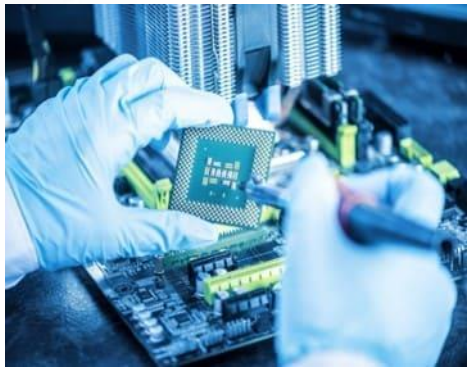
TESSOLVE

A HERO ELECTRONIX VENTURE

Refining ISO 26262 Practices by adopting GenAI ✨

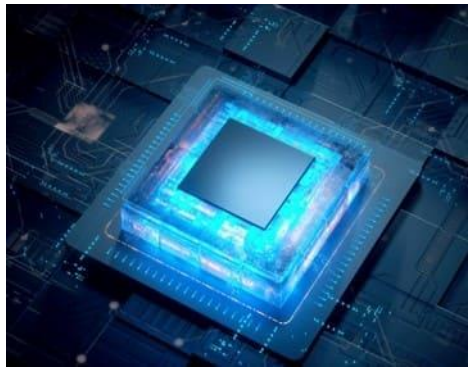
Mike Bartley, SVP, CoE | Marmik Soni, Lead, CoE

Chip Design



Test Engineering

Hardware Design

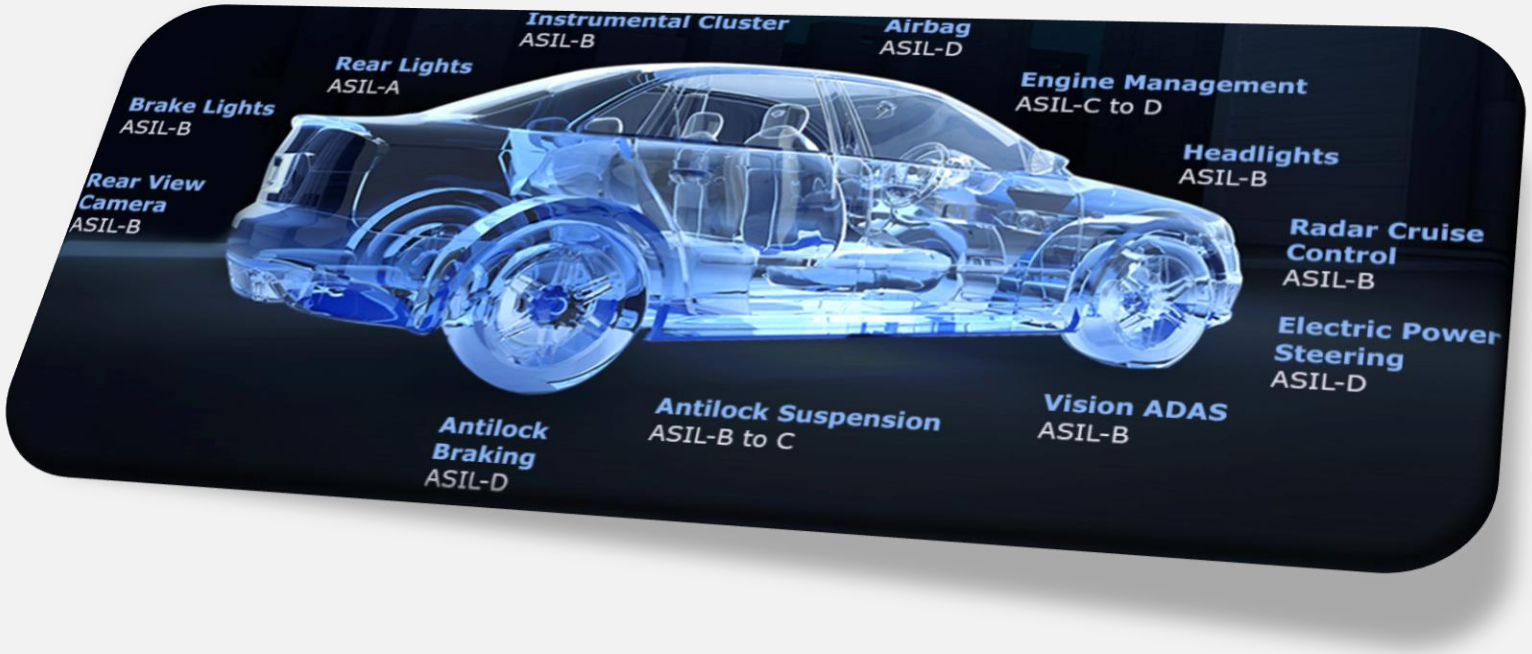


Embedded Systems

Ver0.1MS

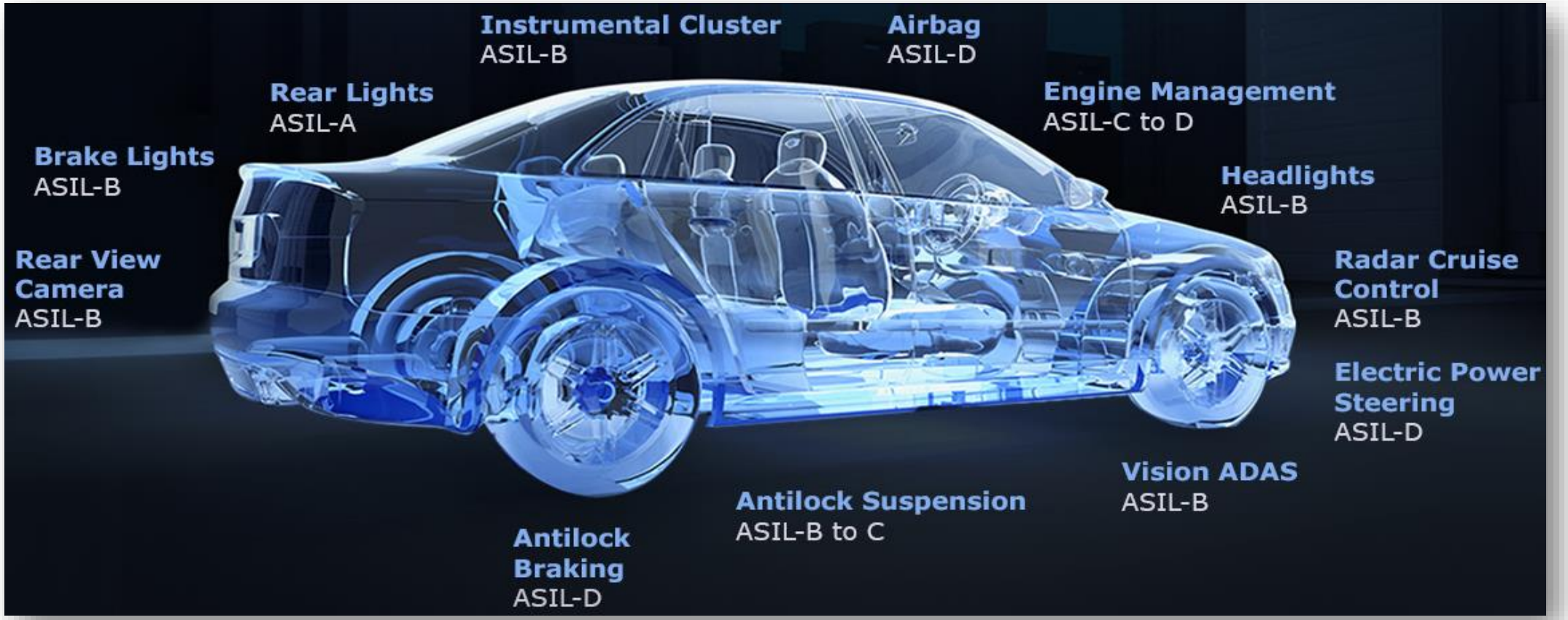
Outline

- ISO26262 – Automotive Functional Safety
- Challenges
- AI Strategy
- AI – Automation in DV
- AI Roles
- FuSa key steps
- Use cases
- Caution & Path Forward



ISO26262 – Automotive Functional Safety

- ISO 26262 is an international standard for the functional safety of electrical and electronic systems in production automobiles.
- A framework to ensure that safety-related systems perform reliably and safely throughout their lifecycle.



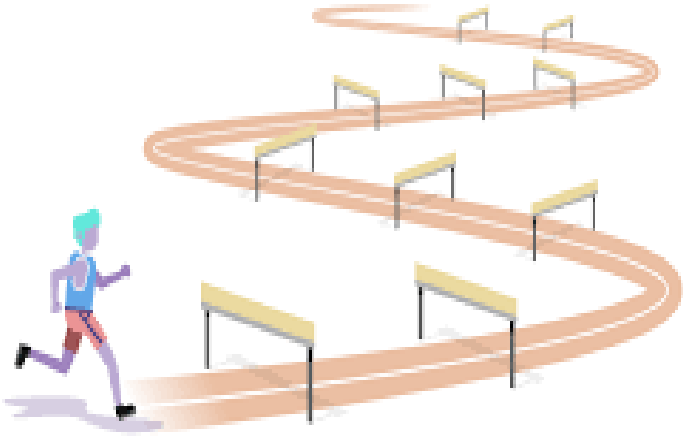
1

Challenges

Lack of Awareness
- Insufficient training and education
- Potential for critical safety aspects and increased accident risks.

Complex and Time Consuming
- Extensive documentation, testing, and validation processes
- Changes and unforeseen issues in design
- Requires robust project management practices
- Efficient planning and automated tools can help streamline these processes especially (e. g. Requirement management, traceability etc.)

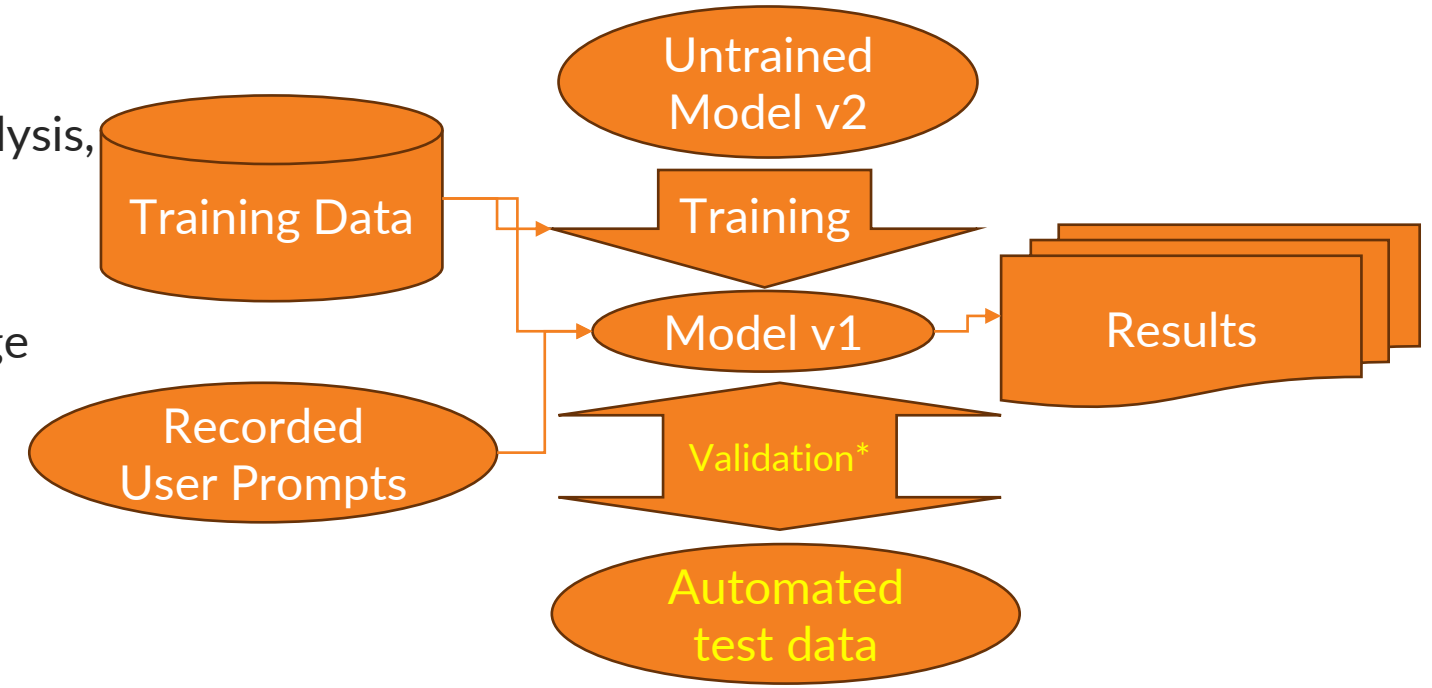
Resource Scarcity (30% Lack in Next Two Years)[2]
- Growing demand for skilled professionals outpaces supply
- Increased project costs and delays, with potential compromises in safety
- Need to leverage automation and AI technologies to help



AI Strategy

Features:

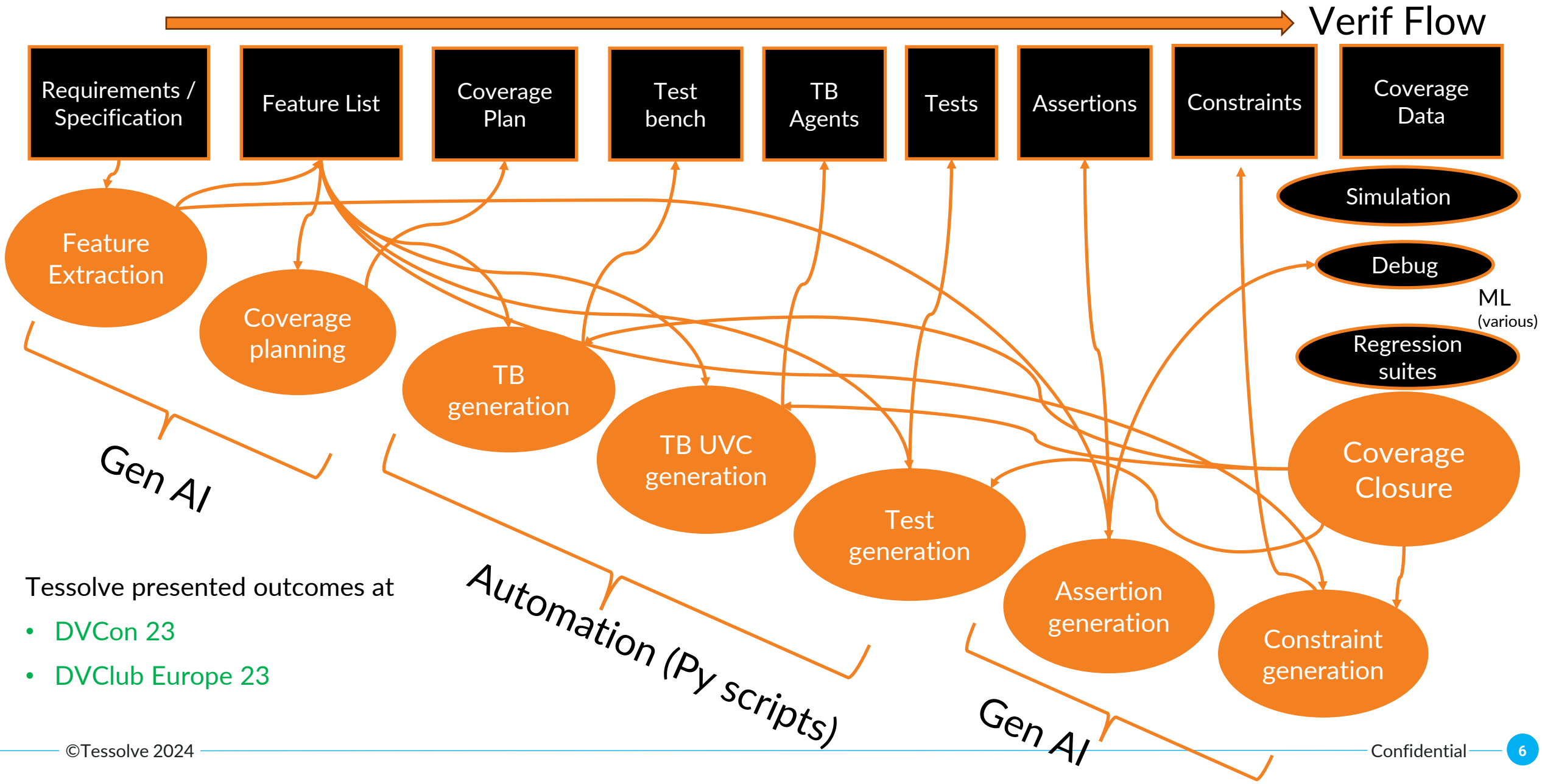
- Preserved training data
- Preserved prompts
- Model selection & upgrades
  (for conversational, coding assistance, analysis, computational needs)
- Response validation
- Migration to AI agents
- Needs and security-based AI solution range



Currently validation is manual*

AI Automation in DV PDF Spec to Test cases

TESSOLVE
A HERO ELECTRONIX VENTURE



Tessolve presented outcomes at

- DVCon 23
- DVClub Europe 23

AI Roles

- Tasks on behalf of tools
- Supportive assistant (Copilot)
- Human like support
- Tools, e.g., **Car Digital Twin** for owner and vendor

DV Flow	Training bots	Process	Quality	Predictive diagnosis
• Spec analysis • Feature extraction • Test plan components • Simple assertions	• Helping new engineers to adapt to FuSa with terminologies, QnA, Definitions, Summary etc.	• HARA • Requirement Management, • Safety Analysis • ASIL • Traceability • Briefing on IP, SoC • Design specs	• Quality assistance bots for VLSI, Test processes, guidelines, recommendation	• Digital twin of car for customer & service station

Spec Analysis

Specification

Signal Name	I/O	Description
DIN[N:0]	Input	Data Input
WR_EN	Input	Write Enable (request)
WR_ACK	Output	Write Acknowledge: Handshake signal indicates successful write operation
WR_ERR	Output	Write Error: Handshake signal indicates unsuccessful write operation
RD_EN	Input	Read Enable (request)
RD_ACK	Output	Read Acknowledge: Handshake signal indicates successful read operation
RD_ERR	Output	Read Error: Handshake signal indicates unsuccessful read operation
CLK	Input	Clock for read and write operations
SINIT	Input	Synchronous initialization of all FIFO functions, flags, and pointers
DOUT[N:0]	Output	Data Output
FULL	Output	Full Flag: Indicates that no additional writes can be performed
EMPTY	Output	Empty Flag: Indicates that no data is present
DATA_COUNT[C:0]	Output	Data Count: Vector

Features to be Verified:

Data Read and Write Operations:

Verify that data presented at the data-input port (DIN) is correctly written into the FIFO on a rising clock edge when the write-enable input (WR_EN) is high.

Verify that data can be read out of the FIFO via the data-output port (DOUT) in the order it was written by asserting read-enable (RD_EN) prior to a rising clock edge.

Status Flags:

Verify the behavior of the memory-full status output (FULL) to indicate when no more empty locations are available in the internal memory.

Verify the behavior of the memory-empty status output (EMPTY) to indicate when no more data resides in the internal memory.

Invalid Request Handling:

Verify that the FIFO status is not corrupted by invalid read or write requests.

.....

Spec Analysis for Feature Extraction ✨

TESSOLVE
A HERO ELECTRONIX VENTURE

The textra32 register is used to configure additional trigger functionalities for RV32 systems, enhancing the debugging capabilities by providing extra control over trigger conditions.

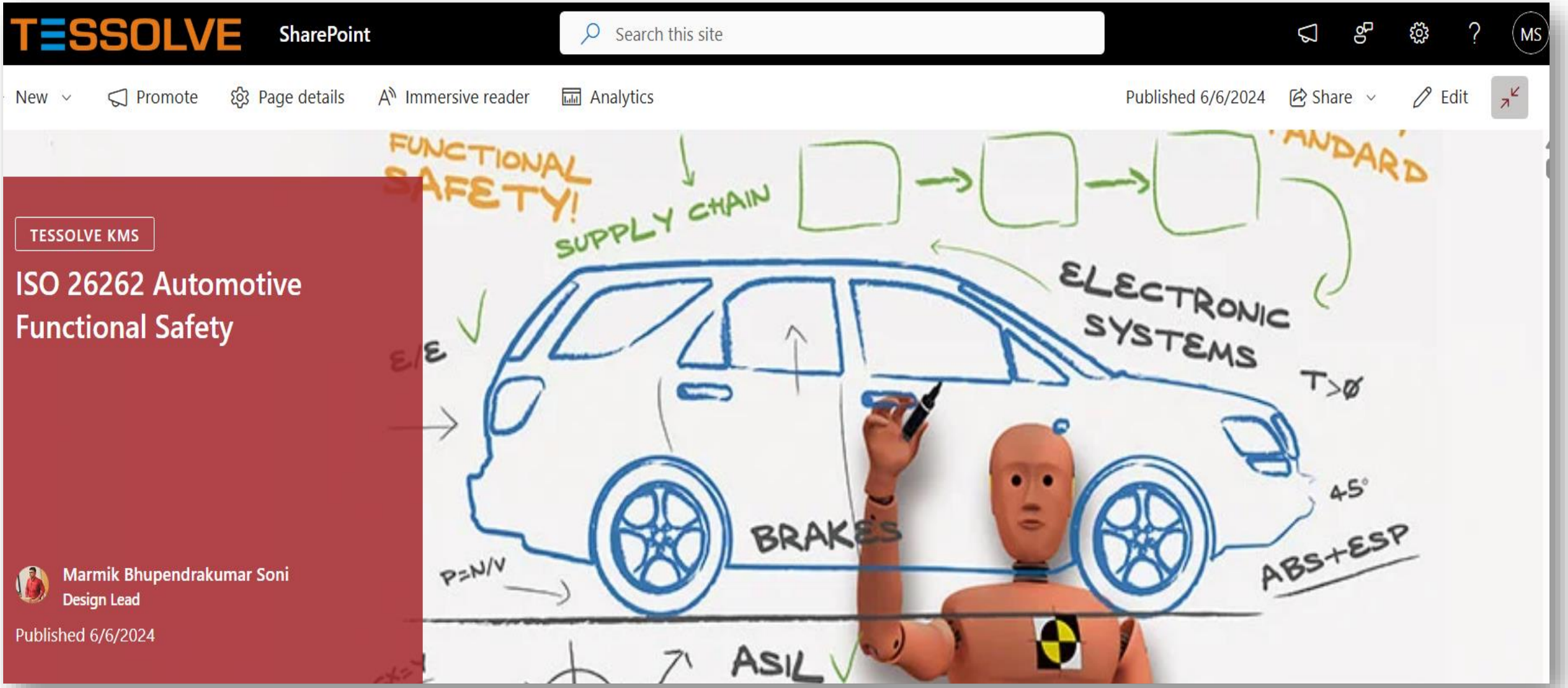
ID	Requirement	Description
1	Extra Trigger Setup	The **textra32** register must be configured to specify additional trigger conditions.
2	Trigger Condition Detection	The Debug Module must detect the specified additional trigger conditions.
3	Hart Response to Trigger	Upon detecting the specified trigger condition, the hart must enter Debug Mode.
4	Trigger Handling	The trigger condition should be handled in a way that allows the hart to transition into Debug Mode seamlessly.
5	Debug Mode Entry	The hart must enter Debug Mode upon the occurrence of the specified trigger condition.
6	Cause Update	The cause of entering Debug Mode due to the trigger condition should be updated in the Debug Control and Status Register (dcsr).

The textra64 register is used to configure additional trigger functionalities for RV64 systems, enhancing the debugging capabilities by providing extra control over trigger conditions

ID	Requirement	Description
1	Extra Trigger Setup	The **textra64** register must be configured to specify additional trigger conditions.
2	Trigger Condition Detection	The Debug Module must detect the specified additional trigger conditions.
3	Hart Response to Trigger	Upon detecting the specified trigger condition, the hart must enter Debug Mode.
4	Trigger Handling	The trigger condition should be handled in a way that allows the hart to transition into Debug Mode seamlessly.
5	Debug Mode Entry	The hart must enter Debug Mode upon the occurrence of the specified trigger condition.
6	Cause Update	The cause of entering Debug Mode due to the trigger condition should be updated in the Debug Control and Status Register (dcsr).

Use case - FUSA AI Center

TESSOLVE
A HERO ELECTRONIX VENTURE



ASIL

ASIL: Automotive Safety Integrity Level

- **Risk Classification system** defined by the ISO26262 standard for the functional safety of road vehicles
- Defines probability and acceptability of harm
- Makes it easy to understand and establish safety requirement, processes and components compliance

		Probability class	Controllability class		
			C1	C2	C3
Severity class	S1	E1	QM	QM	QM
		E2	QM	QM	QM
		E3	QM	QM	A
		E4	QM	A	B
	S2	E1	QM	QM	QM
		E2	QM	QM	A
		E3	QM	A	B
		E4	A	B	C
	S3	E1	QM	QM	A
		E2	QM	A	B
		E3	A	B	C
		E4	B	C	D

Use case - ASIL Determination ✨

TESSOLVE
A HERO ELECTRONIX VENTURE

Tessolve FUSA AI Expert

Do the ASIL determination for brake failure and give answer in table when, car is on express way, night, raining road, and speed is 120KMPH.

Certainly! Here is the ASIL determination for brake failure under the specified conditions in table format:

Criteria	Description	Rating
Severity (S)	Life-threatening injuries (survival uncertain), fatal injuries	S3
Exposure (E)	High probability (driving on expressway at night in rain increases hazard likelihood)	E4
Controllability (C)	Difficult to control or uncontrollable (high speed, poor visibility, and slippery roads)	C3

ASIL Calculation

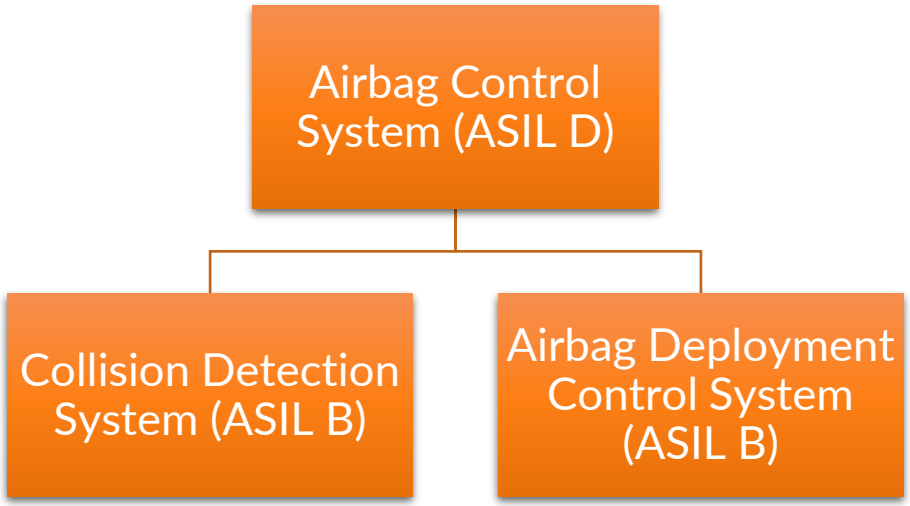
Severity (S)	Exposure (E)	Controllability (C)	ASIL Level
S3	E4	C3	ASIL D

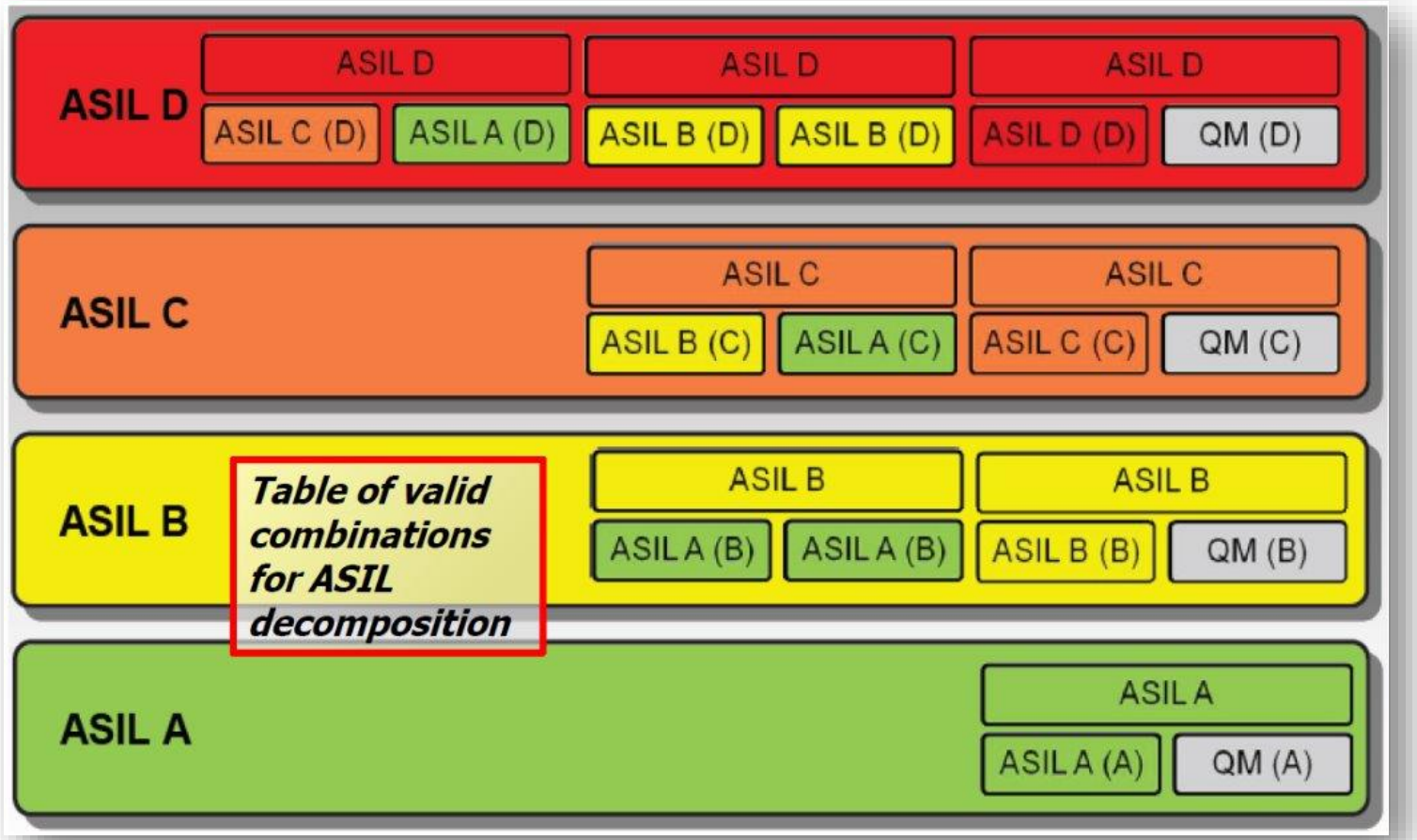
		Probability class	Controllability class C1	C2	C3
Severity class	S1	E1	QM	QM	QM
		E2	QM	QM	QM
		E3	QM	QM	A
		E4	QM	A	B
	S2	E1	QM	QM	QM
		E2	QM	QM	A
		E3	QM	A	B
		E4	A	B	C
	S3	E1	QM	QM	A
		E2	QM	A	B
		E3	A	B	C
		E4	B	C	D

ASIL Decomposition

ASIL decomposition allows the distribution of safety requirements across multiple redundant components or subsystems. This approach helps in managing and reducing the complexity and cost of achieving high safety levels for automotive systems. Here's how it works and its importance:

Example:
Airbag Controller System (ASIL D)





Use case - ASIL Decomposition ✨

TESSOLVE
A HERO ELECTRONIX VENTURE

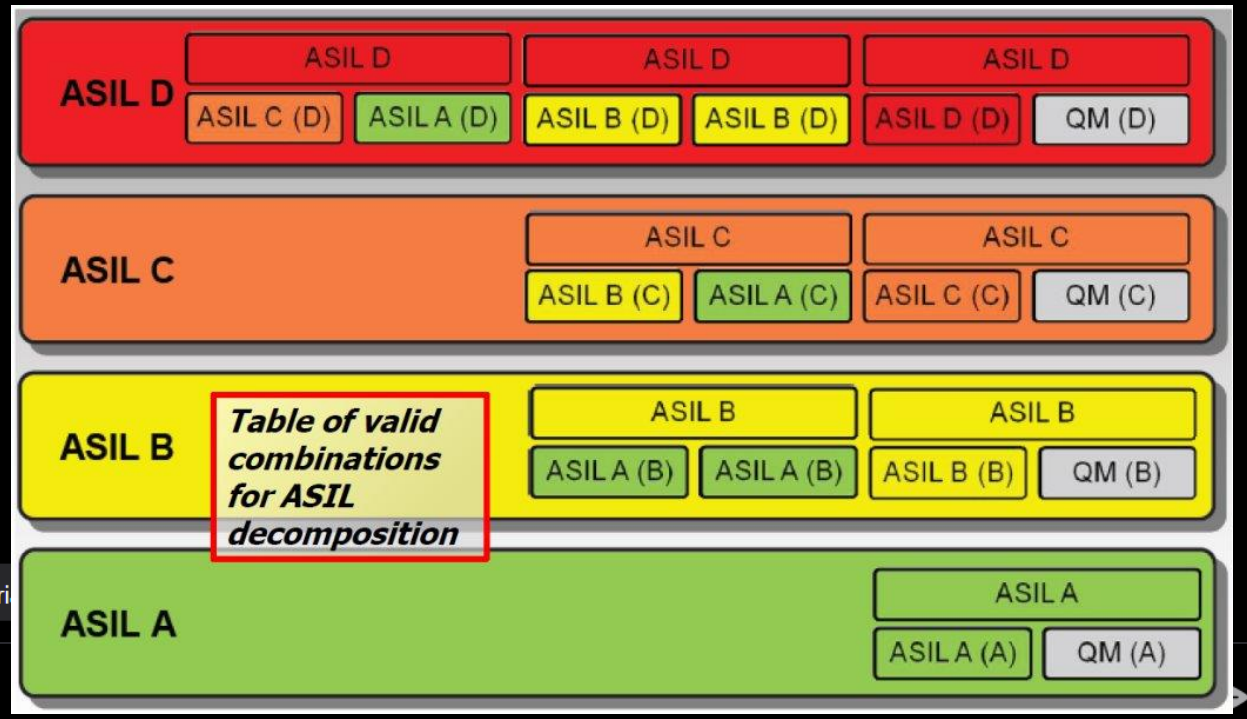
Tessolve FUSA AI Expert

In summary, ASIL decomposition is a strategic approach to balancing safety, cost, and design flexibility within automotive functional safety standards.

What are 3 main advantages of ASIL decomposition. Explain each point in 1 line.

Certainly! Here are three main advantages of ASIL decomposition, each explained in one line:

1. **Cost Reduction**: It allows the use of less expensive components by lowering the ASIL requirements for individual parts.
2. **Safety Enhancement**: By creating redundant systems, it improves overall safety through fault tolerance.
3. **Design Flexibility**: It provides greater flexibility in design, enabling the integration of diverse technologies and existing components.



What is ASIL? | What is Functional Safety? | What is the need of ASIL decomposition? | What are the criteri

Ask your question here..

HARA

- Identify malfunctions that could lead to hazards
- Analyze relevant risks of hazards, and to formulate safety goals
- The determination of ASIL and Safety Requirements

Severity (S)	Class			
	S0	S1	S2	S3
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain)

(a)

Exposure Probability (E)	Class				
	E0	E1	E2	E3	E4
Description	Incredible	Very low probability	Low probability	Medium probability	High Probability

(b)

Controllability (C)	Class			
	C0	C1	C2	C3
Description	Controllable in general	Simply controllable	Normally Controllable	Difficult to control or uncontrollable

(c)

HARA

ID	Function/ Output	Guideword	Hazard	Situation	Hazardous event	Person at risk	S	E	C	ASIL	Safety Goal	Safety Goal ID
EB-H1	Function : engine/ Exhaust brake	Commission of engine brake	Unwanted engine brake torque is applied sponta neously	Driving on a curved, wet road with speed > 60km/h	The engine brake is applied, locking the wheels when driving on a curved , wet road	Occupants of subject vehicle	S3	E3	C3	C	Unwanted engine braking shall not occur (ASIL C)	EB-SG1

SG ID	FSR ID	FSR Description	ASIL
SG1	FSR1.1	The state of the EB outputs/actuators shall be monitored for unwanted behavior	C
	FSR1.2	The MCU shall disable the EB actuators if unwanted behavior is detected	C
	FSR1.3	Input signals to the EB application software shall either represent the actual state of the sensors or convey an error message	C
	FSR1.4	The EB application software shall, based on inputs, calculate the correct desired state of the EB	C
	FSR1.5	The microcontroller's internal data paths shall be covered by the safety mechanisms	C
	FSR1.6	A mechanism shall be available that monitors the MCU supply voltage	C
	FSR1.7	The MCU shall be monitored by a watchdog	C
	FSR1.8	The MCU shall be supervised by an error monitor	C
	FSR1.9	A safe state control mechanism shall be available	C

Use case - HARA

TESSOLVE
A HERO ELECTRONIX VENTURE

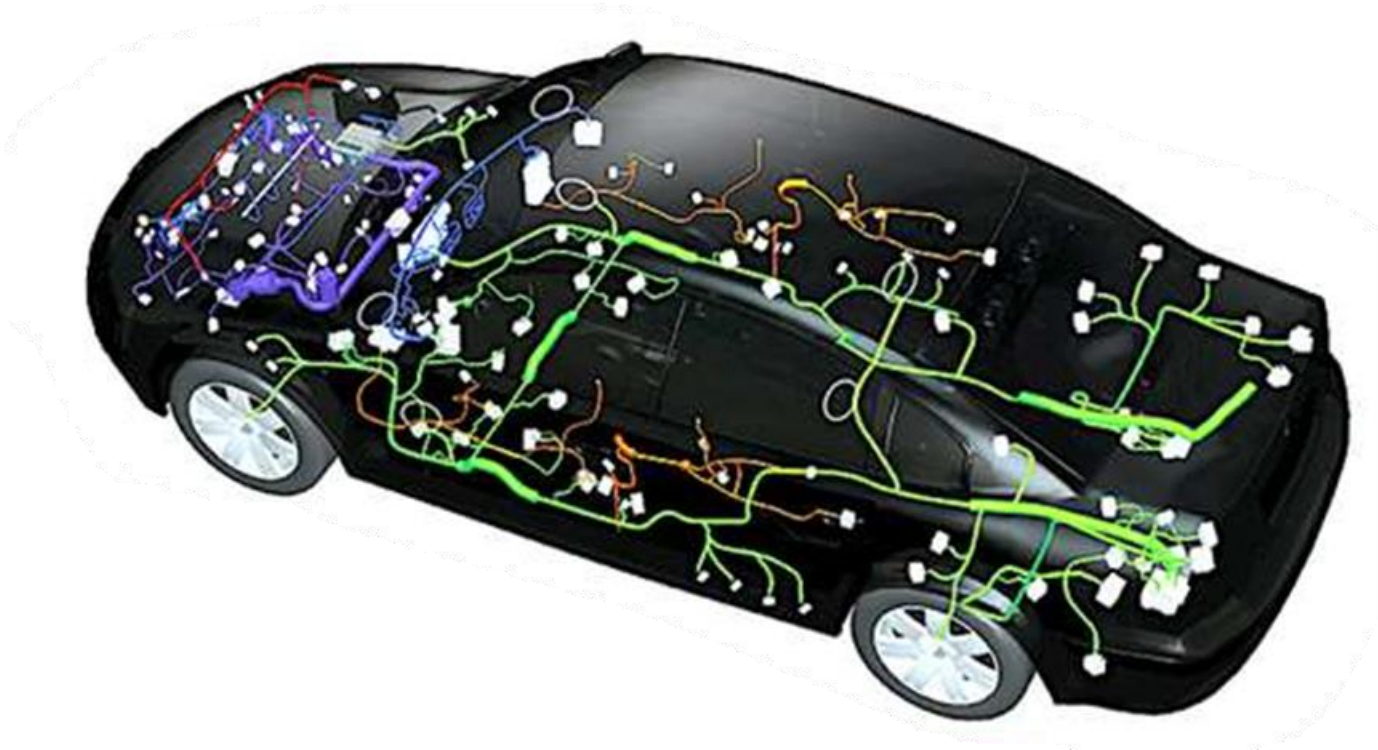
Hazard ID	Hazard Description	Severity (S)	Exposure (E)	Controllability (C)	ASIL	Safety Goal (SG)	Safety Measure (SM)
H1	Both headlights fail simultaneously	S3	E3	C3	ASIL C	SG1: Ensure both headlights do not fail simultaneously	SM1: Use redundant power supplies and control circuits. Design the headlight system with dual independent circuits.
H2	One headlight fails	S2	E3	C2	ASIL B	SG2: Ensure at least one headlight remains operational if the other fails	SM2: Implement diagnostic checks that can isolate a failed headlight and ensure the other continues to function.
H3	Headlights fail to switch to low beam from high beam	S2	E3	C2	ASIL B	SG3: Ensure proper switching between high and low beam	SM3: Use reliable sensors and control algorithms to manage the switching of beams based on real-time data. Employ adaptive lighting systems that respond to oncoming traffic and environmental conditions.
H4	Headlights do not turn on automatically in low light conditions	S3	E2	C2	ASIL B	SG4: Ensure automatic activation of headlights in low light conditions	SM4: Incorporate ambient light sensors and fail-safes to activate headlights when low light conditions are detected. Regularly test and calibrate sensors.

Safety Mechanism

TESSOLVE
A HERO ELECTRONIX VENTURE

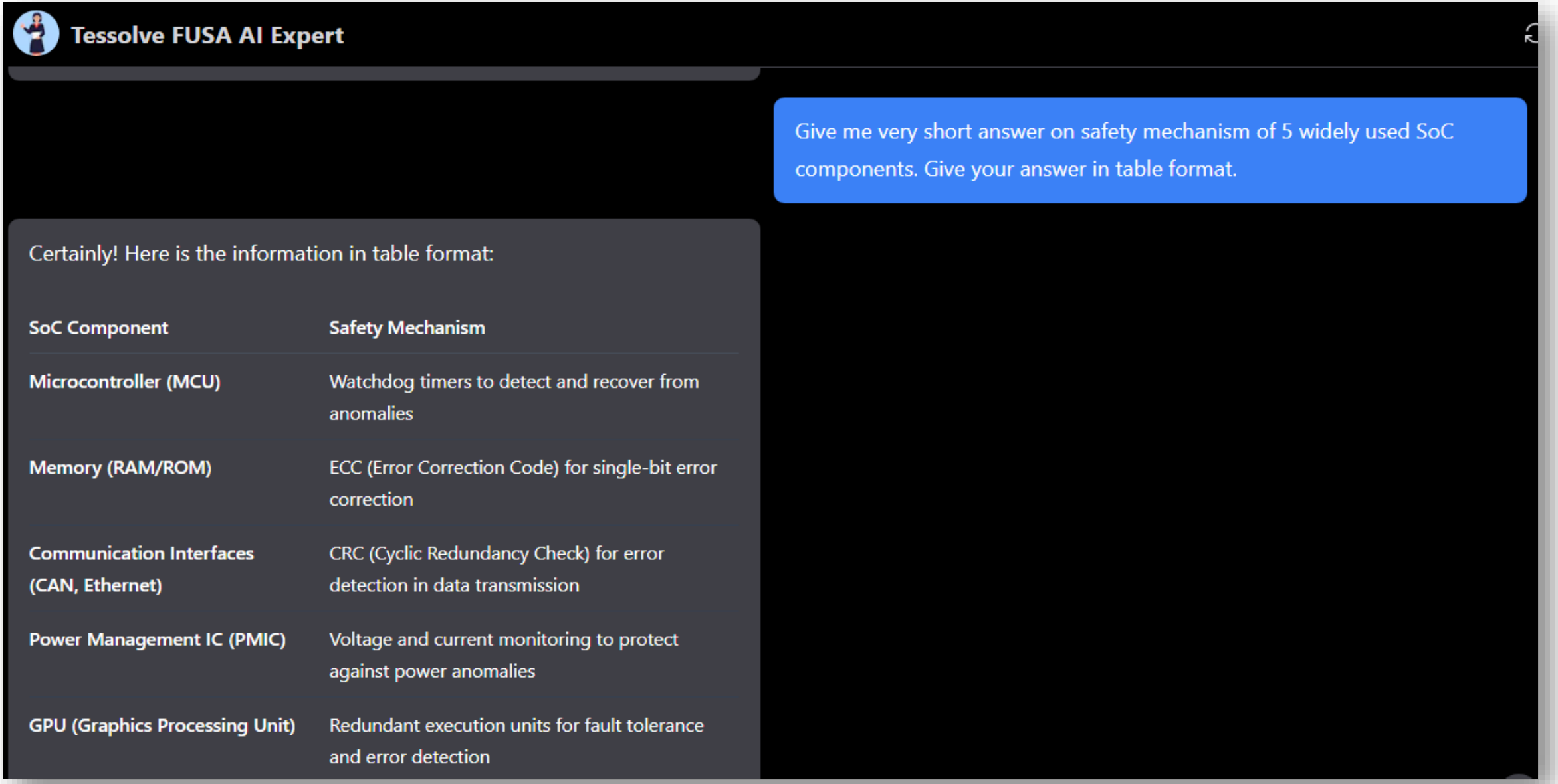
- Design element or function that does **Detection**, **Indication** or **Reaction** on fault or failure to achieve or maintain a safe state of the system.

- Few methods:
  - Redundancy
  - Error detection & correction
  - Watchdog timers
  - Diagnostic routines
  - Safety monitoring
  - Fail safe designs
  - Isolation etc.



Use case - Safety Mechanism ✨

TESSOLVE
A HERO ELECTRONIX VENTURE



Use case - Safety Mechanism Recommendation

TESSOLVE
A HERO ELECTRONIX VENTURE

Tessolve FUSA AI Expert

What is the Safety mechanism for PLL?

For Phase-Locked Loop (PLL) components, the safety mechanisms typically include:

1. **Frequency Monitoring:** Ensures the PLL output frequency remains within specified bounds, detecting deviations that could indicate a fault.
2. **Lock Detection:** Monitors whether the PLL has successfully locked onto the reference frequency, triggering a fault response if it fails to lock.
3. **Redundancy:** Implements redundant PLL circuits to provide a backup in case the primary PLL fails.
4. **Self-Test:** Conducts periodic self-tests to verify the correct operation of the PLL circuitry.
5. **Voltage and Temperature Monitoring:** Monitors supply voltage and operating temperature to ensure they remain within safe limits, protecting the PLL from environmental-induced faults.

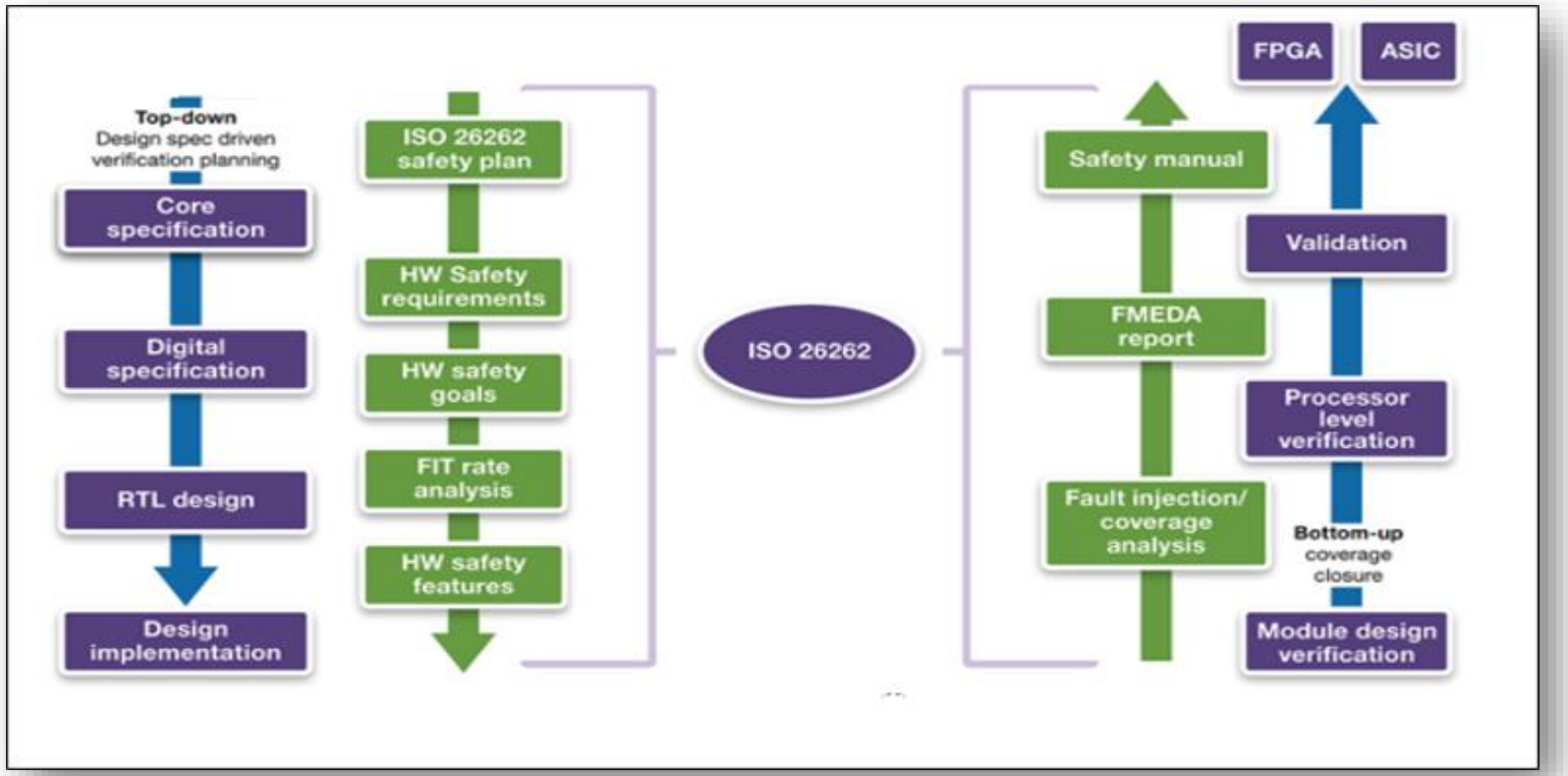
These mechanisms help ensure the reliability and safety of the PLL, critical for maintaining stable and accurate system clocks in automotive applications.

Requirement Management & Traceability

TESSOLVE
A HERO ELECTRONIX VENTURE

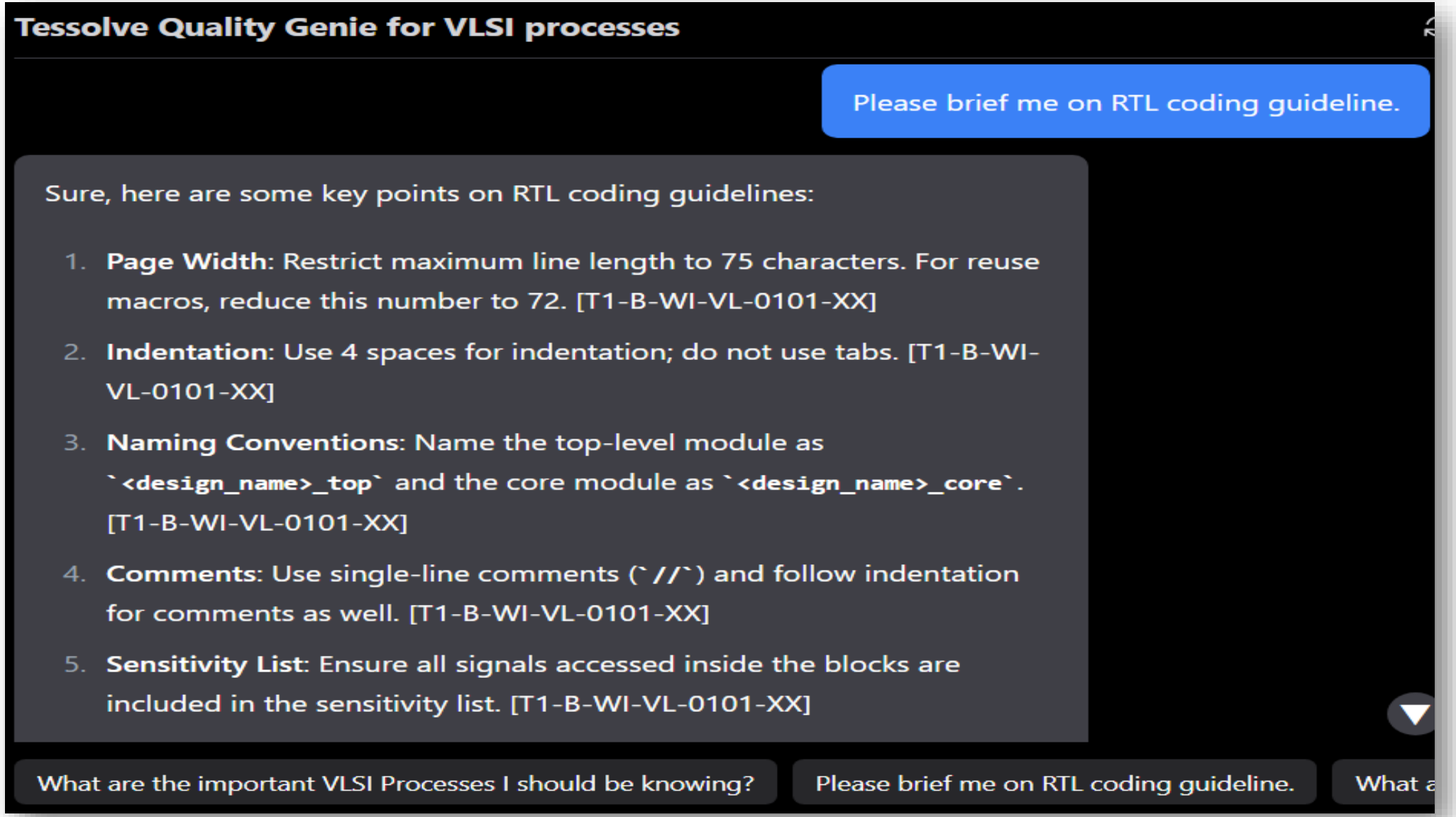
Requirement Management

- The ability to trace a requirement forwards/ backwards in the development lifecycle through development artifacts
- Helps in productively mitigating risk within stipulated time



Use case – Compliance Support for Quality ✨

TESSOLVE
A HERO ELECTRONIX VENTURE



Use case - Traceability ✨

TESSOLVE
A HERO ELECTRONIX VENTURE

which part document has the explanation on IP functional safety compliance?

For IP functional safety compliance, you should refer to **Part 11** of the ISO 26262 standard. This part specifically provides guidelines on the

Tessolve Quality Genie

Hi, I am Tessolve Quality Genie. How may I help you today?

Where I can find the RTL guidelines on Tessolve quality practices for VLSI BU.

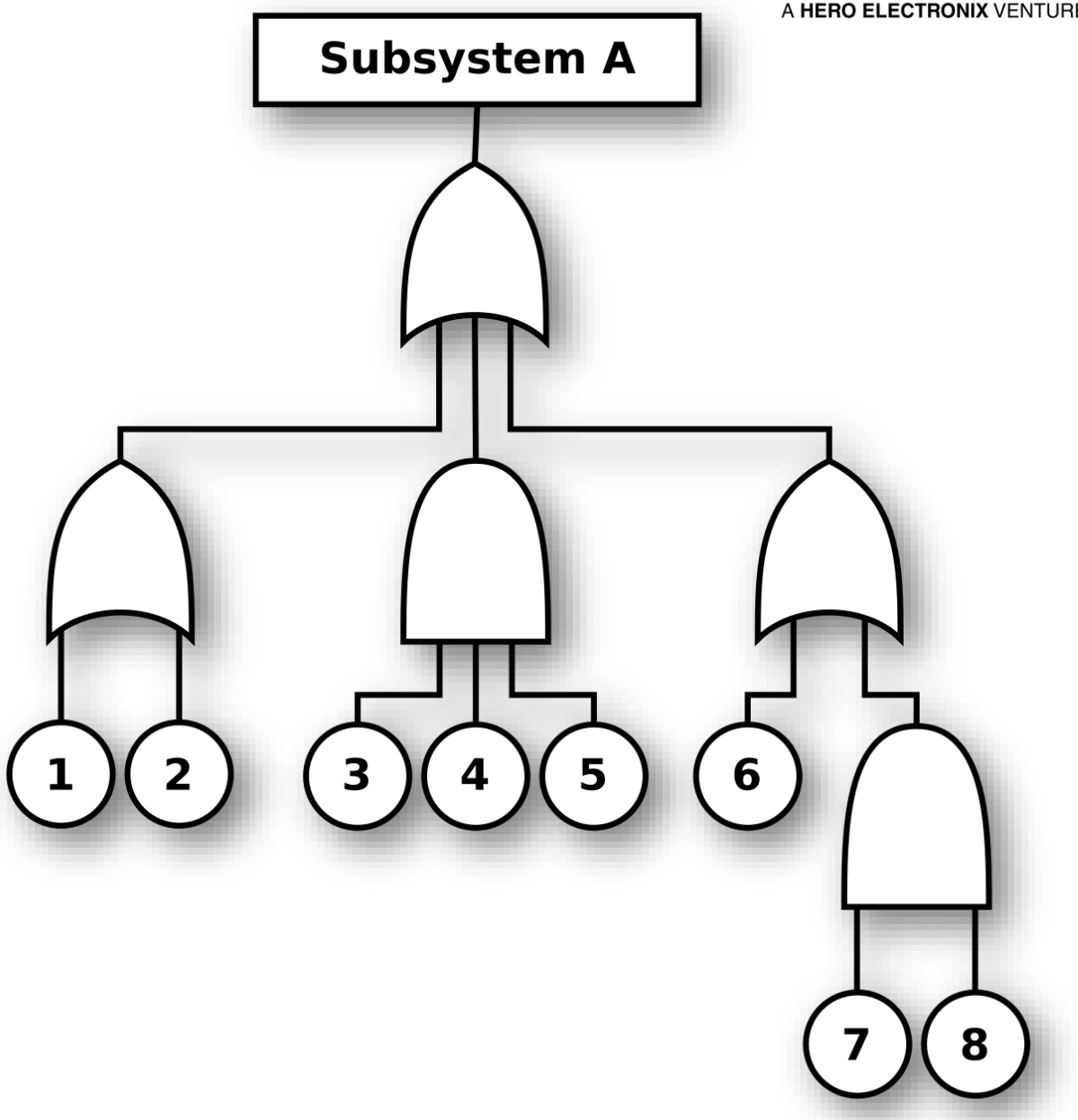
You can find the RTL guidelines under the document titled "VLSI_RTL Coding_Guidelines" with the document number T1-B-WI-VL-0101-00. [Citation: Doc No T1-B-WI-VL-0101-XX]

This is the link for the documents: https://www.tessolve.in/qmsdocuments/Pages/. Please follow the link.

FTA

Fault tree analysis (FTA)

- FTA is a **graphical tool** used to explore the causes of system-level failures
- It systematically uses **Boolean logic** to combine a series of lower-level events



Use case - FTA Analysis

Top Event: Braking System Failure at Crossroad

1.1 Hydraulic Brake Failure

1.1.1 Brake Fluid Leak

1.1.1.1 Damaged Brake Line

1.1.1.2 Faulty Brake Cylinder

1.1.2 Air in Brake Lines

1.1.2.1 Improper Bleeding of Brakes

1.1.2.2 Brake System Seal Failure

1.2 Electronic Brake Control Failure

1.2.1 ABS (Anti-lock Braking System) Failure

1.2.1.1 Sensor Malfunction

1.2.1.2 ECU (Electronic Control Unit) Failure

1.2.2 ESP (Electronic Stability Program) Failure

1.2.2.1 Software Glitch

1.2.2.2 Hardware Malfunction

1.3 Traction Loss Due to Slippery Road

1.3.1 Insufficient Tire Tread

1.3.2 Inadequate Tire Pressure

1.4 Driver Reaction Time

1.4.1 Delayed Response

1.4.2 Incorrect Braking Force Applied

Basic Events (Root Causes)

1.1.1.1 Damaged Brake Line

- Physical wear and tear, corrosion.

1.1.1.2 Faulty Brake Cylinder

- Manufacturing defect, wear and tear.

1.1.2.1 Improper Bleeding of Brakes

- Maintenance error.

1.1.2.2 Brake System Seal Failure

- Aging, material defect.

1.2.1.1 Sensor Malfunction

- Environmental factors, aging, manufacturing defects.

1.2.1.2 ECU Failure

- Software bugs, hardware faults.

1.2.2.1 Software Glitch

- Inadequate testing, unexpected scenarios.

1.2.2.2 Hardware Malfunction

- Component failure, environmental factors.

1.3.1 Insufficient Tire Tread

- Wear and tear, poor maintenance.

1.3.2 Inadequate Tire Pressure

- Poor maintenance, slow leaks.

1.4.1 Delayed Response

- Driver distraction, fatigue.

1.4.2 Incorrect Braking Force Applied

- Panic response, lack of training.

FMEA

- Failure Modes and Effects Analysis (FMEA) is a systematic, step-by-step approach for identifying potential failure modes in a product or process, analyzing the effects of those failures, and prioritizing actions to mitigate the risks associated with the.

FMEA Steps	Description
Define Scope	Identify the system or component to be analyzed.
Identify Failure Modes	Determine potential ways each component can fail.
Analyze Effects	Assess the impact of each failure mode on the system.
Determine Causes	Identify the root causes of each failure mode.
Evaluate Controls	Review existing measures to detect or prevent failures.
Calculate RPN	Rate severity, occurrence, and detection to prioritize risks.
Recommend Actions	Suggest measures to mitigate high-priority risks.

Use case - FMEA

TESSOLVE
A HERO ELECTRONIX VENTURE

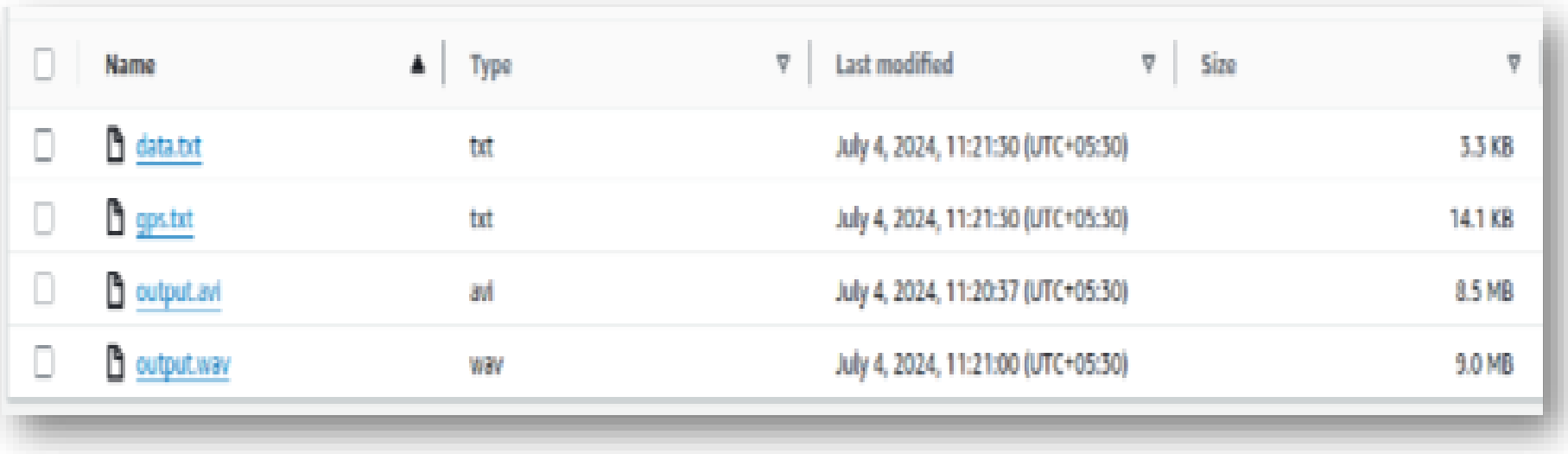
Function	Potential Failure Mode	Potential Effect(s) of Failure	Severity (S)	Potential Cause(s)/Mechanism(s) of Failure	Occurrence (O)	Current Design Controls	Detection (D)	RPN (Risk Priority Number)	Recommended Action(s)
Timing Signal Generation	Clock signal stops	System halt, loss of functionality	10	Power failure, oscillator failure	3	Power redundancy, clock monitoring	4	120	Enhance power redundancy, improve clock monitoring systems.
	Clock signal drifts	Incorrect timing, synchronization issues	8	Temperature variation, component aging	4	Temperature compensation, periodic calibration	3	96	Implement better temperature compensation, schedule regular calibrations.
	Clock signal jitter	Data corruption, communication errors	7	Noise interference, poor signal integrity	5	Shielding, filtering	3	105	Improve shielding, enhance filtering mechanisms.
	Clock signal phase shift	Timing errors, loss of synchronization	8	Signal interference, improper routing	3	PCB design reviews, signal integrity checks	4	96	Improve PCB design practices, conduct thorough signal integrity checks.
Frequency Stability	Frequency deviation	System malfunction, inaccurate timekeeping	7	Environmental factors, aging components	4	Environmental testing, component selection	3	84	Use high-quality components, perform rigorous environmental testing.
Power Supply	Power loss to clock	Complete loss of timing signals	10	Power supply failure, connector issue	2	Power monitoring, redundant power supply	4	80	Implement more robust power supply design, improve power monitoring.
	Over-voltage on clock circuit	Damage to clock circuit, loss of functionality	9	Power surge, incorrect voltage level applied	2	Over-voltage protection circuits, regular voltage checks	3	54	Enhance over-voltage protection, introduce regular voltage level checks.
Clock Distribution	Signal degradation over distance	Timing errors, loss of synchronization	7	Signal attenuation, poor routing	4	Signal boosters, routing optimization	3	84	Use signal boosters, optimize PCB routing for minimal signal loss.
Backup Clock	Backup clock failure	Loss of redundancy, increased risk of system failure	8	Component failure, poor switching mechanism	3	Regular testing, quality components	3	72	Improve backup clock reliability, perform frequent testing and maintenance.

Digital Twin for Predictive Analysis and Diagnosis

TESSOLVE
A HERO ELECTRONIX VENTURE

Predictive analysis with GenAI for better maintenance and safety

- Impact audio, video
- Humidity, temperature, tire pressure, speed, fuel efficiency, sensor data
- Driver authentication, gesture, facial feature alerts



Name	Type	Last modified	Size
data.txt	txt	July 4, 2024, 11:21:30 (UTC+05:30)	3.3 KB
gps.txt	txt	July 4, 2024, 11:21:30 (UTC+05:30)	14.1 KB
output.avi	avi	July 4, 2024, 11:20:37 (UTC+05:30)	8.5 MB
output.wav	wav	July 4, 2024, 11:21:00 (UTC+05:30)	9.0 MB

Digital Twin for Predictive Analysis and Diagnosis ✨

TESSOLVE
A HERO ELECTRONIX VENTURE

Generative AI for data analytics

Data Analysis Report: Car Safety Status

Date: (Assuming date is relevant to the provided data)

Time Period: 11:19:13 - 11:20:13 (Assuming timestamps are sequential)

Data Source: (Specify source of LDR, Speed, Brakes data)

Executive Summary:

The provided dataset raises concerns regarding the safety of the vehicle and its passengers. Key findings include:

* **Consistently High Speed:** The vehicle maintains a high speed, averaging around 138.5, with frequent spikes above 140. This suggests potential speeding, especially if exceeding legal limits for the area.
* **Brakes Not Applied:** The data consistently shows the brakes as "ON:No", indicating the brakes were not engaged during the recorded period. This is particularly alarming given the high speeds.
* **Potential for Light Sensitivity (LDR):** While LDR values fluctuate within a relatively narrow range (29-34), their meaning is unclear without context. LDR sensors typically measure light intensity. Further investigation is needed to determine if these values indicate a safety hazard (e.g., driving with compromised visibility).
* **GPS Data Inconsistencies:** A significant portion of the GPS data is missing ("Latitude or Longitude is not available"). This hinders route analysis and makes it impossible to assess if the vehicle was in a safe or appropriate location for the recorded speeds.

Recommendations:

1. **Immediate Attention:** The combination of high speed and unapplied brakes warrants immediate attention. This could indicate a serious malfunction or driver error.
2. **Context for LDR Values:** Define the role of LDR in the vehicle system. Are the values within safe operating ranges? Correlate LDR fluc

Caution & Path Forward

- Model accuracy
- Rigorous validation
- Reliability
- Data security
- Life safety
- Legal aspect
- Standard for GenAI usage

References

1. ISO 26262 & Software Development for Functional Safety of Automotive Systems with ASIL (promwad.com)
2. ISO 26262 Functional Safety – An Approach for Compliance Readiness (sae.org)
3. the-application-of-artificial-intelligence-in-functional-safety.pdf (theiet.org)
4. ISO - AI management systems: What businesses need to know
5. National Institute of Standards and Technology (nist.gov)
6. What is ISO 26262 Functional Safety Standard? | Synopsys Automotive

TESSOLVE

A **HERO ELECTRONIX** VENTURE

THANK YOU

www.tessolve.com

mike.bartley@tessolve.com

Click to add text

Chip Design

Test Engineering

Hardware Design

Embedded Systems