TATA CONSULTANCY SERVICES

Building on belief

33rd Annual INCOSE international symposium

hybrid event

Honolulu, HI, USA
July 15 - 20, 2023

A CASE STUDY ON MIGRATING TOWARDS FUNCTIONALLY SAFE ZONAL ARCHITECTURE USING MBSE

Abstract

The increasing market demands in recent times are driving complexity in machines and their control architectures. To satisfy these demands, their architecture needs frequent updates and up-grades which in turn require significant efforts from architects. This paper presents a case study on **architecture migration** in automotive industry using **Model Based System Engineering (MBSE)** which will lend a helping hand in successfully rearchitecting any complex system.

The Automotive industry is currently undergoing a massive transformation towards software defined vehicles driven by **Connected, Autonomous, Shared and Electrification (C.A.S.E).** This is possible only with the support of a robust and flexible vehicle Electrical and Electronics (EE) architecture. Taking the C.A.S.E driven transformation into consideration, the present domain control architecture is migrating towards zonal architecture.

This paper presents **RAZA (Rearchitecting Approach for Zonal Architecture)** which is based on the INCOSE defined technical process and ISO/IEC/IEEE 15288:2015

Highlights

Topics to be covered

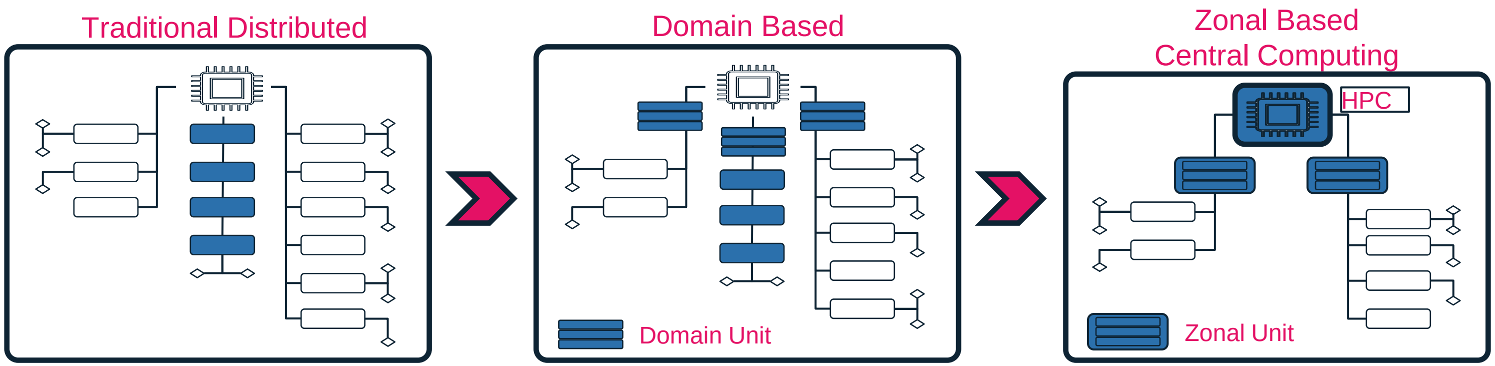
- **A** INTRODUCTION TO ZONAL ARCHITECTURE
- **B** CHALLENGES OF RE-ARCHITECTING
- **C** RAZA DEFINITION AND DEPLOYMENT
- **D** CONCLUSION
- **E** FUTURE WORK AND LIMITATION

A. INTRODUCTION TO ZONAL ARCHITECTURE

Journey towards Next Gen E/E Architecture

E/E Architecture - Evolution

Collaborative
Upgradable
Connected
Updatable
Portable
Security
Fail-safe



Distributed Control
- Collaboration of ECUs with domain
- Domains: Body & Comfort, Chassis, Powertrain, Infotainment
- 3-4 Independent communication networks
- Limited cross domain communication

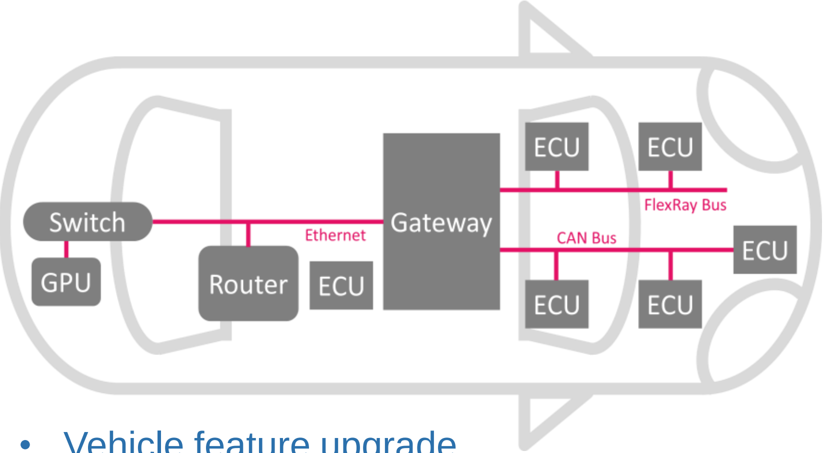
Domain Centralized
- Central domain controller
- Consolidation of functions
- Stronger communication via gateway
- Cross functional communication
- Ability to handle complex functions

Vehicle Centralized
- Virtual domain controller
- Limited dedicated hardware
- Ethernet Communication
- High complexity/computing functions
- Server-based vehicle network

>> 2020 >>2025 | 2020 >> 2025 >> 2030 | 2027 >> 2030 >> 20XX

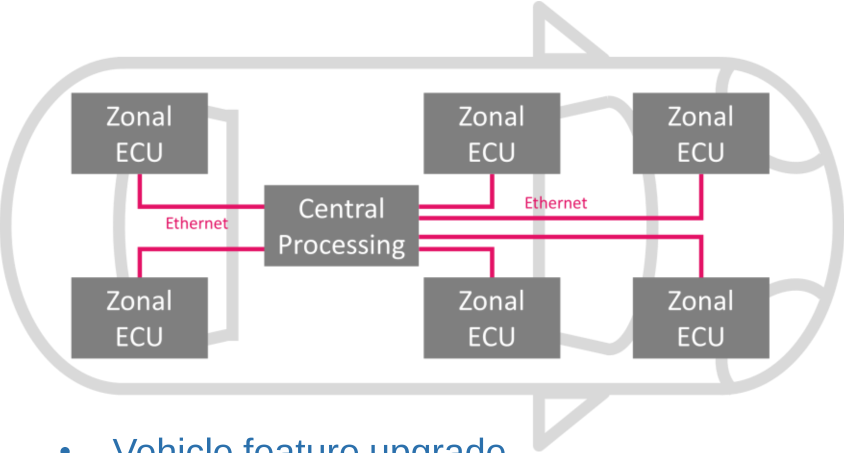
Comparison Legacy and Zonal Architecture

Legacy distributed architecture



- Vehicle feature upgrade
- Legacy software being tightly coupled
- Lack of portability
- The addition of new features increases wiring and thereby complexity of the vehicle system

Zonal architecture



- Vehicle feature upgrade
- Ease of maintenance and repair
- Eases component interchangeability.
- Eases addition of new vehicle feature

B. CHALLENGES OF RE-ARCHITECTING

Challenges of Re-Architecting

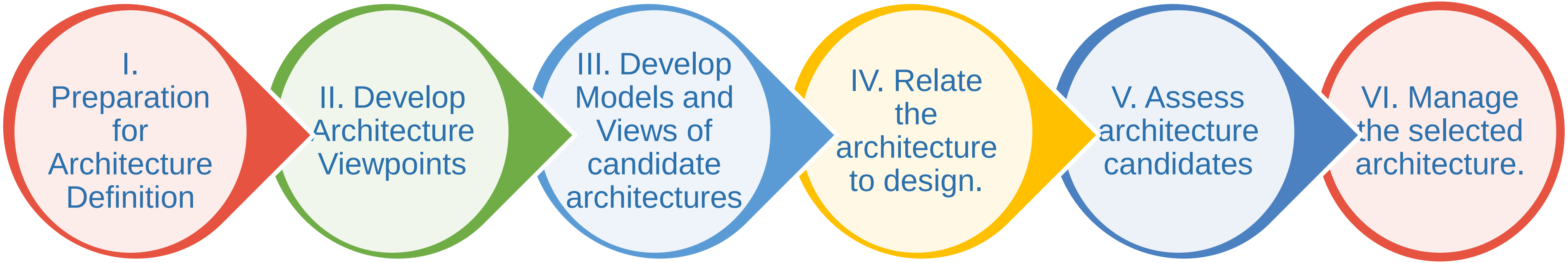
- Consolidation of legacy vehicle features.
- Impact analysis after legacy function distribution on performance of vehicle.
- Reusability of architecture elements.
- Traceability between legacy functions with next generation EE architecture elements.
- Maintaining different variants of same vehicle platform.
- Understanding the interdisciplinary interfaces and dependencies.

C. Defined Approach- RAZA

RAZA (Rearchitecting Approach for Zonal Architecture) approach

- RAZA (Rearchitecting Approach for Zonal Architecture) is
  - MBSE with systematic approach
  - Based on INCOSE system engineering guidelines
  - Implemented using Cameo Systems Modeler 19.0 SP3 tool.
- Deployed on body domain lighting features i.e.
  - Lighting features like Adaptive Head Lamp (AHL),
  - Lock-Unlock, Turn Indicator,
  - Driver Courtesy Lamp,
  - Interior Room Lamp.

RAZA - Steps


I. Preparation for Architecture Definition
II. Develop Architecture Viewpoints
III. Develop Models and Views of candidate architectures
IV. Relate the architecture to design.
V. Assess architecture candidates
VI. Manage the selected architecture.

I. Preparation for Architecture Definition

1. Analyze stakeholder requirements - detailed study of the existing lighting features
2. Analyzing legacy System requirements, safety requirements etc.
3. Decide the strategy and roadmap to re-architecture -
   - Challenges of legacy architecture , fundamentals of zones and central computer
   - Tools and technologies required
   - Merits and Demerits of existing and new architecture
   - Brainstorming on key attributes for ex. Redundancy, Complexity, Robustness, Maintainability, Safety and Security, Reusability of zonal ECUs and central comp
   - Sub-systems which should go for re-architecture

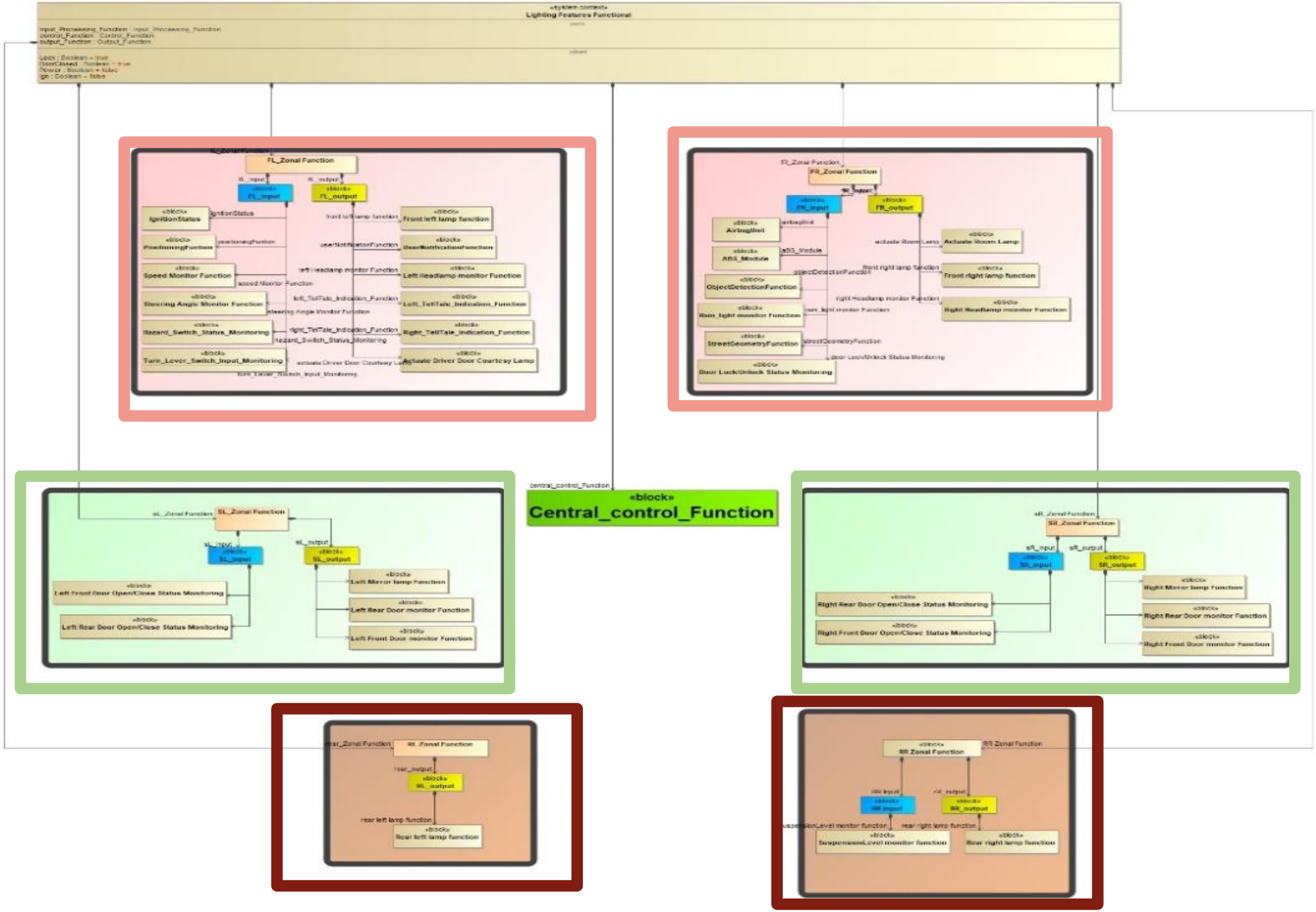
I. Preparation for Architecture Definition

4. Defined and implemented steps for architecture migration
    - Function distribution –
        - Developed consolidated functional architecture
        - Understanding the inputs, outputs, control(complexity of algo, processing bandwidth)
    - Identification of the roles played by sensors, actuators, zonal ECU, and central computer and Interfaces between them.
    - Move selected domain to zonal structural framework and repeat until all domains are completed.
    - Architecture tradeoff and optimization (performance, safety, security, power consumption, weight).

II. DEVELOP ARCHITECTURE VIEWPOINTS

- Primary view of initial architecture of AHL(adaptive head lamp) vehicle feature with
  - Initial distribution of functions to zonal ECU and central computer
  - Study of architecture elements ex. Smart sensors and actuators study
  - Study of Multiple topologies of networking ex: Ring, Start etc.
  - Functional Safety consideration in the architecture
- Discussion with multiple stakeholders i.e., Domain and arch team, Component team, safety team, NW team

Initial Architecture View



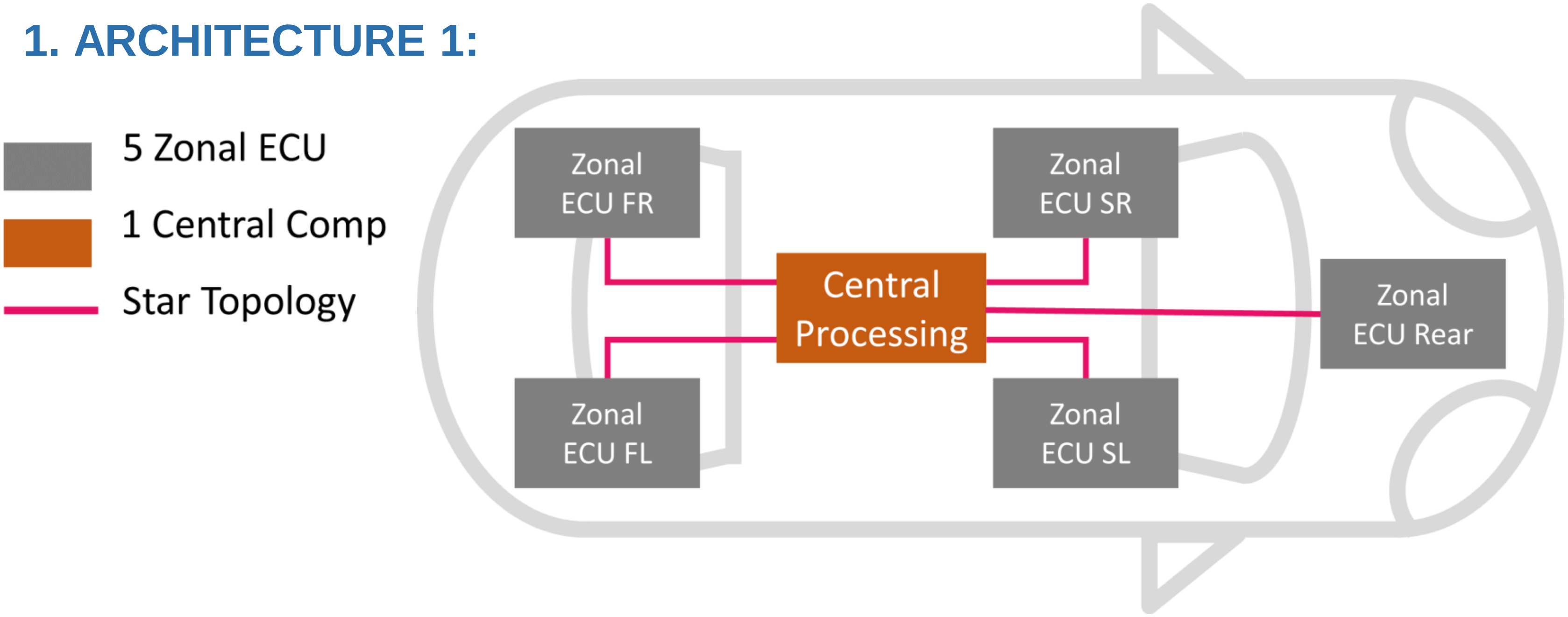
Front Zone

Side zone

Rear Zone

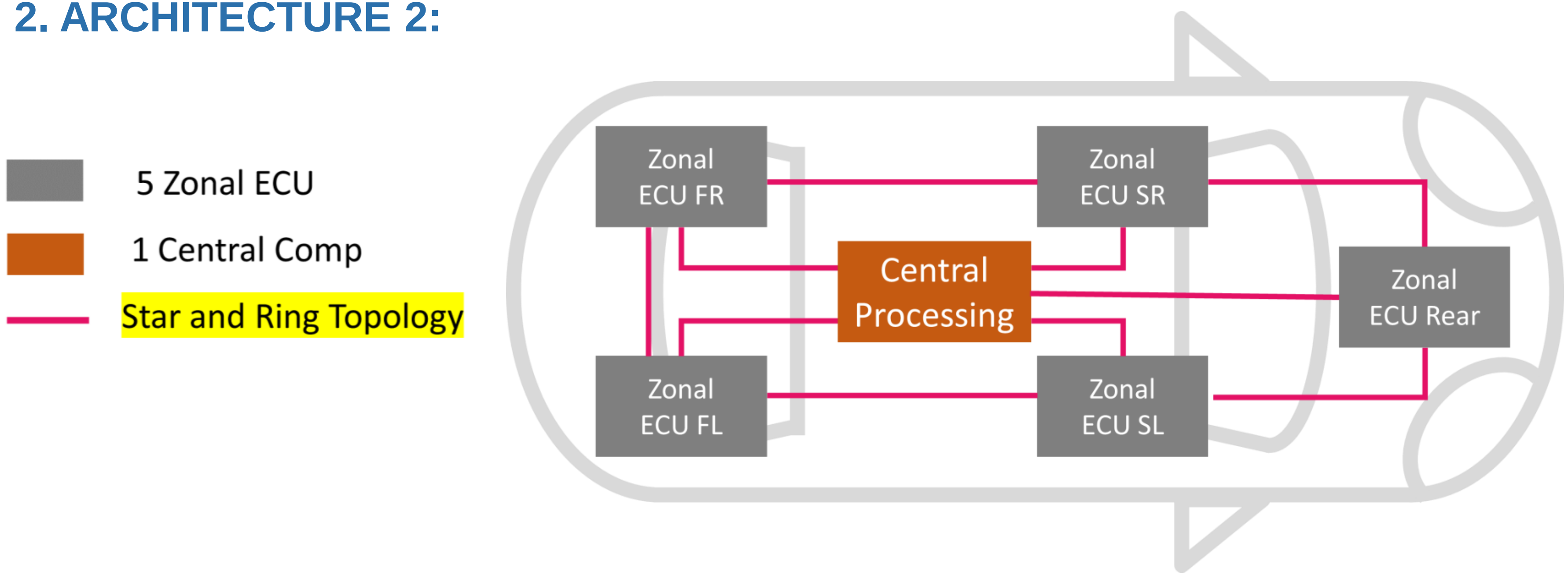
III. DEVELOP MODELS AND VIEWS OF CANDIDATE ARCHITECTURES

1. ARCHITECTURE 1:



III. DEVELOP MODELS AND VIEWS OF CANDIDATE ARCHITECTURES

2. ARCHITECTURE 2:



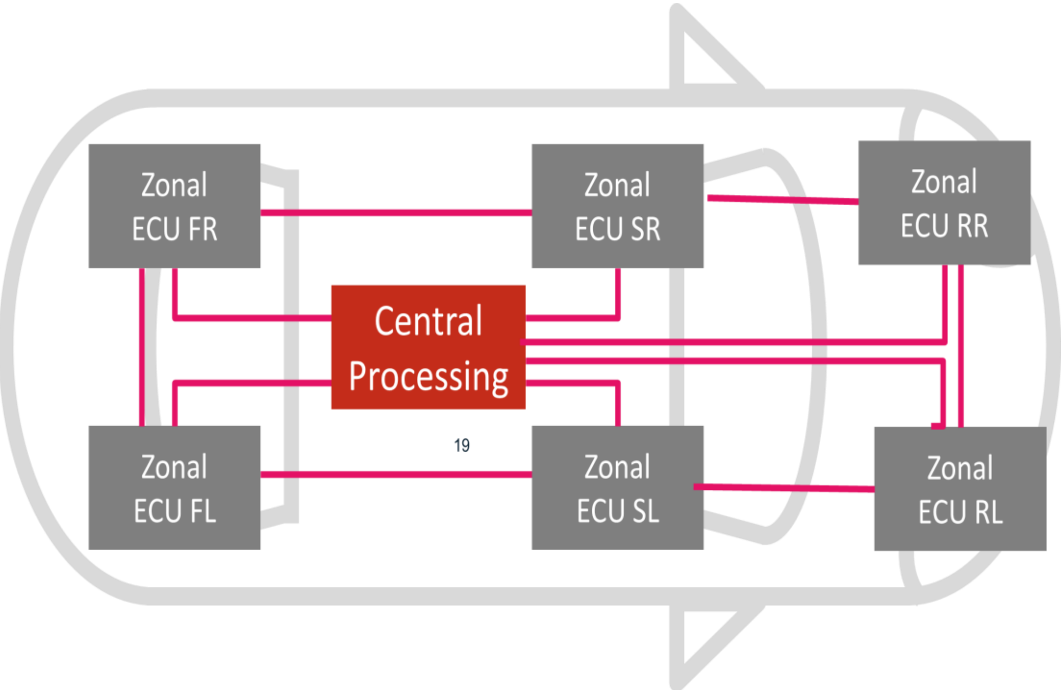
III. DEVELOP MODELS AND VIEWS OF CANDIDATE ARCHITECTURES

3. ARCHITECTURE 3:

6 Zonal ECU

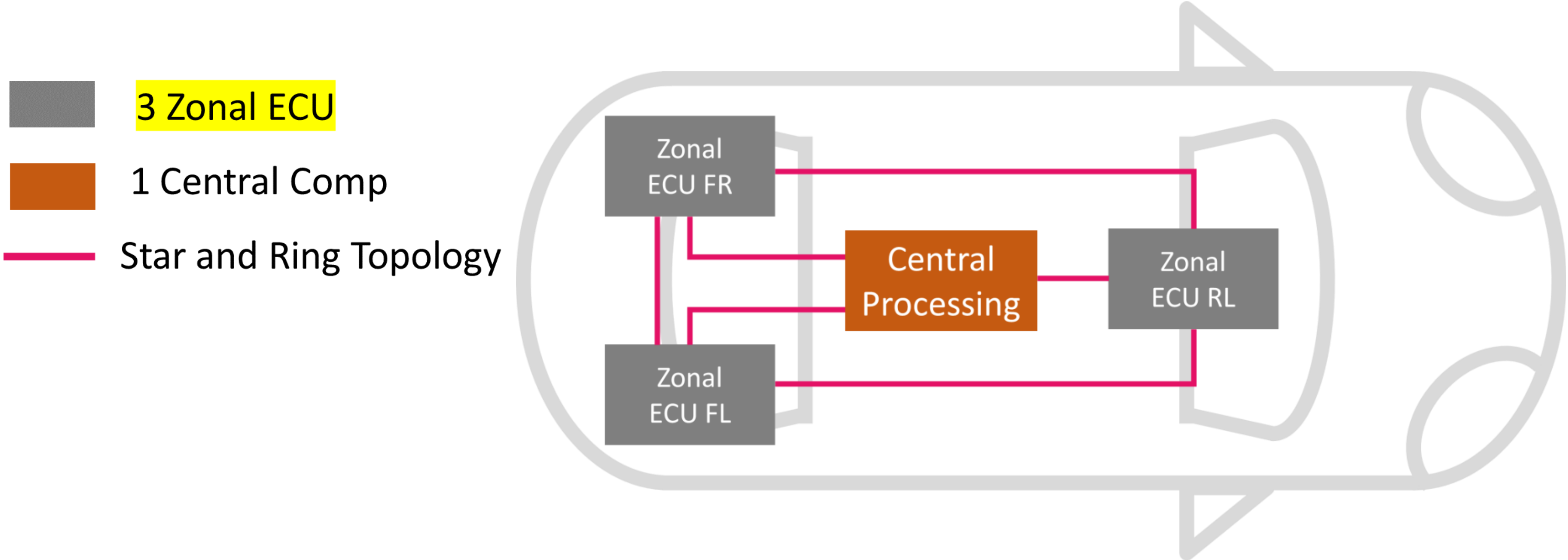
1 Central Comp

Star and Ring Topology



III. DEVELOP MODELS AND VIEWS OF CANDIDATE ARCHITECTURES

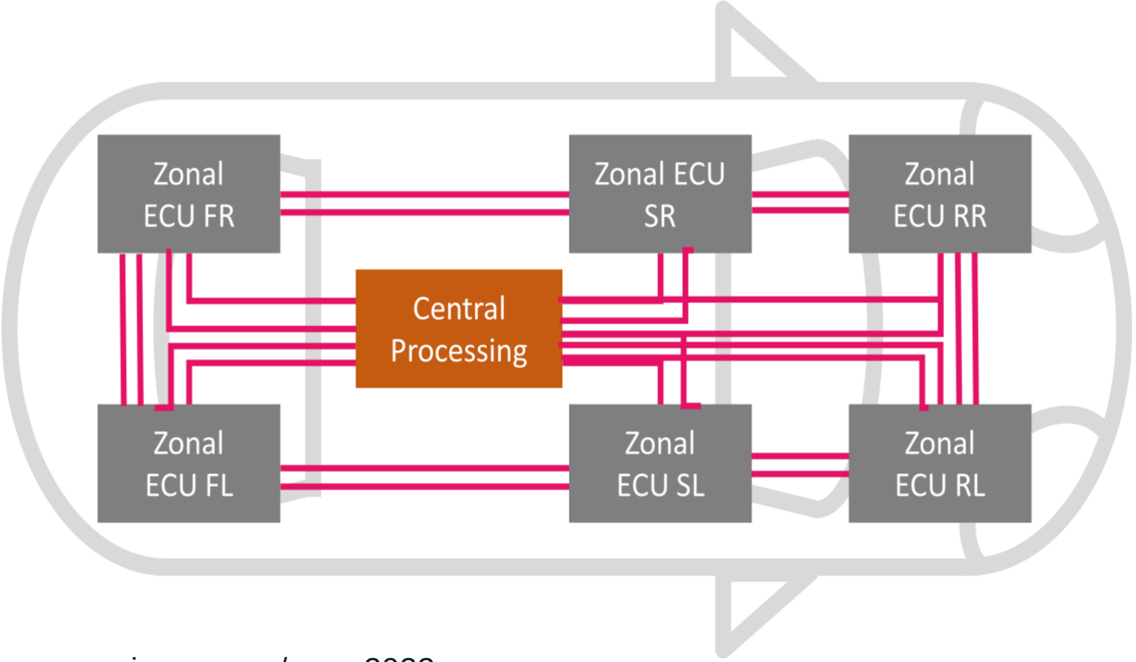
4. ARCHITECTURE 4:



III. DEVELOP MODELS AND VIEWS OF CANDIDATE ARCHITECTURES

5. ARCHITECTURE 5:

- 6 Zonal ECU
- 1 Central Comp
- Double Ring Topology



IV. RELATE THE ARCHITECTURE TO DESIGN:

- Mapping of Sub system elements with components
- System requirements were refined
- Replacing individual legacy actuators with smart actuators wherever it was required
- Defined Interfaces between all Zonal ECU and Central Computer
- Interface Automotive Safety Integrity Level (ASIL) allocation to signals
- Traceability with architecture elements

Delete | Remove From Table | Columns | Show Parts | Export

Criteria

Element Type: Connector ... Context: 04_IBD_System_ICD ... Filter:

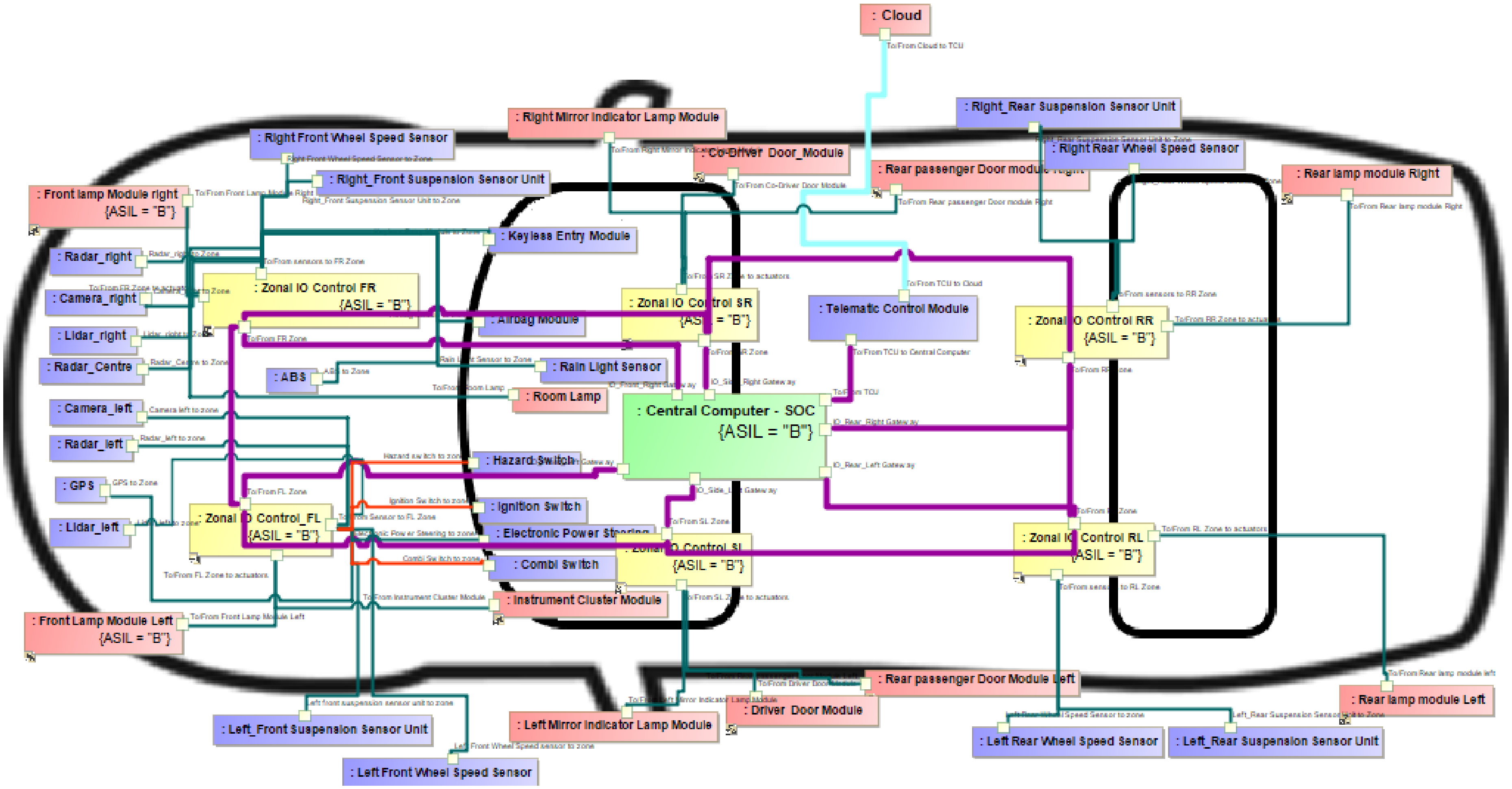
#	Part A	Port A	Item Flow	Port B	Part B	Signal_ASIL
1	: Rain Light Sensor	Rain Light Sensor to Zone	▶ Visibility_data	To/From sensors to FR Zone	: Zonal IO Control FR	+ASIL = B
			▶ Rain_data			+ASIL = QM
			▶ Feedback_Rain_Light_data			+ASIL = B
2	: Combi Switch	Combi Switch to zone	▶ Headlamp_off	To/From Sensor to FL Zone	: Zonal IO Control_FL	+ASIL = QM
			▶ Low beam			+ASIL = QM
			▶ High beam			+ASIL = QM
			▶ indicator_left_up			+ASIL = A
			▶ indicator_right_down			+ASIL = A
			▶ indicator_off			+ASIL = A
3	: Zonal IO Control_FL	To/From FL Zone	▶ Headlamp_off	IO_Front_Left Gateway	: Central Computer	+ASIL = QM
			▶ Low beam			+ASIL = QM
			▶ High beam			+ASIL = QM
			◀ beam_activation_data			+ASIL = B
			◀ selective_beam_activation_data			+ASIL = QM
			◀ horizontal_adjustment_angle_val			+ASIL = QM
			◀ vertical_adjustment_angle_value			+ASIL = QM
			▶ steering_angle			+ASIL = B
			▶ wheel_speed_data			+ASIL = B
			▶ suspension_data			+ASIL = QM
			▶ Camera_data			+ASIL = B
			▶ Radar_object_data			+ASIL = B
			▶ Deceleration_data			+ASIL = QM
			▶ lidar_object_data			+ASIL = B
			▶ GPS_data			+ASIL = A
			▶ ignition_status			+ASIL = A

V. ASSESS ARCHITECTURE CANDIDATES:

- Identification of key decision criteria for ex. portability, safety, modularity, portability, Latency etc.
- Selection of one architecture as a reference architecture
- Architecture evaluation using a qualitative decision matrix and defined criteria.

V. ASSESS ARCHITECTURE CANDIDATES:

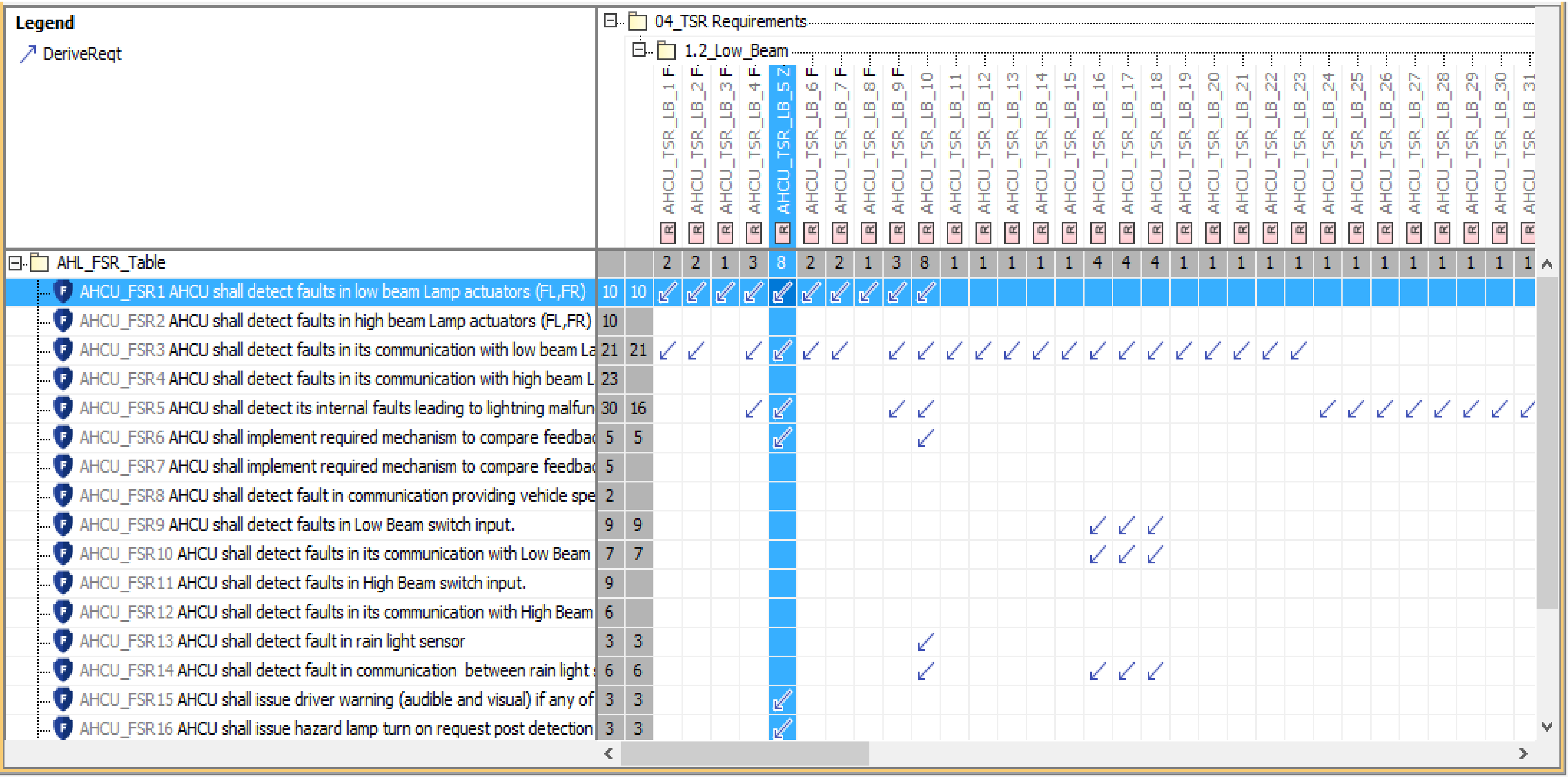
#	Name	ARCH1	ARCH2	ARCH3	ARCH4	ARCH5
1	CAN & ETHERNET COMPARATIVE STU	+	0	0	+	-
2	REUSABILITY OF ZONES AND CENTR	0	0	0	0	0
3	PORTABILTY	0	0	0	0	0
4	MODULARITY	0	0	0	-	0
5	SCALABILITY	0	0	0	0	0
6	FLEXIBILTY	-	-	0	-	0
7	REDUNDANCY	-	0	0	0	+
8	INTERFACES	0	0	0	0	0
9	COMPLEXITY	+	0	0	0	-
10	ROBUSTNESS	-	0	0	0	0
11	MAINTAINABILTY	+	0	0	-	-
12	Safety and Security	-	0	0	0	+
13						
14	Sum of +	3	0	0	1	2
15	Sum of -	4	1	0	3	3
16	Sum of 0	5	11	12	8	7
17	Netscore ((Sum of +) - (Sum of -))	-1	-1	0	-2	-1
18	Rank	2	2	1	3	2



: Cloud
: Right Mirror Indicator Lamp Module
: Right_Rear Suspension Sensor Unit
: Right Front Wheel Speed Sensor
: Co-Driver Door_Module
: Right Rear Wheel Speed Sensor
: Rear passenger Door module Right
: Rear lamp module Right
: Front lamp Module right {ASIL = "B"}
: Right_Front Suspension Sensor Unit
: Keyless Entry Module
: Radar_right
: Zonal IO Control FR {ASIL = "B"}
: Camera_right
: Airbag Module
: Telematic Control Module
: Zonal IO Control RR {ASIL = "B"}
: Lidar_right
: Radar_Centre
: ABS
: Rain Light Sensor
: Room Lamp
: Camera_left
: Central Computer - SOC {ASIL = "B"}
: Radar_left
: Hazard Switch
: GPS
: Ignition Switch
: Lidar_left
: Zonal IO Control_FL {ASIL = "B"}
: Electronic Power Steering
: Zonal IO Control RL {ASIL = "B"}
: Combi Switch
: Instrument Cluster Module
: Front Lamp Module Left {ASIL = "B"}
: Rear passenger Door Module Left
: Rear lamp module Left
: Driver Door Module
: Left Mirror Indicator Lamp Module
: Left_Front Suspension Sensor Unit
: Left Rear Wheel Speed Sensor
: Left_Rear Suspension Sensor Unit
: Left Front Wheel Speed Sensor

VI. MANAGE THE SELECTED ARCHITECTURE

- Refinement of
  - System and sub-system requirements
  - Technical safety requirements (TSR)
  - Architecture
- End to end traceability
- Reviews with relevant stakeholders and domain experts


Legend
DeriveReqt
04_TSR Requirements
1.2_Low_Beam
AHCU_TSR_LB_1 F
AHCU_TSR_LB_2 F
AHCU_TSR_LB_3 F
AHCU_TSR_LB_4 F
AHCU_TSR_LB_5 Z
AHCU_TSR_LB_6 F
AHCU_TSR_LB_7 F
AHCU_TSR_LB_8 F
AHCU_TSR_LB_9 F
AHCU_TSR_LB_10
AHCU_TSR_LB_11
AHCU_TSR_LB_12
AHCU_TSR_LB_13
AHCU_TSR_LB_14
AHCU_TSR_LB_15
AHCU_TSR_LB_16
AHCU_TSR_LB_17
AHCU_TSR_LB_18
AHCU_TSR_LB_19
AHCU_TSR_LB_20
AHCU_TSR_LB_21
AHCU_TSR_LB_22
AHCU_TSR_LB_23
AHCU_TSR_LB_24
AHCU_TSR_LB_25
AHCU_TSR_LB_26
AHCU_TSR_LB_27
AHCU_TSR_LB_28
AHCU_TSR_LB_29
AHCU_TSR_LB_30
AHCU_TSR_LB_31
AHL_FSR_Table
2 2 1 3 8 2 2 1 3 8 1 1 1 1 1 4 4 4 1 1 1 1 1 1 1 1 1 1 1 1 1
AHCU_FSR1 AHCU shall detect faults in low beam Lamp actuators (FL,FR) 10 10
AHCU_FSR2 AHCU shall detect faults in high beam Lamp actuators (FL,FR) 10
AHCU_FSR3 AHCU shall detect faults in its communication with low beam La 21 21
AHCU_FSR4 AHCU shall detect faults in its communication with high beam L 23
AHCU_FSR5 AHCU shall detect its internal faults leading to lightning malfun 30 16
AHCU_FSR6 AHCU shall implement required mechanism to compare feedbac 5 5
AHCU_FSR7 AHCU shall implement required mechanism to compare feedbac 5
AHCU_FSR8 AHCU shall detect fault in communication providing vehicle spe 2
AHCU_FSR9 AHCU shall detect faults in Low Beam switch input. 9 9
AHCU_FSR10 AHCU shall detect faults in its communication with Low Beam 7 7
AHCU_FSR11 AHCU shall detect faults in High Beam switch input. 9
AHCU_FSR12 AHCU shall detect faults in its communication with High Beam 6
AHCU_FSR13 AHCU shall detect fault in rain light sensor 3 3
AHCU_FSR14 AHCU shall detect fault in communication between rain light 6 6
AHCU_FSR15 AHCU shall issue driver warning (audible and visual) if any of 3 3
AHCU_FSR16 AHCU shall issue hazard lamp turn on request post detection 3 3

D. CONCLUSION

Advantages of RAZA approach

- Better visualization of functional redistribution

- Impact analysis

- Easy cross functional team interactions
- Single central knowledge base

- Faster design and tradeoff analysis
- Reduction of development time

E. FUTURE WORK AND LIMITATION

Future scope –RAZA deployment

- Deployment in multiple integrated domains.
- Use of formal methods for trade study
- Formal analysis method to know the number of HPCs required, their performance and safety characteristics when integrated
- Simulating and early validation of
  - The appropriate portioning of functionalities in the HPC for optimal performance and safety goals.
  - Variant management of features and its various permutation and combinations in a single vehicle platform.
  - Network bandwidth and its performance and safety assessment when loaded with actual real time sensor and actuator data.
- Incorporation of SOA (Service Oriented Architecture)

33rd Annual INCOSE international symposium

hybrid event

Honolulu, HI, USA
July 15 - 20, 2023

www.incose.org/symp2023
#INCOSEIS