ISO26262 & SAE J2980– Gestão da Qualidade no contexto do "Software Embarcado Automotivo"

T01G04 - 2020

AGENDA DE HOJE

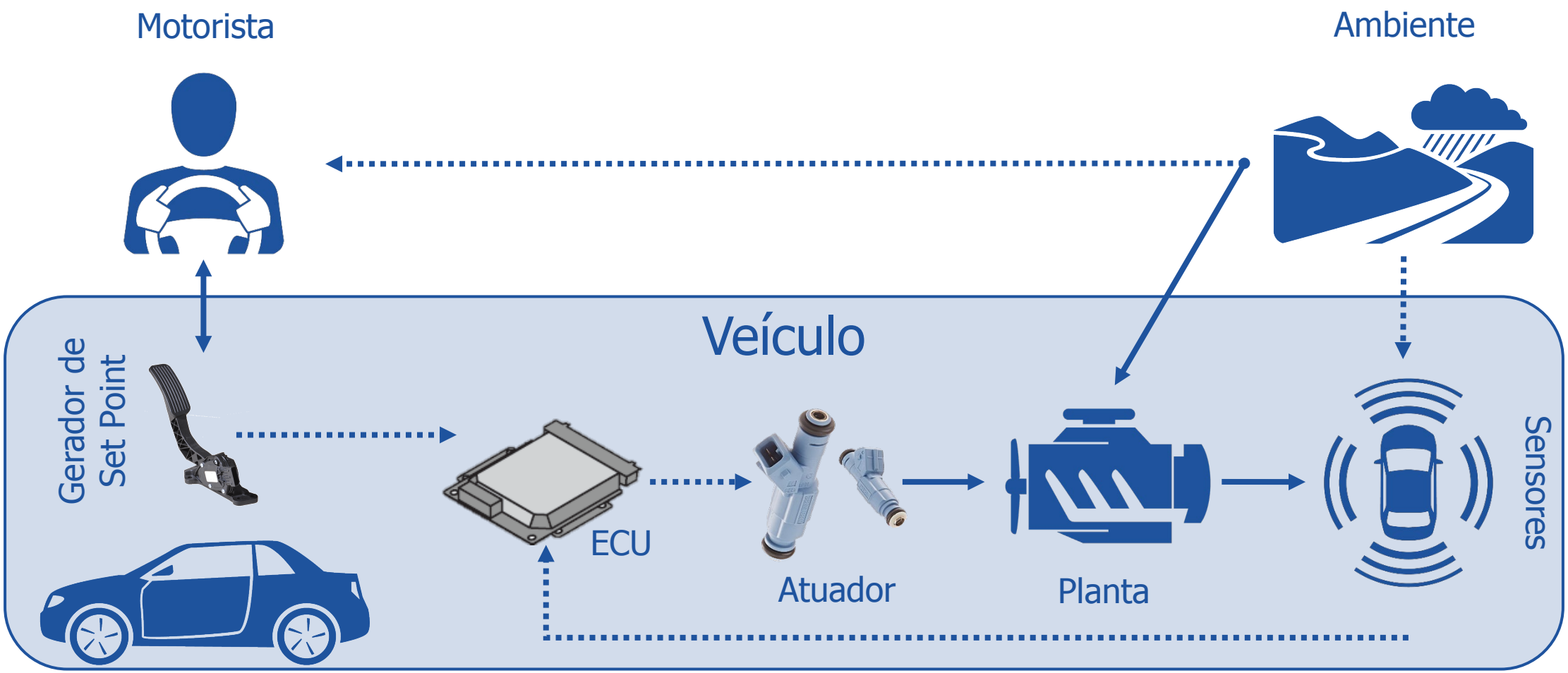
1. **Contextualização** – O que é um software embarcado automotivo?
   Quais são seus requisitos específicos em termos de qualidade e segurança?

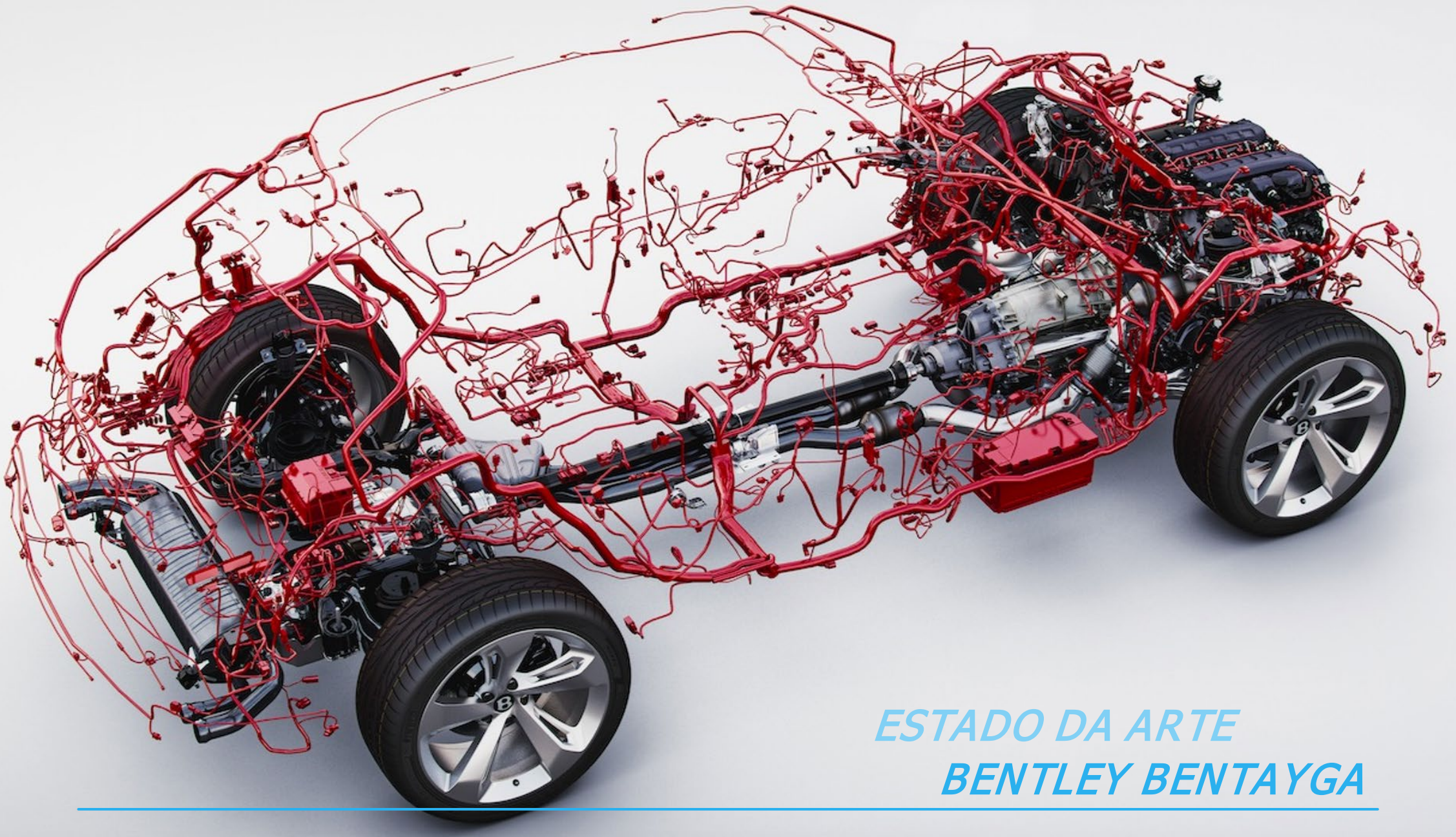
2. **ISO26262: Road Vehicles –Functional Safety**
   A importância da normatização para engenharia de software embarcado.

3. **SAEJ2980: Considerations for ISO 26262 ASIL Hazard Classification**
   Definindo requisitos de qualidade e segurança de forma objetiva

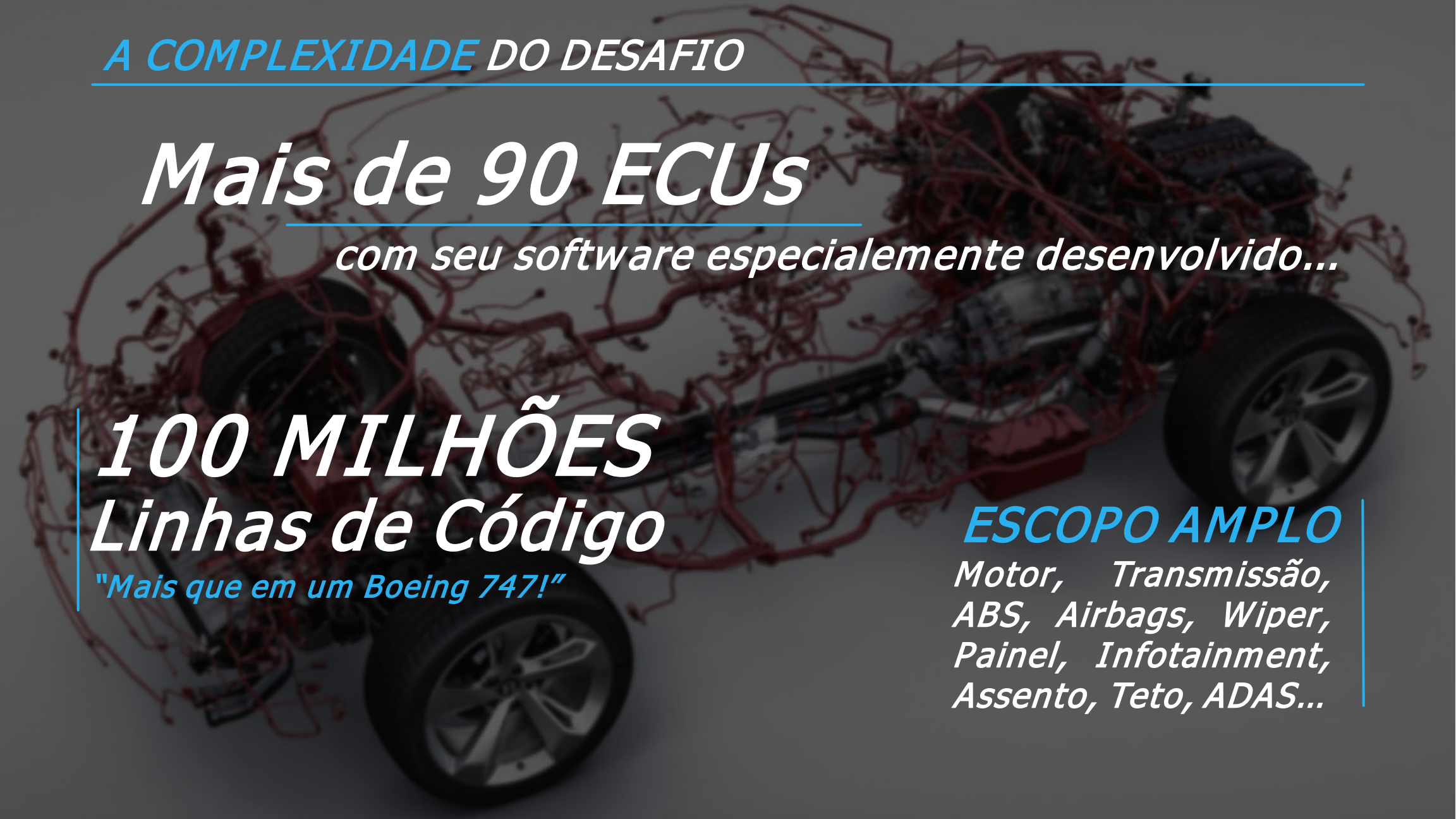
O que é um sistema de controle em malha fechada?

Exemplo – Controle em malha fechada automotivo





ESTADO DA ARTE
BENTLEY BENTAYGA



A COMPLEXIDADE DO DESAFIO

Mais de 90 ECUs

com seu software especialemente desenvolvido...

100 MILHÕES
Linhas de Código

"Mais que em um Boeing 747!"

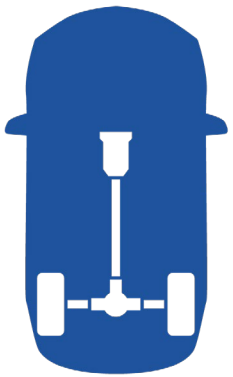
ESCOPO AMPLO

Motor, Transmissão, ABS, Airbags, Wiper, Painel, Infotainment, Assento, Teto, ADAS...

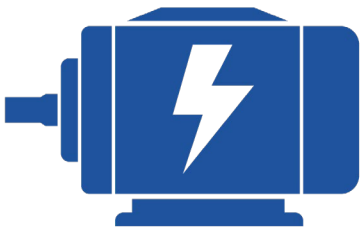
“The Modern Picture” - Tudo é controlado!

Gerenciamento de Motor

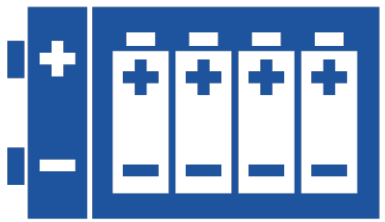
Transmissão



Motor Elétrico



Gerenciamento de Bateria



Sensores Automação

Freio/ABS

Dinâmica/ESP

Luzes, Wiper AC, Vidro

Quais são os desafios enfrentados pelo SW Embarcado?

Demandas em "Tempo Real"

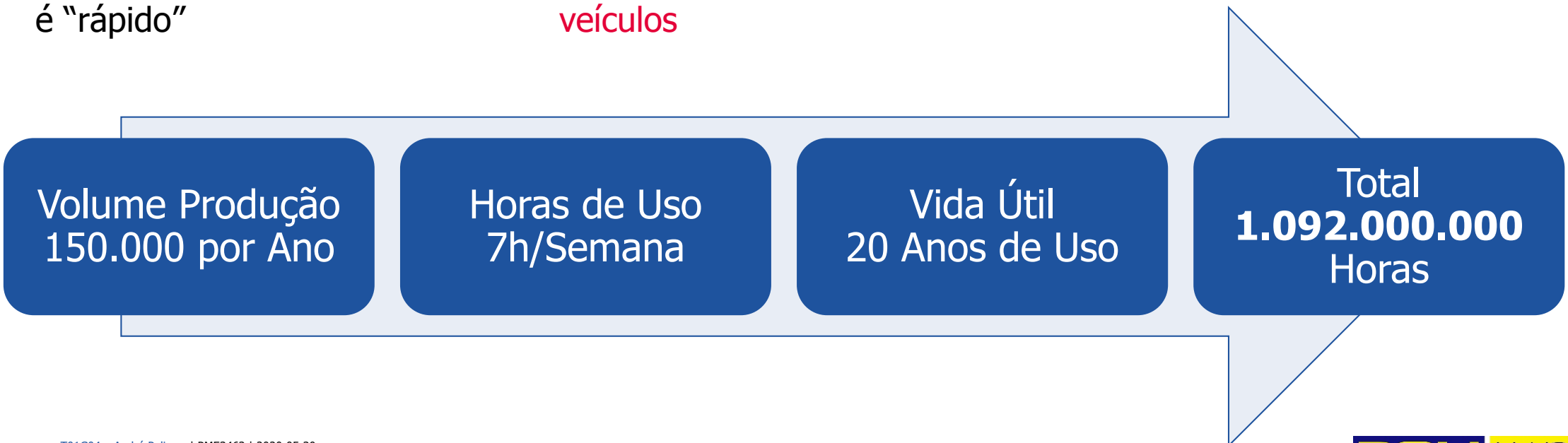
- Funções são "Time Crictical"
- E.g. timing de injeção e ignição, Airbag, ABS/ESP
- Hardware é limitado: 2Mb Flash ROM é "muito", 200Mhz é "rápido"

Volume de produção muito alto

- Uma média de 50 à 100 ECUs por veículo rodando um software próprio/especializado
- Escala de produção na faixa de centenas de milhares de veículos

Safety Crictical

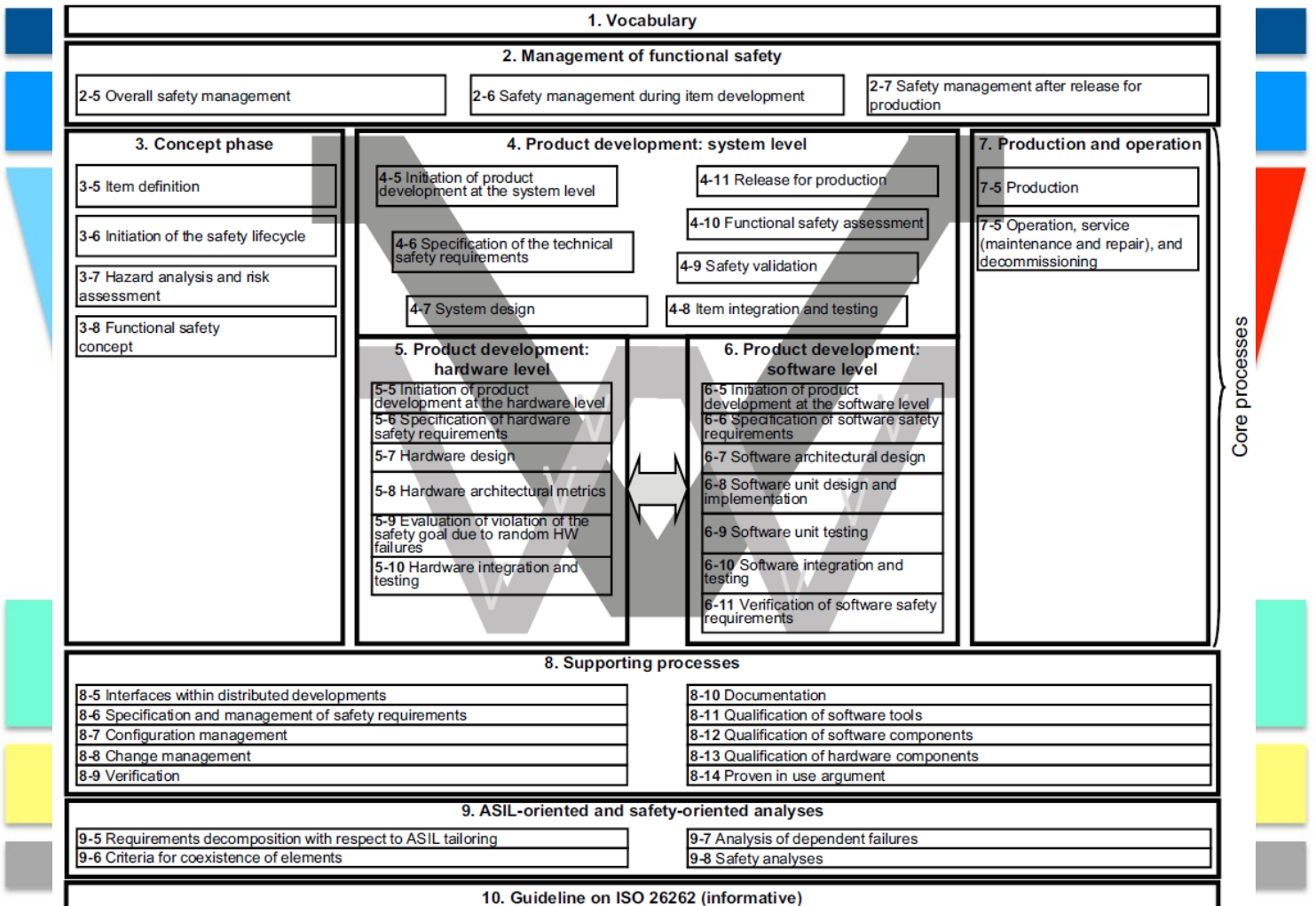
- Demandas de confiabilidade
- Erros são fatais!
- Não existe "Reset" em um carro
- Mais de um bilhão de "horas de vôo"



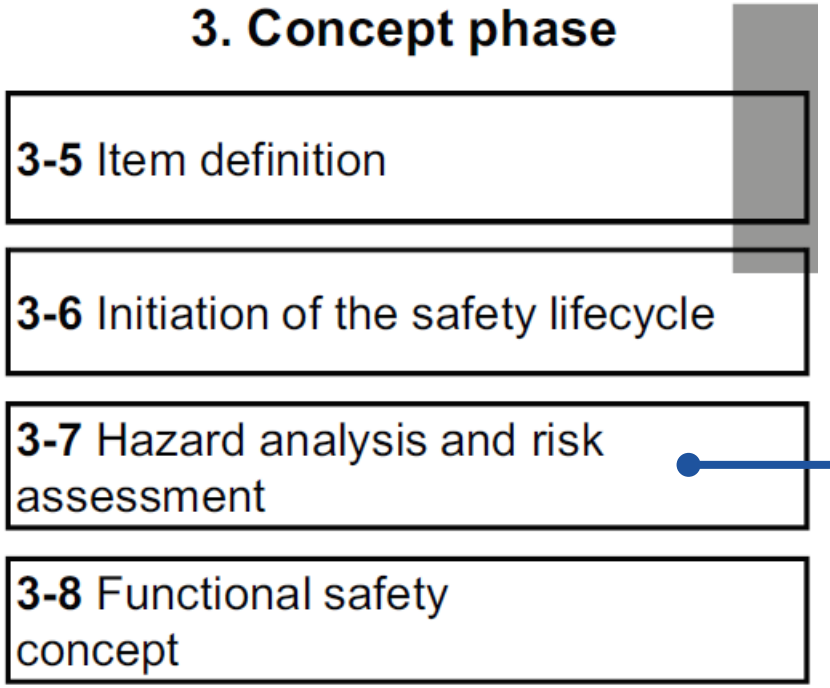
Como a indústria se organiza para enfrentar os desafios apresentados e entregar um produto robusto?

Normatização, gerenciamento de requisitos de segurança e qualidade: ISO26262 & SAEJ2980

Visão Geral – ISO26262



Aplicando a ISO 26262: Definição de requisitos de projeto



"**HARA** is an analysis procedure that identifies potential hazards, develops a set of specific hazardous events, and assesses the risk of each hazardous event to determine the **ASIL** and the safety goal. Functional safety requirements are derived from the safety goals. "

ASIL - Automotive Safety Integrity Level

Hazard Analysis and risk assessment - HARA → **Classificação ASIL** → **Requisitos de Projeto**

J2980 – "Considerations for ISO 26262 ASIL Hazard Classification"

Como encontrar o nível ASIL para cada controlador do veículo?

Passo 1 – HAZOP: functional hazard and operability analysis

Function Vs. Guidewords	Loss of Function	Function provided incorrectly when intended			Unintended Activation of Function (Function provided when not intended)	Output Stuck at a Value (Failure of function to update as intended)
		Incorrect Function (More than intended)	Incorrect Function (Less than intended)	Incorrect Function (Wrong direction)		
Steering Assist Function	*Loss of Steering Assist*	*Excessive Steering Assist*	*Reduced Steering Assist*	*Steering in the Opposite Direction*	*Unintended Steering Assist*	*Locked Steering (Steering Output Stuck at Value)*
Brake Control Function (conventional brake control)	*Loss of Braking*	*Excessive Braking*	*Insufficient Braking*	-	*Unintended Braking*	*Locked Braking (Brake Output Stuck at Value)*

Fonte: "*Considerations for ISO 26262 ASIL Hazard Classification* (SAEJ2980)" – Página 7, Tabela 1

J2980 – "Considerations for ISO 26262 ASIL Hazard Classification"

Como encontrar o nível ASIL para cada controlador do veículo?

Passo 2 – Mapear o impacto da falha em termos de risco para o veículos

Malfunctioning Behaviors	Vehicle Hazards
Unintended Steering Assist	*Unintended vehicle lateral motion/Unintended yaw*
Excessive Steering Assist	
Steering in the opposite Direction	
Locked Steering (Steering output stuck at value)	*Loss of vehicle lateral motion control*
Reduced Steering Assist	*Increased Manual Effort to Steer*
Loss of Steering Assist	

Fonte: "*Considerations for ISO 26262 ASIL Hazard Classification* (SAEJ2980)" – Página 7, Tabela 2

J2980 – "Considerations for ISO 26262 ASIL Hazard Classification"

Como encontrar o nível ASIL para cada controlador do veículo?

Passo 2 – Mapear o impacto da falha em termos de risco para o veículos

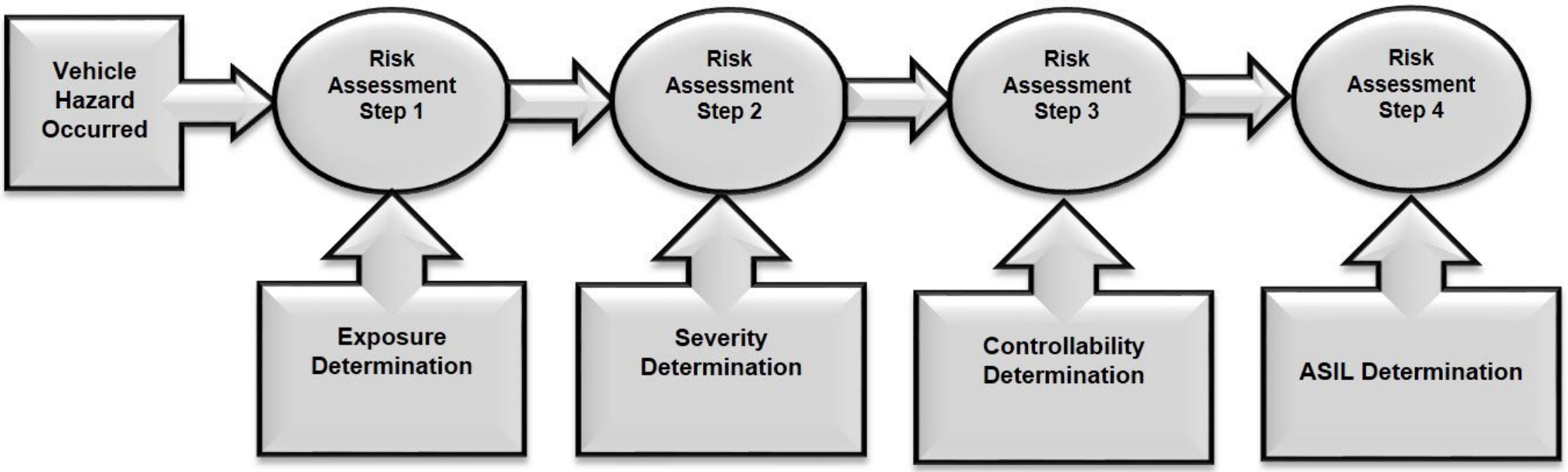
Malfunctioning Behaviors	Vehicle Hazards
Unintended Braking	*Unintended vehicle longitudinal deceleration*
Excessive Braking	
Locked braking (Brake output stuck at value)	
Loss of Braking	*Unintended reduction in vehicle deceleration*
Insufficient Braking	
Unintended Braking	*Unintended vehicle lateral motion*
Excessive Braking	
Locked braking (Brake output stuck at value)	

Fonte: "*Considerations for ISO 26262 ASIL Hazard Classification* (SAEJ2980)" – Página 8, Tabela 3

J2980 – "Considerations for ISO 26262 ASIL Hazard Classification"

Como encontrar o nível ASIL para cada controlador do veículo?

Passo 3 – Para cada "Risco" encontrado, determinar exposição, controlabilidade e severidade:



Fonte: "*Considerations for ISO 26262 ASIL Hazard Classification* (SAEJ2980)" – Página 8, Figura 1

J2980 – "Considerations for ISO 26262 ASIL Hazard Classification"

Como encontrar o nível ASIL para cada controlador do veículo?

Passo 3A – Determinação da "Exposure" ou "Exposição ao Risco"

Table 4 - Exposure class description per ISO 26262:2011 [1]

Class	Description	Informative criteria for Exposure based on frequency (see [1], part 3 Table B.3)	Informative criteria for Exposure based on duration (see [1] part 3 Table B.2)
E0*	Incredible	Not specified	Not specified
E1	Very low probability	Occurs less often than once a year for the great majority of drivers	Not specified
E2	Low probability	Occurs a few times a year for the great majority of drivers	<1 % of average operating time
E3	Medium probability	Occurs once a month or more often for an average driver	1 % to 10 % of average operating time
E4	High probability	Occurs during almost every drive on average	>10 % of average operating time
* No ASIL is assigned for E0			

Fonte: "*Considerations for ISO 26262 ASIL Hazard Classification* (SAEJ2980)" – Página 9, Tabela 4

J2980 – "Considerations for ISO 26262 ASIL Hazard Classification"

Como encontrar o nível ASIL para cada controlador do veículo?

Passo 3B – Determinação da "Severity" ou "Grau de Ferimentos do Ocupante"

Table 5 - Severity class description per ISO 26262:2011 [1]

1. Type of collision – such as planar (for example head on, rear end, side impacts)
2. Relative speed between collision participants or at the time of single vehicle events
3. Relative size, height, and structural integrity of the vehicle(s) involved (i.e., crash compatibility)
4. Health and age of vehicle occupants and non-occupants exposed to collision forces
5. Use or not by vehicle occupants of safety protection equipment (e.g., seat belts, child restraints)
6. Availability and response of qualified, rapid emergency assistance (first aid teams)

Fonte: "*Considerations for ISO 26262 ASIL Hazard Classification* (SAEJ2980)" – Página 12, Tabela 5

J2980 – "Considerations for ISO 26262 ASIL Hazard Classification"

Como encontrar o nível ASIL para cada controlador do veículo?

Passo 3C – Determinação da "Controlability" ou "Controlabilidade" do risco:

Table 6 - Controllability class description per ISO 26262:2011 [1]

Controllability Class	Title	Description
C0*	Controllable in general	If dedicated regulations exist for a particular hazard, Controllability may be rated C0 when it is consistent with the corresponding existing experience concerning sufficient Controllability. For use of C0 refer ISO 26262-3:2011, 7.4.3.8.
C1	Simply controllable	99% or more of all drivers or other traffic participants are usually able to avoid the specified harm.
C2	Normally controllable	90% or more of all drivers or other traffic participants are usually able to avoid the specified harm
C3	Difficult to control or uncontrollable	Less than 90% of all drivers or other traffic participants are usually able to avoid the specified harm
* No ASIL is assigned for C0 NOTE: Description has used the "specified harm" based on ISO 26262-3:2011, 7.4.3.7, Note 2		

Fonte: "*Considerations for ISO 26262 ASIL Hazard Classification* (SAEJ2980)" – Página 13, Tabela 6

Exposure – how often does the operational situation occur?

Class	E0	E1	E2	E3	E4
Description	Incredible	Very low probability	Low probability	Medium probability	High Probability

Severity – how severe is the potential harm?

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

Controllability – are the occupants, or operator, able to take control to mitigate any potential injuries?

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

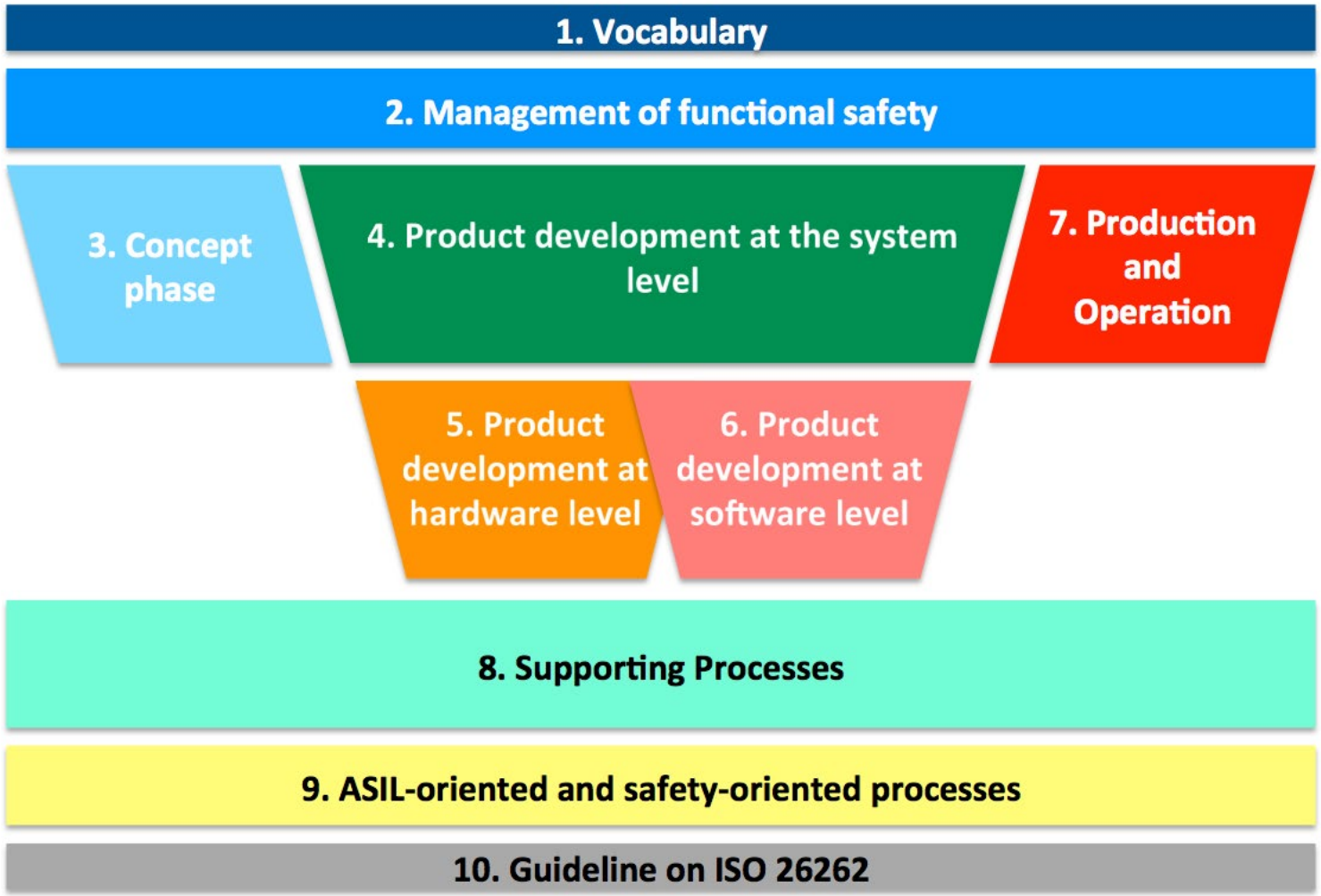
J2980 – "Considerations for ISO 26262 ASIL Hazard Classification"

Como encontrar o nível ASIL para cada controlador do veículo?

Passo 4 – Determinação do grau ASIL:

Severity	Exposure	Controllability		
		C1 - Simple	C2 - Normal	C3 - Difficult
S1 - Light	E1 (very low)	QM	QM	QM
	E2 (low)	QM	QM	QM
	E3 (medium)	QM	QM	A
	E4 (high)	QM	A	B
S2 - Severe	E1 (very low)	QM	QM	QM
	E2 (low)	QM	QM	A
	E3 (medium)	QM	A	B
	E4 (high)	A	B	C
S3 - Fatal	E1 (very low)	QM	QM	A
	E2 (low)	QM	A	B
	E3 (medium)	A	B	C
	E4 (high)	B	C	D

Visão Geral – ISO26262



O que o futuro reserva?

SAEJ3016 - Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles

SAEJ3018 - Safety-Relevant Guidance for On-Road Testing of SAE Level 3, 4, and 5 Prototype Automated Driving System (ADS)-Operated Vehicles


Muito Obrigado!
Perguntas?