**EMERGING TECH CONFERENCE – Edge Intelligence**

Volume 03, 2024, Pages 74 – 80

**Proceedings of Emerging Tech Conference: Edge Intelligence 2024**

# A novel approach on continual operation of compromised ECU functions: REWIRE Perspective

Athanasios Athanasiadis[1], Christoforos Koutsianoudis[1], Konstantinos Lamaris[1] and Tilemachos Matiakis[1]
[1] *KENOTOM P.C., Kalamaria-Thessaloniki, Greece*
a.athanasiadis@kenotom.com, c.koutsianoudis@kenotom.com, k.lamaris@kenotom.com, t.matiakis@kenotom.com

## Abstract

As the complexity of automotive Electronic Control Units (ECU) constantly increases with functionalities such as Autonomous Driving (AD), Advanced Driving Assistance Systems (ADAS), and Augmented Reality (AR), new trends emerge in automotive ECU network topologies and software engineering. Centralized ECU architectures are gaining traction, consolidating more vehicle functions into fewer ECUs to reduce network load and improve efficiency, in comparison to traditional de-centralized ECU architectures. However, this shift introduces new challenges, particularly in terms of security and the continual operation of critical functions. A major challenge is that a potential security breach and the subsequent ECU compromise would impact numerous vehicle functionalities. Therefore, ensuring the reliability and security of these systems requires innovative solutions. This paper proposes an approach that addresses these challenges by presenting the concept of "vehicle functions migration" to alternative or auxiliary ECUs, enhancing the overall system's robustness and security. Finally, the implementation and demonstration of this approach within the EU funded project "REWIRE" is presented.

## 1 Introduction

Traditional automotive electrical/electronic (E/E) architectures primarily utilize a "decentralized" approach, where each specific vehicular function is managed by an individual ECU, connected through a common bus network (e.g. CAN, CAN-FD, FlexRay, LIN). This method has been prevalent for many years and is widely implemented in most current production vehicles. Decentralized vehicular E/E architectures offer several advantages, including:

- Separation of Concerns: They allow specific functions to be managed by individual ECUs, simplifying verification processes.
- Ease of Replacement: Lightweight ECUs can be easily replaced when damaged.
- Simplicity in Integration: With limited functionality per ECU, integrating them into a network is straightforward.

However, this decentralized approach presents several drawbacks and challenges, particularly in terms of scalability and communication [1].

In response to these challenges, “centralized” ECU network architectures are gaining significant traction, with many OEMs and Tier 1 suppliers exploring these solutions. Unlike the decentralized approach, centralized “Domain” automotive architectures group more vehicle functions or even entire vehicle domains (Powertrain, Chassis, etc.) into more powerful and less in number ECUs (Figure 1 ”Domain centralized architecture”) , while a fully centralized “Zonal" architecture (Figure 1 ”Vehicle centralized E/E architecture”) would only have a single central computing platform to handle the majority of vehicle’s functions, and multiple simplistic control units that would only serve as “smart actuators” or gateway units.

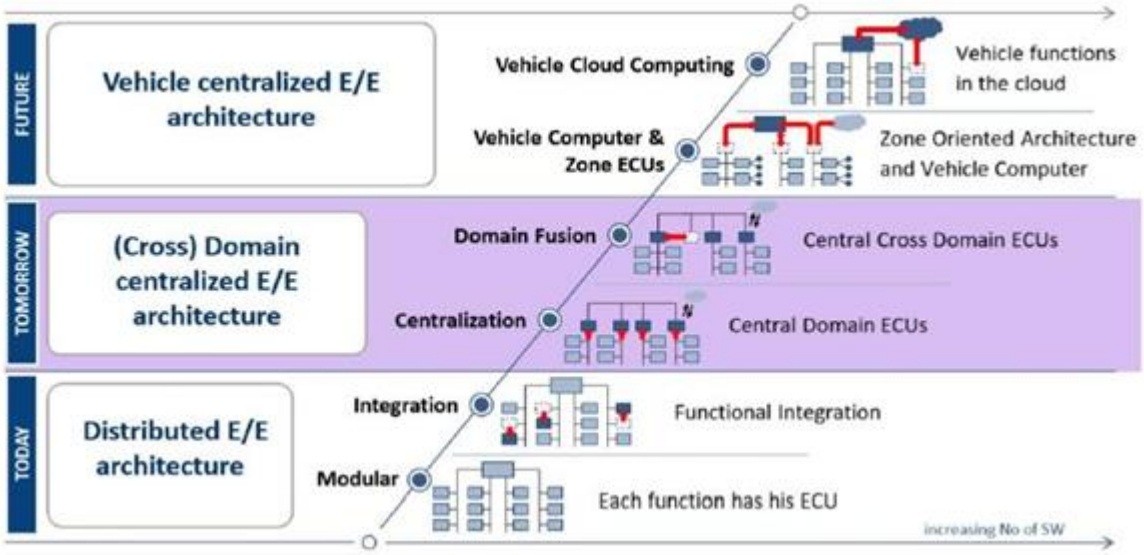


**Figure 1:** Possible evolution of vehicular E/E architectures. Figure adopted by [5]

Overall, centralized architectures signify an architectural shift more tailored to the current automotive needs, presenting various benefits:

- Enhanced scalability through the centralization of functions, allowing for: easier management of vehicle functions, easier software updates, while reducing complexity and maintenance costs.
- A smaller number of ECUs reduces needed network relations and improves communication efficiency.
- Provides a better suited platform for latest automotive trends, such as ADAS, Over-The Air (OTA) updates and vehicle connectivity.
- Standardization of Zonal/Domain ECUs (e.g. with respect to a standard communication interfaces)

However, centralized ECU architectures introduce new challenges. A potential security breach could compromise a Domain or Zonal ECU, which on centralized architectures manages numerous vehicle functionalities. For example, on the Domain architecture the Functional Domain Controller would group large portions of the functionalities of a given domain (e.g. Powertrain, Chassis, etc.) with the lower-level ECUs within that network acting as ‘smart sensors/actuators”. As a result, fail-safe mechanisms and rollback measures become increasingly necessary in order to maintain at least portions of the functionality in the case of a compromise.

This paper presents the novel concept of maintaining the operation of critical functions through "vehicle function migration" to alternative, auxiliary ECUs. This concept will be explored within the automotive use case, undertaken by KENOTOM, within the REWIRE project. REWIRE aims to develop a novel security and trust assessment framework, for Next-Generation connected "Systems-of Systems" (SoS) covering the strict security, safety, and resilience requirements during the entire lifecycle of a Cyber Physical System (CPS). The REWIRE framework will enable real-time protection through the implementation of a continuous security improvement process covering [2]:

- the design phase based on overarching system requirements
- the runtime phase covering the operation, update re-configuration, and even decommissioning of a compromised device.

## 2 Compromised ECU migration

In order to maintain the compromised ECU functionality, migration to a neighboring or back-up ECU will guarantee the reliability and the continuity of safety-critical services. Within the REWIRE project, the migration will be implemented and demonstrated in the following discrete steps:

- Device attestation, attack and subsequent compromise detection. Within the REWIRE ecosystem, physical, software, side-channel, and denial-of-service attackers are listed as examined cases that can compromise the security guarantees of the system.
- Extraction of the latest safe state of the ECU and the relevant functions to be migrated.
- Deployment of functions on other predefined ECUs that can handle the workload.

Expanding more on the REWIRE approach on the migration of functions, on the following exemplary setup Figure 2, Zonal/Domain Controllers are serving the role of collecting and processing data from a given sub-network of low-level ECUs. These ECUs can act as lower level, simplified "smart actuators" for example VCM (Vehicle Control Module) is responsible for operating the vehicle's engine, or collecting brake pedal position, with the ADAS ECU used to perform lower-level vehicle motion control (e.g. steering or acceleration). Following that setup, higher level vehicle decisions, like motion or driving strategies (e.g. ECO or SPORT modes, V2X communication, etc.), could be performed on a higher level, "master ECU", that would serve as a central High-Performance Computer (HPC), or even as a server to off-load the computational tasks on the cloud. Zonal/Domain Controller 1 (ZCU1) is the main on-board REWIRE edge device that will include the REWIRE security artefacts, along with the exemplary automotive demo application. ZCU2 is the second REWIRE-specific board that demonstrates migration of functions, an identical with ZCU1, GENESYS2 board. Migration could be facilitated either via a direct connection of ZCU1 and ZCU2 or through ZCU2 connection to higher level ECU systems (e.g. Central HPC), through the **REWIRE Trusted Execution Environment (TEE)**[*] of each ZCU, by establishing a security key between the TEEs. Security of the migration will be independent of how secure the physical network is, since REWIRE TEE will undertake this task.

[*] A **Trusted Execution Environment (TEE)** is a secure area of a main processor. It helps the code and data loaded inside it be protected with respect to confidentiality and integrity. Data confidentiality prevents unauthorized entities from outside the TEE from reading data, while code integrity prevents code in the TEE from being replaced or modified by unauthorized entities [4].

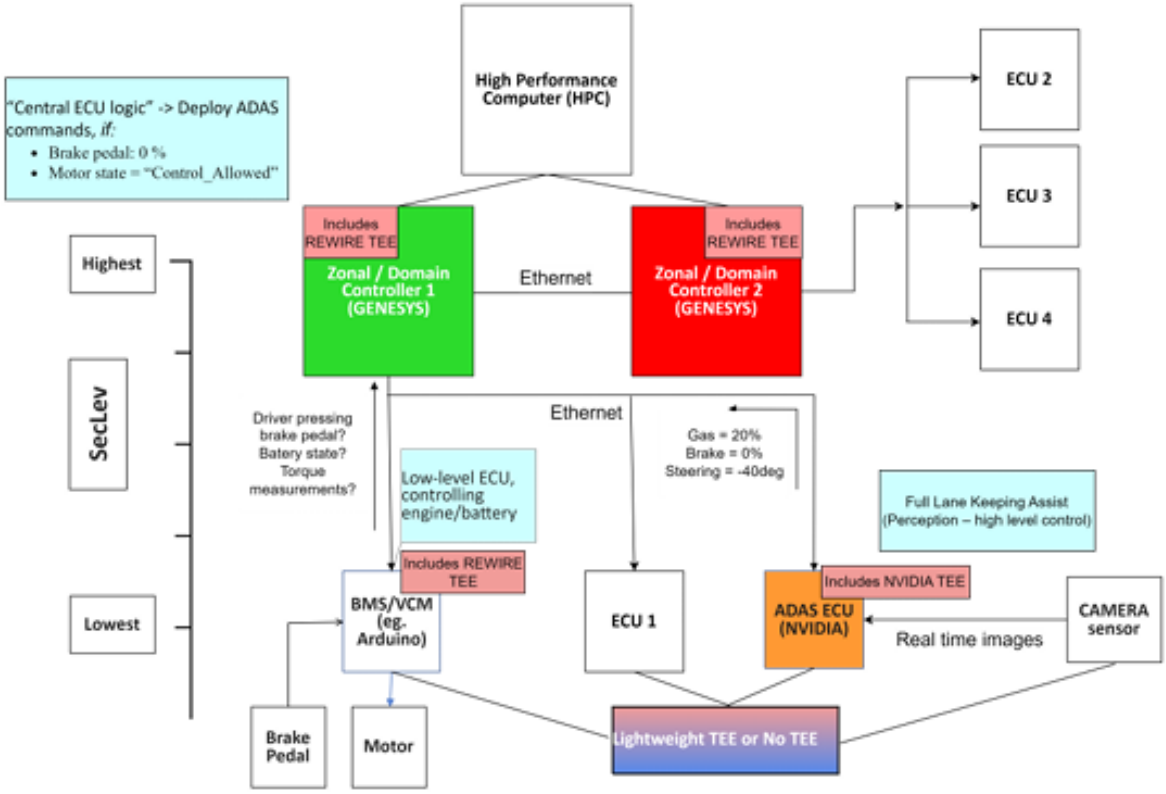


**Figure 2:** Exemplary vehicle network including automotive use case demo (example 1)

A potential security attack on a given Zonal Control Unit (ZCU), for example Figure 2, Zonal/Domain Controller 1, could compromise a significant portion of the underline sub-system, posing increased problems in comparison to a decentralized architecture, where each function would be grouped to a dedicated ECU (e.g. Motor, Transmission, ABS Control Units, etc.). To compensate that, ZCU1 functionalities could be migrated to a neighboring ZCU2, or to the "centralized", High Performance Computer as well, to either maintain some vehicle functionality or to handle the deployment of a fail-safe mechanisms on a clean and secure environment. Current vehicles do not have such a concept in any kind of form, since typically, if a specific ECU is compromised (e.g., system malfunction or security breach), safety SW intervenes to drive the system to a "minimum" safe state. Nevertheless, ECU safety SW interventions could be also compromised at a successful or extended security breach.

In Figure 3, a sketch of the demo setup along with its components is presented for the actual "test bed" demonstrator of REWIRE.

This demo setup could be thought of as part of a hypothetical vehicle-internal architecture as depicted in Figure 2. In this architecture, ZCU2 would be primarily responsible for a different domain (e.g. ECU2, ECU3, ECU4) than that of ZCU1 and would undertake the migration load. In Figure 2, some exemplary signals of a theoretical ADAS application are also depicted.

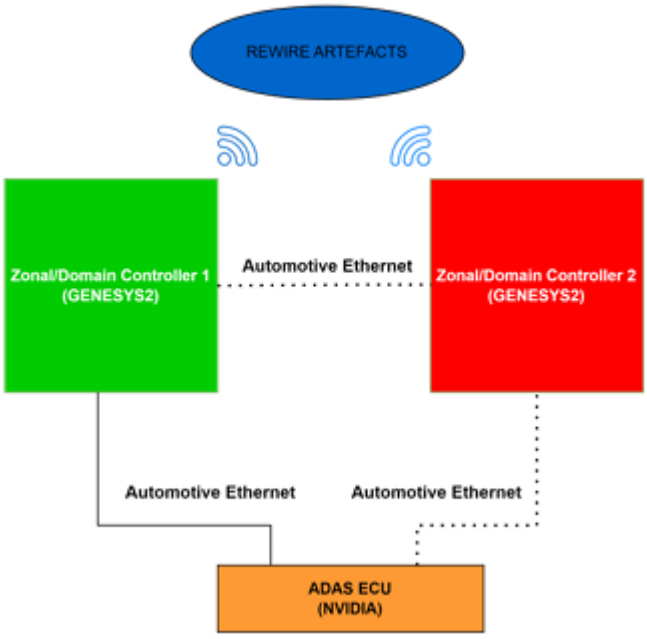


**Figure 3:** Automotive Use Case Setup

Should there be no possibility to migrate the compromised vehicle functions, the concept still holds validity for the deployment of fail-safe mechanisms. In this case, although no functionality migration is possible, transferring and deploying the compromised SW on a neighboring controller would allow the deployment of the fail-safe mechanisms of the attacked system itself (driver warnings, emergency braking, V2X communication, etc.), but on a "clean" and secure environment. Such an exemplary case is depicted below on Figure 4.

On this setup, an exemplary V2X communication is depicted, with the High-Performance Computer (HPC) receiving V2X data (adversary vehicle speeds, positions, etc.) and transmitting them to ZCU1 (Zonal Controller 1) for subsequent usage at the ADAS ECU. Similarly, ZCU1 handles transmission of speed, motion, etc. data of the vehicle itself to the HPC for informing adversary vehicles. Here, we depict a potential successful compromise on ZCU1 or/and a portion of the underlined ECUs ("X" crossed-section area). Such a case could happen for instance through a successful manipulation of network messages on VCM or ZCU1 to constantly accelerate the vehicle. Upon detecting such an abnormality, a function migration to the neighboring ZCU2 is deployed and due to the inability of gaining access to the engine itself, an appropriate message is transmitted to the adversary vehicles, to notify for the malfunction (e.g. "Vehicle compromised. Yield crossing priority, if needed").

Finally, the REWIRE project, with the automotive application SW and test setup for each board already implemented, excitedly enters the next demonstration phase where these concepts will be integrated with REWIRE security framework and artifacts.

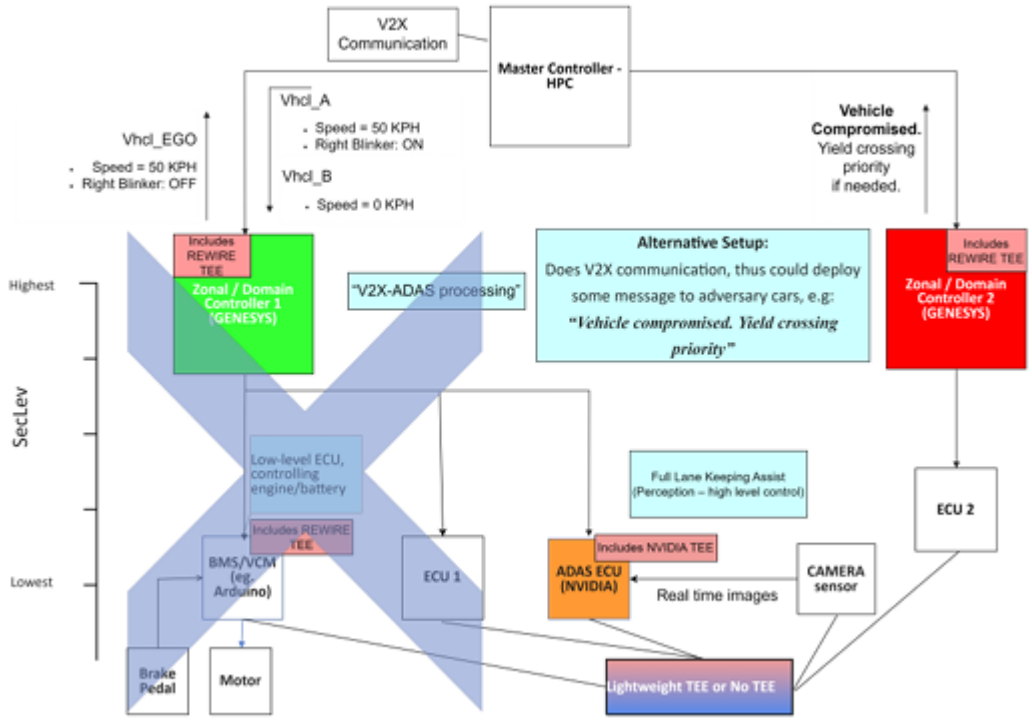


**Figure 4:** Exemplary vehicle network including automotive use case demo (example 2)

## 3 Conclusion

In conclusion, the evolution of automotive electrical/electronic (E/E) architectures from decentralized to centralized systems presents both opportunities and challenges. While centralized architectures offer benefits such as reduced network load and fewer ECUs, they also present security challenges. In particular, the potential compromise of a given ECU that manages numerous vehicle functionalities, underscores the necessity for robust fail-safe mechanisms and rollback measures.

This paper presented the innovative concept of "vehicle function migration" to alternative ECUs as a means to ensure the continual operation of critical functions. By leveraging REWIRE's functionalities, this approach enhances the overall reliability, robustness, and security of the vehicle's E/E architecture.

## References

[1] V. Bandur, G. Selim, V. Pantelic and M. Lawford, "Making the case for centralized automotive E/E architectures," pp. 1230-1245, 2021.

[2] "REWIRE_D2.1-REWIRE-Operational-landscape-requirements-and-Reference Architecture-Initial-Version-V1.0," [Online]. Available: https://www.rewire-he.eu/wp content/uploads/2024/01/REWIRE_D2.1-REWIRE-Operational-landscape-requirements-and Reference-Architecture-Initial-Version-V1.0.pdf.

[3] "E/E architectures: Optimize their development for automotive projects," [Online]. Available: https://www.techdesignforums.com/blog/2021/11/17/balancing-the-requirements-of-e-e-

architectures-for-automotive-design/

[4] Wikipedia, "Trusted Execution Environment," [Online]. Available: https://en.wikipedia.org/wiki/Trusted_execution_environment.

[5] V. M. Navale, K. Williams, A. Lagospiris, M. Schaffert and M.-A. Schweiker, ""(R)evolution of E/E architectures," SAE International Journal of Passenger Cars-Electronic and Electrical Systems, vol. 8, no. 2, p. 282–288, 2015.