Autonomous and connected vehicles: Collaboration of Aeronautic and Automotive industries to face the huge challenges for safe and secure embedded systems.

Gerard Ladier, Pascal Traverse, Hervé Delseny, David Lopez, Christian Assier, Jean-François Sencerin, Yves Dordet

Autonomous and connected vehicles: Collaboration of Aeronautic and Automotive industries to face the huge challenges for safe and secure embedded systems.

By : Gérard LADIER (Aerospace Valley / Airbus), Pascal TRAVERSE (Airbus), Hervé DELSENY (Airbus), David LOPEZ & Christian ASSIER (NXP), Jean François SENCERIN (Renault), Yves DORDET (Aerospace Valley / Continental)

Introduction

The development of autonomous vehicles is one of the major challenges of the beginning of this century. Their development will drastically modify the mobility and it corresponds to a technological rupture which will redistribute the roles and business model of the major players.

These autonomous vehicles are a concentrate of technologies, including smart sensors, embedded intelligence, safety architecture and concepts.

Besides, these vehicles will always be connected to the rest of the world to manage the real-time information needed to ensure a safe operation for passengers. To achieve this goal, the security of exchanged information must be absolutely guaranteed.

Systems invaded aviation before the automotive industry because of some basic needs that can be filled only with systems: navigation (finding the plane position, determining the route) and communication with the Air Traffic Control. Hence, electronics appeared quite early in aviation. This has likely motivated early introduction of vehicle control systems (auto-pilot, engine control, flight control …) and thus of embedded systems with very high dependability requirements.

Conversely, the automotive industry started with vehicle (engine and braking) control and is now implementing automated functions to assist or substitute the driver. As these systems become one important criterion when choosing a car model, all car manufacturers are deeply investing efforts to propose ADAS (Advanced Driver-Assistance Systems) functions like Emergency Brake Assist, Active Cruise Control, or Park Assist.

In parallel, public transportation, goods transportation and agriculture are building strategies to manage autonomous vehicles fleets.

In the meantime, we see emergence of autonomous flying vehicle to carry in large scale goods or people, like drones or air taxi concepts.

For all these innovative projects, great technological challenges are still to solve, requiring large investment. Each month are announced collaborations between companies and research institutes to combine competences and objectives.

Even if there are differences in standards used for the development, safety system architecture, critical events and certification methods, a convergence of the need must lead to a close collaboration between the players from aeronautic and automotive fields.

Safety concept in Aeronautics:

Let us take the example of Airbus : the safety principle is based on the redundancy of dissymmetric functions, combined with a very rigorous and demanding development & verification processes of the Software & Hardware needed to implement these functions, to reach an acceptable safety level (Development Assurance Level A in line with a quantitative safety objective of 10^{-9} failure per hour).

The original system architecture of the Airbus A320, certified in 1988, is based on a dual computer operation called “control/monitor architecture”.

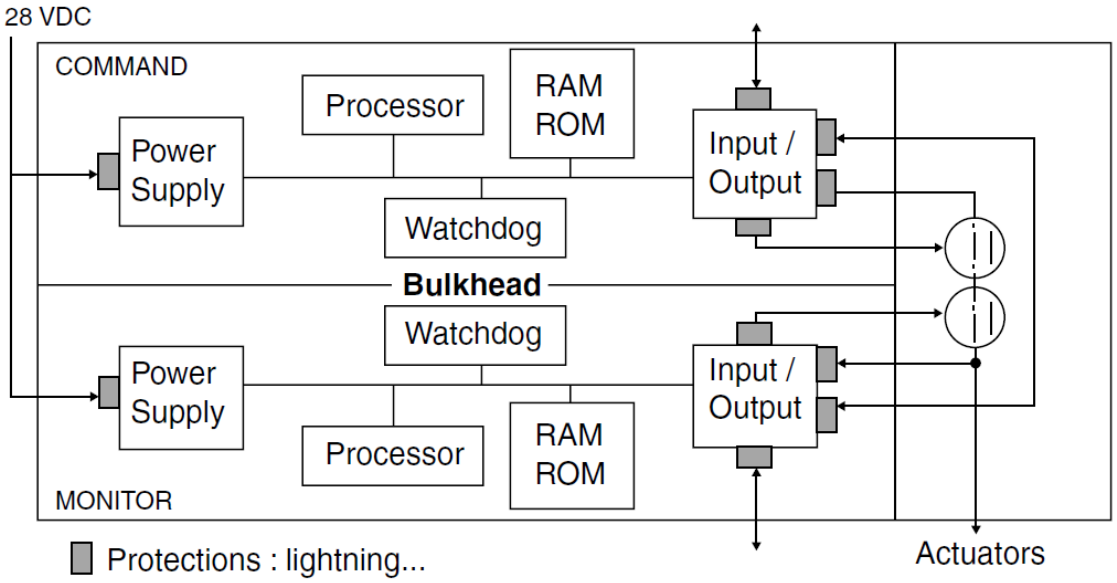

FIGURE 1: Command and monitoring computer architecture

Airbus Fly-by-Wire system is basically composed of one set of command and monitoring computers (3 “PRIM” on most airplane, 2 “ELAC” on A320 family) ensuring the normal control of the airplane and another set (2 or 3 “SEC” depending on the airplane model) to provide a dissimilar – and simpler – control.

This original architecture ensures the safety and the availability needed for fly-by-wire systems (quantitative objective – the famous 10-9/flight Hour – but also qualitative ones: particularly the demonstration of the absence of any common point of failure).

The disadvantage of such safe architecture is the cost of the function due to the duplication of functional blocks.

As mentioned before, these architectural principles are completed by very rigorous and demanding development & verification processes of the software and hardware needed to implement these functions.

The requirements on these development processes are compiled in several standards documents, well known in Aeronautics and even out of these domains, as Aeronautics has played a pioneering

role in the definition of such requirements (DO-178 was first released in 1982): DO-178 for the software, and later on DO-254 for the hardware and ARP 4754 for the system layer.

These documents define the requirements related to the life cycle and to each process of the life cycle and the life cycle data to provide (~ documents). The requirements vary according to the Development Assurance Level (DAL, 5 levels with DAL A as the most critical and DAL E the less critical) and for each DAL, these documents define the applicable objectives and outputs for each process, the level of independency required to perform the activities and some other considerations. We can summarize these requirements in the following way, taking the example of Software. The DO-178 standard mandates that each and every line of code is:

- Specified in requirements
    - Coming from and traceable to system requirements
    - Developed in compliance with standards
        - Approved by the methods/quality teams of the developer
        - Controlled by the quality teams of the manufacturer
        - Validated by the certification authorities
    - Verified through analysis and reviews (compliance, consistency, accuracy, HW compatibility, verifiability) with independence
- Allocated in the SW architecture and designed in refined requirements :
    - Traceable to requirements
        - Developed in compliance with standards
        - Approved by the methods/quality teams of the developer
        - Controlled by the quality teams of the manufacturer
    - Validated by the certification authorities
    - Verified through analysis and reviews (compliance, consistency, accuracy, HW compatibility, verifiability) with independence
- Coded
    - To realize the applicable requirements
    - In compliance with standards
        - Approved by the methods/quality teams of the developer
        - Controlled by the quality teams of the manufacturer
        - Validated by the certification authorities
    - Verified through analysis and reviews (compliance, consistency, accuracy, HW compatibility, verifiability) with independence
- Integrated
    - With the rest of the software and within the target
    - Verified by review (completeness, correction)
    - Tested with test cases
        - Developed in compliance with standards
        - Approved by the methods/quality teams of the developer
        - Controlled by the quality teams of the manufacturer
        - Validated by the certification authorities
        - Based on requirements
            - With full functional coverage
            - With data inside and outside of the validated range values
            - Reviewed with independence (functional and structural coverage)
    - Managed under configuration/modification control
        - In compliance with standards
            - Approved by the methods/quality teams of the developer
            - Controlled by the quality teams of the manufacturer

        - Validated by the certification authorities
        - With Root Cause Analysis of delivered anomalies to improve the processes
- Developed and verified with tools which are
    - All identified in documents
    - Qualified if necessary
    - With the same constraints as above for code generators…

Safety concept in Automotive industry:

In Automotive industry, the safety architecture is based on a functional layer associated with a survey layer which checks the integrity of the function. Both are managed by a supervision layer with is defining safe modes operation in case of failure. This concept leads to less expensive systems and reach the same probability level AsilD (10^{-9} failure per hour).

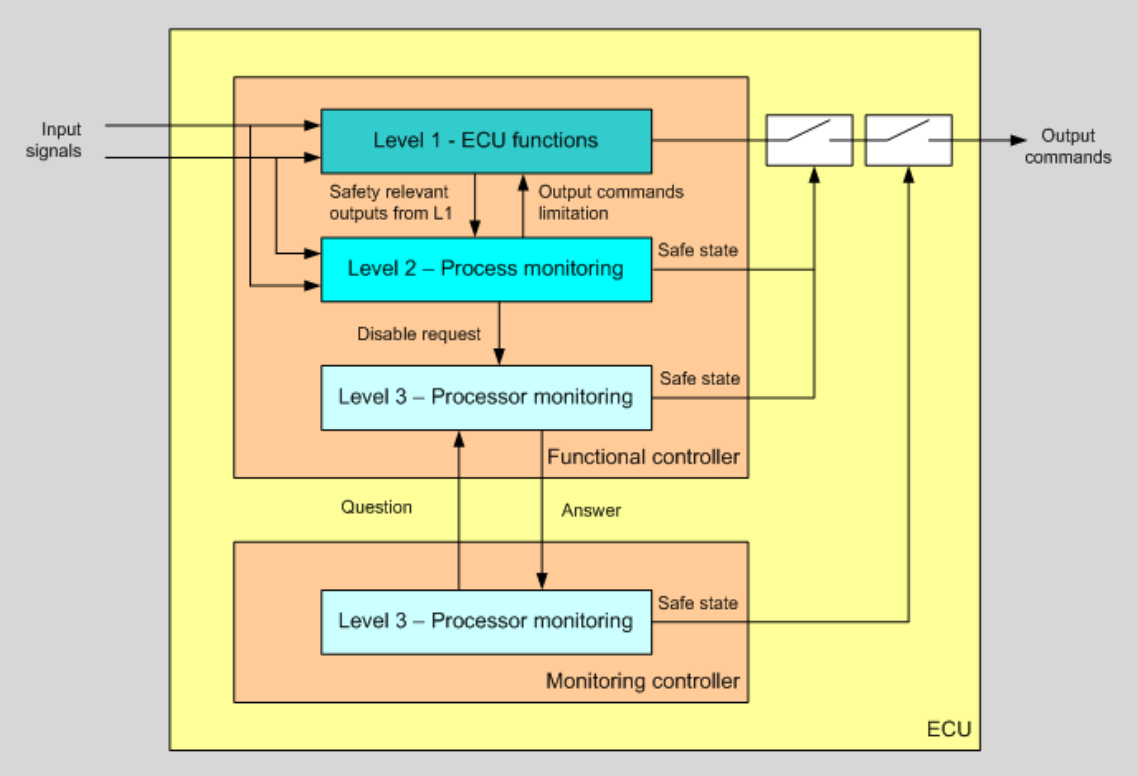

FIGURE 2: Safety architecture of non-automated vehicle Electrical Power Steering function

Anyway, to reach the 10^{-9} failure per driving hour, an electrical power steering system assumes that, in case of assistance lost, the driver is available and able to manage a non-assisted safe mode.

For an autonomous vehicle, it must be reconsidered. Currently, new systems are rising based on redundant actuators to replace the driver operation with in parallel the use of multicore microcontroller with a distribution and parallelization of functions and survey are being developed. The request of “availability” in this case is closer to the aeronautic needs.

To decide the trajectory of the autonomous vehicle, the technical challenge is to detect and categorize the objects all around the vehicle. This definition is based on the fusion of radar, lidar and camera embedded in the vehicle assuming a minimal impact on the infrastructure (i.e. without modification of road posts, addition of beacons etc.).

The main concern of terrestrial driving is the infinite critical events which could be faced, combination of the traffic (vehicles, pedestrians, animals…), the weather, the quality of the infrastructure etc.…

In front of all these cases the embedded intelligence must drive the vehicle dynamic command. It means that the model used for the decision has also to consider the plausibility of all the information delivered by the sensors, the vehicle and the driver monitoring. These data are not binary and for example the cameras and radars performance could be affected by poor weather conditions.

To build up and test these complex algorithms, the current trend is to develop simulation of critical events in several driving conditions to save millions kilometer tests, to develop deep learning models etc…

Currently the car makers are concerned by the safety level of the functions based on the standard ISO26262. Anyway, as soon we consider that no driver is available to be back on driving operation, the availability of the function must be considered and it drives to requirements close to the aeronautic concerns. These requirements lead us to turn to the aeronautic industry.

Synergies:

This example demonstrates that the two worlds are currently using two different ways to converge to equivalent safety goals for autonomous systems facing different critical events.

Aeronautics was clearly leading the development of autonomous operation for many years. Anyway, these safety systems are currently developed and validated. The main effort of the plane maker is more focused today on the reduction of costs. Aeronautics could take advantage to the large investments for the innovations developed for autonomous vehicles in automotive industry..

In parallel Automotive is spending huge R&D efforts to develop safe autonomous and connected vehicles. To reach this ambitious target, new methods for design, embedded intelligence, simulation, tests and safety demonstration are currently under development. For sure these concepts are also driven by the serial cost optimization. The safety is more and more integrated in the architecture at each control unit level, cable or connector, thanks to the large number of serial product on the market and capitalization of field return of experience.

The consideration on the real environment and infrastructure is also a key for terrestrial operation to anticipate the decision based on high definition and interactive maps based on secure communication between the vehicle and the cloud.

In parallel, for Urban Air Mobility and parcel deliveries purpose, autonomous vehicles are developed, integrating the 3rd dimension. The drones and air taxi will take place in the mobility landscape of tomorrow. They will be used for logistic or people transportation. Their specific requirements are not yet set but they are very likely to re-use and adapt safety architecture concepts, development standards, cartography, simulation and field test operation.

Standards:

ISO26262, the standard for automotive safety systems, was already defined in close collaboration of experts from Aeronautics. This standard is under reconsideration to include autonomous ground vehicle operation, not initially considered. The impact is huge due to the introduction of availability requirements and to the probabilistic approach for false detection of sensors. One of the goals will be

to specify how to quantify the risk of autonomous mode and when to decide to activate a safe mode or a request to go back to manual mode, based on driver monitoring information.

Software and autocoding:

The Software in Aeronautics is based on the DO-178 standard which is based on a deep qualification of software tools and huge tests of the code. The functions model could be developed with SCADE® and autocoded with a alleviation of code verification for certification, thanks to a huge effort done for the qualification of the tool.

In Automotive, it is a trend for car makers or systems developers to provide a model of the needed function in place of huge Doors® specification. It gives more flexibility for the development, limits documentation effort and allows the management of intellectual property of functions improvement . The most used tool for autocoding is Matlab®. From the model, the autocoding is done using "embedded coder from Mathwork" or Targetlink. Unfortunately, both autocoding tools are not certified, it means that no "safety stamp" can be argued for the safety demonstration of the software. For safety applications, the test and software documentation correspond to huge effort. Recent improvements in this method allow today an automatic generation of test plan and software tests to ensure a perfect matching between the provided model and the corresponding code.

Simulation:

The simulation is fully efficient in Aeronautics and daily used for the qualification of safety flight operation and training of pilots. It will be largely used for demonstration of safety procedures and systems, allowing the planes to start their first real flying tests with a good level of confidence.

In Automotive, the qualification is currently done by real field operation tests. It is driven by the complexity of the environment of the vehicle and the scope of weather and road conditions which could be faced by the autonomous vehicle. For example, the qualification of an Emergency Brake Assist function requires more than one million kilometers road tests. The way to reduce the corresponding costs is to develop simulation tools able to recreate the multiplicity of critical events which could be faced. The simulation for cameras is already done (CarMaker from IPG, SCANeR™ from Oktal…). A virtual dynamic scene is created with the landscape, with the different objects all around the vehicle and with the weather condition which can be changed. It gives the possibility to recreate critical situations and to develop corresponding driving strategies.

For the Radars and Lidars the simulation is more complex. Developments are ongoing, based on Aeronautics simulation software (Oktal-SE) to recreate artificially the signal of automotive radars in correlation with virtual scene of the camera simulator. The synergy is more from Aeronautics to Automotive but in parallel Aeronautic is more and more focusing of the use of Automotive sensors, at first for ground anti-collision systems.

This close collaboration is demonstrated by the recent alliance of Sogeclair and Renault for the creation of Autonomous Vehicle Simulation (AVS) which will focus of improvement of SCANeR™ for automated driving simulation. Another example is the use of the NVidia platform for image processing for the air taxi "Vahana" that is developed by Airbus in San José, CA.

High Definition and dynamic map:

The autonomous vehicle guidance requires a position accuracy of few centimeters, especially in lateral position. For example, the accurate positioning regarding the lane is mandatory for the definition of trajectory during lane changing or insertion in the traffic. Today the accuracy given by the GPS is far away from this need (around 10 meters) and even the improvement with the introduction of Galileo constellation will not be enough. Some strategies are developed to improve the vehicle positioning but they are quite CPU in terms of resources consuming.

A way to improve the positioning is to use the information given by the smart camera of the vehicle.

These cameras and the software behind can classify the objects and recognize specific ones which are linked to accurate position on the map. By triangulation methods the location of the vehicle can be determined regarding the known position of these “landmarks”. In parallel the link between a high information map including the position of all the traffic signs and traffic lights will be very useful to driving in poor visibility conditions. This very efficient information is based on a collaboration of all vehicles equipped with such intelligent camera and connected to the cloud. Each car will get the information coming from the preceding ones on a collaborative and dynamic mode. It allows an anticipation of dangerous situation by adjusting the speed of the position of the vehicle to the situation located behind, even without visibility.

For example, your vehicle will be informed that a truck is stopped just after the next turn and that your vehicle must brake or change its lane.

This HD and dynamic map is currently setting up as a consortium in a close collaboration of major players in automotive field members

Collaboration:

The challenge of the autonomous vehicle development is so huge that no company, alone, will be able to ensure a safe operation on public road. Each month, the collaboration, merging between big players in autonomous vehicle field can be found in the news.

This need to combine effort to keep a competitive place on the market was clearly understood by several countries and by Europe.

We can notify the large number of H2020 projects pushed by Europe.

In Germany, a large project “Pegasus” with all major car makers, tier ones and universities, funded by the government to support the autonomous vehicle driving on highway.

In France, a large collaborative project was initiated in 2014 to accelerate the development and launch of autonomous vehicles on public road.

This project named “Nouvelle France Industrielle – véhicule autonome” is a close collaboration of all the major car makers, tier ones, research institutes, was initiated and supported by the French government. The goal is join effort, in dedicated working groups to release all the blocking points (technologies, legal, standards, insurance etc...). This common approach allow a coherence between the different projects (national or European), of experimentations, of simulations tools etc…

In parallel all the partner are able to speak with one voice in front of French government; European instance or equivalent initiatives in different countries.

STAC:

To initiate and manage these synergies Aerospace Valley has already created a project called "System of Transportation, Autonomous and Connected" (STAC).

Initiated by Aerospace Valley, STAC enables collaboration between players from different fields to benefit from synergies based on complementary know how for different autonomous vehicle makers.

The goals are:

- To apply our industrial excellence and scientist in critical embedded systems to the development of the STAC.
- To contribute to the local development of a world spot in IoT and mobility of the future.
- To leave/in support principal actors in these "new applications" present locally (Continental, Actia, Easymile, etc).
- To feed back the innovation in aeronautical products (drones, autonomy in the cockpit,…) and to open in this field of new opportunities of applications and services.
- To support the mobility transition linked to the new economic models offered by the autonomous and connected vehicles.

The expected partners are coming from Aeronautics, Automotive, public transportation, trucks, rail, drones, air taxis, logistic vehicle and self-driving robots, etc….in strong collaboration with universities, high schools and laboratories to take benefit of the high academic level of our regions.

All together we will combine competences and, thanks to this partnership, will prepare a safer future in Occitanie and Nouvelle Aquitaine.

The main objectives for the project setup are:

1. Setup of experimentation center for validation / certification of autonomous vehicles in urban conditions using the university campus of Paul Sabatier (Toulouse). 70ha dedicated to autonomous experimentation (cars, taxi, shuttles, bus, logistics vehicle, drones and flying cars)
2. Aeronautics – Automotive safety system architecture: including connectivity, Data register, map and cybersecurity
3. Collaboration / communication V to X
4. Virtual pilot/driver: assistance, interaction with machine, trouble shooting.
5. From 2D to 3D environment – how to take benefit of larges development of terrestrial autonomous vehicles for flying ones.
6. Sensor fusion for environmental measurement.

Several workshops have been done to support the emergence of ideas for new developments and projects.

The kick off in January 2018 is the starting point for closer and closer collaboration between different industrial worlds focusing on common objectives. It will be achieved through collaborative projects with the support of Aerospace Valley for project setuo.

Conclusion:

The Technology challenge of the autonomous vehicle development requires a close collaboration of all the main players at international level but also at national and local level. The convergence of Aeronautics and Automotive requirements for the development, the validation and the certification for a safe and secured future mobility, will benefit from a stronger collaboration between the different players. The project STAC has been created to allow such close collaboration, thanks to Aerospace Valley who ensure the networking of more the 800 companies.