CHIPLET-POWERED JLR

A Chiplet Revolution in the Automotive Industry

Team Name: **Team 69**

Date of Sub: **December 12, 2023**

Index

For Going to the Mid Submission Click the Link

1 Market Findings

1.1 Parts of the complete chiplet architecture/package

1. Lost Communication

   - **Available Components:** Bluetooth Module, WiFi Module, LoRA Module, 3G Data Transfer Module.
   - **Innovation Required:** Integration of all communication modules on an interposer, creating a comprehensive package. Additionally, a specialized module connecting to the IoT node for cloud communication needs to be developed.
   - **Recommendation:** Design the integrated communication module package in-house to ensure seamless compatibility and optimal performance. The cloud communication module should be sourced from reputable suppliers, ensuring reliable connectivity.

2. Battery Management System (BMS)

   - **Available Components:** Battery measuring devices are available, but conversion of analog signals to digital signals is required for centralized decision-making.
   - **Innovation Required:** Integration of chiplets with separate battery measuring devices, processing and providing data to the central chiplet. Development of a reserve chiplet for redundancy and replacing worn-out chiplets.
   - **Recommendation:** Design the integration of chiplets and battery measuring devices in-house to ensure compatibility and efficiency. Evaluate existing digital-analog converters in the market for potential off-the-shelf adoption.

3. Accidental Emergency

   - **Available Components:** None (Entirely Innovative Solution).
   - **Innovation Required:** Development of chiplets for various parts of the car, connected to a central chiplet analyzing signals for cumulative decision-making. Cloud communication for real-time updates on the vehicle's condition. Integration with Lost Communication Module for emergency contact.
   - **Recommendation:** Design and manufacture all chiplets in-house to create a proprietary solution differentiating JLR from competitors. Invest in advanced signal analysis algorithms for robust decision-making.

4. Software Over the Air (SOTA)

   - **Available Components:** High-performance CPUs and GPUs,AI accelerators, Vision processors,High-bandwidth memory,Sensor suite, High-speed communication interfaces, Automotive-grade chiplet packaging, Real-time operating systems (RTOS)
   - **Innovation Required:** Advanced interconnect technology,Specialized chiplets for specific tasks,AI hardware co-design,Sensor fusion advancements,Power-efficient designs .

- **Recommendation:** Secure boot, data encryption, and secure communication protocols are essential for protecting sensitive data in connected vehicles also since ADAS systems require high levels of functional safety and fault tolerance , Choose components and software platforms certified for automotive use and consider using open standards and platforms to ensure interoperability with future technologies and avoid vendor lock-in.

5. Kalman Filters over Chiplet

   - **Available Components:** The necessary sensors like LIDAR, Camera, IR Distance measurement etc. FPGA implementation of Kalman filter has been done. Scheduling algorithms available for Short term scheduling.
   - **Innovation Required:** Implementation of Kalman filter through chiplet and integration of said filter with its varying application like trajectory tracking through the use of sensors, Battery tracking on the BMS using extended Kalman filters, and sensor fusion to name a few.
   - **Recommendation:** In-house manufacturing of chiplets will result in a proprietary solution and thus JLR could make greater profits by maintaining exclusive control over the make and model of sensors the consumers can use.

1.2 Differentiation Strategy for JLR:

To differentiate itself from other OEMs, JLR should focus on the following strategies:

- **In-House Design and Integration:** Develop and integrate critical components, such as the communication module for Lost Communication and battery measuring devices for BMS, in-house to ensure seamless compatibility and superior performance.
- **Proprietary Solutions:** Innovate and manufacture proprietary chiplets for Accidental Emergency, offering a unique and advanced solution for real-time vehicle health monitoring and emergency response.
- **Advanced Signal Analysis:** Invest in sophisticated signal analysis algorithms for the Accidental Emergency solution, ensuring accurate decision-making and proactive communication with emergency services.
- **Redundancy and Reliability:** Implement redundancy features, such as reserve chiplets in BMS, to enhance the reliability of IoT solutions, showcasing JLR's commitment to user safety and vehicle longevity.

By combining in-house design, proprietary solutions, advanced technologies, and a commitment to reliability, JLR can position itself as an industry leader in IoT-based vehicle management and safety systems.

2 Micro-architecture diagrams

2.1 General Processor Architecture

Before we go into detailed architecture, we will look into the architecture of a processor

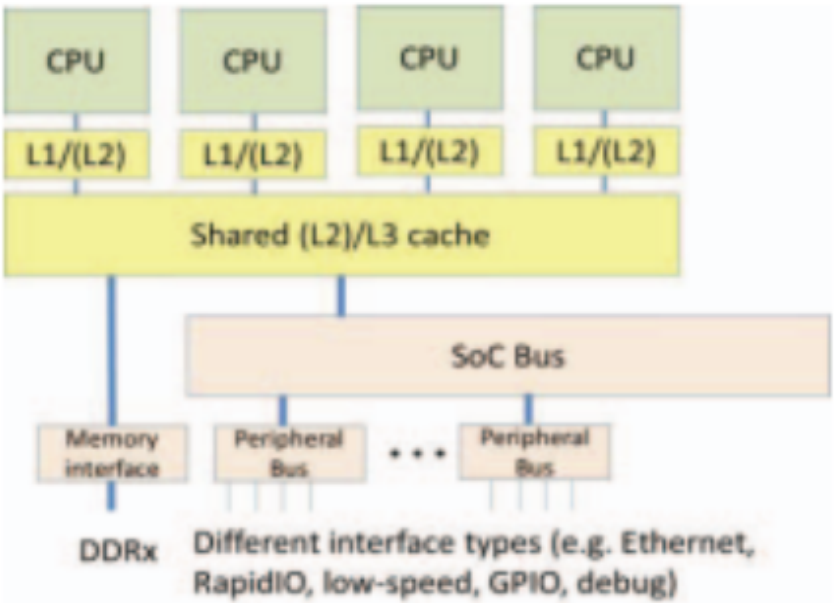


Figure 1

This is a quad-core structure as a SoC. This is connected to (L1) cache.
What are these levels of cache?
L1 cache
The fastest but smallest cache for data and instructions. It's also called the primary cache.
L2 cache
Slower, but bigger, cache for data only. It's also called the secondary cache.
L3 cache
The slowest but biggest cache for data only.
All of this is controlled by a high-performance dedicated bus.

This is for quad-core, and we can have a similar architecture for n-core. They will all have a common bus. As shown in the figure. We can convert this to a chiplet base approach. A shared cache is not required in a chiplet base approach. What we do is basically we have a primitive building block, one better in terms of economics ie a larger area.

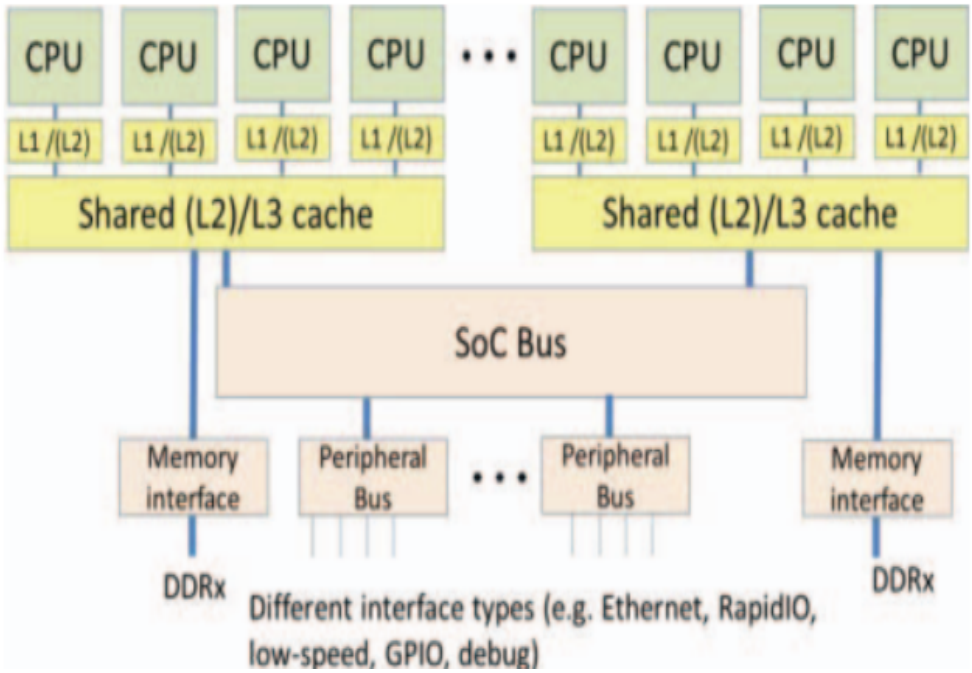
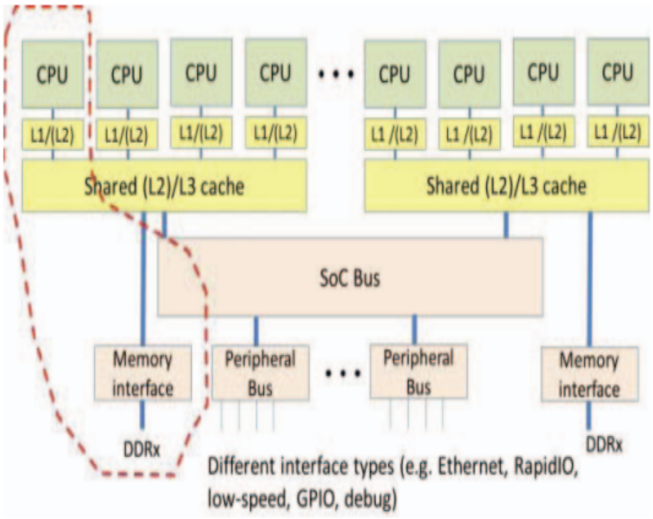
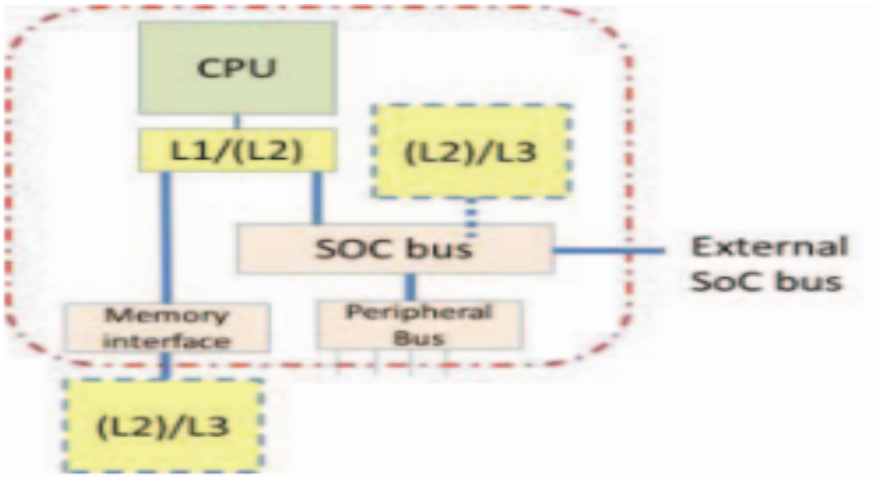

CPU
CPU
CPU
CPU
CPU
CPU
CPU
CPU
L1 /(L2)
L1 /(L2)
L1 /(L2)
L1 /(L2)
L1 /(L2)
L1 /(L2)
L1 /(L2)
L1 /(L2)
Shared (L2)/L3 cache
Shared (L2)/L3 cache
SoC Bus
Memory interface
Peripheral Bus
Peripheral Bus
Memory interface
DDRx
DDRx
Different interface types (e.g. Ethernet, RapidIO, low-speed, GPIO, debug)

Figure 2


CPU
CPU
CPU
CPU
CPU
CPU
CPU
CPU
L1/(L2)
L1/(L2)
L1/(L2)
L1/(L2)
L1 /(L2)
L1 /(L2)
L1 /(L2)
L1 /(L2)
Shared (L2)/L3 cache
Shared (L2)/L3 cache
SoC Bus
Memory interface
Peripheral Bus
Peripheral Bus
Memory interface
DDRx
DDRx
Different interface types (e.g. Ethernet, RapidIO, low-speed, GPIO, debug)


CPU
L1/(L2)
(L2)/L3
SOC bus
External SoC bus
Memory interface
Peripheral Bus
(L2)/L3

(b)

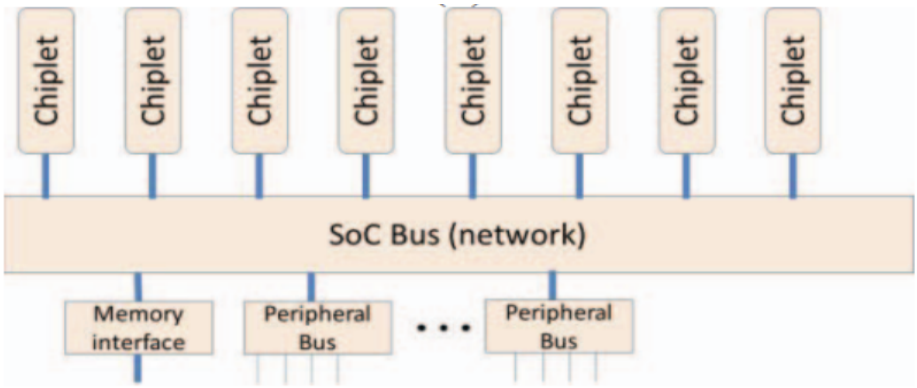


Figure 3. SoC decomposition. (a) Focal partition (in red). (b) Reduced complexity chiplet core (single core version) (c) Reformulation of SoC from chiplets.

Figure 3

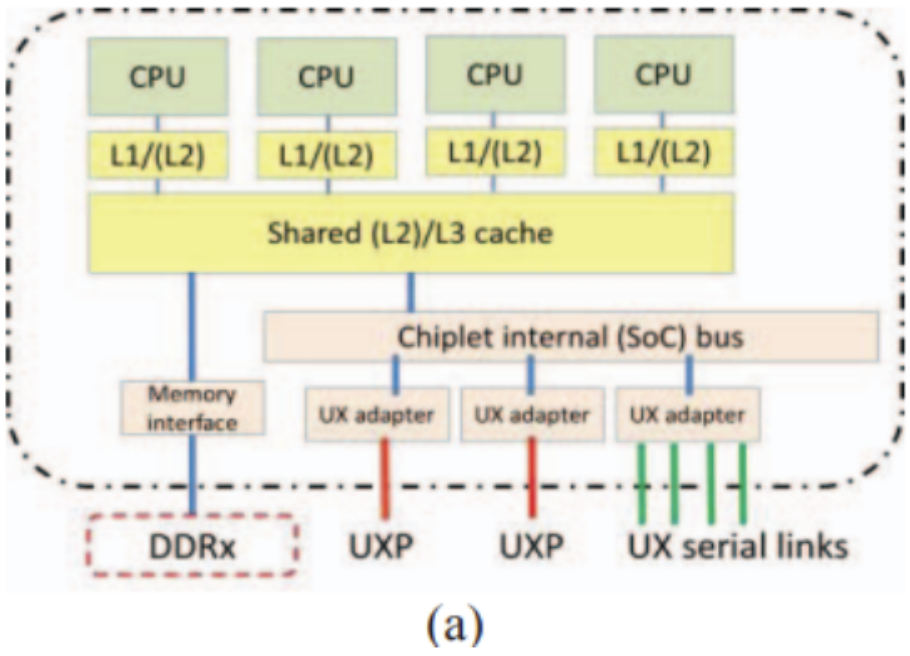
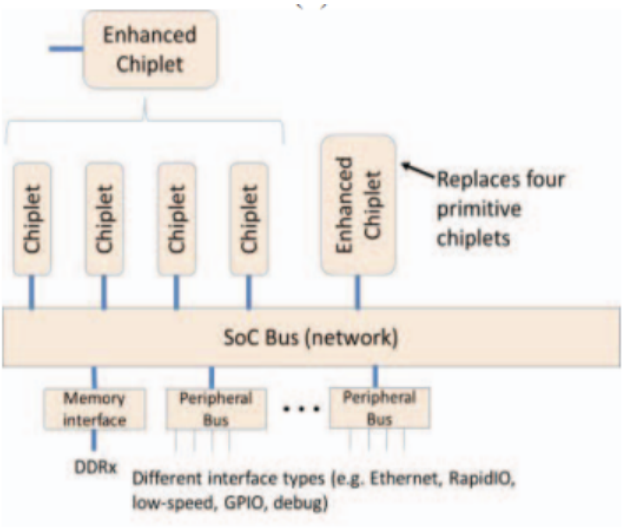


Figure 4

Packaging of chiplet processors:- To enhance bandwidth/coupling, the optimal diagonal links can be used. In Multichip module(MCM) we need a high-density interconnect medium. The MCM can operate at a much higher bisection bandwidth.

Bisection bandwidth gives the true bandwidth available in the entire system. Bisection bandwidth accounts for the bottleneck bandwidth of the entire network. Therefore, bisection bandwidth represents the bandwidth characteristics of the network better than any other metric.



(b)

Figure 5. Multicore chiplet. (a) Quad-core embodiment. (b) Replacing more primitive chiplets.

Figure 5

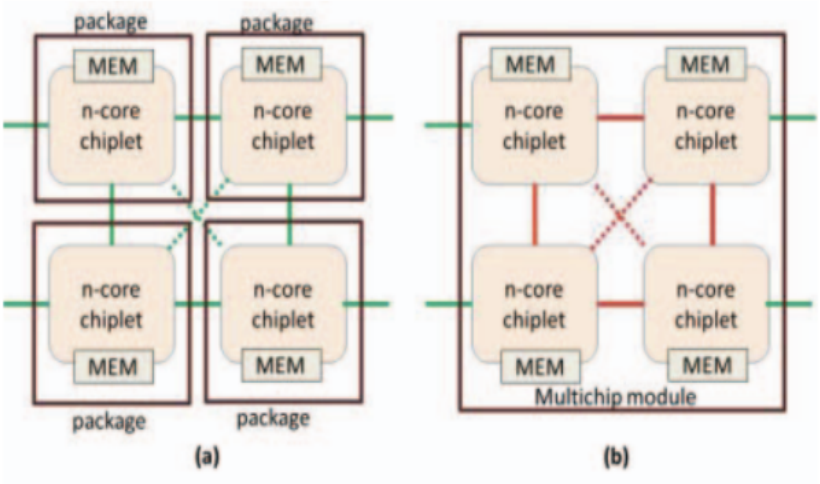
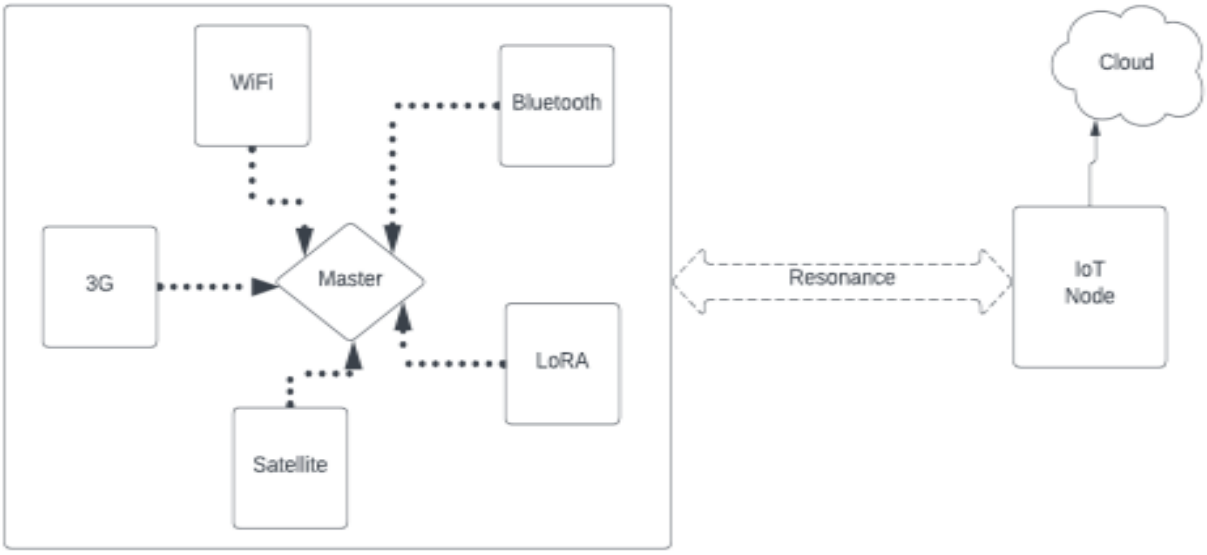


Figure 6. Alternate packaging embodiments. (a) Based on single-chip packages. (b) Based on tightly coupled multichip module packages.

Figure 6

2.2 Lost Communication Emergency(Communication in remote area)



We will now look at how each of these sub-parts is implemented. Each of these sub-parts can be made its own chiplet, or we can even make a chiplet out of wifi module, Bluetooth, 3/4G module so on.

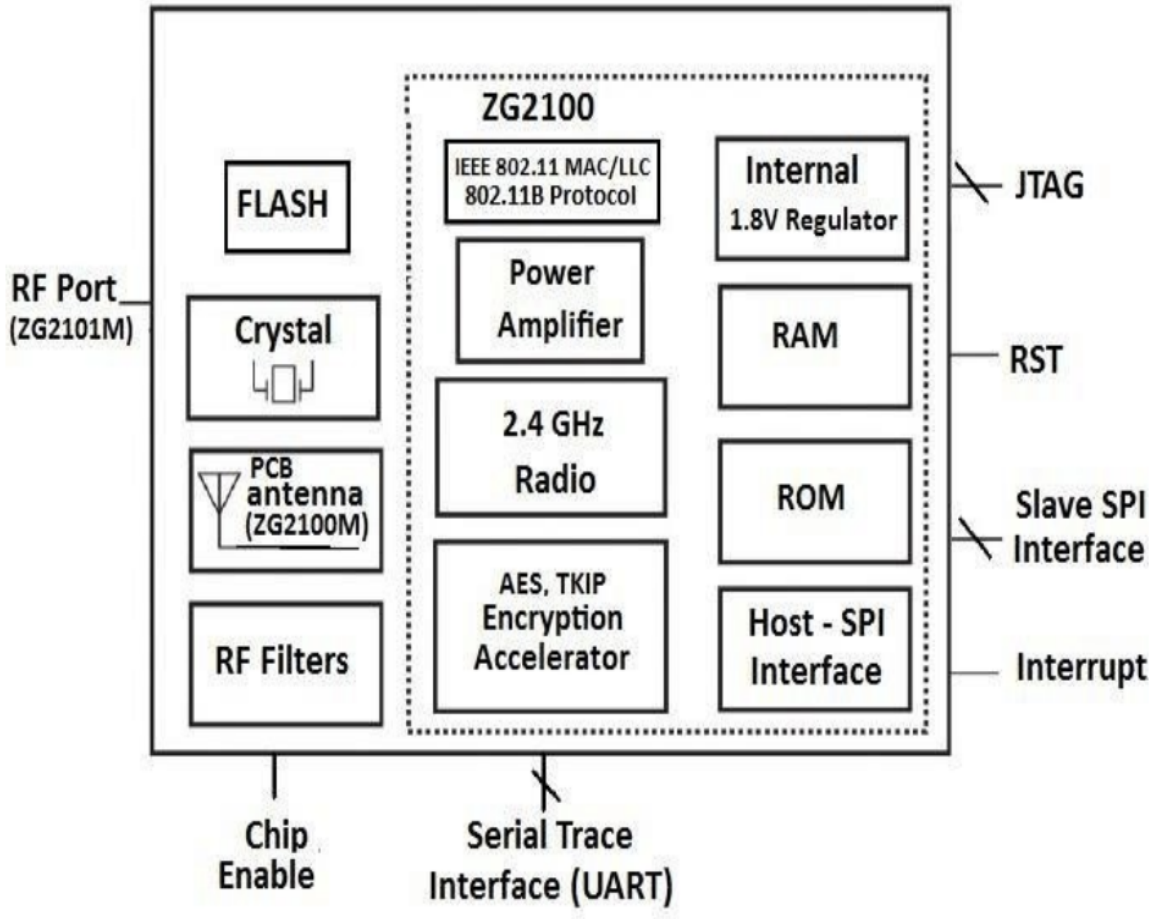


Figure 7: Wifi module

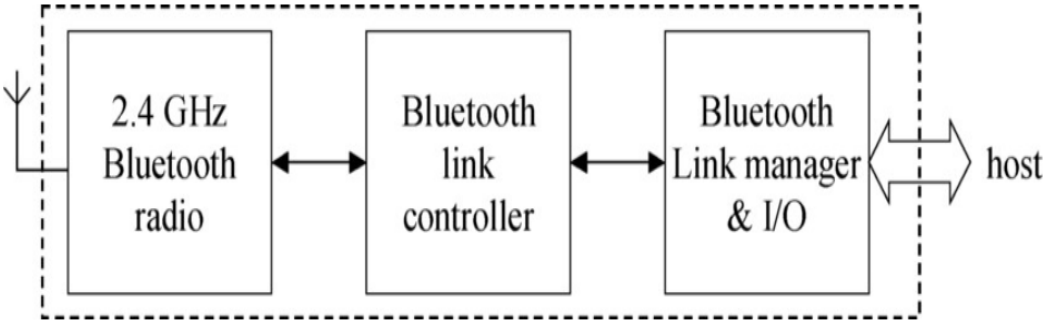


Figure 8: Bluetooth Module

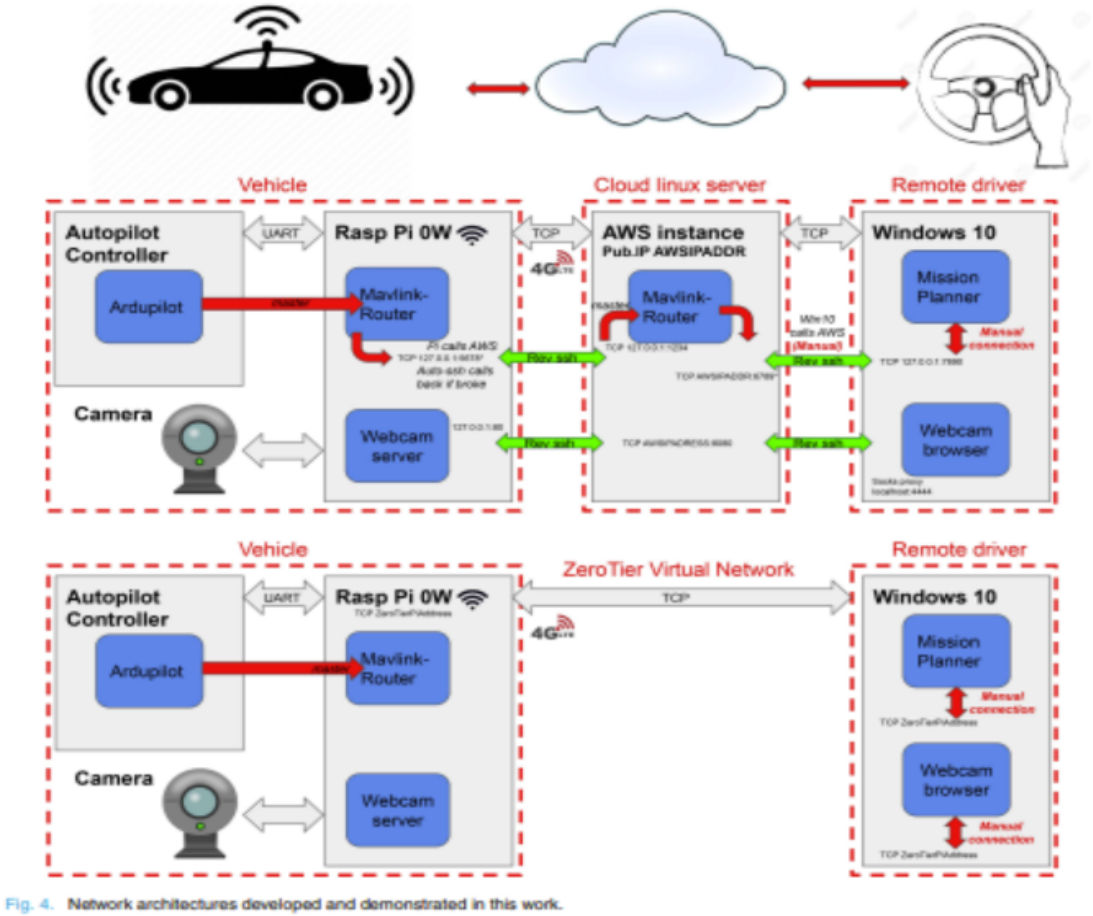


Fig. 4. Network architectures developed and demonstrated in this work.

Figure 9: A 4G-Connected Micro-Rover

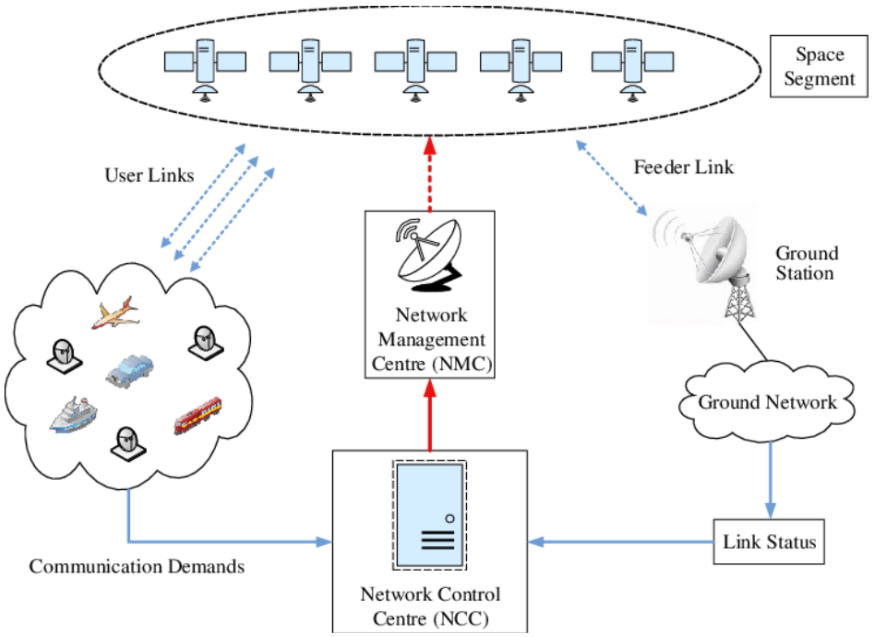


Figure 10: Diagram of a satellite communication system architecture

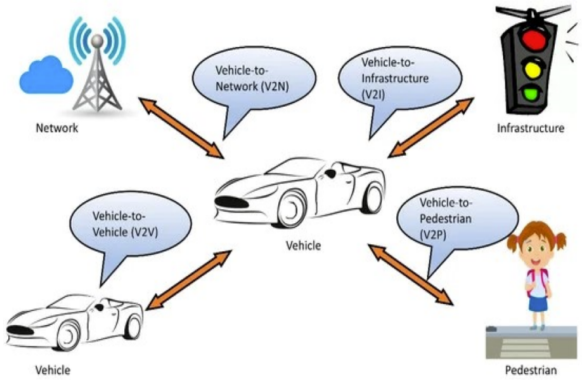
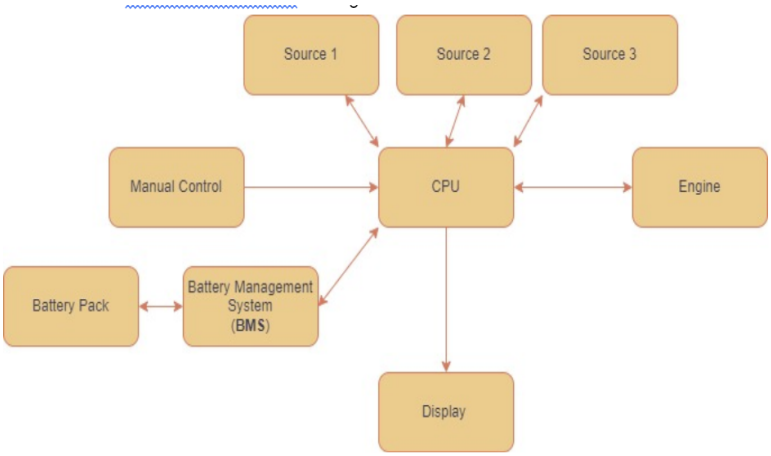


Figure 11: LoRA

2.3 BMS and other sources of simultaneous management



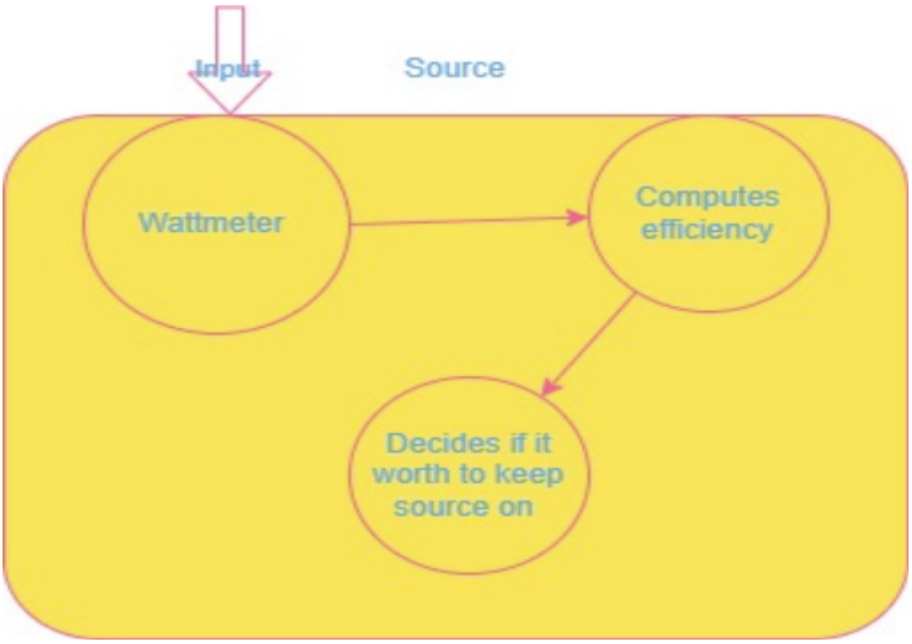


Figure 12: The architecture inside each source chiplet

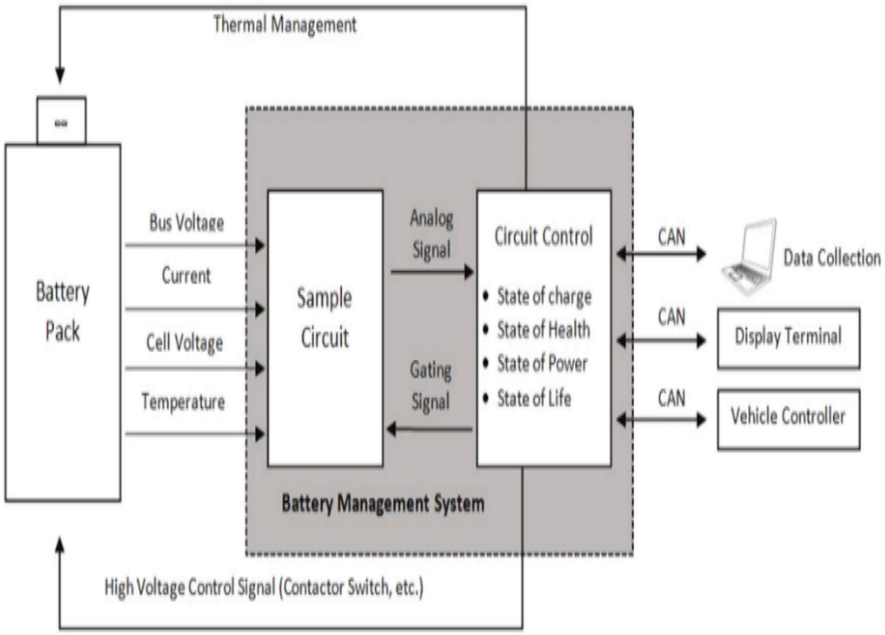


Figure 13: The structure inside BMS

We are not going into detail on how BMS works for that, we refer the reader to [2] in our references. They have got in a great deal of depth in explaining how the BMS actually works.

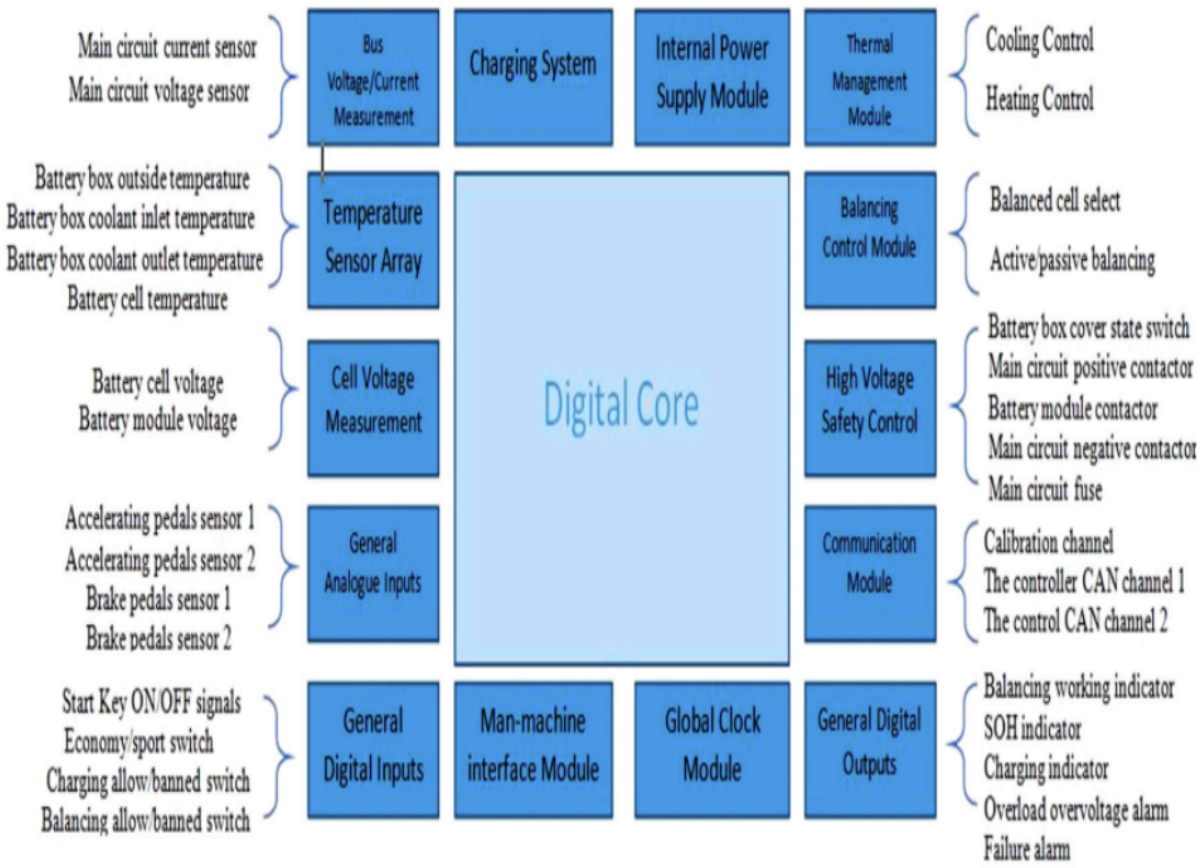

Main circuit current sensor
Main circuit voltage sensor
Bus Voltage/Current Measurement
Charging System
Internal Power Supply Module
Thermal Management Module
Cooling Control
Heating Control
Battery box outside temperature
Battery box coolant inlet temperature
Battery box coolant outlet temperature
Battery cell temperature
Temperature Sensor Array
Digital Core
Balancing Control Module
Balanced cell select
Active/passive balancing
Battery cell voltage
Battery module voltage
Cell Voltage Measurement
High Voltage Safety Control
Battery box cover state switch
Main circuit positive contactor
Battery module contactor
Main circuit negative contactor
Main circuit fuse
Accelerating pedals sensor 1
Accelerating pedals sensor 2
Brake pedals sensor 1
Brake pedals sensor 2
General Analogue Inputs
Communication Module
Calibration channel
The controller CAN channel 1
The control CAN channel 2
Start Key ON/OFF signals
Economy/sport switch
Charging allow/banned switch
Balancing allow/banned switch
General Digital Inputs
Man-machine interface Module
Global Clock Module
General Digital Outputs
Balancing working indicator
SOH indicator
Charging indicator
Overload overvoltage alarm
Failure alarm

Figure 14

2.4 Accident Emergency

There will be a few types of sensors:-

- Pressure sensors
- Vibration sensors
- Driver condition sensor

We will use only a few sensors for representation purposes, but the number of sensors used in the actual application should be higher.
Short forms used in diagram.
PS - Pressure sensors,
VS - Vibration sensors
DC - Driver condition sensor

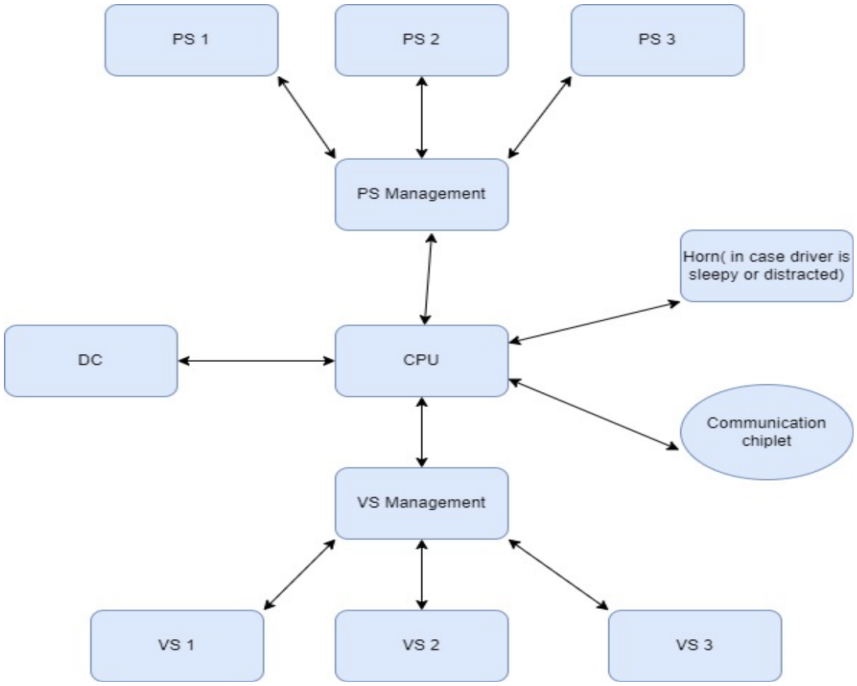


Figure 15

The simple logic is once we calibrate the sensors, we will be able to detect and alert the appropriate authorities as soon as possible, ensuring the safety of our passengers.

Now there are many off-the-shelf products for this, but we would suggest, based on crash test data the company design its own sensors with appropriate sensitivity.

2.5 Kalman Filter

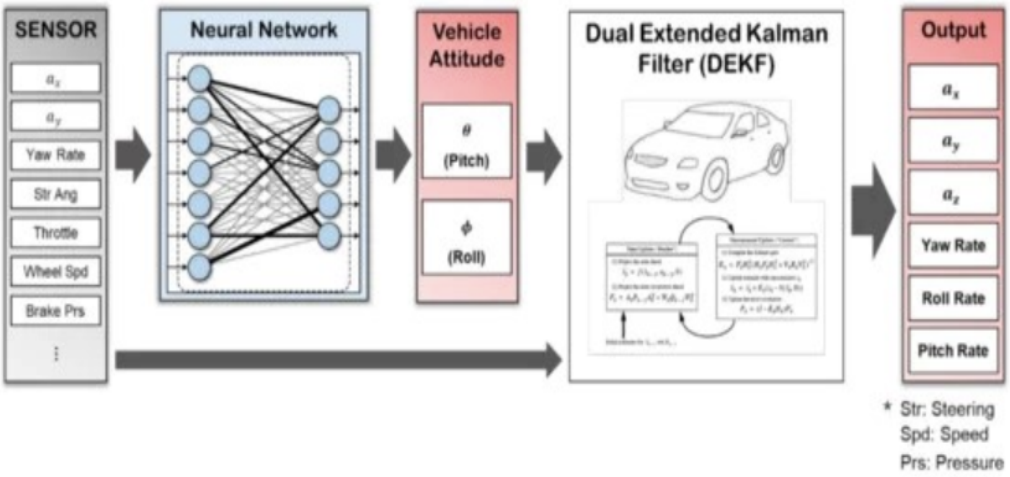


Figure 16: Kalman Filter

The following GitHub link contains the C++ code of Kalman filter.
Git hub :-
https://github.com/hmartiro/kalman-cpp/commit/8e0553ea0d2441c429281beb0010ff1ab3840b3e

We will now show a block diagram of the Kalman filter.

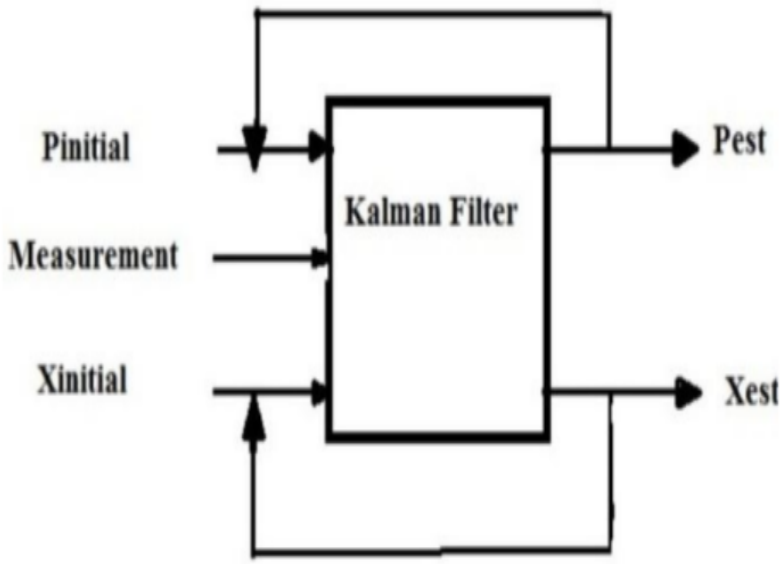


Figure 17: Basic block diagram of Kalman filter

Pinitial is the predicted variance
Xinitial is the predicted state
Pest is the estimated variance
Xest is the estimated state

The basic equation of Kalman filter is as follows:-

$$x(k+1) = Ax(k) + Bu(k) + w(k) \tag{1}$$

This equation shows the prediction state for the time (k+1) where A is the state transition matrix, B is the input transition matrix, u(k) is the uncontrolled vector which is taken zero for the simplification, w(k) is the process additive noise

This type of equations are commonly used in control systems,

$$Y(k+1) = Cx(k+1) + v(k+1) \tag{2}$$

, This is the measurement equation where C is the observation matrix, v (k+1) is the measurement additive noise

$$X(k+1) = x(k+1) + K(k+1)[Y(k+1) – x(k+1)] \tag{3}$$

This equation shows the corrected estimated output

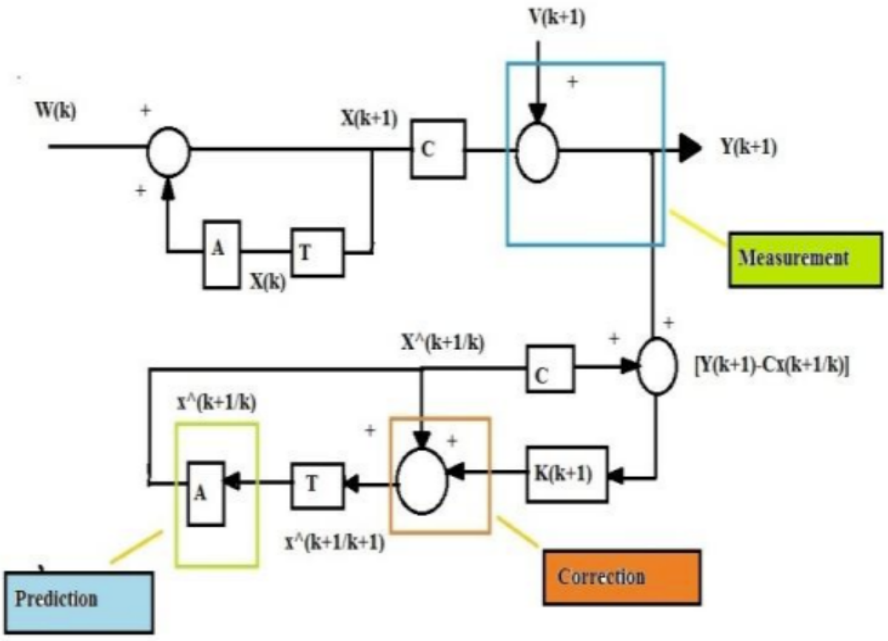


Figure 18

Architecture hardware design approach of Kalman filter implementation on FPGA board is shown below.

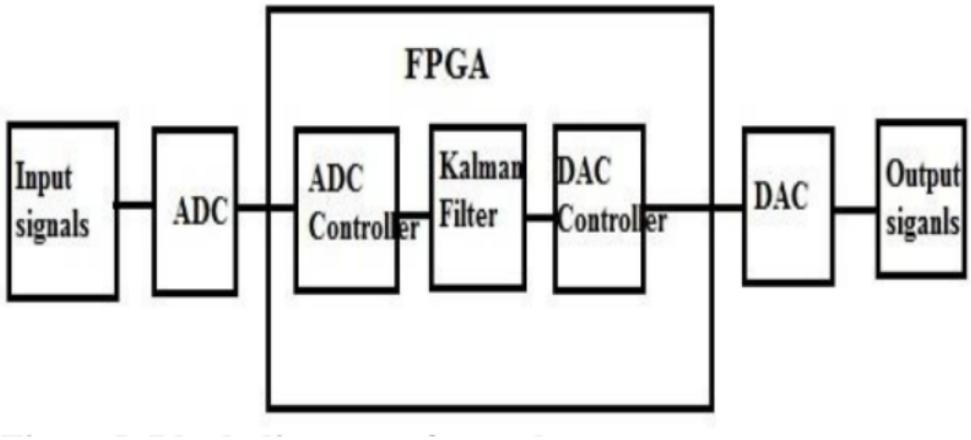


Figure 19: ADAS

2.6 Advanced driver assistance systems (ADAS)

For detailed explanations, please refer to [5] in references.

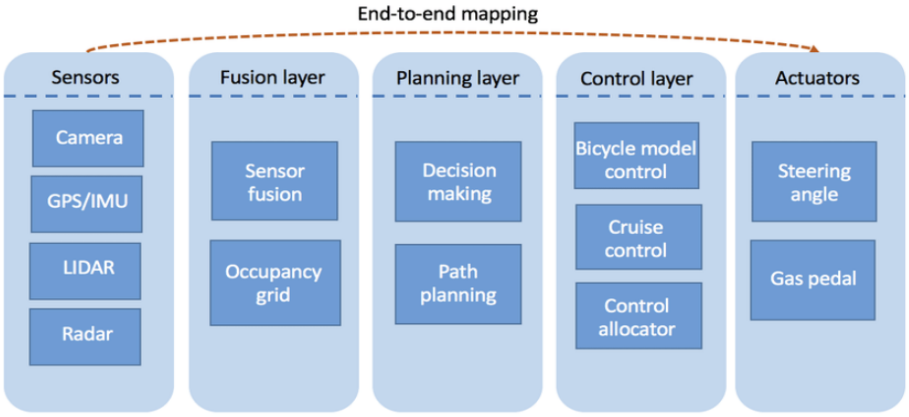
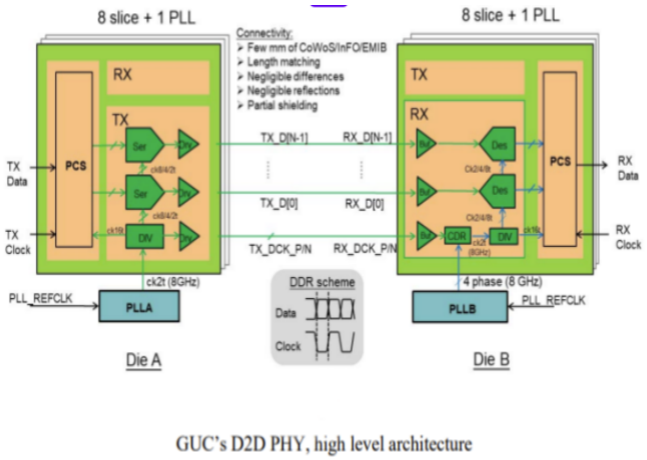


Figure 20



GUC's D2D PHY, high level architecture

Figure 21

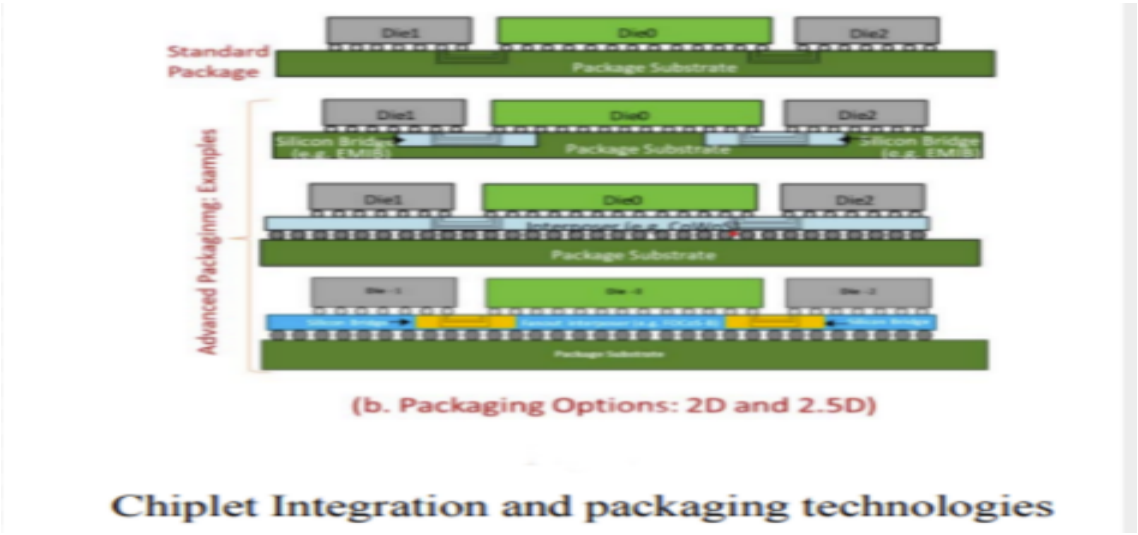


Figure 22

As research shows, we can implement ML models using chiplets[6][7].
YOLO can be implemented, so we can train a new model according to the needs.

3 Interconnect Technologies

3.1 Battery Management Systems (BMS)

Controller Area Network (CAN FD (Flexible Data-rate)) can be used as Interconnect Technology in BMS since:

- Chiplet Architecture:
  - BMS chiplets, as part of a distributed architecture, communicate with each other and with the Master BMS using the CAN bus.
  - The chiplet design allows for scalability, enabling the addition or removal of chiplets without disrupting the overall communication infrastructure.
- CAN FD support a higher data rate compared to traditional CAN. In the context of BMS, where monitoring and managing numerous parameters of the battery is crucial, the higher data rate of CAN FD allows for faster and more efficient communication. This is particularly beneficial when dealing with large sets of data such as voltage, current, and temperature measurements from multiple battery cells.
- BMS involves continuous monitoring of various parameters across multiple cells within a battery pack. CAN FD's increased bandwidth facilitates the transmission of a greater volume of data in a given time frame. This is advantageous for BMS applications, where real-time data from various sensors and modules need to be collected and analyzed promptly.
- CAN FD optimizes data transmission efficiency by allowing larger data payloads per frame. In BMS, where information such as cell voltages and temperatures needs to be transmitted, the

ability to send more data in a single frame reduces the overall communication overhead and enhances the system's efficiency.

- BMS systems often need to scale to accommodate different battery pack configurations, from small-scale applications to large electric vehicles. CAN FD's scalability allows it to adapt to varying system sizes, making it suitable for diverse BMS implementations.
- CAN FD offers low-latency communication, vital in BMS applications for real-time monitoring and response. Quick communication between battery cells and the central management unit supports timely decision-making, contributing to the overall safety and performance of the battery system.
- CAN FD maintain the robust error-detection and fault-tolerant features of traditional CAN. In BMS applications, where the accuracy of data is critical, the ability to detect and manage errors ensures the reliability of the information being transmitted. This is particularly important for maintaining the health and safety of the battery.

3.1.1 Latency:

- CAN is known for its deterministic communication, meaning it provides a predictable and consistent latency in transmitting messages. In the context of Battery Management Systems (BMS), this is crucial for real-time monitoring and control of the battery.
- Low to moderate latency in CAN enables the BMS to receive and process real-time data from individual battery cells or modules. This is vital for timely decision-making, especially in situations requiring rapid adjustments to battery charging, discharging, or balancing.
- The deterministic nature of CAN allows the BMS to quickly detect faults or anomalies within the battery system. In case of issues, the BMS can respond promptly to mitigate potential risks, ensuring the safety and health of the battery.

3.1.2 BMS Communication Efficiency:

- CAN's efficiency in terms of bandwidth utilization is particularly advantageous for BMS. The protocol optimally uses the available bandwidth to transmit essential data, such as voltage, current, and temperature readings from various battery components.
- CAN employ a robust error-checking mechanism, ensuring the integrity of data transmitted between the BMS and individual battery modules. This is critical in maintaining accurate information for effective battery management.
- Automotive environments can be electrically noisy due to various components and systems. CAN's robustness in the presence of electrical noise ensures that communication remains reliable, and the BMS can receive accurate data even in challenging conditions.

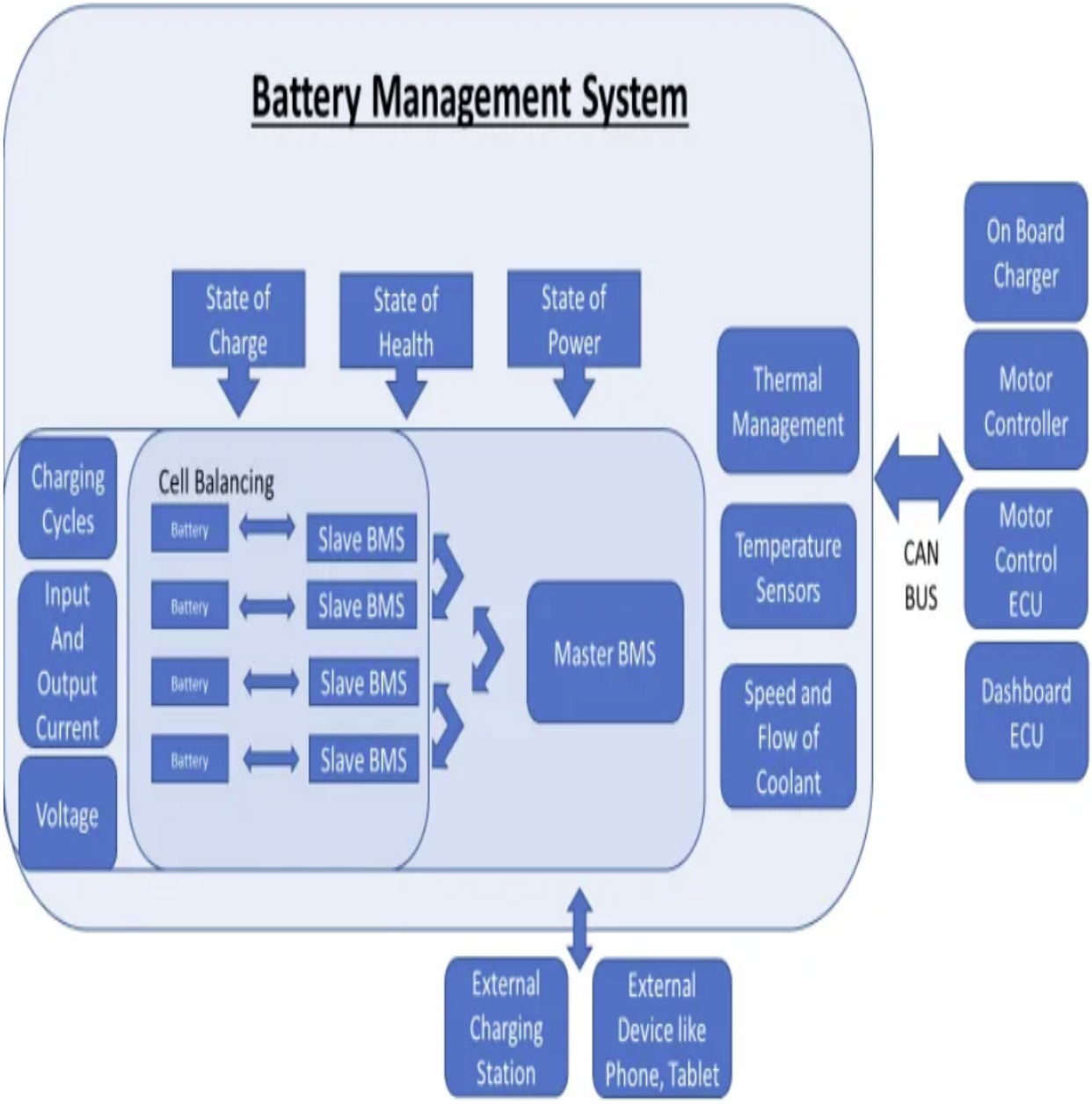


Figure 23: BMS

3.2 Lost Communication Emergency (Communication in remote areas):

V2X (Vehicle-to-Everything) Communication can be used as Interconnect Technology in Lost Communication Emergency since:

- In emergency situations, time is of the essence. V2X communication ensures that messages related to critical events, such as accidents or road closures, can be transmitted with minimal delay. This low-latency feature allows for quick responses, improving the overall effectiveness of emergency services.
- V2X operates on a decentralized model, meaning that vehicles can communicate directly with each other without relying heavily on centralized infrastructure like cell towers. In remote areas

where such infrastructure might be scarce, V2X's self-sufficiency becomes crucial. Vehicles act as both transmitters and receivers, creating a dynamic and responsive communication network.

- V2X enables real-time communication between vehicles and infrastructure, providing instant updates on road conditions, traffic, and potential hazards. This real-time information exchange enhances situational awareness, allowing all connected entities to make informed decisions promptly.

- Remote areas often present diverse challenges, such as rough terrains or unpredictable weather conditions. V2X communication allows vehicles to share information about these challenges, promoting adaptability. For example, if one vehicle encounters a road obstruction, it can relay this information to others, enabling them to adjust their routes accordingly.

- V2X introduces redundancy by allowing multiple vehicles to serve as nodes in the communication network. If one vehicle loses connectivity, others can still relay critical information. This redundancy enhances reliability, ensuring that emergency messages reach their intended recipients even in the face of disruptions.

- V2X empowers vehicles to make decentralized decisions based on real-time information. In emergency scenarios, conditions can change rapidly. V2X allows vehicles to adjust their routes, speeds, or other parameters autonomously in response to evolving situations, contributing to dynamic and effective decision-making.

- V2X optimizes resource utilization by enabling direct communication between vehicles. Rather than constantly relying on a central hub for communication, vehicles can exchange information directly. This reduces the strain on network resources, conserving energy and bandwidth, which is especially valuable in remote areas with limited resources.

- LTE-V2X, another communication technology for V2X services, offers a more stable latency, with communication delay via the PC5 interface consistently below 100 ms. Looking ahead, the advent of 5G networks is expected to revolutionize V2X communication, providing delays of less than 1 ms and ensuring a remarkable stability level of 99.999% . This technological advancement positions 5G networks as robust supporters of V2X services, particularly beneficial in emergency scenarios where reliable and low-latency communication is imperative.

3.2.1 Latency:

V2X communication prioritizes low latency, especially in emergency situations. This emphasis on minimal delay is crucial for enabling rapid and effective communication between vehicles and infrastructure. The goal is to reduce the time it takes for critical information to be transmitted and received, allowing for quick response and decision-making. Standardization efforts, such as those reflected in IEEE 802.11p, play a key role in defining protocols and technologies that focus on minimizing communication delays. By achieving low latency, V2X contributes to enhancing overall safety and responsiveness in emergency scenarios.

3.2.2 Communication efficiency:

V2X is specifically designed to ensure efficient communication, particularly in remote areas where connectivity challenges may exist. The emphasis on efficiency goes beyond mere data transmission and includes aspects such as optimizing the use of available bandwidth, minimizing energy consumption, and enhancing the reliability of connectivity. In the context of vehicular ad-hoc networks (VANETs), research, such as that conducted by F. Dressler et al. in 2015, underscores the importance of V2X communication efficiency. Efficient communication in remote areas is vital for maintaining reliable connectivity, facilitating seamless information exchange, and supporting applications like Lost Communication Emergency, where robust and swift communication can be critical in saving lives or preventing further harm.

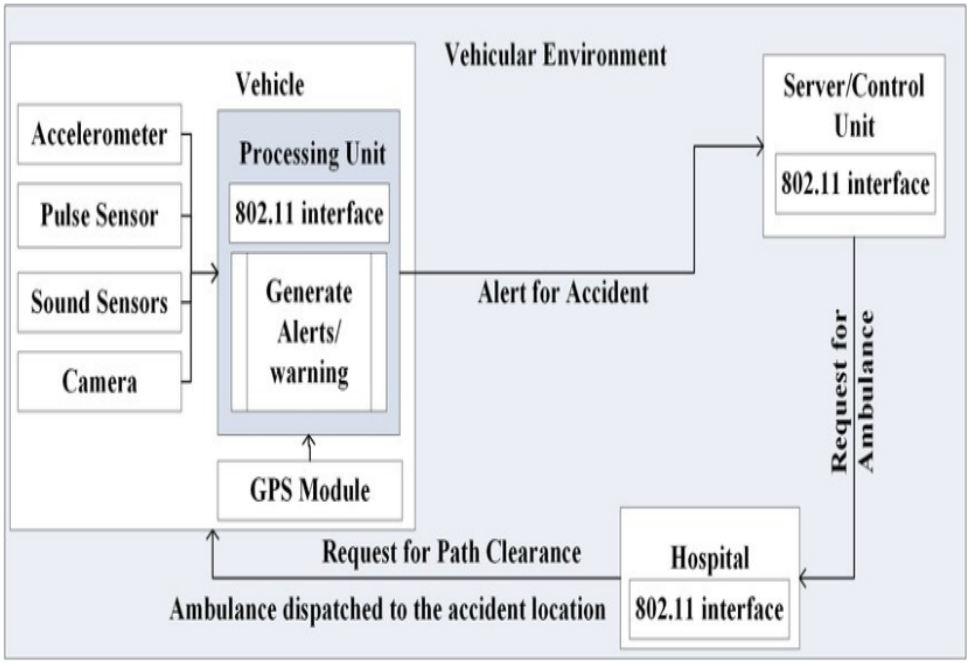


Figure 24

Some types of testing are carried out to improve latency, communication efficiency, and security:

- Conformance Testing:
  - Protocol conformance is fundamental for V2X communication, ensuring interoperability. ETSI and 3GPP provide abstract test systems for V2X conformance testing using TTCN-3.
  - Challenges include the complexity of standards, the need for automated testing systems, and ensuring sufficient test cases.

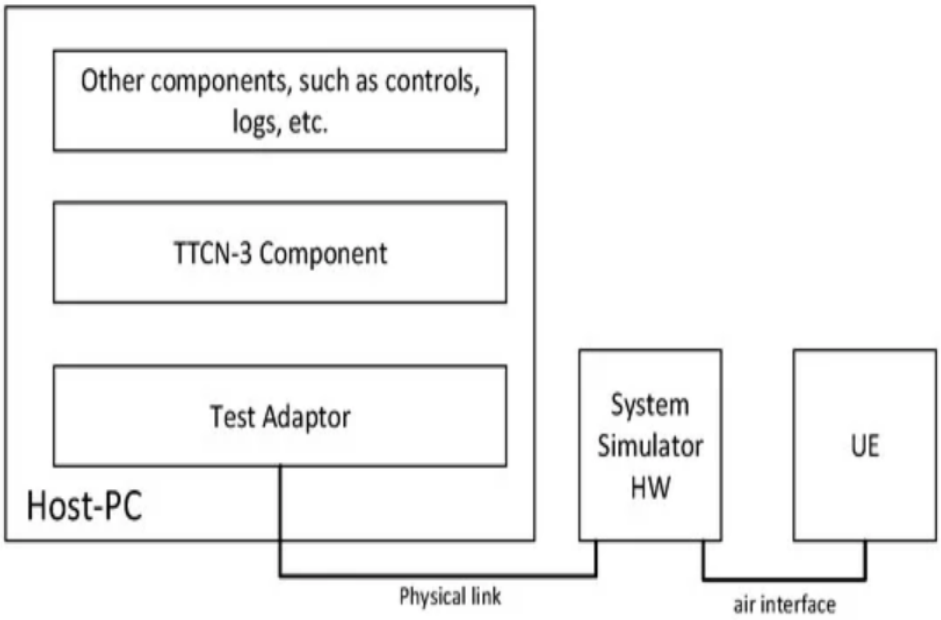


Figure 25

- Function Testing:
  - Application function testing assesses the triggering and response of V2X applications in different scenarios.

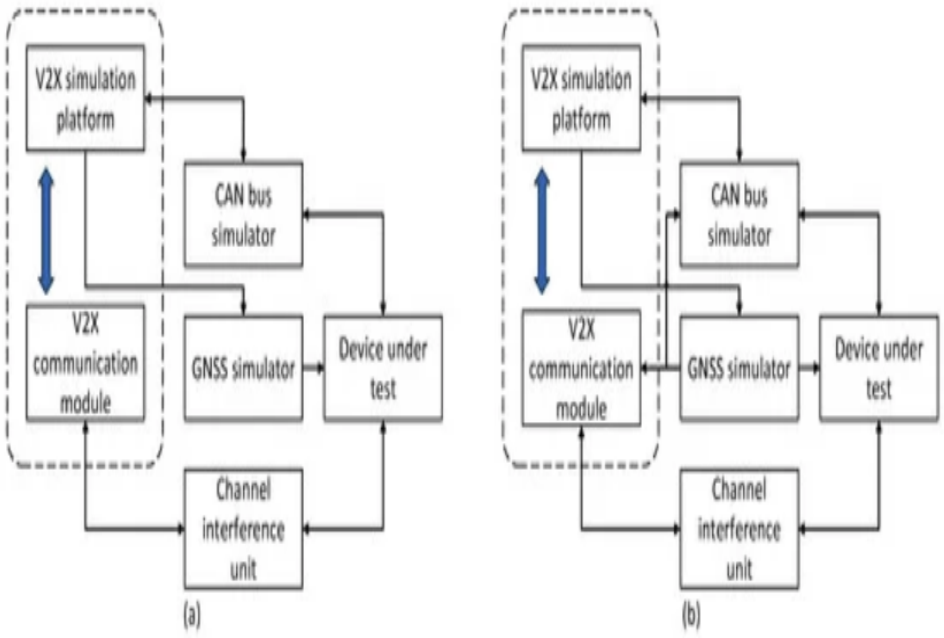


Figure 26

- Performance Testing:
  - Performance testing evaluates end-to-end communication delay, packet delivery success rate, and parameters like signal strength.

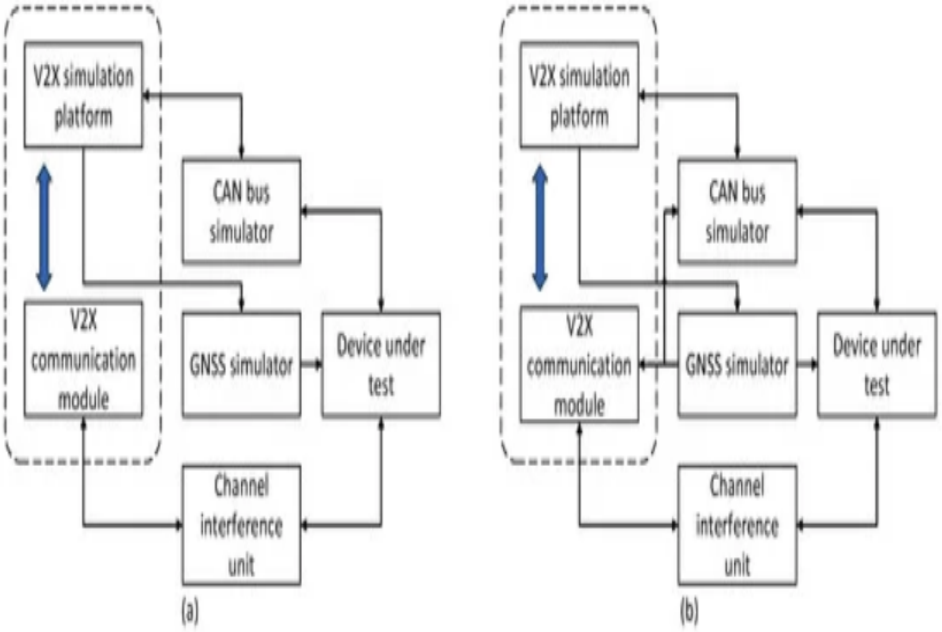


Figure 27

- Vehicle Gateway Testing:
  - Ensures the correct operation of vehicle gateways to meet V2X network security needs.
  - Test architecture involves the system under test and a test system, verifying expected results against actual results.

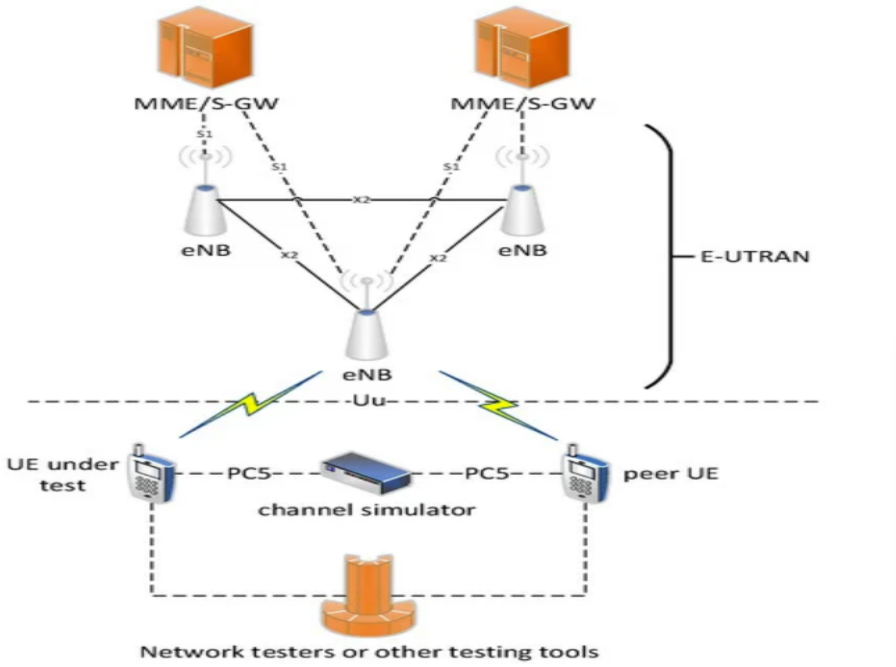


Figure 28

- Penetration Testing:
  - Simulates malicious attacks to test the security of V2X systems.

– Includes white box, black box, and gray box testing, focusing on identifying vulnerabilities and assessing their severity.

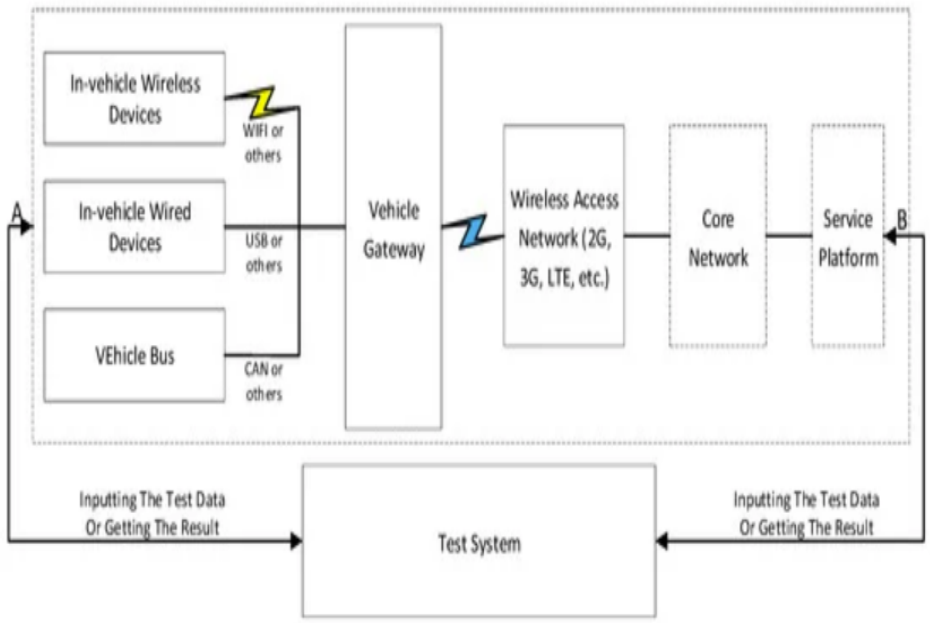


Figure 29

- Accelerated Testing:
  - Aims to reduce cost and time in vehicle reliability verification.
  - Challenges include building realistic models with real-world data and ensuring the validity of iterative data.
- Field Testing:
  - Essential for evaluating V2X applications in real-world environments.
  - Large-scale demonstrations, such as Safety Pilot Model Deployment, SCMS, and M-City, provide valuable insights.

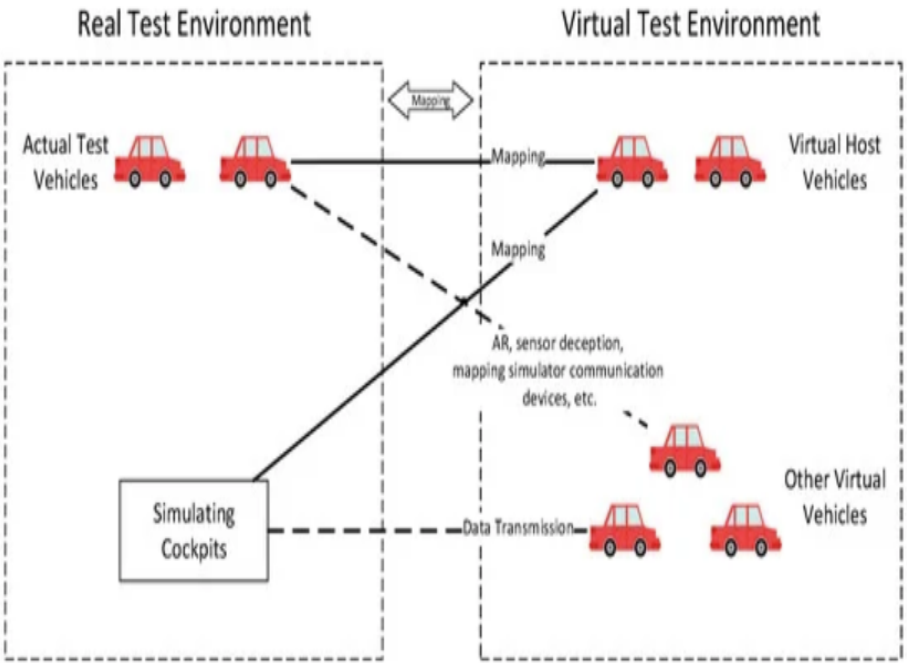


Figure 30

3.3 Accidental Emergency (Safety Feature) and Remote Diagnostics and Over-the-Air (OTA) Updates :

Ethernet with Time-Sensitive Networking (TSN) can be used as Interconnect Technology in Accidental Emergency and Remote Diagnostics and Over-the-Air (OTA) Updates since:

- TSN introduces mechanisms for deterministic communication, ensuring that critical messages are delivered with precise timing. This determinism is crucial in safety-critical applications, where the timing of communication events is essential for effective and reliable operation during emergencies.
- TSN minimizes communication latency by enabling time synchronization and scheduled communication. This is vital for safety features in Accidental Emergency situations, where rapid response times can be critical for preventing accidents or mitigating their impact.
- TSN allows for the reservation of bandwidth, ensuring that safety-critical messages have dedicated resources. This minimizes the risk of congestion and interference from non-essential traffic, contributing to improved communication efficiency.
- TSN supports different levels of Quality of Service, allowing prioritization of critical messages over less time-sensitive data. This prioritization ensures that safety-related information is given precedence, enhancing the efficiency and reliability of communication.
- TSN includes features for fault tolerance and redundancy, increasing the overall reliability of the communication network. This is crucial in emergency scenarios, where the robustness of the communication infrastructure can impact the effectiveness of safety features.

- TSN is an extension of standard Ethernet, making it compatible with existing Ethernet technologies. This compatibility facilitates integration into diverse systems and environments, providing a seamless upgrade path for applications that already rely on Ethernet.
- TSN is supported by industry standards, ensuring interoperability and widespread adoption. This makes it a reliable and well-supported choice for applications requiring high reliability and low latency, such as safety features in Accidental Emergency situations.
- In the context of Accidental Emergency scenarios, latency and communication efficiency are critical factors in ensuring the effectiveness of safety features. Let's explore how these aspects apply to the Interconnect Technology: Ethernet with Time-Sensitive Networking (TSN).

3.3.1 Latency:

- Accidental Emergency situations demand rapid response times. Ethernet with TSN is designed to meet stringent latency requirements, providing low and deterministic communication delays.
- TSN introduces mechanisms to support time-sensitive traffic, ensuring that safety-critical messages are prioritized and transmitted within specified time bounds.
- Precise time synchronization across network devices is a key aspect of TSN, enabling coordinated actions and reducing communication delays.
- TSN standards define deterministic latency, meaning that the time taken for a message to traverse the network is known and predictable. This predictability is crucial for safety-critical applications.
- TSN aims to minimize packet jitter, the variation in packet arrival times. Consistent and predictable communication patterns contribute to stable and reliable latency.

3.3.2 Communication Efficiency:

- Ethernet with TSN optimizes the use of network resources, ensuring that bandwidth is allocated efficiently. This is essential for delivering critical messages without unnecessary delays.
- TSN incorporates QoS mechanisms that allow the prioritization of traffic. Safety-critical data can be assigned higher priority, guaranteeing timely delivery and reducing the risk of congestion.
- TSN supports redundancy mechanisms, enhancing the reliability of communication. In safety-critical scenarios, having redundant paths and devices ensures continuous connectivity, even in the presence of failures.
- TSN enables the reservation of dedicated bandwidth for critical communication. This ensures that safety-related messages have the necessary resources, avoiding contention with less time-sensitive data.
- TSN standards define deterministic network behavior, allowing for precise control over communication parameters. This determinism contributes to the overall efficiency of the network.

- Ethernet with TSN can seamlessly integrate with existing Ethernet networks, providing a backward-compatible solution. This facilitates the adoption of TSN without requiring a complete overhaul of infrastructure.
- TSN standards are designed to coexist with legacy Ethernet systems, allowing for a gradual transition to time-sensitive capabilities. This compatibility ensures that investments in existing infrastructure are preserved.

To improve the communication efficiency and latency of Ethernet with Time-Sensitive Networking (TSN) in the context of Accidental Emergency scenarios, several strategies can be followed:

- We can design the network layout to minimize hops and potential congestion points, implementing redundant paths for enhanced fault tolerance.
- Using Quality of Service (QoS) settings, we can give priority to safety-critical data to ensure it takes precedence over non-essential information.
- By implementing protocols like Precision Time Protocol (PTP), we can achieve sub-microsecond synchronization accuracy across all network devices.
- We can reserve specific bandwidth for safety-critical messages, preventing congestion and guaranteeing timely delivery.
- Through the use of bandwidth shaping mechanisms, we can control data flow, allocating resources based on priority.
- Configuring QoS settings, we can grant higher priority access to critical messages, effectively reducing latency for emergency communications.
- We can optimize queuing mechanisms within switches and routers to minimize packet jitter and ensure consistent communication.
- Deploying traffic shaping, we can smooth data flow and minimize variations in packet arrival times.
- By introducing redundancy in critical components using protocols like Parallel Redundancy Protocol (PRP) or High-availability Seamless Redundancy (HSR), we can ensure seamless communication during failures.
- Regularly updating firmware and software on network devices, we can benefit from performance improvements and bug fixes. Devices will be configured with compatible and optimized TSN settings.
- By implementing monitoring tools, we can assess network performance continuously, analyzing data to identify optimization areas and fine-tuning settings.
- By staying engaged with standardization bodies and industry forums, we can adopt the latest TSN standards and contribute to the development of new standards addressing emerging challenges.

- By exploring advancements in hardware, protocols, and network architectures, we can enhance TSN capabilities. Consideration will be given to innovations like edge computing to reduce latency by offloading processing from central devices.

3.4 Kalman Filter:

High-speed serial Links (e.g., PCIe) can be used as Interconnect Technology in Kalman Filter applications since:

3.4.1 Latency:

- High-Speed Serial Links, particularly PCIe, are known for their low-latency characteristics. In the context of implementing Kalman Filters on chiplets for applications like ADAS systems, low latency is crucial for achieving real-time data processing.
- The efficient communication between chiplets facilitated by PCIe ensures minimal delays in transmitting and receiving data, contributing to the overall responsiveness of the system.
- The low-latency nature of PCIe enables rapid data exchange between chiplets, supporting real-time information processing by Kalman Filters.
- This is essential in scenarios where quick decision-making is critical, such as in ADAS applications, where timely and accurate data processing can prevent accidents and enhance safety.

3.4.2 Communication Efficiency:

- PCIe provides high bandwidth, allowing for efficient and rapid data transfer between chiplets. This high bandwidth is advantageous for applications like Kalman Filters, which require the seamless exchange of large volumes of data for processing.
- PCIe supports scalable configurations, enabling the integration of multiple chiplets in a system. This scalability aligns well with the parallel processing capabilities of chiplet technology, contributing to enhanced overall efficiency in the data processing.
- High-Speed Serial Links, including PCIe, come with robust error detection and handling mechanisms. This ensures reliable data transmission, preventing errors or data corruption during communication. The reliability of communication is crucial for the accurate functioning of Kalman Filters, which rely on precise data for their calculations.
- High-Speed Serial Links are known for their energy efficiency. The efficient exchange of data between chiplets through PCIe contributes to lower power consumption, aligning with the goal of energy-efficient systems.

To enhance the latency and communication efficiency in the context of implementing Kalman Filters on chiplet technology with High-Speed Serial Links (e.g., PCIe), several strategies can be followed:

- Fine-tuning the protocol stack of the High-Speed Serial Link to minimize overhead and streamline communication is something we can continually work on.
- Enhancing error detection and correction mechanisms to swiftly identify and address any transmission errors, thereby reducing the likelihood of retransmissions that could introduce latency, is an area we can improve.
- Effectively leveraging the parallel processing capabilities of chiplet technology by optimizing the distribution of computational tasks among chiplets is a strategy we can employ.
- Implementing mechanisms to dynamically scale the number of chiplets based on processing demands, ensuring efficient utilization of resources without compromising latency, is something we can incorporate.
- Implementing precise clock synchronization protocols to maintain accurate and consistent timing across chiplets, thereby minimizing synchronization-related delays, is a measure we can take.
- Integrating data compression algorithms to reduce the volume of data transmitted between chiplets, optimizing bandwidth usage, and decreasing communication latency is a technique we can apply.
- Implementing Quality of Service (QoS) settings to prioritize critical data associated with Kalman Filter calculations, and ensuring that safety-critical information receives expedited processing, is a step we can take.
- Reserving specific bandwidth for safety-critical messages related to Kalman Filter operations, preventing congestion, and ensuring timely delivery of critical information is a practice we can adopt.
- Implementing traffic shaping mechanisms to control the flow of data, preventing bottlenecks, and ensuring a smooth and consistent data stream is an approach we can implement.
- Keeping the firmware and software of the chiplets and associated components up to date to benefit from performance improvements, bug fixes, and optimizations is a routine we can follow.
- Implementing monitoring tools to continuously assess network performance, analyzing data to identify areas for optimization, and fine-tuning settings accordingly is a process we can integrate.
- Staying engaged with standardization bodies and industry forums to adopt the latest standards and best practices in High-Speed Serial Links, PCIe, and chiplet technology is an ongoing effort we can commit to.

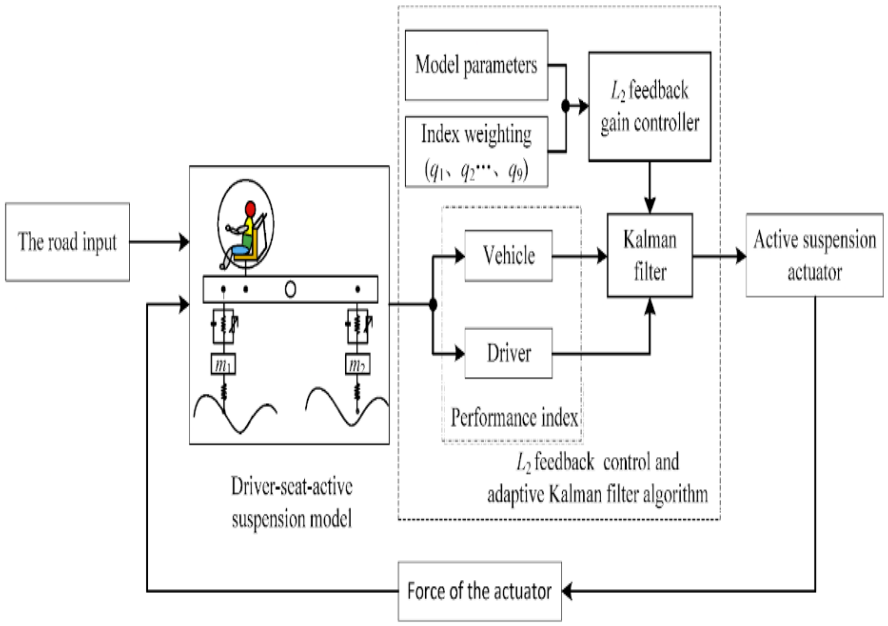


Figure 31

4 CYBERSECURITY PROCESSES

4.1 End-to-End Encryption (E2EE) in Chiplets

1. Properties
   - Objective: Secures data transmission between chiplets, ensuring confidentiality and protection against unauthorized access.
   - Components: Encryption Algorithm, Key Management, Data Segmentation, Secure Key Exchange, Authentication, Integrity Protection.
   - Security Mechanisms: Cryptographic encryption, key management, secure channels.
2. Applications:
   - Commonly Used In: Multi-chip modules, automotive systems, industrial automation, secure data processing environments.
   - Critical for: Protecting sensitive data during chiplet communication.
3. Implementation:
   - Encryption Algorithm: Selects strong encryption algorithms like AES(Advanced Encryption Standard.
   - Key Exchange: Implements secure protocols for exchanging encryption keys.
   - Authentication: Verifies the identity of participating chiplets.
   - Secure Channels: Uses protocols like TLS(Transport Layer Security) or DTLS(Datagram Transport Layer Security) for secure communication

Chiplet:

- Role: Secures data transmission between chiplets, protecting confidentiality.

4.2 Intrusion Detection System (IDS):

1. Properties:
    - Real-time Analysis: Provides real-time analysis of system activities for immediate threat detection. Behavioral Analysis: Utilizes behavioral analysis to identify anomalies.
2. Applications:
    - Network Security: Commonly deployed in network security to detect and respond to intrusions.
    - Critical Infrastructure: Used in critical infrastructure systems to safeguard against cyber threats.
3. Use Cases:
    - Threat Detection: Detects and responds to potential security threats in real-time.
    - Incident Response: Assists in rapid incident response and mitigation.
4. Implementation:
    - Strategically deploying network sensors to monitor traffic and anomalies.
    - Integrating the IDS with a Security Information and Event Management (SIEM) system for centralized analysis and automated response.

Chiplet:

- Role: Monitors and detects suspicious activities within chiplet-based systems.
- Implementation: Utilizes IDS components to analyze chiplet communication for anomalous patterns.

4.3 Secure Over-the-Air (OTA) Update

1. Properties:
    - Encryption: Encryption safeguards the integrity and confidentiality of the update data.
    - Authentication: Prevents malicious entities from injecting unauthorized updates.
    - Integrity Verification: Ensures that the update has not been corrupted or tampered with during transmission.
    - Rollback Protection: Protects against vulnerabilities present in outdated software versions.
    - Secure Boot: Safeguards against the installation of compromised firmware.

2. Applications:

    - IoT Devices:
    - Connected Vehicles: Ensures that software in vehicles, including in-car entertainment systems and safety-critical components, is regularly updated for performance and security improvements.
    - Consumer Electronics: Fix bugs and address security vulnerabilities

3. Implementation:

    - Secure Channels: Use secure communication channels such as HTTPS for delivering updates securely over the internet.
    - Code Signing: Digitally sign the update packages using cryptographic keys to verify their authenticity.
    - Two-Factor Authentication: To verify the identity of the device requesting an update to add an extra layer of security from unauthorization.
    - Version Management: Maintain a secure version management system to track the current software version on each device and prevent rollbacks.
    - Fallback Mechanism: Include a fallback mechanism in case an update fails, allowing the device to revert to the previous known-good version.

Chiplet:

- Facilitates secure firmware updates for chiplets in distributed systems. Ensures encrypted and authenticated over-the-air updates for individual chiplets.

4.4 Firmware Integrity Checks:

1. Properties:

    - Objective: Ensures the integrity of firmware by detecting unauthorized modifications or tampering.
    - Components: Hash Functions, Firmware Signing, Public Key Infrastructure (PKI), Secure Key Storage.
    - Security Mechanisms: Cryptographic hashing, digital signatures, secure key storage.

2. Applications:

    - Commonly Used In: Embedded systems, IoT devices, firmware-based applications.
    - Critical for: Preventing unauthorized modifications to firmware.

3. Implementation:

    - Hash Functions: Utilizes cryptographic hash functions (e.g., SHA-256) for generating checksums.
    - Firmware Signing: Digitally signs firmware using private keys.
    - PKI: Establishes a secure PKI for key management and signature verification.
    - Secure Boot Process: Integrates firmware integrity checks into the system's boot process.

Chiplet:

- Role: Verifies and maintains the integrity of firmware in chiplet-based systems.
- Implementation: Integrates into chiplet communication, often during the boot process.

4.5 Secure Boot

1. Properties

    - Objective: Ensures the integrity of the boot process by validating the authenticity of firmware and preventing the execution of unauthorized or malicious code.
    - Components: Root of Trust, Boot ROM or Bootloader, Cryptographic Verification, Secure Key Storage.
    - Security Mechanisms: Cryptographic verification, secure key storage, chain of trust.

2. Applications

    - Commonly Used In: Computers, servers, embedded systems, IoT devices, and more.
    - Critical for: Preventing bootkits, rootkits, and unauthorized firmware execution.

3. Implementation

    - Hardware Support: Utilizes dedicated hardware components like Trusted Platform Module (TPM) or Hardware Security Module (HSM).
    - Boot Process Integration: Embedded in the system's boot process to verify firmware integrity.
    - Key Management: Involves secure storage and management of cryptographic keys.
    - Policy Enforcement Adheres to predefined security policies for signature verification.

Chiplet:

- Role: Ensures the integrity of the boot process in chiplet-based architectures.
- Implementation: Integrates into chiplet communication, verifying firmware integrity during boot.

Table 2 Cybersecurity scenarios with regards to generic BMS

Target	Context	Possible method	Reaction	System results
Compromise temperature sensors in the battery pack modules	Requires physical access	Placing a resistor on the sensor line	BMC reduces limits, thermal management systems kick in and PRA opens contactors	Loss of power to vehicle
Compromise voltage sensors in battery pack modules	Requires physical access	Physical tampering (e.g. damaging the sensor line)	BMC would instruct PRA to open contactors.	Loss of power to vehicle.
Remove connection between battery pack modules and BMM	Requires physical access unless connection is wireless, in which case would likely require proximity	Causing a short circuit (physical) or jamming (wireless)	BMM sends a warning, BMC tells PRA to open contactors	Loss of power to vehicle
Interfere with connection between BMC and BMM	Requires physical access unless connection is wireless in which case would likely require proximity	Physical tampering or jamming	PRA opens contactors	Loss of power to vehicle
		Injection of invalid or random data	This would interfere with state estimation (e.g. charge instead of discharge), which would lead to abuse conditions. Possible BMS shutdown	Accelerated battery degradation. If all cells are tampered with, then safety issues are possible with overcharge or over-discharge. Loss of power to vehicle.
		Flooding	PRA opens contactors	Loss of power to vehicle.
Modification of software that performs calculations on BMM	Requires access to supply chain	Introduce error in software calculations or spoof incorrect voltages	Affect performance or shutdown the pack	Anything from battery degradation to loss of power and possible safety concern.
Modification of software that performs calculations on BMC			Could lead to overcharge, over-discharge, shutdown, and the BMC becoming not able to control the pack	
Compromise random access memory	Requires physical access or access to supply chain	Rowhammer attack[19] through compromised BMS (can cause memory cells to leak charge and electrically interact, which may also cause corruption or leakage from nearby memory rows)	Could lead to overcharge, over discharge or damage to cells	Battery degradation, BMS shutdown (Loss of power to vehicle)
Disruption of scheduling routines on the BMC	Requires access to the supply chain	Modification of controller software, or physical sabotage (e.g. using a non-spec chip with insufficient processing power)	Limitation of BMS functionality due to missing potentially crucial signals, eventually leading to shutdown	Loss of power to vehicle
Modify the external charger	Requires access to supply chain	Physical tampering of the charger	Incompatible charging leading to lack of charge to the vehicle.	Eventual loss of power to vehicle
Compromise communication between BMC and external charger	Requires physical access unless connection is wireless, in which case would likely require proximity	Spoof current request to external charger	Battery could be overcharged. BMC instructs shutdown	Loss of power to vehicle
Compromise externally facing communication (CAN) to the BMC	Requires physical access unless a wireless device is attached to the vehicle, or another ECU with a wireless interface is compromised (for example through pivoting)	Send "vehicle ignition" off signals into CAN bus	BMC instructs shutdown	Loss of power to vehicle
		Transmit a zero for HVIL value	BMC instructs shutdown	Loss of power to vehicle
		Fuzzing the BMC using CAN protocol (as the BMC performs handshakes via CAN with the charger)	BMC instructs shutdown	Loss of power to vehicle
Compromise current sensor within the BMS	Requires physical access	Spoof current to non-zero	Manipulates state of charge, which can trigger conditions for shutdown	Loss of power to vehicle
Indirect compromise of the battery pack	Requires access to the CAN bus	Disable or interfere with sub-vehicular systems with large battery usage (e.g. disable regenerative braking systems)	Eventual shutdown	Loss of power to vehicle Battery draining and degradation.

Figure 32: FOR BMS

Target	Context	Possible method	Reaction	System results
Machine learning algorithm for state estimation within the battery pack	Requires access to training and test dataset	Poisoning the training set (e.g. deliberately performing aberrant automotive drive cycles during data acquisition), or changing the labelling of any dataset Poisoning the test dataset	Subsequent models would be inaccurate, causing misestimation of battery behaviour as states are not as transparent as when directly measured	Could compromise performance as optimisation might be inaccurate (e.g. thinking that the pack is newer than it is could lead to abuse of battery, or through the VCU have other effects such as loss of power)
Compromising algorithms on the vehicle outside the battery pack			Could compromise information given to the VCU which in turn gives incorrect information to the BMC	If BMS is predicting parameters such as range, this would lead to inaccurate optimisations at system level
External intelligent algorithms (e.g. grid or charging stations)	Charger is bidirectional	Charger could be compromised such that it tells the battery to continuously discharge	SoC goes to minimal level	Loss of power to vehicle
Responses to environmental data	Requires proximity to external facing sensors for environmental data Possible long-range action possible (e.g. through cellular and GPS)	Spoofing vehicle operation modes, spoofing environmental data that leads to incorrect conclusions about traffic data, interfering with GPS	Could compromise information given to the VCU which in turn gives incorrect information to the BMC	If BMS is predicting parameters such as range, this would lead to inaccurate optimisations at system level

Figure 33: FUTURE CYBERSECURITY MEASURES IN BMS

4.6 For communication efficiency (basically for CAN)

There are several security solutions for CAN-based networks available: SecOC by Autosar, Stinger transceiver by NXP, and many other options including the internationally standardized ISO transport layer method (see ISO 14229/ISO 15765). SAE is working on cybersecurity measures for J1939 and CiA develops according solutions in its working groups.
IG04 SIG01 TF "CAN XL security" works on adding cybersecurity to CAN XL. The CANsec security protocol is an add-on function for CAN XL networks. It uses a part of the XLFF data field. Thus, cybersecurity can become a part of CAN XL data link layer hardware. CANsec is going to be specified in the CiA 613-2 (CAN XL add-on services – Part 2: Security). IG06 "Safety and security" specifies generic security options for CAN CC and CAN FD protocols. The CiA 720 document series under development specifies a cybersecurity higher-layer add-on function. Being of general interest, the approach is pursued by defining generic objects, parameters, and roles required in such a way, that they can be mapped for example to CANopen CC and CANopen FD. Mapping to other communication networks (e.g. I2C or EIA 485) is possible. Additionally, IG06 is planning to specify a generic document considering security threats on all OSI (Open Systems Interconnection model from ISO) layers.[12]

4.7 Server Market:

1. Focus on Data Security:

   - Primary Concern: Protection of sensitive data and ensuring the confidentiality, integrity, and availability of information.
   - Threat Landscape: Targets include unauthorized access, data breaches, and denial-of-service attacks.

- Security Measures: Strong encryption, access controls, secure authentication, and continuous monitoring.

2. Network Security Emphasis:
   - Critical Aspect: Safeguarding networks and communication channels.
   - Security Measures: Firewalls, intrusion detection/prevention systems, secure protocols (SSL/TLS), and virtual private networks (VPNs).
3. Remote Access Challenges:
   - Challenge: Management of remote servers and cloud-based infrastructure.
   - Security Measures: Multi-factor authentication, secure remote access tools, and secure configurations.
4. Regular Software Updates:
   - Importance: Regular application of security patches to address vulnerabilities.
   - Security Measures: Automated patch management systems and strict update policies.

4.8 Automotive Industry:

1. Safety-Critical Systems:
   - Primary Concern: Safety-critical systems and the physical well-being of occupants.
   - Threat Landscape: Manipulation of control systems, unauthorized access to in-vehicle networks, and potential physical harm.
   - Security Measures: Secure coding practices, intrusion detection/prevention systems, and separation of critical and non-critical systems.
2. Embedded Systems and ECUs:
   - Critical Aspect: Security of embedded systems and electronic control units (ECUs).
   - Security Measures: Secure boot processes, firmware integrity checks, and hardware-based security modules.
3. Unique Communication Challenges:
   - Challenge: Securing in-vehicle communication networks (CAN, LIN, Ethernet).
   - Security Measures: Encryption, authentication, and network segmentation to prevent unauthorized access.
4. Lifecycle Considerations:
   - Importance: Long lifecycle of automotive systems and the need for ongoing security measures.
   - Security Measures: Over-the-air (OTA) updates, secure software development practices, and continuous monitoring.

4.9 Common Aspects:

1. Secure Development Practices:
    - Shared Priority: Both industries emphasize the importance of secure coding practices during software development.
2. Supply Chain Security:
    - Concern: Ensuring the integrity and security of components within the supply chain.
    - Security Measures: Vendor assessments, secure supply chain practices, and hardware-based security.

5 2.5D/3D Interconnect Technologies:

- In 2.5D interconnect technology Integration of different chips on a single package, supports versatile ADAS system design and enhances system efficiency. In 3D Stacking multiple layers of active components, enabling the integration of complex ADAS functionalities. This optimizes the Compact form factor and reduces interconnect lengths.
- Shorter interconnect lengths for high-speed processing, minimizing signal delays. This reduces signal delays, Enhances computational speed, increases the efficiency of parallel processing, and improves responsiveness
- Contributes to a smaller form factor by integrating multiple components on a single package in 2.5D and Further contributes to a compact form factor by stacking components directly. This makes us save the Space for ADAS systems with limited space and improves thermal management.
- Integration of various sensors on a single package in 2.5D while in 3D the stacking of multiple sensor layers for detailed perception benefits us in Comprehensive environmental perception, simplified system architecture, and Multilayer sensor fusion improves sensor communication.
- Contributes to improved thermal management with efficient heat dissipation, Enhances thermal management by optimizing component stacking. Effective heat dissipation leads to overall system reliability Efficient cooling, is crucial for component reliability.
- Both technologies contribute to lower power consumption in ADAS systems. Energy-efficient operations are performed.
- Offers high bandwidth communication between different ADAS components and Provides faster data transfer between stacked layers, enhancing overall bandwidth. Efficient data exchange for real-time sensor fusion and Enhanced data throughput for improved efficiency.

5.1 OUT OF BOX:

1. **Photonics-Based Interconnects:**

   Photonics-based interconnects involve the use of light signals to transmit data, providing an alternative to traditional electronic interconnects. This technology has several advantages, including high data transfer rates, low latency, and immunity to electromagnetic interference. In the context of ADAS chiplets, incorporating photonics-based interconnects offers unique benefits:

   - Photonics-based interconnects leverage light signals, enabling significantly higher data transfer rates compared to traditional electronic interconnects. This enhances the transmission of large volumes of sensor data in real time, crucial for ADAS applications that demand rapid processing.
   - For Low Latency, Light signals travel at the speed of light, resulting in minimal latency in data transmission. This Reduces signal delays and contributes to real-time responsiveness in processing sensor data, improving overall system performance.
   - Unlike electronic interconnects, photonics-based interconnects are immune to EMI, ensuring reliable communication in electromagnetically challenging environments which enhances reliability in ADAS systems where electromagnetic interference could disrupt electronic signals.
   - Photonics-based interconnects can be more energy-efficient than electronic interconnects, especially over long distances. This reduces power consumption which is advantageous for ADAS applications, contributing to energy-efficient operation.
   - Photonics-based interconnects facilitate efficient communication between different chiplets within the ADAS system and support seamless integration of diverse functionalities, such as image processing, sensor data fusion, and decision-making, across chiplets.
   - Photonics-based interconnects can be implemented in compact and integrated designs, contributing to a smaller form factor for ADAS chiplets. This leads to Space-saving solutions are crucial for automotive applications where physical space is limited.
   - Photonics technology allows for the integration of optical sensors directly onto the chiplets and enables comprehensive environmental perception by combining electronic and optical sensor data for a more accurate representation of the vehicle's surroundings.
   - Photonics-based interconnects generate less heat compared to traditional electronic interconnects. This contributes to improved thermal management, maintaining the reliability and longevity of ADAS components.
   - Photonics-based communication can enhance security by reducing the susceptibility to certain types of cyber-attacks. This Ensures secure and reliable communication, critical for safety-critical applications in automotive environments.
   - Utilizing fiber optic cables for photonics-based interconnects provides high bandwidth and reliable communication. It supports high-bandwidth communication over longer distances, enhancing the flexibility of ADAS system architecture.

- Challenges and Methods to encounter them:
  - Integrating photonics-based interconnects requires specialized design considerations and manufacturing processes. For this Collaborate with semiconductor experts, and we can develop standardized integration approaches.
  - Initial costs associated with photonics technologies can be higher. Continued research can reduce production costs, Can also explore economies of scale in manufacturing.
  - Selecting materials compatible with both photonics and semiconductor technologies is essential. Research into materials that provide the required optical and electronic properties, ensuring reliability.

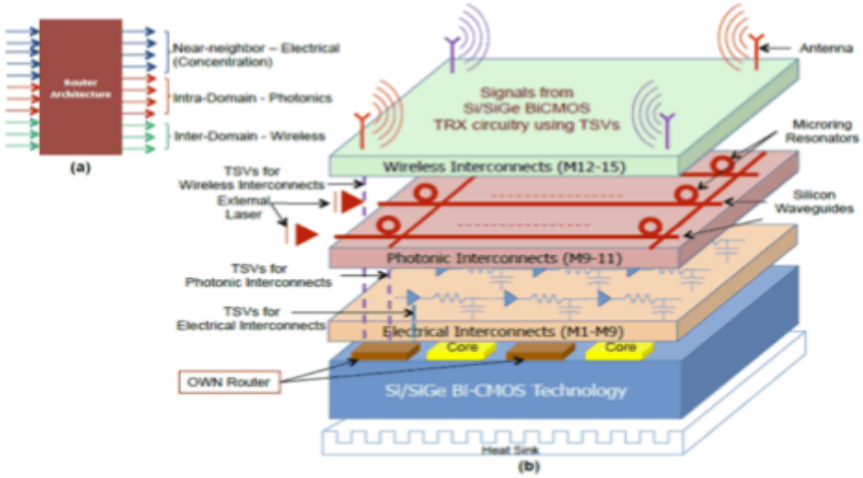


Fig. 7. (a) Proposed router microarchitecture that combines near-neighbor (electrical), intra-domain (optical) and inter-domain (wireless) links. Note that the actual radix will be a function of media access protocol (SWMR/MWSR) and wireless connectivity. (b) Its multi-layer implementation via diverse technology.

Figure 34

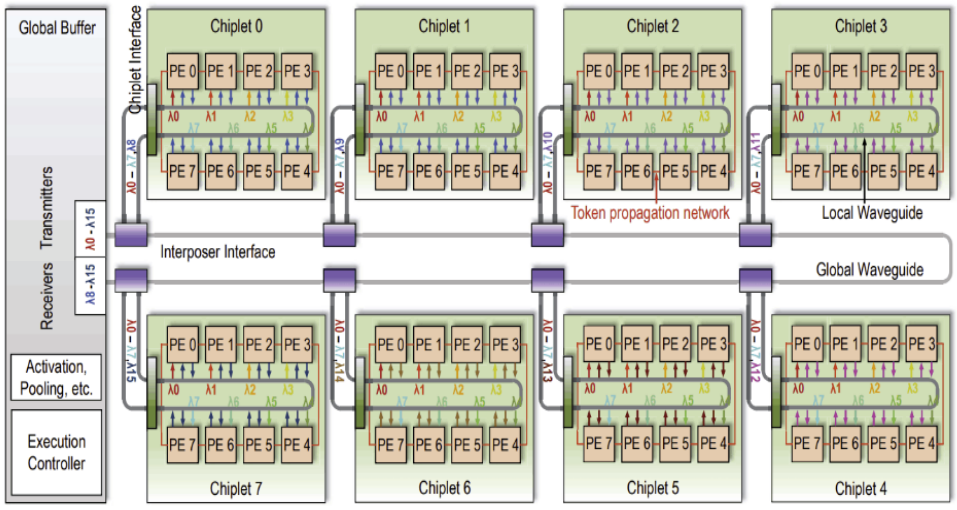


Figure 35

Conclusion:

Photonics-based interconnects represent a cutting-edge technology with the potential to revolutionize ADAS chiplet communication. Their high data transfer rates, low latency, and immunity to EMI make them particularly well-suited for the demanding requirements of ADAS applications. As research and development in photonics continue, their integration into ADAS chiplets holds promise for advancing the capabilities and reliability of automotive safety and automation systems. Collaborative efforts among photonics experts, semiconductor engineers, and automotive manufacturers will be pivotal in realizing the full potential of this technology in the automotive industry.

2. **Neuromorphic Interconnects:**

Neuromorphic interconnects draw inspiration from the architecture and communication principles of biological neural networks. These interconnect emulate the efficient and parallel processing capabilities of the human brain, offering potential advantages for ADAS chiplets in terms of adaptability, learning, and energy efficiency.

- Neuromorphic interconnects facilitate parallel processing, allowing chiplets to simultaneously analyze and respond to multiple streams of sensor data. This Enhances adaptability to dynamic driving conditions, supporting real-time decision-making.
- Implementation of spiking neural networks in interconnects enables event-driven communication, mimicking the spiking behavior of neurons. This makes efficient utilization of computational resources and reduces power consumption.
- Neuromorphic interconnects can support on-chip learning algorithms, enabling ADAS chiplets to adapt and improve their performance over time. Continuous improvements can be made in system functionality based on experience and exposure to diverse driving scenarios.
- The event-driven nature of neuromorphic interconnects contributes to energy-efficient communication by transmitting information only when significant events occur. Reduces overall power consumption which is critical for automotive applications with limited energy resources.
- Neuromorphic interconnects facilitate real-time fusion of sensor data from various sources, supporting a holistic perception of the vehicle's environment. This develops Comprehensive and timely awareness of surroundings, essential for driving safety.
- Chiplets with neuromorphic interconnects can dynamically adjust signal processing parameters based on contextual information. Optimizes signal processing for different driving conditions, improving system efficiency.
- The distributed and redundant nature of neuromorphic interconnects provides inherent fault tolerance. Enhances reliability, as the system can adapt and reroute information in the presence of faults.

- Neuromorphic interconnects support a distributed architecture, allowing for the decentralization of processing tasks across chiplets. Improves scalability, enabling the addition of chiplets without causing bottlenecks in the system.
- Chiplets with neuromorphic interconnects can dynamically reconfigure their connections and processing units based on changing requirements. Flexible to adapt to varying computational demands, maximizing resource utilization.

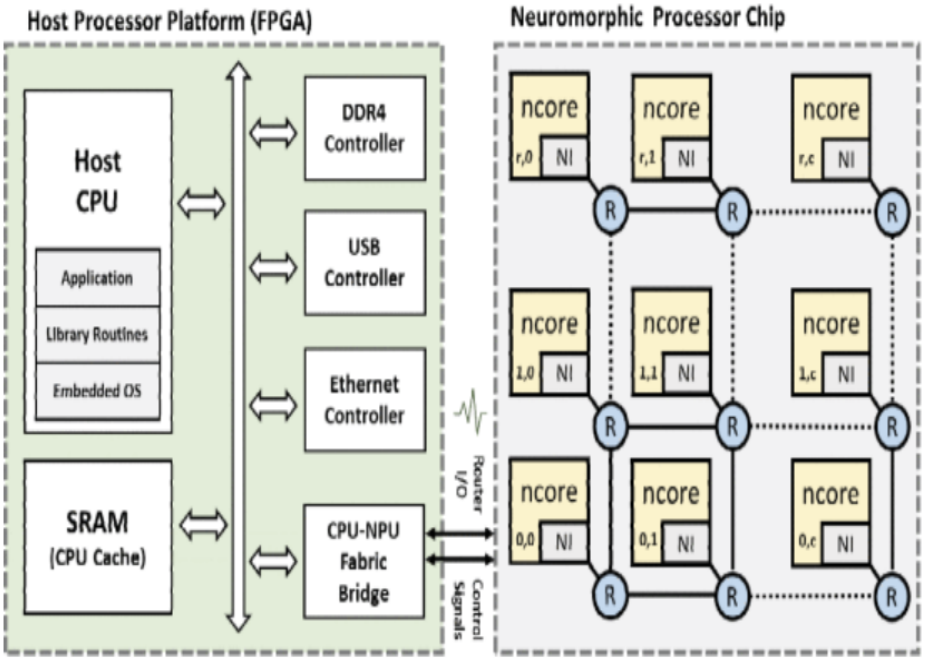


Figure 36

- Challenges and Methods to encounter them:
  - Implementing neuromorphic algorithms and interconnects introduces complexity in algorithm design and optimization. To face this we can research to simplify and optimize neuromorphic algorithms for practical implementation in ADAS chiplets.
  - Ensuring seamless integration of neuromorphic interconnects with existing hardware architectures poses challenges. Collaborative efforts between neuromorphic hardware designers and automotive chiplet manufacturers to develop standardized interfaces can be made.
  - Learning capabilities in neuromorphic chiplets raise concerns about data privacy and security. We can implement secure learning algorithms, adherence to privacy regulations, and robust encryption methods.

Conclusion:

Neuromorphic interconnects hold promise for revolutionizing the capabilities of ADAS chiplets by introducing principles inspired by the human brain's efficient processing. The potential for on-chip learning, adaptability, and energy efficiency aligns well with the demanding requirements of autonomous vehicles and advanced driver assistance systems. While challenges

exist in terms of algorithmic complexity and hardware integration, ongoing research and collaborative efforts are likely to pave the way for the practical implementation of neuromorphic interconnects in ADAS chiplets, contributing to safer and more intelligent vehicles.

3. **Quantum Entanglement-Based Interconnects:**

   Quantum entanglement-based interconnects leverage the principles of quantum physics to establish entangled states between chiplets. This technology offers unique features that can revolutionize communication in ADAS chiplets.

   - Quantum entanglement allows two or more particles to become correlated in such a way that the state of one particle instantly influences the state of the other, regardless of the distance between them. This allows us to develop Instantaneous and secure communication between chiplets, even over large distances.
   - Quantum superposition allows particles to exist in multiple states simultaneously, enabling the transmission of complex information using quantum bits or qubits. This Increases data transmission capacity and the ability to process multiple states in parallel.
   - QKD utilizes the principles of quantum entanglement to establish secure cryptographic keys for communication. This develops Unhackable key distribution which ensures the confidentiality and integrity of communication in ADAS chiplets.
   - Quantum teleportation enables the transfer of quantum information from one entangled particle to another without physical transmission. Ultra-fast and secure information transfer between chiplets, contributing to low-latency communication can be achieved.
   - Quantum entanglement-based communication is inherently secure due to the no-cloning theorem, making it resistant to eavesdropping. This Enhances cybersecurity and is crucial for safeguarding sensitive information in automotive applications. Entanglement swapping allows the creation of entangled states between chiplets indirectly connected through an intermediate entangled pair. Extending entanglement over longer distances and enabling scalable quantum networks for ADAS systems can optimize communication efficiency.
   - Quantum repeaters amplify and extend entangled states over long distances, addressing the challenge of quantum information loss in transmission. Facilitates reliable quantum communication over extended distances that can be encountered in automotive environments.
   - Quantum interference allows the manipulation of quantum states to perform specific quantum operations. Enabling quantum computing tasks that could enhance the processing capabilities of ADAS chiplets.
   - Quantum systems are susceptible to decoherence, where quantum states lose coherence over time. Various techniques are employed to mitigate decoherence effects. This ensures the stability and reliability of quantum information in ADAS chiplet communication. Challenges and Methods to encounter them:
     - Quantum systems are often sensitive to temperature fluctuations, requiring stable environmental conditions. By Implementing temperature control measures to maintain

the stability of quantum states in automotive environments can be encountered by this.

- Quantum entanglement-based communication requires sophisticated hardware setups, including entangled photon sources and detectors. Researching to develop compact and robust quantum hardware suitable for automotive applications.
- Quantum systems are susceptible to errors, and error correction techniques are essential for maintaining the integrity of quantum information. Advancements in quantum error correction methods can be done to enhance the reliability of quantum communication in ADAS chiplets.

Conclusion:
Quantum entanglement-based interconnects represent a cutting-edge approach for secure and ultra-fast communication in ADAS chiplets. The inherent features of quantum entanglement, such as superposition and quantum teleportation, offer unprecedented capabilities for secure and efficient data transmission. While challenges exist in terms of temperature sensitivity and hardware complexity, ongoing research and development in the field of quantum communication hold the potential to bring these advanced interconnects to practical implementation in automotive safety and automation systems.

5.1.1 Conclusion for "OUT OF BOX"

There can be Some Other box Interconnects like 3D Stacked Wireless interconnects and Elastic Interconnects

- Wireless Interconnects:
  Implements wireless communication between chiplets using advanced millimeter-wave or terahertz technologies. This Eliminates physical connectors, providing greater flexibility in chiplet placement. Simplifies the system architecture by eliminating physical wires, reducing complexity.Allows for dynamic placement of chiplets, facilitating adaptable configurations. Wireless communication can be more robust against environmental conditions.

- Elastic Interconnects
  Creates interconnects with dynamic reconfigurability to adapt to varying workloads and connectivity requirements.Utilizes materials with tunable properties. Dynamically adjusts to different workloads, optimizing resource utilization. Reduces energy consumption during idle periods by dynamically adapting to workload changes.Can adapt to hardware failures by rerouting connections dynamically.

- 3D Stacked Wireless Interconnects
  Stacks chiplets in a 3D configuration with built-in wireless interconnects between layers. Utilizes advanced antennas and beamforming technologies for efficient communication.Addresses miniaturization demands, crucial for automotive applications with limited space. Wireless communication reduces interconnect lengths, minimizing communication delays. Improved thermal dissipation in the 3D configuration.

	Emerging Computing Technology			
	Quantum	**Optical**	**In-Memory**	**DNA**
Applications	Cryptography, unstructured search, combinatorial optim., generative chemistry	Deep neural networks, scientific computing	Deep neural networks, genomics, signal processing, recomm. systems, data analytics	Ultra-massive storage of data, bio-compatible processing, theranostics
Required Bandwidth	1 Tb/s	10 Tb/s	1 Tb/s	1 Gb/s
Required Efficiency	1–10 fJ/bit	1–10 fJ/bit	0.1-1 pJ/bit	<1 aJ/bit
Required Latency	1–10 ns	1–10 ns	10–100 ns	~1 hour
Interconnect Alternatives	Electrical, Photonic, Wireless	Photonic	Electrical, Photonic, Wireless	Microfluidic, Photonic, Electrical, Wireless
Analog–Digital Conversion?	Depends on the qubit control/readout scheme	Yes (if computing is implemented using analog data signals)	Yes (if computing is implemented using analog data signals)	Yes
Inter-Technology Data Conversions?	Depends on the qubit readout and quantum state transfer schemes, which could be optical	Depends on whether the architecture is all-optical or not	None, if electrical or wireless interconnects are used	From/to the biochemical domain via photo-chemistry, microfluidics, EM transduction
Challenges for Interconnect Design	Cryogenic operation, thermalization, limited cooling power of dilution refrigerator, latency and bandwidth	Thermal and fabrication variations, crosstalk, aging, tuning power, side-channel attacks	Thermal, analog noise, ADC area/energy/ bandwidth, fabrication challenges, DRAM cost, programming interface	High error rates, slow operation, domain conversion, waste management.
Compatibility requirements from memory/storage subsystems	Compatible with most memory/storage technologies, though at cryogenic operation	High-speed optical transceivers at the storage/memory interface	Implementations vary, but compatible with most memory/storage technologies	Suitable for long-term, massive storage and bio-compatible operation

Figure 37

Each of these technologies represents a groundbreaking approach to chiplet interconnects, offering unique advantages and addressing specific challenges in the context of ADAS applications. The success of these innovations would not only enhance the performance and efficiency of automotive systems but also redefine the possibilities in semiconductor design.

6 Cooling Solution

6.1 Introduction

The slowing down of the moore's law and the increasing cost of making the transister's with shorter channel length has prompted the exploration of 3D IC techniques as a promising avenue to extend Moore's Law. The concept of 3D ICs holds potential in addressing the current interconnection bottleneck at the nanometer scale, thereby facilitating the continued progression of Moore's Law. This advanced technology involves vertically stacking multiple cores, memory, and logic units in a single unit, offering advantages such as increased clocking speed, reduced transmission losses, lower power consumption, and a smaller footprint .

Nevertheless, the adoption of 3D ICs comes with substantial challenges that must be overcome for the technology to be practical. One of the most significant hurdles is the issue of overheating due to escalating power flux and higher thermal resistance. The 3D IC technology introduces the possibility of localized hotspots within stacked structures, leading to elevated local heat fluxes and an overall increase in the chip's temperature. The increase in heating on these chips degrades chip performance and reliability. The performance , reliability, and power dissipation of both interconnects and transistors are strongly affected by the operating temperature. Consequently, effective chip-level cooling has become imperative, particularly in high-performance chips with substantial power dissipation. The International Technology Roadmap for Semiconductors (ITRS) has projected a significant increase

in the power density of a single package, reaching thousands of W/cm^2 for performance applications in 2030. This upward trend in power density becomes more pronounced as more chips are integrated into a single package, as illustrated in Figure below.

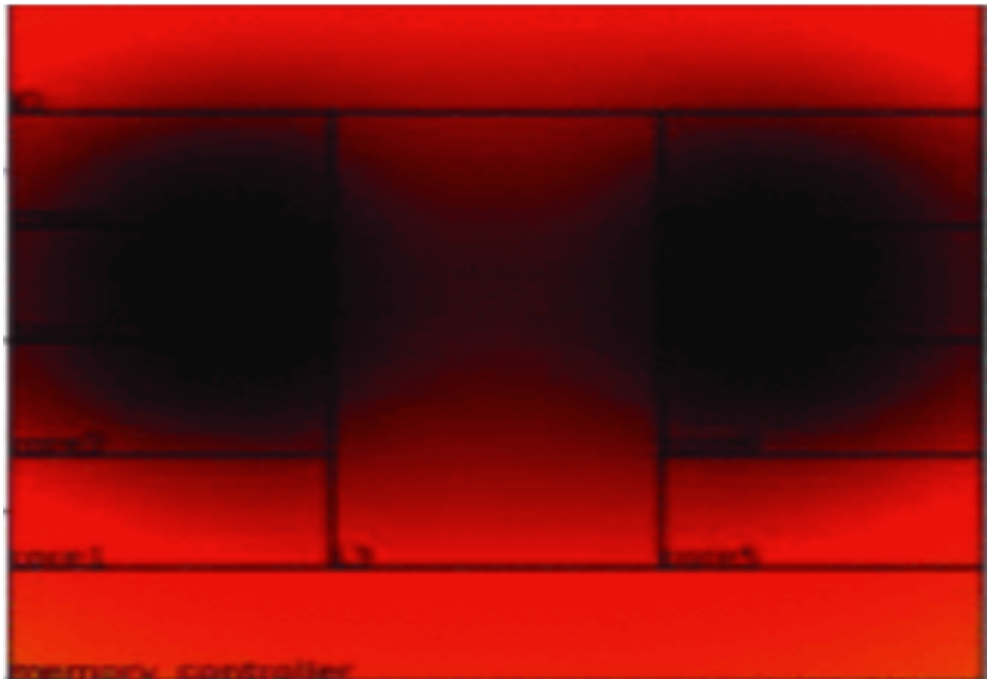


Figure 38

Therefore, the development of effective cooling structures is crucial for unlocking the full potential of 3D IC technologies beyond the confines of Moore's Law . Numerous cooling methods for chips have been proposed, falling into two main categories , active and passive cooling methods:

- Active cooling, on the other hand, involves the input of power and requires external components such as pumped loops (like heat exchangers and cold plates) , active convection devices (ex. fans and nozzles) , and refrigerators (including Peltier thermoelectric and vapor-compression-based systems) .

- Passive methods involve thermal conduction (metal lines ,utilizing pastes, and vias), passive convection (involving finned heat sinks and ventilation slots), radiation (utilizing coatings and paints), heat pipes, and thermosyphons . While passive devices are easy to design and relatively inexpensive, they often underperform compared to their active counterparts.

Passive cooling methods face challenges when trying to be embedded within 3D IC structures due to size constraints and limitations in providing effective cooling. Moreover, they struggle to address the diverse thermal profiles encountered in an integrated circuit. Microfluidics, also known as lab-on-a-chip, is a field that deals with the manipulation of small fluid volumes using channels or flat platforms with dimensions ranging from tens to hundreds of micrometers . In 2004, microfluidics was highlighted as one of the seven technologies poised to revolutionize industries by American Business 2.0 magazine, recognizing its potential for groundbreaking business opportunities . In July 2006, Nature magazine dedicated a special issue to microfluidics, acknowledging it as "the technology of

the century" and providing insights into its origins, future, basic principles, and applications . While initial research predominantly focused on applications in biology, chemistry, materials science, and medical science, microfluidic cooling has emerged as a promising solution for 3D ICs with high power density.

The U.S. Defense Advanced Research Projects Agency (DARPA) started the Intra/Inter Chip Enhanced Cooling (ICECool) program in 2012 to find a solution for cooling challenges. As a result of their findings microfluidic cooling came out as an effective thermal management technique to directly cool heat generation sites within the chip, substrate, and/or package .

6.2 Microfluidic Cooling Structure

The ICECool programs envisaged micro/nano-scale microfluidic channels and structures embedded within 3D ICs, with high thermal conductivity. Along with it, they proposed the utilization of thermoelectric materials to establish connections between on-chip hotspots and microfluidically cooled microchannels. The suggested intra/inter chip-enhanced cooling techniques must align with the material properties, fabrication processes, and thermal management requirements associated with both homogeneous and heterogeneous integration within 3D chip stacks. Figure below illustrates a proposed ICECool structure .

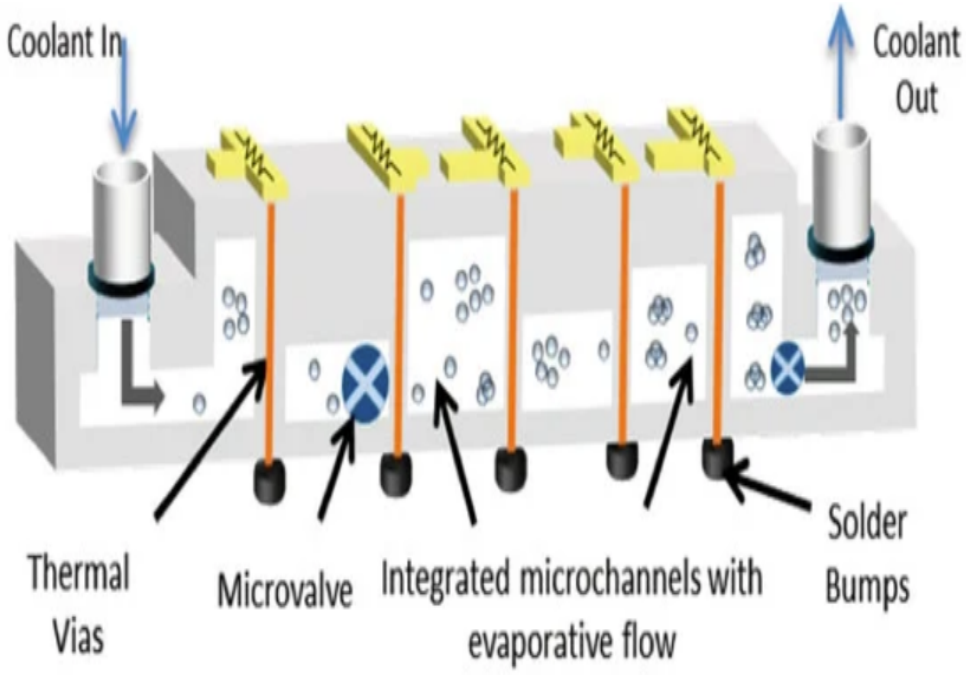


Figure 39

Intra-chips incorporate directly fabricated micropores and microchannels . Meanwhile, the inter-chip strategy employs microgaps as cooling channels between chips within three-dimensional stacks . Drawing inspiration from the ICECool program's conceptual model, various structures of embedded microfluidic cooling in 3D ICs have been introduced. Yue Zhang et al. introduced a tier-specific microfluidic cooling technology, as experimentally showcased in a 3D stack depicted in Figure 40 . In comparison to conventional microfluidic cooling, this tier-specific cooling approach demonstrates

a 37.5% reduction in pumping power, thereby preventing overcooling under specified operating temperatures.

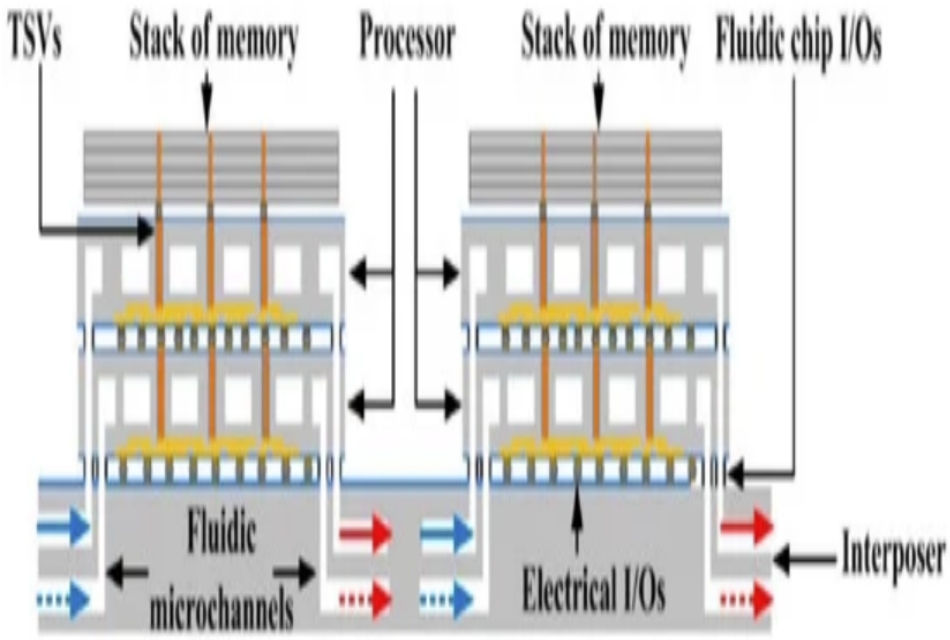


Figure 40

In Figure 40, the cold coolant flow is indicated by blue arrows, while the hot coolant flow is represented by red arrows. Minhaj Hassan et al. conducted a study to understand the impact of temperature on circuit performance and explored the benefits of employing microfluidic technology for ongoing performance scaling in the structure depicted in Figure above. Experimental findings validated that conventional air cooling solutions impose limitations on 3D stacks . Yassir Madhour et al. introduced a patterned die-to-die thin film bonding method tailored for 3D chip stacks with integrated microfluidic cooling to address stack bonding challenges. The method was developed and successfully tested . Following this, Paragkumar et al. demonstrated the fabrication and characterization of a thick silicon interposer featuring low-loss polymer-embedded vias and two dice. This silicon interposer incorporated an integrated microfluidic heat sink, as well as fluidic and electrical I/Os, supporting high-performance 3D system integration .

Additionally, Figure 41 showcases modified microfluidic cooling structures that have been investigated. Each chip in this configuration possesses its own fluidic inlet and outlet. The flow direction and rate were independently adjusted for each die based on individual requirements . This approach achieved independent cooling for each tier, providing flexibility for various temperature distributions and velocities.

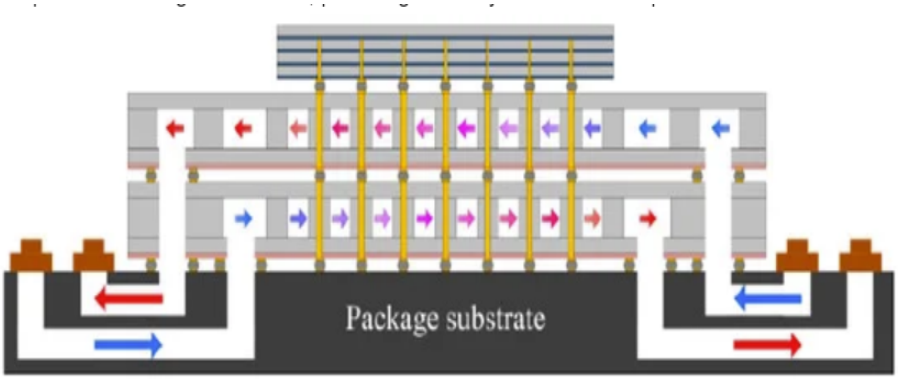


Figure 41

The microfabrication processes for Through Silicon Vias (TSVs) integrated into 3D ICs involve intricate procedures, as outlined in Figure 42. The sequence begins with the deposition of silicon dioxide, followed by the application of a metal layer. In Figure 42b, a thin chrome layer serves as the etch mask. Utilizing this chrome mask, the silicon dioxide layer undergoes etching, and the remaining chrome is removed with a CR-7S chrome etchant, resulting in the silicon dioxide functioning as an etch mask, as depicted in Figure 42c. The high-aspect-ratio Bosch process is then employed to etch via holes through the silicon wafer, as illustrated in Figure 42d. Wet oxidation is subsequently applied to isolate the vias from the silicon substrate. Titanium and copper seed layers are deposited on the backside of the wafer using an e-beam evaporator. Additionally, chemical mechanical polishing is employed to remove the overburden, as shown in Figure 42e. This process yields a micropin-fin heat sink structure, as depicted in Figure 42f. Finally, a glass slide is assembled into the testbed, incorporating fluidic inlet/outlets for fluid delivery, as shown in Figure 42g .

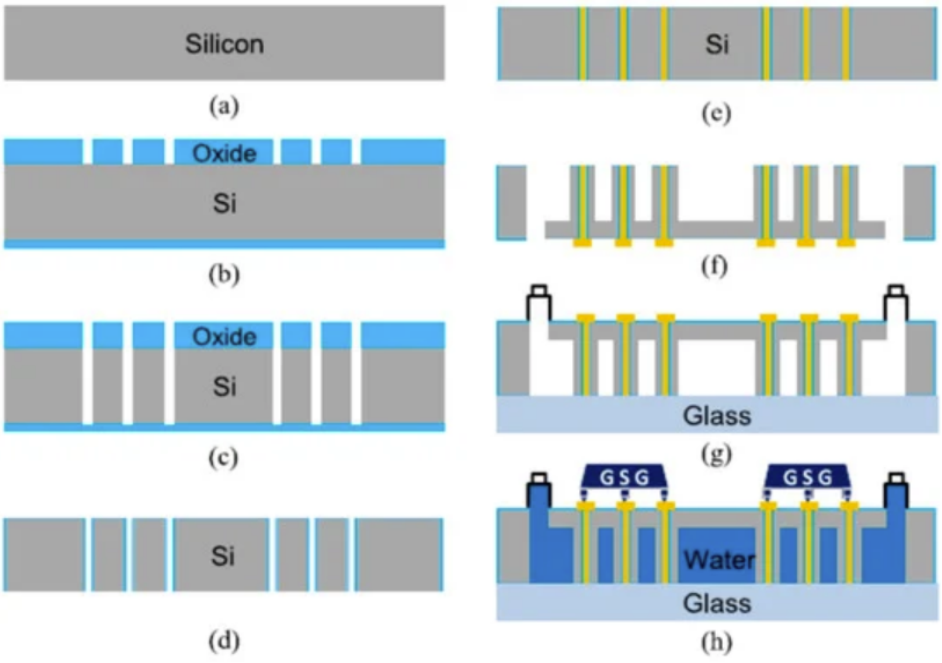


Figure 42

6.3 Co-Design in 3D Integrated Circuits (ICs)

Co-design, a unified approach integrating computational, electrical, physical, thermal, and reliability aspects, has emerged as a game-changer for IC design. By overcoming the limitations of independent optimization, it optimizes design configurations for high performance.

This concept becomes increasingly crucial for 3D ICs with microfluidic cooling. The intricate interplay between cooling structures, interlayer coupling, and component connectivity necessitates co-design for optimal performance. Embedded microfluidics further amplifies this need, as it significantly impacts factors like hotspot distribution, power, and reliability.

Several recent advancements showcase the power of co-design in this realm:

- **Electrical-thermal co-simulation methods** estimate voltage drop and temperature distribution in 3D systems with fluidic cooling, accounting for air convection and Joule heating.
- **Multicore architecture and microfluidic co-design** utilizes cycle-level microarchitecture simulators and benchmark programs to optimize cooling for 3D-stacked ICs under liquid cooling conditions.
- **Hybrid 3D-IC cooling solutions** combine thermal TSVs with microfluidic channels, achieving enhanced cooling capabilities with reduced power requirements compared to pure microchannel cooling.
- **Multi-domain co-optimization and co-simulation frameworks** enable co-design of 3D CPU architectures with both microfluidic and air cooling options.
- **Interlayer microfluidic heat sink co-design** explores trade-offs between heat removal efficiency and parasitic effects associated with TSVs.

These examples demonstrate the significant potential of co-design in unlocking the full potential of 3D ICs with microfluidic cooling, leading the way towards more efficient, powerful, and reliable chip architectures.

6.4 Influence on Through Silicon Vias

Microfluidic cooling integrated in 3D chip stacks can significantly impact electrical characteristics, particularly at high frequencies. This necessitates careful investigation of its influence on Through Silicon Vias (TSVs). Studies have shown promising results, with experimental data indicating a substantial decrease in leakage current (66.2%) for a CMOS chip with microfluidic cooling. Furthermore, frequency-dependent electrical behavior has been observed when integrating liquid coolants with L-band filters, enabling the tuning of corner frequencies. Additionally, using different coolants, like distilled water and methanol-water mixtures, in a tunable RF sensor has demonstrated the ability to adjust the operating frequency across a wide range. However, the presence of coolants between ground and signal interconnects can affect signal propagation, impacting factors like integrity, loss, and crosstalk.

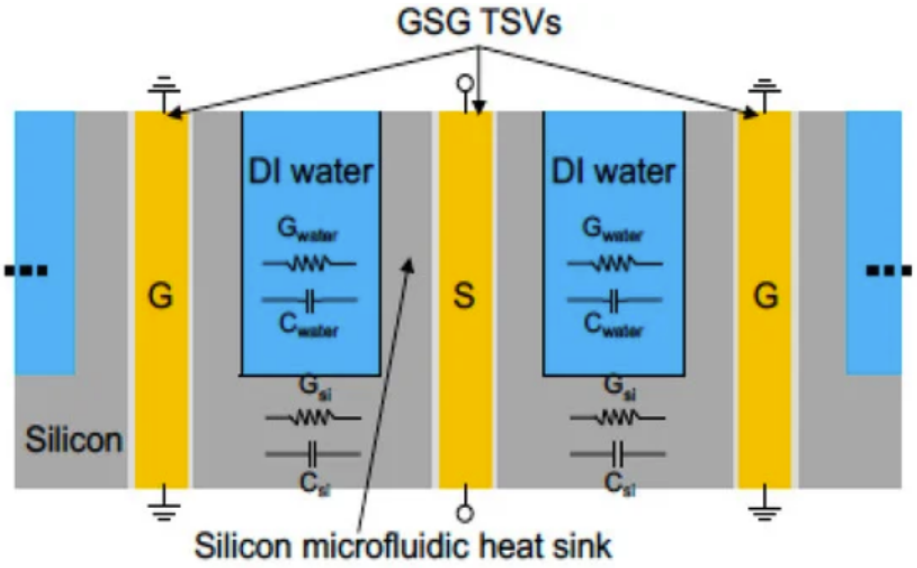


Figure 43

Research by Hanju Oh et al. focused on creating highly insulated Through Silicon Vias (TSVs) with a remarkable aspect ratio of 23:1. They explored integrating these high-aspect-ratio TSVs into a microfluidic heat sink using various fabrication techniques. Notably, they proposed a 3D system with TSVs embedded within interlayer microfluidic channels, offering valuable insights into the fabrication and electrical characterization of such structures in a micropin-fin heat sink. Their findings revealed that distilled water, a common coolant, can influence the electrical performance of TSVs. Figure 44 showcases equivalent circuit models of TSVs in both a silicon substrate and a micropin-fin heat sink filled with distilled water. This model serves as a tool for understanding how liquid cooling affects TSV performance within a microfluidic testbed.

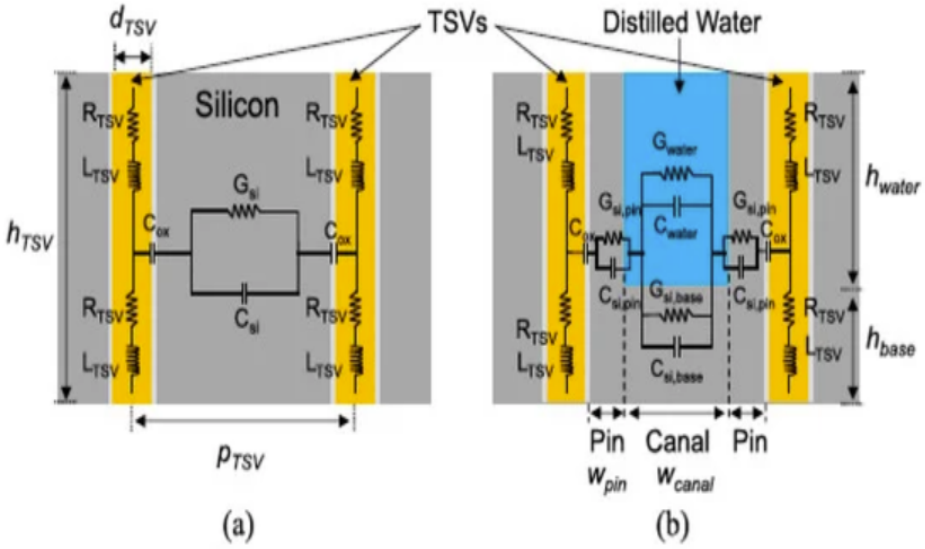


Figure 44

Hanhua Qian et al. developed a sophisticated thermal simulator for analyzing both sink-cooled and microfluidic-cooled 3D ICs. This tool accurately predicts the heat transfer through Through Silicon Vias (TSVs) at a detailed level. It achieves this by calculating the equivalent thermal conductivity of each grid cell in the model, taking into account the presence of TSVs and their anisotropic

nature. This approach efficiently estimates the thermal impact of TSVs with fine granularity. Additionally, the simulator considers the specific thermodynamics of microfluidic cooling, including the influence of microchannel entrances on heat transfer.

6.5 Specific Applications of Microfluidic Cooling

Microfluidic cooling is revolutionizing thermal management in 3D chip stacks, opening doors to exciting possibilities:

1. Performance Boost:
   -
   - 3D processor stacks with microfluidic cooling achieve 2.4x higher performance compared to air cooling (Serafy et al.).
   - Optimal microchannel designs in 3D FPGAs lead to 80.3% energy efficiency improvement and 124% higher operating frequency (Yang et al.).
   - Microfluidic cooling unlocks the full potential of 3D CPUs, with 2.3x performance gains through co-optimized floor plans (Serafy et al.).
2. Design Innovation:
   -
   - Microfluidic heat sink integration allows higher inlet water temperatures (up to 50°C) for efficient heat exchange (Serafy et al.).
   - Tier microfluidic cooling with high-aspect-ratio TSVs and a vacuum cavity protects sensitive components from temperature fluctuations (Zhang et al.).
   - Silicon interposer platforms with microfluidic cooling enable high-bandwidth signaling between logic and memory stacks** (Zheng et al.).
3. Beyond Cooling: Microfluidic boiling emerges as a potential cooling method for high-performance servers, offering insights into design and implementation (Schultz et al.).

Microfluidic cooling is not just about cooling; it's a game-changer for 3D chip design, unlocking unprecedented performance and paving the way for innovative architectures.

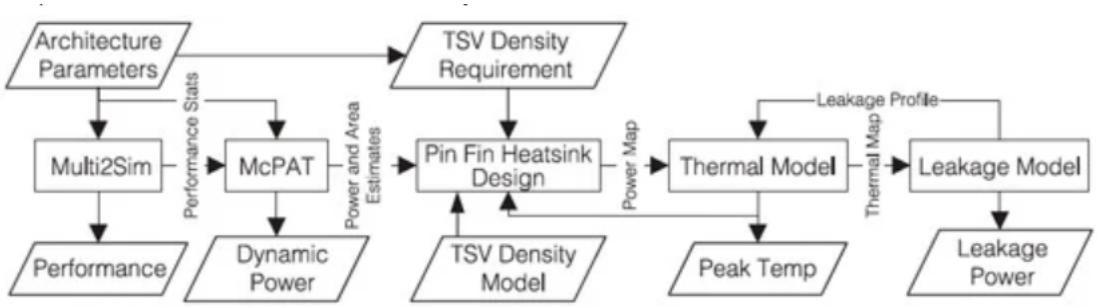


Figure 45

6.6 Thermal Models, Characteristics, and Transmissions in Microfluidic Cooling

Enhancing Thermal Precision in 3D ICs :

1. Predicting Overall Thermal Resistance:
    - Chlieh et al. built a thermal model for organic heat sinks in microfluidic channels, validated by experiments with varying channel thicknesses.
    - Model predictions aligned with temperature measurements of resistors, proving its accuracy.
2. Coupling Power and Thermal Analysis:
    - Wan et al. developed a power-thermal simulator for 3D ICs with on-chip micropin-fin cooling, generating detailed hotspot maps.
    - Leakage power dominated, accounting for 55.8% of dynamic power consumption, with minimal influence from ambient heat transfer coefficient.
3. GaN Microfluidics: Heterogeneous Integration:
    - Agarwal et al. created numerical thermal models for GaN devices with microfluidic cooling, compatible with integration with silicon-based CMOS.
    - This paves the way for efficient thermal management in heterogeneous chip designs.
4. Microfluidic Heat Sink Structures:
    - Wang et al. analyzed heat transfer and friction in microchannels with various micro-rib structures (rectangular, triangular, semicircular).
    - Micro-ribs enhanced heat transfer but increased pressure drop, requiring careful design optimization.
5. Micropin-Fin Density Matters:
    - Zhang et al. designed and tested micropin-fin arrays for 3D IC thermal testbeds.
    - Their findings highlight the significant impact of micropin-fin density on thermal performance, allowing for targeted design choices.

6.7 Conclusions

The preceding discussion encompasses all the available publications on the application of microfluidic cooling in 3D ICs. The majority of research works in this domain have been published within the last five years, concentrating on fundamental principles, models, and practical examples of microfluidic cooling applications. Drawing insights from the analyses conducted, several recommendations for future research are proposed:

1. The exploration of methods and models for evaluating hotspots is crucial for implementing microfluidic cooling in 3D ICs, especially in scenarios involving non-uniform heating. However, specific methodologies and models for hotspot evaluation are yet to be established.

2. Digital microfluidics has proven to be an effective approach in cooling processes. Future research should focus on understanding how drive voltage requirements can be reduced when integrating cooling structures into 3D stacked ICs.

3. There is a need for more systematic advancements in the manufacturing, testing, and design methods associated with the utilization of microfluidic cooling in 3D ICs. A comprehensive approach is essential to address challenges and optimize the implementation of this cooling technology.

7 Image Credits

(1) Wifi module -

Image copyright = Visconti, Paolo Primiceri, Patrizio Cavalera, Giorgio. (2016). Wireless Monitoring System of Household Electrical Consumption with DALY-based Control Unit of Lighting Facilities Remotely Controlled by Internet. Journal of Communications Software and Systems. 12. 10.24138/jcomss.v12i1.86.

(2) Bluetooth Module

Image copyright- Ferrigno, Luigi Paciello, Vincenzo Pietrosanto, Antonio. (2005). A Bluetooth-Based Proposal of Instrument Wireless Interface. Instrumentation and Measurement, IEEE Transactions on. 54. 163 - 170. 10.1109/TIM.2004.840245.

(3) A 4G-Connected Micro-Rover-

Image copyright - IEEE JOURNAL ON MINIATURIZATION FOR AIR AND SPACE SYSTEMS, VOL. 1, NO. 3, DECEMBER 2020 Peter J. Burke , Senior Member, IEEE

(4) Diagram of a satellite communication system architecture

Image copyright - Al-Hraishawi, Hayder Chougrani, Houcine Kisseleff, Steven Lagunas, Eva Chatzinotas, Symeon. (2022). A Survey on Non-Geostationary Satellite Systems: The Communication Perspective. IEEE Communications Surveys Tutorials. PP. 1-1. 10.1109/COMST.2022.3197695.

(5) LoRA

Image copyright - LoRa Architecture for V2X Communication: An Experimental Evaluation with Vehicles on the Move by Khandaker Foysal HaqueORCID,Ahmed Abdelgawad,Venkata Prasanth Yanambaka andKumar Yelamarthi *ORCID

(6) Kalman Filter

Image copyright - Estimation of Vehicle Attitude, Acceleration, and Angular Velocity Using Convolutional Neural Network and Dual Extended Kalman Filter

(7) ADAS

Image credit :- Moghadam, Majid Elkaim, Gabriel. (2019). A Hierarchical Architecture for Sequential Decision Making in Autonomous Driving using Deep Reinforcement Learning. by Minseok Ok 1ORCID,Sungsuk Ok 2 andJahng Hyon Park 1,*ORCID

8 References

[1]Chiplet Based Approach for Heterogeneous Processing and Packaging Architectures Gabriel Mounce, Jim Lyke Air Force Research Laboratory 3550 Aberdeen Ave Kirtland AFB, NM 87112 gabriel.mounce.3@us.af.mil , james.lyke.2@us.af.mil Stephen Horan NASA Langley Research Center stephen.j.horan@nasa.gov Wes Powell NASA Goddard Space Flight Center wesley.a.powell@nasa.gov Rich Doyle, Rafi Some Jet Propulsion Laboratory California Institute of Technology richard.j.doyle,rafi.some@jpl.nasa.gov

[2]Characteristics of Battery Management Systems of Electric Vehicles with Consideration of the Active and Passive Cell Balancing Process Muhammad Uzair 1,*, Ghulam Abbas 2 and Saleh Hosain

[3] Implementation of Kalman Filter using VHDL JOLLY BALIYAN1 , ATIIKA AGGARWAL2 , ASHWANI KUMAR3

[4]Architecture, Chip, and Package Co-design Flow for 2.5D IC Design Enabling Heterogeneous IP Reuse Jinwoo Kim, Gauthaman Murali, Heechun Park, Eric Qin, Hyoukjun Kwon, Venkata Chaitanya Krishna Chekuri, Nihar Dasari, Arvind Singh, Minah Lee, Hakki Mert Torun, Kallol Roy, Madhavan Swaminathan, Saibal Mukhopadhyay, Tushar Krishna, and Sung Kyu Lim

[5]V. Agrawal, F. Piednoel, I. Elkanovich, D. Sil and M. Jahan, "Level 4 Autonomous Driving SoC, leveraging chiplet, advanced package and UCIe," 2023 IEEE Symposium on High-Performance Interconnects (HOTI), CA, USA, 2023, pp. 9-14, doi: 10.1109/HOTI59126.2023.00016.

[6]Bo Jiao, Haozhe Zhu, Jinshan Zhang, Shunli Wang, Xiaoyang Kang, Lihua Zhang, Mingyu Wang, and Chixiao Chen. 2021. Computing Utilization Enhancement for Chiplet-based Homogeneous Processing-in-Memory Deep Learning Processors. In Proceedings of the 2021 on Great Lakes Symposium on VLSI (GLSVLSI '21). Association for Computing Machinery, New York, NY, USA, 241–246. https://doi.org/10.1145/3453688.3461499

[7]A TRANSFERABLE APPROACH FOR PARTITIONING MACHINE LEARNING MODELS ON MULTI-CHIP-MODULES Xinfeng Xie 1 2 Prakash Prabhu 1 Ulysse Beaugnon 1 Phitchaya Mangpo Phothilimthana 1 Sudip Roy 1 Azalia Mirhoseini 1 Eugene Brevdo 1 James Laudon 1 Yanqi Zhou 1

[8] https://static.horiba.com/fileadmin/Horiba/Company/Readout/E53/R53E_18_082.pdf

[9]M. Cheah, J. W. Bryans, D. Fowler and S. A. Shaikh, "Threat Intelligence for Bluetooth-Enabled Systems with Automotive Applications: An Empirical Study," in 3rd Workshop on Safety and Security in Vehicles (SSIV): Dependable Systems and Networks Workshop (DSN-W) 2017, Denver, 2017.

[10]M. Tehranipoort and F. Koushanfar, “A Survey of Hardware Trojan Taxonomy and Detection,” IEEE Design and Test of Computers, vol. 27, no. 1, pp. 10-25, 2010.

[11]G. D. Maso-Gentile, A. Bacà, L. Ambrosini, S. Orcioni and M. Conti, “Design of CAN to Bluetooth gateway for a Battery Management System,” in 12th IEEE International Workshop on Intelligent Solutions in Embedded Systems, Ancona, 2015.

[12]https://www.can-cia.org/can-knowledge/can/cybersecurity-for-can/

[13]A. Ganguly et al., ”Interconnects for DNA, Quantum, In Memory, and Optical Computing Insights From a Panel Discussion,” in IEEE Micro, vol. 42, no. 3, pp. 40-49, 1 May-June 2022, doi: 10.1109/MM.2022.3150684.

[14]https://hpcat.seas.gwu.edu/Research06.html

[15]https://www.allaboutcircuits.com/news/innovative-interconnects-the-future-of-chiplet-ba

[16] J. Lan, V. P. Nambiar, R. Sabapathy, M. D. Rotaru and A. T. Do, ”Chiplet-based Architecture Design for Multi-Core Neuromorphic Processor,” 2021 IEEE 23rd Electronics Packaging Technology Conference (EPTC), Singapore, Singapore, 2021, pp. 410-412, doi: 10.1109/EPTC53413.2021.9663898.

[17]https://ieeexplore.ieee.org/abstract/document/5653749/authors#authors

[18]https://ieeexplore.ieee.org/abstract/document/1650228

[19]https://www.mdpi.com/2072-666X/9/6/287

[20]http://www.ncbi.nlm.nih.gov/

[21]https://ijari.org/

[22]https://ecommons.cornell.edu/

[23]https://hdl.handle.net/

[24]https://www.wovo.org/

[25]https://www.bakirlab.gatech.edu/

[26]https://websta.me/