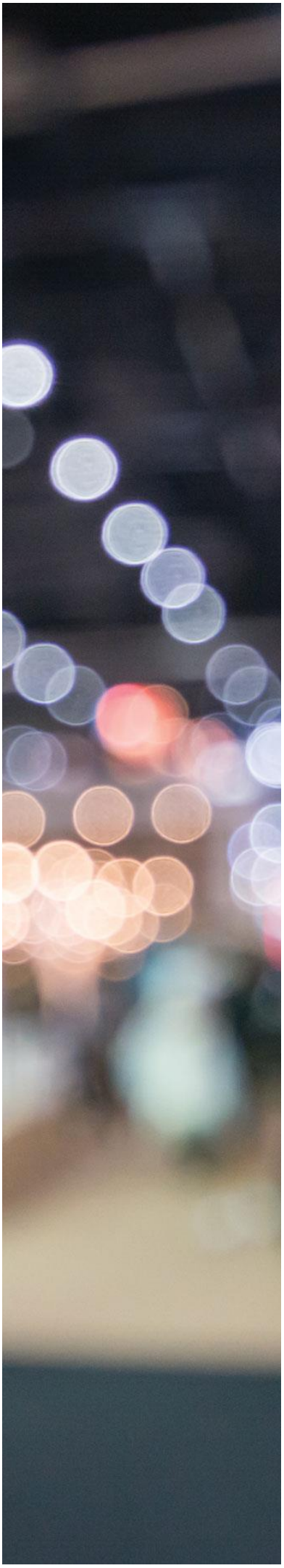
PRESS KIT

BAUMA 2022



Join-us

https://www.linkedin.com/showcase/actia-off-highway/

Press Contact:
Vaiana.krieger@actia.fr
+ 00 33 (0)5.82.08.05.36

PRESS releases
BAUMA - MUNICH 2022

SUMMARY

With its 2nd generation of on-board ECUs, ACTIA has taken another step towards the SuperECU

ACTIA has been working with **vehicle command and control** systems for many years, to meet specific customer needs via its range of generic products.
Today, ACTIA is enhancing the functionality of its **ACTI-Ways** range of on-board ECUs, with a new generation of ECUs aimed at aligning the characteristics and performance of hydraulic functions in off-road vehicles.

The new **ACTI-Ways** range, represented by the SPU 30-17 and SPU 70-66 ECUs, is particularly well suited to the evolving market of special machinery operating in harsh environments. In addition to its increased capabilities and performance, which open up new functionalities, it integrates **operational** reliability and **cybersecurity** constraints.

Access to new functionalities and driving assistance

The new SPU range of ECUs for controlling hydraulic functions has increased input and output capabilities.
ACTI-Ways 2nd generation improves ECU capabilities in order to cover the growing needs of the on-board systems that are also becoming increasingly complex for the off-road vehicle market:

- New microcontroller
- Increased processing performance
- Increased flexibility of I/O configuration
- CAN FD
- LIN.

The change in ECU needs is moving towards:
- A broader range of functions
- The inclusion of a wider range of technologies, in particular for environmental acquisition
- "Smart" over-systems emulating humans – with super ECUs
- Electrification of vehicles.

> *"With this new range of ECUs, ACTIA is pursuing its strategy of expanding SPU capabilities so that they can interact with Super ECUs in autonomous functions*."
> Emphasises **Fabien TRINITÉ**, Director of the Vehicle Automation product line.

Combining operational reliability and cybersecurity

The new generation SPU integrates **operational reliability** and **cybersecurity** constraints.
ACTIA is closely connected to its markets, to monitor changes, including changes to standards. The group has successfully developed its technologies and its organisation to plan ahead for these issues.
ACTIA has set up a centre dedicated to the areas of **cybersecurity**: expertise, monitoring, robustness and penetration testing. This measure aims to improve protection solutions in the specifications and implementations for exposed products. In addition, ACTIA is involved in standardisation committees and is notably a member of ISO SAE 21434.

The trend is the same in the area of **operational reliability**. ACTIA has been designing and producing certified products for 15 years and has established a dedicated business manager: Project Safety Manager. This manager is in charge of coordinating the methods and solutions. ACTIA is able to address a broad range of standards (ISO3849, ISO25119 and ISO26262) with better performance in **reliability**, **safety** and **stricter regulations** for products put on the market.

Plug & Play compatibility with previous vehicle architectures

ACTIA places great importance on continuity in the development of its products. The electrical and mechanical interfaces of the new SPUs are therefore identical to those of the previous generation (pin to pin compatible); this is to ensure plug-and-play for existing customers:

- Identical dimensions
- Equivalent performance for existing functions
- BSP with similar API, functions and behaviour.

As regards the software, these products are also designed to require minimal application porting effort, which is very welcome for customers who need to manage several types of machines.

> "*ACTIA's ECU offer is for different vehicle families with common needs but their own specific features: HGVs, buses and coaches or special machinery. Thus, ACTIA is able to diversify its solutions on these different markets. This generates real added value.*" Concludes **Catherine LEDEUIL**, Head of Marketing and Sales for VEA (Vehicle Electronic Architecture).

ACTIA accelerate its resilience plan to face the components crisis

ACTIA, as a global player in the automotive electronics industry, has built up solid experience in managing its supply chain. In this highly disrupted global context, ACTIA strengthens its 3 pillars its **relationship with its suppliers**, its experience in **managing the obsolescence** of electronic components and its **electronic card redesign program** to minimize the impacts of the crisis and ensure delivery continuity to its customers.

Resilience of ACTIA's supply chain

The supplier panel or the extended enterprise

ACTIA's purchasing strategy is based on its **market intelligence** and the **creation of a supplier panel** with which ACTIA develops **close and long-term partnerships.**

> « *We involve our suppliers very early on in the projects:* starting from the innovation and consultation phase for an invitation to tender*. This allows our suppliers to understand what our emerging needs will be. For their part, they provide us with their innovation roadmap for their components. This enables early incorporation of innovations into our designs. In this respect, the supplier ecosystem is an* extended enterprise*. Suppliers are strategic partners for our innovation, the quality of our products, and our competitiveness. The components crisis has obviously furthered this trend.* » Explains **Vincent TURMEL**, ACTIA Purchasing Director.

A dedicated purchasing team

The key phase in establishing a resilient supply chain is during **product development.** It is during this stage that the risk mitigation actions are most effective. Therefore, ACTIA has a **dedicated purchasing team** that is an integral part of the product development team.

This team is tasked with **analysing risks** throughout the product development period, based on data collected by the **Components observatory**. The risk analysis is exhaustive and relates to all of the references in the parts list.

Securing future supplies
ACTIA is carrying out an **in-depth analysis** of its supply chain and suppliers, to **secure procurement in the future.**

Some criteria for evaluating semiconductor suppliers:

– The longevity of the range of components
Their production capacities in relation to overall demand.
– The front-end and back-end manufacturing sites.
– Their dependence on subcontracting.
– their multi-FAB strategy, etc.

ACTIA has expanded its database to include a new criterion, **procurability,** and according to these criteria, a component will be rated as more or less “procurable”.

The Components observatory: more than 15 years of experience

For more than 15 years, ACTIA has had a dedicated group of at least 20 people in place to continuously monitor the electronics market: **the Components observatory.** It provides precise information about the electronic components market in order to make the best sourcing decisions, and also to monitor and manage product obsolescence.

“ACTIA is one of the few market players to integrate an organization dedicated to the analysis and management of component obsolescence.”

This organization uses the component information bases which it completes and consolidates, so that, in the development phase, as in series production, the engineers have a precise vision of the state of all the items in their nomenclature in order to identify and remove risks.

Finally, this organization participates in the process of creating new items, in particular to ensure **multisourcing,** which is essential to ACTIA's supply chain resilience strategy.

Multisourcing is THE rule at ACTIA

Working with multiple supply sources is key for mitigating risks and securing the supply chain. Multisourcing is the rule at ACTIA. Sole sourcing is a risk and only applies to very specific components (CPU, PCB, power ICs, etc.). Carried out when a new reference is issued, it allows to:

- Manage the end of life of components,
- Reduce the risks of redesign,
- Address supplier quality issues.

Multisourcing is also an ally when it comes to competitiveness, the crisis has not changed anything there.

Redesign to Deliver

The ACTIA R2D program

On-board electronic products have long life cycles: electronic architectures are replaced every ten years or so. Along the way, however, it will now be necessary to update the circuit board, both to manage obsolescence of certain references and to secure the supply of all components.

ACTIA is committed to this approach to redesigning electronic products, in collaboration with its customers: the **Redesign to Deliver** (R2D) programme. Drawing on its engineering capability and its expert knowledge of the components market, the group is a preferred partner for manufacturers in order to ensure deliverability of on-board electronic products.

Smooth revisions

ACTIA's R2D programme has been launched on a selected number of products and takes into consideration:
– the record of all supply issues, since the start of the component's crisis;
– an update of the assessment of risks for the entire bill of materials.

The programme aims to carry out a limited redesign to mitigate the main risks and also to limit time to market and the technical risks. This limited revision is considered an improvement, unlike a complete revision.

Enrich the technological performance of existing products

A redesign is an effective way to give existing products a new lease of life. Indeed, it is the second most common reason for redesigning a board: improving an existing solution and refining its performance.
ACTIA will take advantage of the redesign to upgrade the technology and enhance the capabilities of the products, as soon as this is practicable.

While the components crisis has accentuated the trend, ACTIA is confident that electronics redesigns will now be necessary throughout the life cycle of all electronic products: not only to mitigate component obsolescence, which is accelerating, but also to ensure reliable and sustainable provision of supplies

- A resilient, agile and **sustainable supply chain**;
- More than 15 years of experience in **component obsolescence management;**
- ACTIA's expertise in **card redesign**

ACTIA relies on its organization and its know-how to ensure the deliverability of its products and to face the multiple disturbances of the electronic markets.

ACTIA's new range of SPUs focus on security AND cyber.

Construction machinery is equipped with computers connected to **multiple sensors**. Faced with this profusion of data, designing and developing embedded solutions is a real challenge in terms of **securing embedded systems**. Like all the products developed and produced by ACTIA, the new range of SPUs integrates the levels of **functional safety** AND **cybersecurity** requirements.

Security by Design: from the design and development phases

The concept of “securing” translates into the growing requirements for both **safety** and **cybersecurity.** ACTIA therefore develops its on-board ECU that are compatible with the standards of these two requirements, right from the design phase.

In terms of cybersecurity more specifically, the security of ACTIA products is based on a pragmatic approach based on analysis, risk management and their continuous monitoring.

ACTIA is constructing a CTI (Cyber Threat Intelligence) process that consists in collecting, organising, and analysing information related to cybersecurity risks and threats.
This process, used upstream of the life cycle, allows attacks and threats to be considered in the initial risk analysis, and appropriate protective measures to be defined from the design and development phases.

In the series production phase, it guarantees orchestrated resiliency, adaptation of the architecture to changes in these new attacks or vulnerabilities.
At the same time, ACTIA is embedding cybersecurity requirements and best practice into its design and development processes.

> “Integrity and confidentiality of information carried on the networks is a critical issue for connected vehicles. As a result, ACTIA natively integrates software & data protection requirements and measures from the very start, and throughout the life cycle of the vehicle architectures and systems.”
> Explains **Fabien TRINITÉ**, ECU Automation Product Group director.

ACTIA is involved in the current standards framework

The security needs of architectures and embedded systems require ensuring the

authenticity and **integrity** of components. ACTIA is able to integrate them into its technologies in advance. Thus, the 2nd generation of SPU box takes into account these constraints of both **safety** and **cybersecurity.**

Automotive regulations and standards

The group is developing systems that cover the **safety** recommendations:

- ISO 26262: relating to road vehicle functional safety;
- ISO 13849 & 25119, regarding specialised machinery;

and cybersecurity:

- ISO/SAE 21434: engineering requirements for cybersecurity for road vehicles;
- ISO 27001: Information Security Management System

Cyber protections taken into account

- Firewall and flow-filtering functions in interfaces with external networks;
- Intrusion attempt or other threat (virus) detection and prevention functions;
- Securing the vehicle's CAN bus, the system boot and updates;
- Protection of integrity of vehicle diagnostic inputs (OBD, etc.);
- Protection of internal communications (between ECUs), of communications between the vehicle and information systems, or communications between vehicles and infrastructure (V2X), particularly with encryption and electronic signature;
- Protection of the integrity of on-board ECUs (including data and program protection);
- Globally, securing the information systems involved in the operation of connected and autonomous vehicles.

Cyber threats

In concrete terms, these protective measures meet the objectives of protecting the system from a set of threats, such as reprogramming ECUs through unauthorised access, or modification to communications through network attacks.

These threat scenarios can lead to incidents affecting vehicle operation (able to cause accidents or financial losses), or users (theft of personal data).

"ACTIA is able to support our customers in these integrated **cybersecurity** approaches, acting as a real partner when it comes to these subjects. To this end, ACTIA uses a **risk analysis methodology and requirement traceability tools**, which make it easier to manage these aspects **throughout the life cycle of the product**. These tools highlight the need for intensive collaboration with all stakeholders, and the emergence of a new service-based economic model: monitoring, control and patches related to new threats."

Says **Catherine LEDEUIL**, VEA (Vehicle Electronic Architecture) marketing and sales manager.

Through synergy of its **vehicle architecture**, **diagnostics** and **telematics** expertise, ACTIA is renowned for his high level of understanding of the digital ecosystem in vehicles. The group is working on a daily basis to strengthen his security and cyber protection solutions to offer to manufacturers a high-performance trusted environment. For OEM to be able to adapt to permanent threats, the electronic architecture of the future is to be robust and resilient. Actia is a main actor in this domain.

PRESS releases
BAUMA - MUNICH 2022