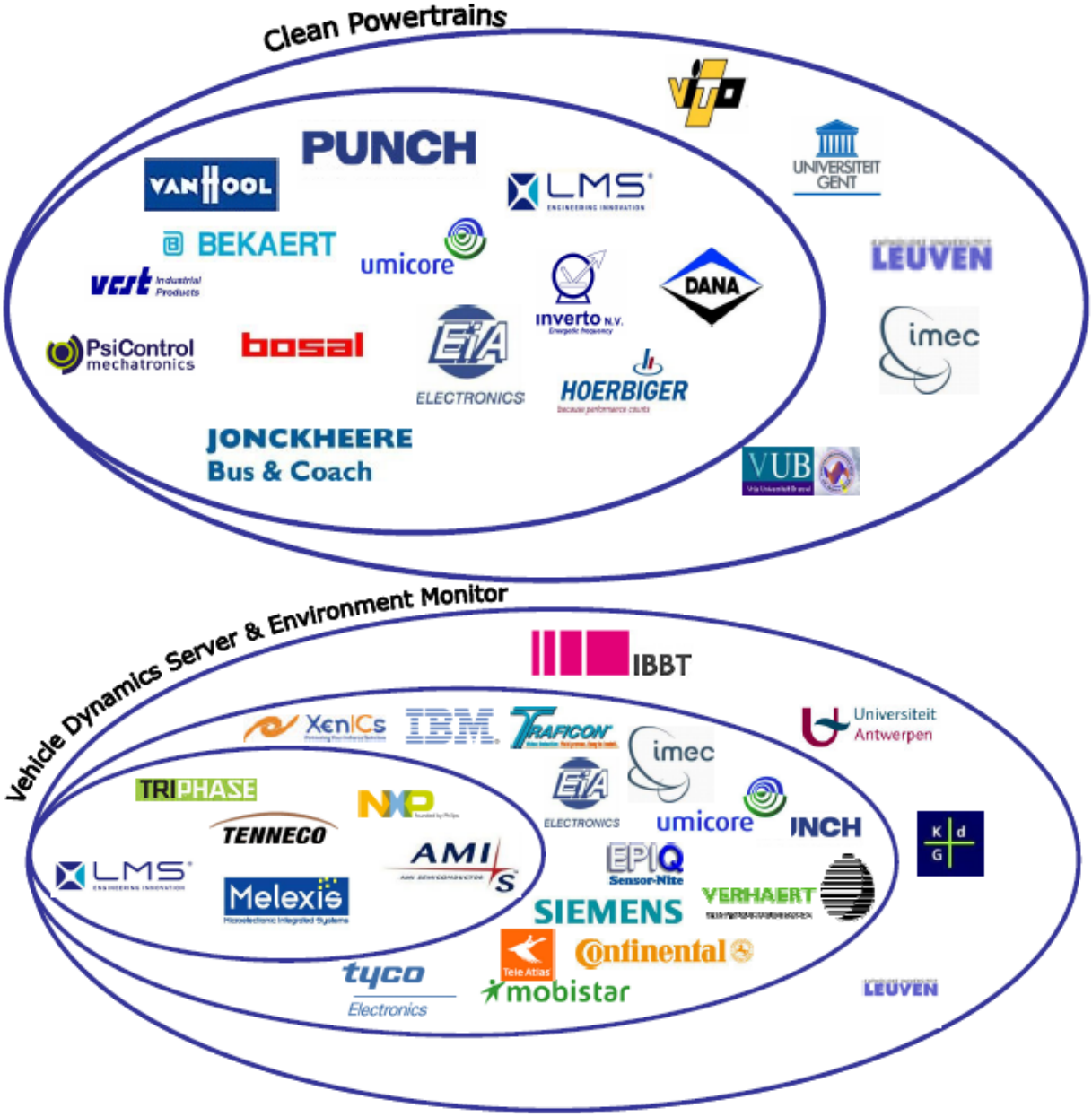


Figure 4: Target groups in the Flemish region based on the different business cases that need process support in product development

The development of the basic competence for embedded software and vehicle dynamics answers the fundamental needs in the new automotive industry. This know-how also gives opportunities for other business cases like hybrid power train, important for the Flemish industry.

Summary

To summarize, the available methodology will support the Flemish OEM's and suppliers that are active in development and/or integration of intelligent systems. This will enable knowledge and competences to be built up in several areas needed to intelligently integrate and explore new technologies and applications in a wide range of domains. There will be a spillover to other sectors like machine construction, avionics and railway.