Shanghai Jiyu Technology Co., Ltd.

Redundant Drive-By-Wire System & Chassis Provider

Offering Super Running Shoes for Autonomous Driving!

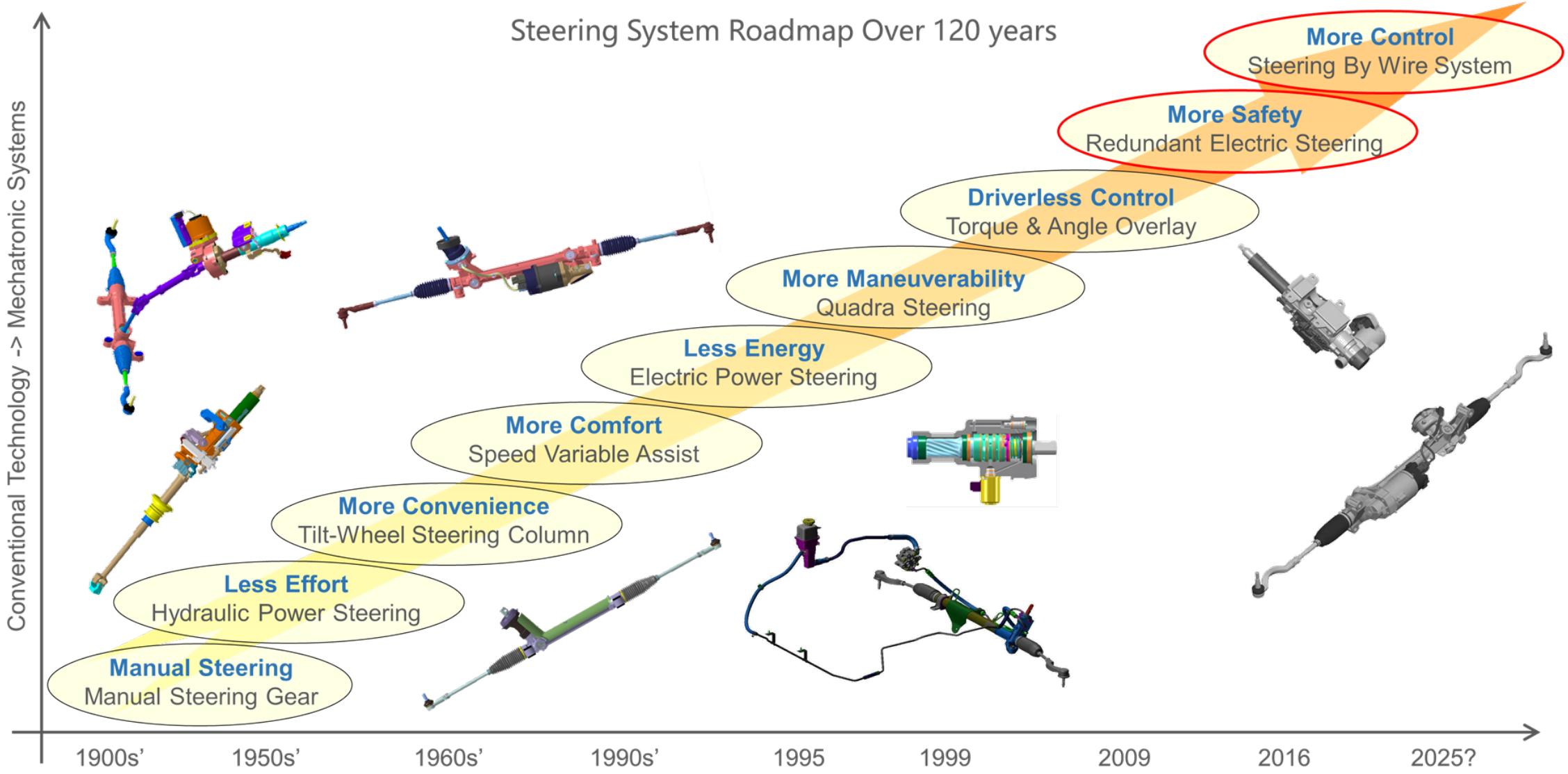
Xia Cunliang (Axel), Co-Founder
Email: xiacunliang@drivitech.com
TEL: (+86) 150 215 77 414

https://www.youtube.com/@JIYU-Chassis-DriveByWire

01

Steering by Wire

Product Introduction


Steering System Roadmap Over 120 years
Conventional Technology -> Mechatronic Systems
Manual Steering
Manual Steering Gear
Less Effort
Hydraulic Power Steering
More Convenience
Tilt-Wheel Steering Column
More Comfort
Speed Variable Assist
Less Energy
Electric Power Steering
More Maneuverability
Quadra Steering
Driverless Control
Torque & Angle Overlay
More Safety
Redundant Electric Steering
More Control
Steering By Wire System
1900s'
1950s'
1960s'
1990s'
1995
1999
2009
2016
2025?

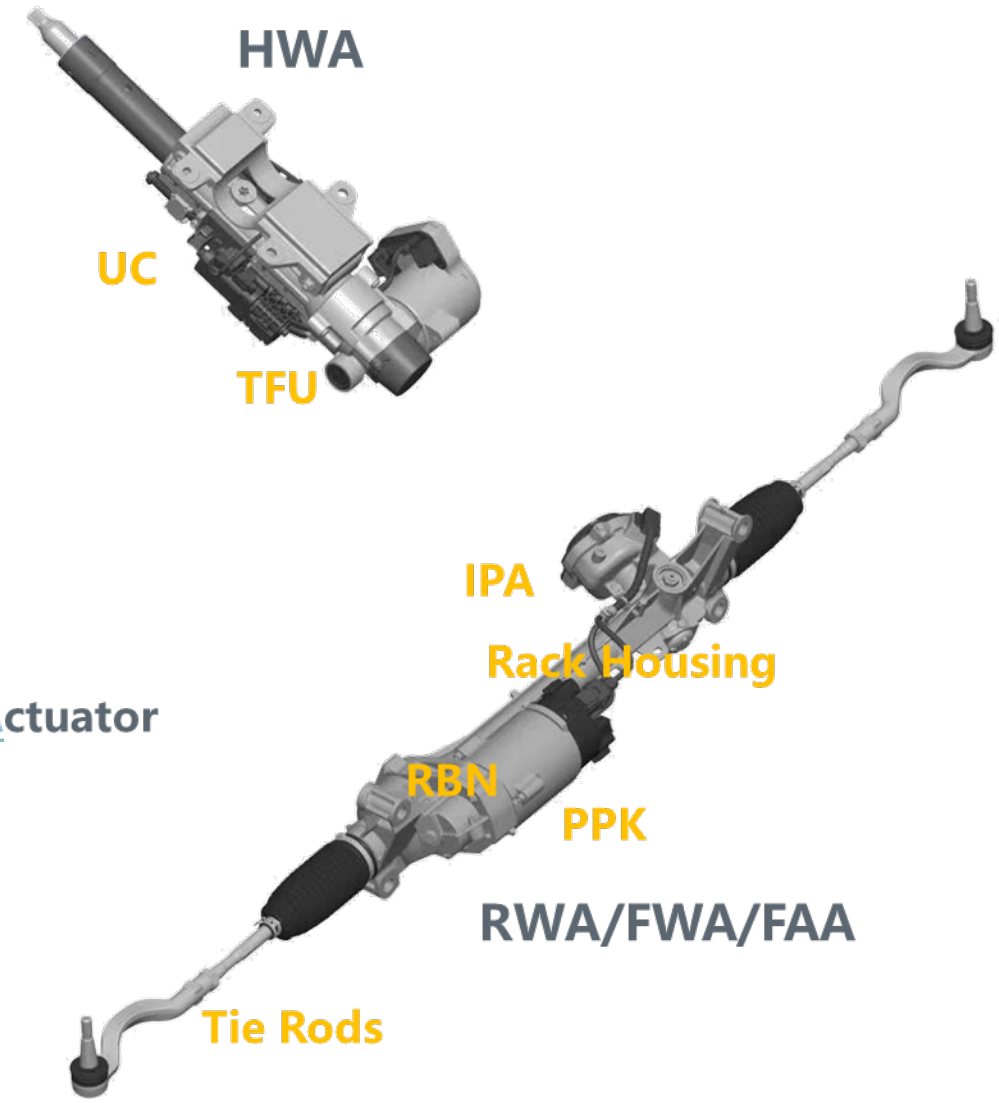
Steering by Wire / components and vocabulary

Hand Wheel Actuator

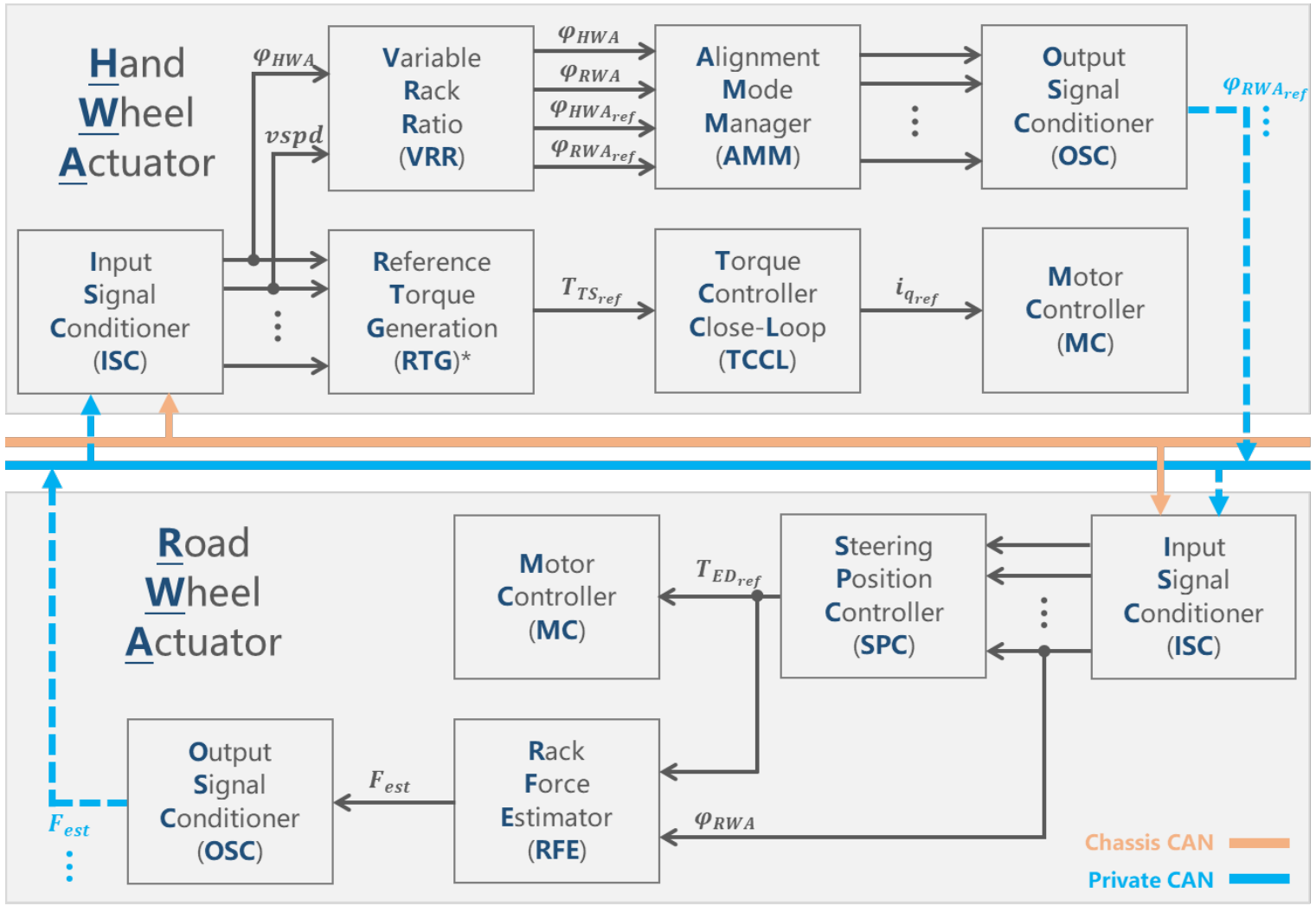
- TFU (Torque Feedback Unit)
  - SQS (Sensor Quill Shaft)
  - WGB (Worm Gear Box)
  - PPK (Power Pack)
  - MTL (Mechanical Travel Limiter)
- UC (Upper Column)
  - PAC (Power Adjust Column)
  - MAC (Manual Adjust Column)

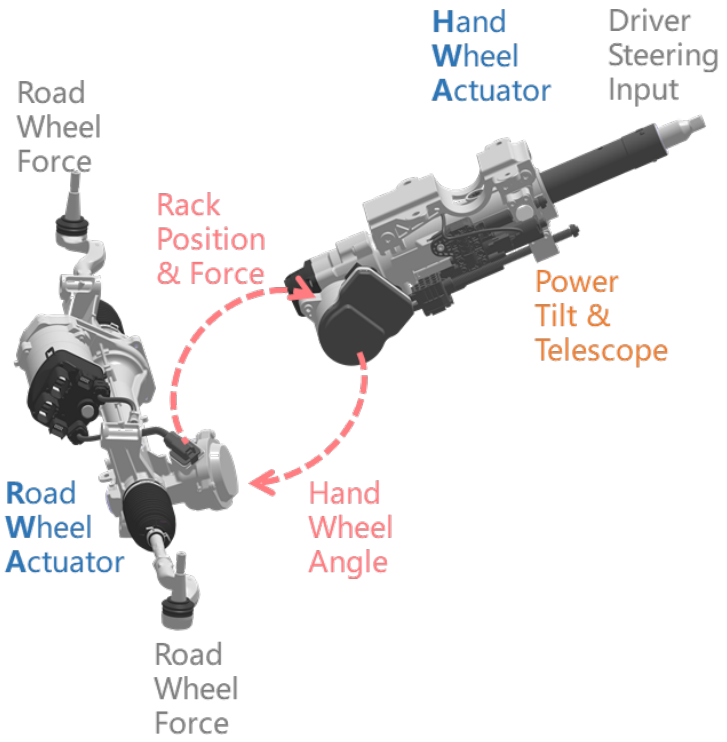
Road Wheel Actuator / Front Wheel Actuator / Front Axle Actuator

- IPA (Input-shaft Pinion-shaft Assembly)
- PPK (Power Pack)
- RBN (Rack Ball Nut)
- Rack Housing
- Tie Rods



Steering by Wire / control functionalities





* Reference Torque Generation incl. Expected Hand Torque, Controlled Return Torque, Damping Torque, Friction Compensation, Inertial Compensation, End Stop Protect, Auto Park Assist, Lane Keep Assist, Pull Drift Compensation, Traffic Jam Assist, and etc.

Steering by Wire / safety req. drives SW complexity

JIYU 济驭

- ✓ Software Complexity
- ✓ Number of Independent
- ✓ Multi-Core Processor

SW4 diverse
Software

SW3 *2
Software

SW2 diverse
Software

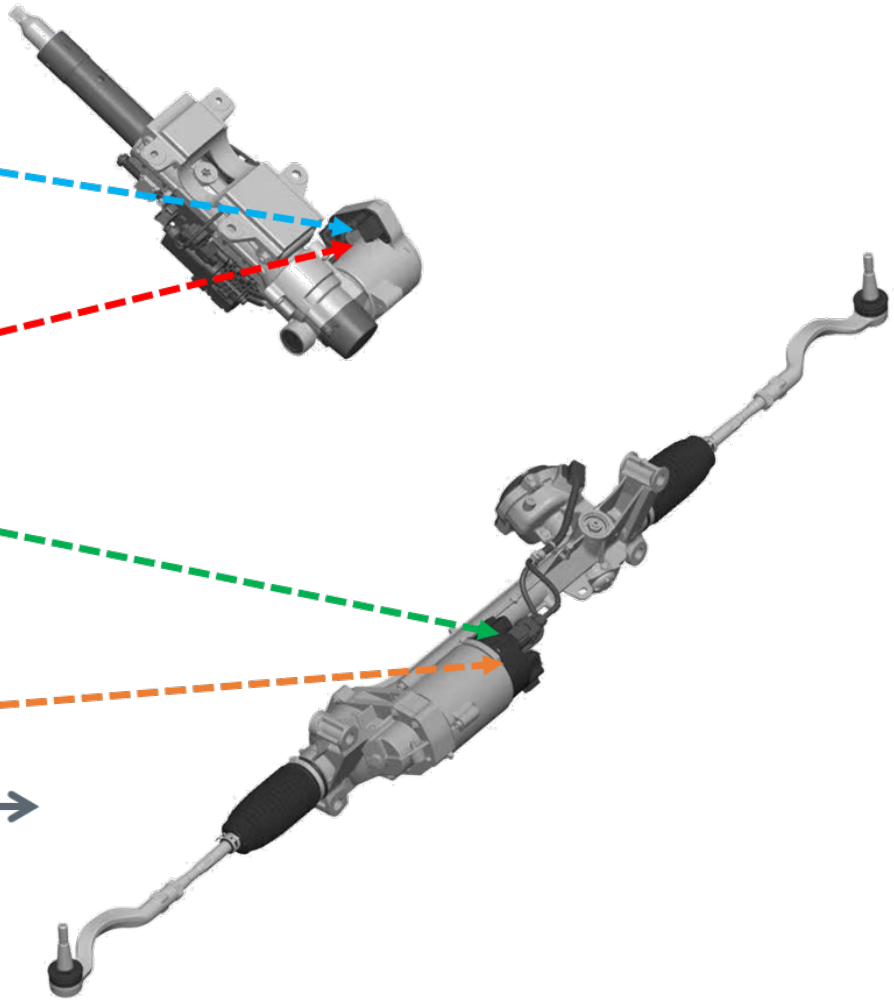
SW2 diverse
Software

SW1
Software

SW1 *2
Software

SW1 *2
Software

SW1 *2
Software



FIT500
uC*1, single core
Power Supply *1
Motor Bridge * 1
CAN * 1

FIT100
uC*2, multi core
Power Supply *1
Motor Bridge * 2
CAN * 2

FIT10
uC*2, multi core
Power Supply *2
Motor Bridge * 2
CAN * 2

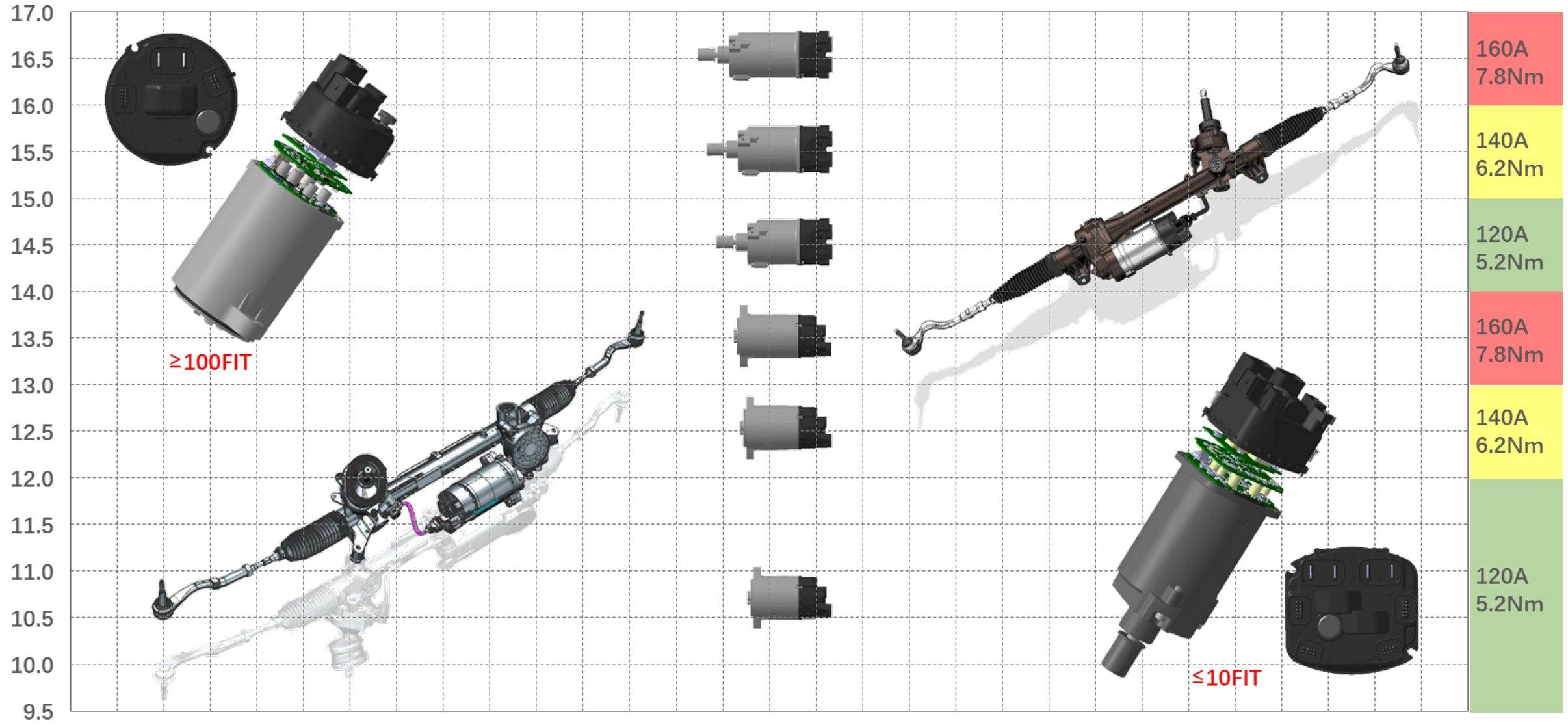
FIT10
uC*2, multi core
Power Supply *2
Motor Bridge * 2
Pri-CAN * 2, Pub-CAN * 2

Fail Safe：mechanical fallback

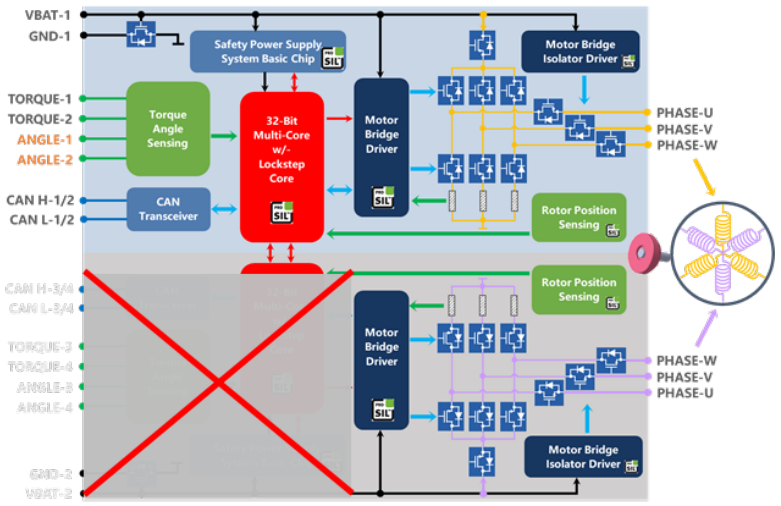
Fail Operational：electronic redundant

Steering by Wire / modulable & scalable PPKs

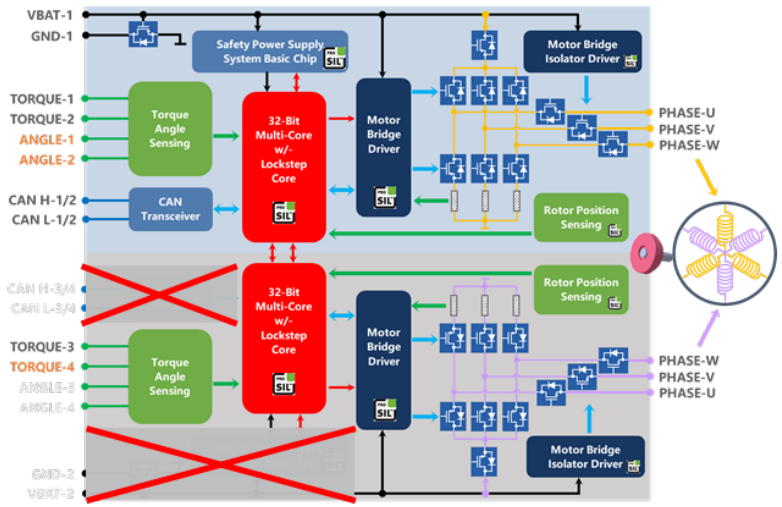
JIYU 济驭



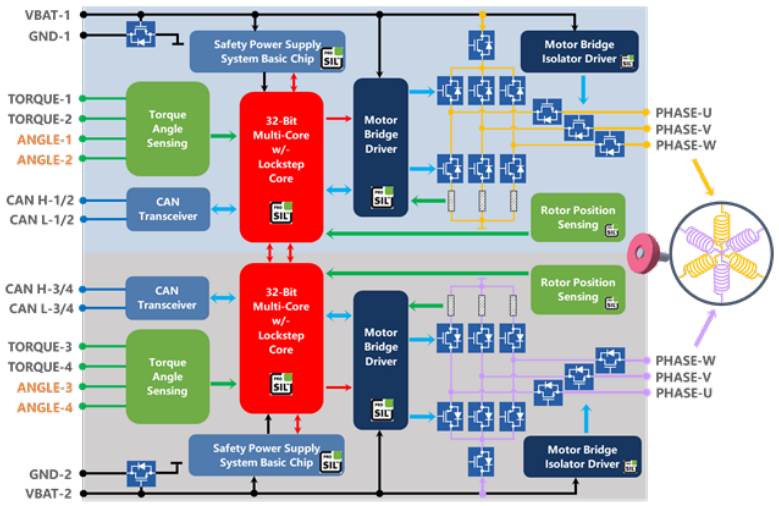
Steering by Wire / hardware architecture



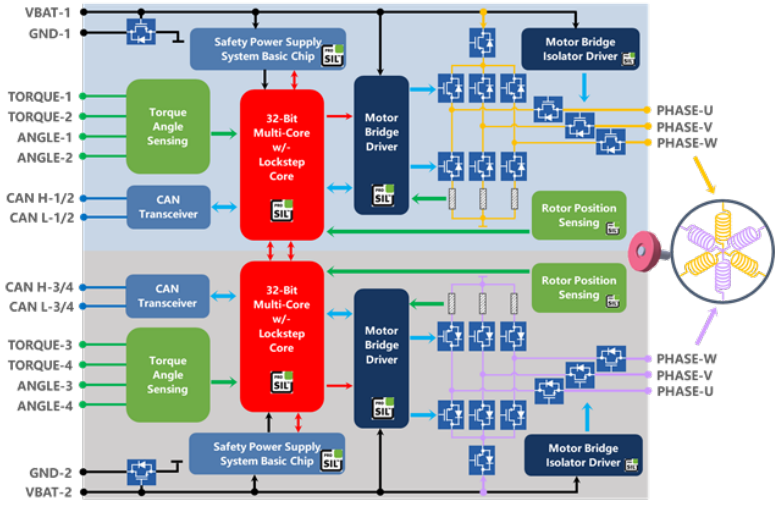
EPS FIT300: uC*1, SBC*1, pre-driver*2



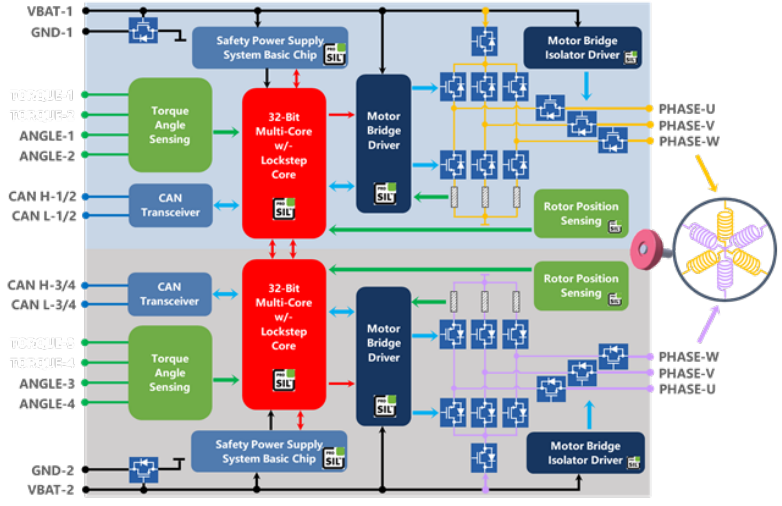
EPS FIT100: uC*2, SBC*1, pre-driver*2



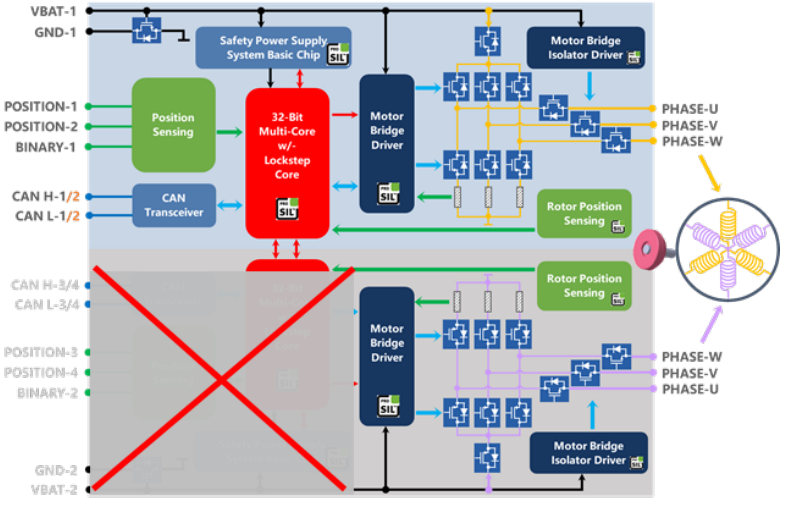
EPS FIT10: uC*2, SBC*2, pre-driver*2



HWA: uC*2, SBC*2, pre-driver*2



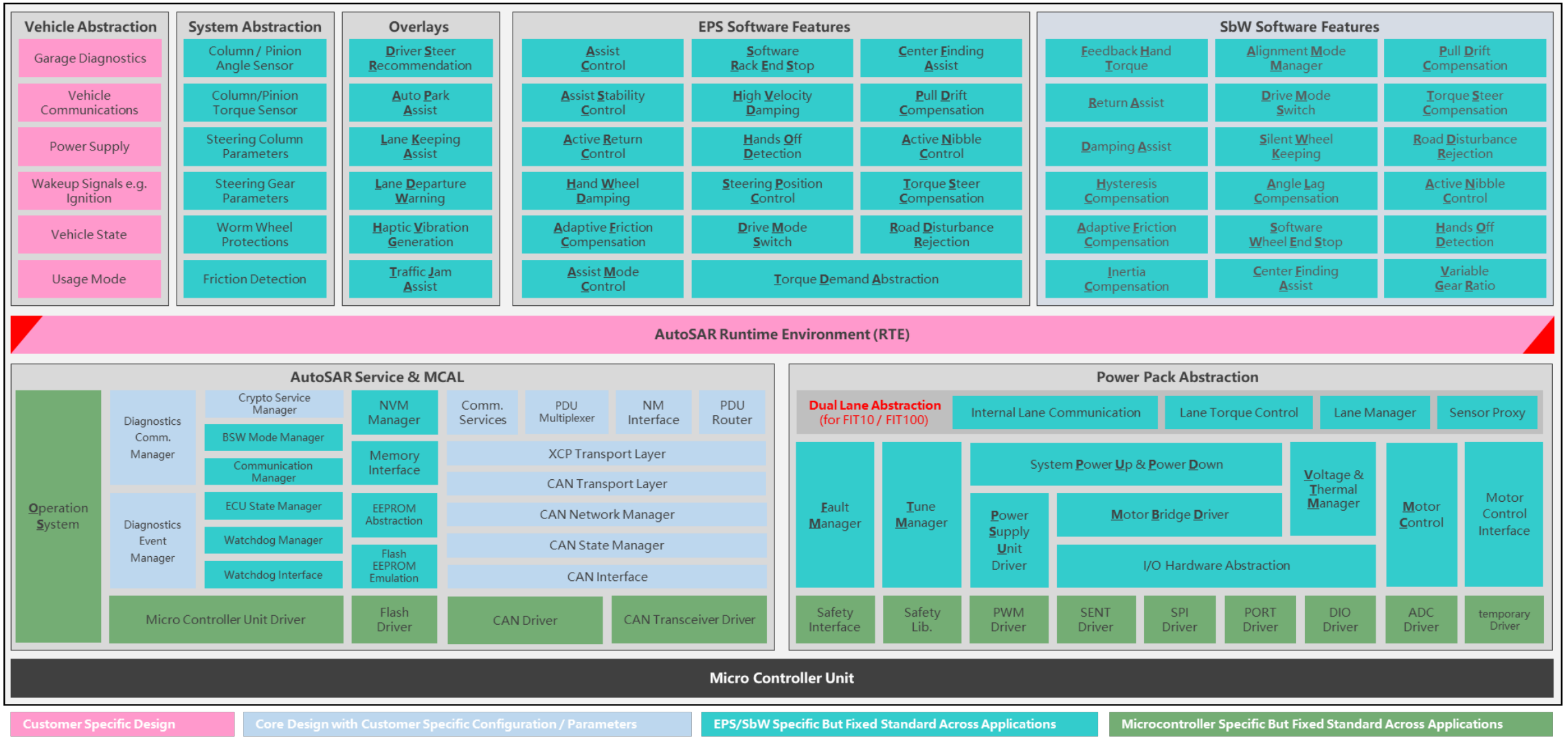
RWA: uC*2, SBC*2, pre-driver*2



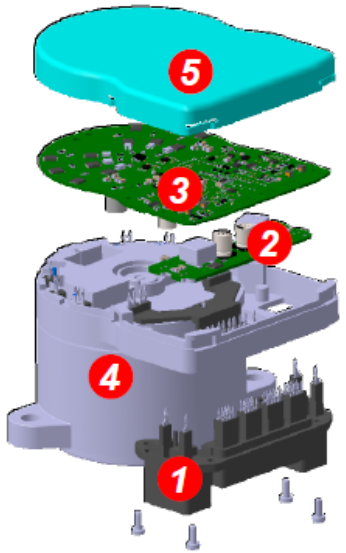
RWS: uC*1, SBC*1, pre-driver*2

Steering by Wire / software architecture

JIYU 济驭



Steering by Wire / power pack for HWA & RWA



Power Pack for Hand Wheel Actuator

1 – connector header

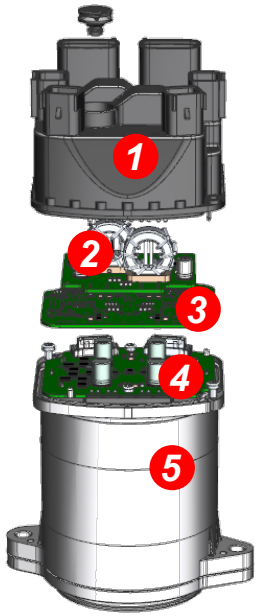
2 – PCBA/power supply

3 – PCBA/control core

4 – motor

5 – ECU cover

Item	Description
Battery Supply Current	85A eff
Protection Grade	IP5KX
Working Temperature	-40~85℃
Working Voltage	9~16V
Motor Type	PMSM (12S8P)
Torque Output	3.5Nm min.
Motor Position Sensor	TMR（Dual-Die）*2
Communication	CANFD*4
μC	Multi-core (Lock-Step)
Torque Angle Sensor	4T4A（TAS）
Quiescent Current	< 200μA



Power Pack for Road Wheel Actuator

1 – ECU housing and header

2 – PCBA/power supply

3 – PCBA/control core

4 – PCBA/drive bridge

5 – motor

Item	Description
Battery Supply Current	113A eff
Protection Grade	IP6k9k
Working Temperature	-40~125℃
Working Voltage	9~16V
Motor Type	PMSM (12S8P)
Torque Output	7.8Nm
Motor Position Sensor	TMR（Dual-Die）*2
Communication	CANFD*2
μC	Multi-core (Lock-Step)
Torque Angle Sensor	0T4A（AOS）
Quiescent Current	< 200μA

Safety Goals vs. operating modes

No	Safety Goal	Operating Mode 1	Operating Mode 2	Operating Mode 3	Operating Mode 4	Operating Mode 5
1	The SbW system shall prevent unintended lateral acceleration. [**ASIL D**]		X	X	X	
2	The SbW system shall provide the correct level of lateral acceleration within 100 ms. [**ASIL D**]		X	X	X	
3	The SbW system shall prevent loss of lateral vehicle motion control. [**ASIL D**]		X	X	X	
4	The SbW system shall prevent incorrect feedback actuation to the driver. [**ASIL D**]		X	X	X	
5	The SbW system shall prevent sudden loss of feedback torque to the driver. [**ASIL D**]		X	X	X	
6	The SbW system shall avoid any steering control output of RPA function when the vehicle speed is more than the 3kph. [ASIL D]		X	X	X	
7	The SbW system shall avoid unintended activation of remote parking assist without driver's request. [ASIL B]		X	X	X	

The following operating modes are for the Functional Safety Concept:

- *Operating mode 1: PowerOn (Electrically Power available).*
- *Operating mode 2: Initialization (Electrically Power available)*
- *Operating mode 3: Operation(Electrically Power available)*
- *Operating mode 4: Safe state(Electrically Power available)*
- *Operating mode 5: PoweOff(Electrically Power unavailable)*

SS ID	Safe State	Driver Notified
SS-1	First fault: Degraded performance Second fault: Hand over to alternative actuator or perform minimal risk maneuver.	Y
SS-2	First fault: Degraded performance Second fault: Hand over to alternative actuator or perform minimal risk maneuver.	Y
SS-3	First fault: Degraded performance Second fault: Hand over to alternative actuator or perform minimal risk manoeuvre.	Y
SS-4	First fault: Degraded performance Second fault: Feedback function is disabled and replaced with fixed steering resistance/damping.	Y
SS-5	First fault: Degraded performance Second fault: Feedback function is disabled and replaced with fixed steering resistance/damping.	Y
SS-6	First fault: Degraded performance Second fault: Feedback function is disabled and replaced with fixed steering resistance/damping.	Y

FSR No.	Functional Safety Requirement	Related Safety Goal No
FSR01	The system shall monitor vehicle speed.	SG1,SG2,SG3
FSR02	The system shall monitor steering wheel torque.	SG1,SG2,SG3
FSR03	The system shall monitor rack position.	SG1,SG2,SG3
FSR04	The system shall monitor rack position target(steering wheel angle).	SG1,SG2,SG3
FSR05	The system shall monitor AD mode request.	SG1,SG2,SG3
FSR06	The system shall monitor pinion angle.	SG1,SG2,SG3
FSR07	The system shall monitor rack force.	SG1,SG2,SG3
FSR08	The system shall monitor motor position.	SG1,SG2,SG3
FSR09	The system shall monitor motor phase current.	SG1,SG2,SG3
FSR10	The system shall monitor motor driver.	SG1,SG2,SG3
FSR11	The system shall monitor motor drive bridge.	SG1,SG2,SG3
FSR12	The system shall monitor motor actuation.	SG1,SG2,SG3
FSR13	The system shall monitor RWA failure state.	SG1,SG2,SG3
FSR14	The system shall monitor HWA failure state.	SG1,SG2,SG3
FSR15	The system shall identify target assist torque.	SG1,SG2,SG3
FSR16	The system shall set target assist arbitration element.	SG1,SG2,SG3
FSR17	The system shall calculate actual assist torque.	SG1,SG2,SG3
FSR18	The system shall compare target assist torque with actual assist torque	SG1,SG2,SG3
FSR19	The system shall monitor system temperature.	SG1,SG2,SG3
FSR20	The system shall monitor the power supply of the system.	SG1,SG2,SG3
FSR21	The system shall use MCU which shall provide some safety mechanism such as lock step,self-test,etc.	SG1,SG2,SG3
FSR22	The system shall use watchdog out of MCU.	SG1,SG2,SG3
FSR23	The system shall provide two independent failsafe path.	SG1,SG2,SG3
FSR24	The system shall implement failsafe path self-test after power on.	SG1,SG2,SG3
FSR25	If some failure detected, the system shall enter in degradation mode or backup mode, send warning to driver and record failure.	SG1,SG2,SG3
FSR26	During driving, when the domain controller does not request to exit HandWheel Tracking, RWA shall avoid system unintended exit HandWheel Tracking.	SG4
FSR27	During driving, when the domain controller does not request to exit AD Tracking, RWA shall avoid unintended exit AD Tracking.	SG5
FSR28	During driving, RWA shall monitor the mode signal to avoid the loss of the mode signal.	SG6
FSR29	During driving, when the domain controller does not request to enter HandWheel Tracking, RWA shall avoid system unintended enter HandWheel Tracking.	SG6

FSR ID	Allocated to	Requirement	FTTI	ASIL
FSR01	RWA Fail Safe Logic	The system shall monitor vehicle speed.	15ms	D

TSR ID	Allocated to	Requirement	FTTI	ASIL	SW/HW	SM
TSR001	RWA Vehicle speed signal process and monitor1	The system shall implement E2E (CRC, RLC,Timeout) check on the CAN message which contains VehSpdLgt1.	15ms	D	HW+SW	SM04
TSR002	RWA Vehicle speed signal process and monitor2	The system shall implement E2E (CRC, RLC,Timeout) check on the CAN message which contains VehSpdLgt1Bkp.	15ms	D	HW+SW	SM28
TSR003	RWA Vehicle speed signal process and monitor1	If the system detects				
TSR004	RWA Vehicle speed signal process and monitor2	If the system detects				
TSR005	RWA Vehicle speed signal process and monitor1	If the system detects				
TSR006	RWA Vehicle speed signal process and monitor2	If the system detects				
TSR007	RWA Vehicle speed signal process and monitor1	If the system detects				
TSR008	RWA Vehicle speed signal process and monitor2	If the system detects				
TSR009	RWA Vehicle speed signal process and monitor1	If the system detects failure				
TSR010	RWA Vehicle speed signal process and monitor2	If the system detects status failure				
TSR011	RWA Fail Safe output1	If RWA1 Veh failure MotorTorqueSum1+M				
TSR012	RWA Fail Safe output2	If RWA2 Veh failure MotorTorqueSum1+M				

FSR ID	Allocated to	Requirement	FTTI	ASIL
FSR29	RWA Fail Safe Logic	During driving, when the domain controller does not request to enter HandWheel Tracking, RWA shall avoid system unintended enter HandWheel Tracking		D

TSR ID	Allocated to	Requirement	FTTI	ASIL	SW/HW	SM
TSR407	RWA Fail Safe Logic1	During driving, when the domain controller does not request to enter HandWheel Tracking, avoid hand HWA1 unexpected enter HandWheel Tracking due to internal fault		D		
TSR408	RWA Fail Safe Logic2	During driving, when the domain controller does not request to enter HandWheel Tracking, avoid hand HWA2 unexpected enter HandWheel Tracking due to internal fault		D	SW	
TSR378	RWA Fail Safe Logic1	The system shall implement E2E (CRC, RLC, Timeout) check on the CAN message which contains FscmCtrlMod.		D	SW	
TSR379	RWA Fail Safe Logic2	The system shall implement E2E (CRC, RLC, Timeout) check on the CAN message which contains FscmCtrlModBkp.		D	SW	
TSR380	RWA Fail Safe Logic1	If the system detects CRC failed, then the system shall confirm FscmCtrlMod CRC failure.		D	SW	
TSR381	RWA Fail Safe Logic2	If the system detects CRC failed, then the system shall confirm FscmCtrlModBkp CRC failure.		D	SW	
TSR382	RWA Fail Safe Logic1	If the system detects RLC failed, then the system shall confirm FscmCtrlMod RLC failure.		D	SW	
TSR383	RWA Fail Safe Logic2	If the system detects RLC failed, then the system shall confirm FscmCtrlModBkp RLC failure.		D	SW	
TSR384	RWA Fail Safe Logic1	If the system detects Timeout failed, then the system shall confirm FscmCtrlMod Timeout failure.		D	SW	
TSR385	RWA Fail Safe Logic2	If the system detects Timeout failed, then the system shall confirm FscmCtrlModBkp Timeout failure.		D	SW	
TSR386	RWA Fail Safe Logic1	The system shall implement E2E (CRC, RLC, Timeout) check on the CAN message which contains FscmCtrlModReq.		D	SW	
TSR387	RWA Fail Safe Logic2	The system shall implement E2E (CRC, RLC, Timeout) check on the CAN message which contains FscmCtrlModReqBkp.		D	SW	
TSR388	RWA Fail Safe Logic1	If the system detects CRC failed, then the system shall confirm FscmCtrlModReq CRC failure.		D	SW	
TSR389	RWA Fail Safe Logic2	If the system detects CRC failed, then the system shall confirm FscmCtrlModReqBkp CRC failure.		D	SW	
TSR390	RWA Fail Safe Logic1	If the system detects RLC failed, then the system shall confirm FscmCtrlModReq RLC failure.		D	SW	
TSR391	RWA Fail Safe Logic2	If the system detects RLC failed, then the system shall confirm FscmCtrlModReqBkp RLC failure.		D	SW	
TSR392	RWA Fail Safe Logic1	If the system detects Timeout failed, then the system shall confirm FscmCtrlModReq Timeout failure.		D	SW	
TSR393	RWA Fail Safe Logic2	If the system detects Timeout failed, then the system shall confirm FscmCtrlModReqBkp Timeout failure.		D	SW	
TSR394	RWA Fail Safe Logic1	FscmSystemState?		D	SW	
TSR395	RWA Fail Safe Logic2	FscmSystemState?		D	SW	
TSR396	RWA Fail Safe Logic1	If the system detects the status of FscmCtrlMod signal is invalid, then the system shall confirm FscmCtrlMod invalid status failure		D	SW	
TSR397	RWA Fail Safe Logic2	If the system detects the status of FscmCtrlMod signal is invalid, then the system shall confirm FscmCtrlModBkp invalid status failure		D	SW	
TSR398	RWA Fail Safe Logic1	If the system detects the status of FscmCtrlModReq signal is invalid, then the system shall confirm FscmCtrlModReq invalid status failure		D	SW	
TSR399	RWA Fail Safe Logic2	If the system detects the status of FscmCtrlModReqBkp signal is invalid, then the system shall confirm FscmCtrlModReqBkp invalid status failure		D	SW	
TSR400	RWA Fail Safe Logic	The system shall identify FscmCtrlMode every xxms.		D	SW	
TSR401	RWA Fail Safe Logic1	The system shall compare FscmCtrlModReq and FscmCtrlMod every xxms.		D	SW	
TSR402	RWA Fail Safe Logic2	The system shall compare FscmCtrlModReqBkp and FscmCtrlModBkp every xxms.		D	SW	

RWA has totally 402 TSRs to meet 29 FSRs.

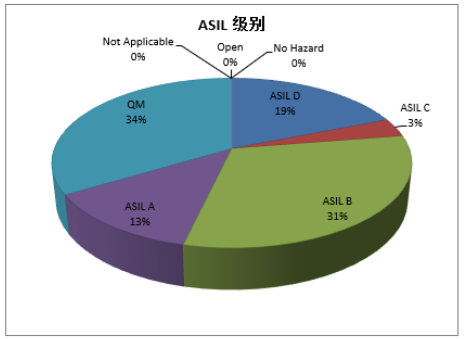
Hazard Analysis & Risk Assess

Hazard Configuration Management 危害配置管理					Allocation of Failure Modes and Situation, Conditions, Modes 分配故障模式，运行场景，环境条件，运行模式					Hazard Identification 危害识别			ASIL Allocation & Safety Goal Derivation 分配ASIL等级 & 安全目标							Review
System 系统	Subsystem 子系统	FM-ID 故障模式-ID	OP-ID 运行模式-ID	Master-Hazard-ID (created by linking row B to G) 危害-主-ID（根据B列-G列自动生成，不要手动输入）	Possible failure modes of the system / sub-system 系统 / 子系统可能的故障模式	Relevant Situations (see section "Situations") 相关场景 (见章节"Situations")				Additional pertaining criteria 附加标准	Reaction on Vehicle Level 整车层面的表现	Potential Hazard (consequence of vehicle reaction in relevant situation) 潜在危害（考虑相关场景下整车的表现）	Comments (opt.) Examples / Assumptions 注释（可选）示例/假设	Description Severity (S) 严重度描述	Description Exposure (E) 危险概率描述	Description Controllability (C) 可控性描述	S	E	C	ASIL	Safety Goal 安全目标	Yellow: to be reviewed (tbr) Red: open / Not ok Green: reviewed & ok
						Usage	Road condit	Road slop	Speed											
EPS-	RES	-FM-	2	-OP-	01	EPS-RES-FM-2-OP-01	Individual rear wheel can provide larger brake force when intended	S3-Braking	O1-High mud	S4-All	O1-High	NA										
EPS-	RES	-FM-	2	-OP-	02	EPS-RES-FM-2-OP-02	Rear axle wheel can provide larger brake force when intended	S3-Braking	O2-Low mud	S4-All	O1-High	NA										
EPS-	ANC	-FM-	3			EPS-ANC-FM-3	IBS can provide smaller brake force than intended															

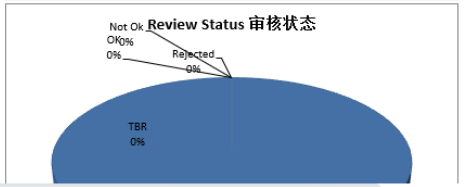
Hazard Analysis and Risk Assessment (HARA)
危害分析与风险评估

System / Project 系统 / 项目:	Intelligent Brake System 智能刹车系统
This Section 本节:	Work Product Evaluation 文件评估
Template Version 模板版本:	v0.1
Project Version 项目版本:	v0.3
Date 日期:	2020/12/3
Responsible 责任人:	xx

ASIL 级别	Quantity 数量
ASIL D	140
ASIL C	26
ASIL B	230
ASIL A	94
QM	248
Not Applicable	0
Open	0
No Hazard	0
Sum	**738**



Review Status 审核状态	Quantity 数量
Open	734
TBR	0
Rejected	0
OK	0
Not Ok	0



			C0	C1	C2	C3
S0	E0	00	NA	NA	NA	NA
	E1	01	NA	NA	NA	NA
	E2	02	NA	NA	NA	NA
	E3	03	NA	NA	NA	NA
	E4	04	NA	NA	NA	NA
S1	E0	10	NA	NA	NA	NA
	E1	11	NA	QM	QM	QM
	E2	12	NA	QM	QM	QM
	E3	13	NA	QM	QM	ASIL A
	E4	14	NA	QM	ASIL A	ASIL B
S2	E0	20	NA	NA	NA	NA
	E1	21	NA	QM	QM	QM
	E2	22	NA	QM	QM	ASIL A
	E3	23	NA	QM	ASIL A	ASIL B
	E4	24	NA	ASIL A	ASIL B	ASIL C
S3	E0	30	NA	NA	NA	NA
	E1	31	NA	QM	QM	ASIL A
	E2	32	NA	QM	ASIL A	ASIL B
	E3	33	NA	ASIL A	ASIL B	ASIL C
	E4	34	NA	ASIL B	ASIL C	ASIL D

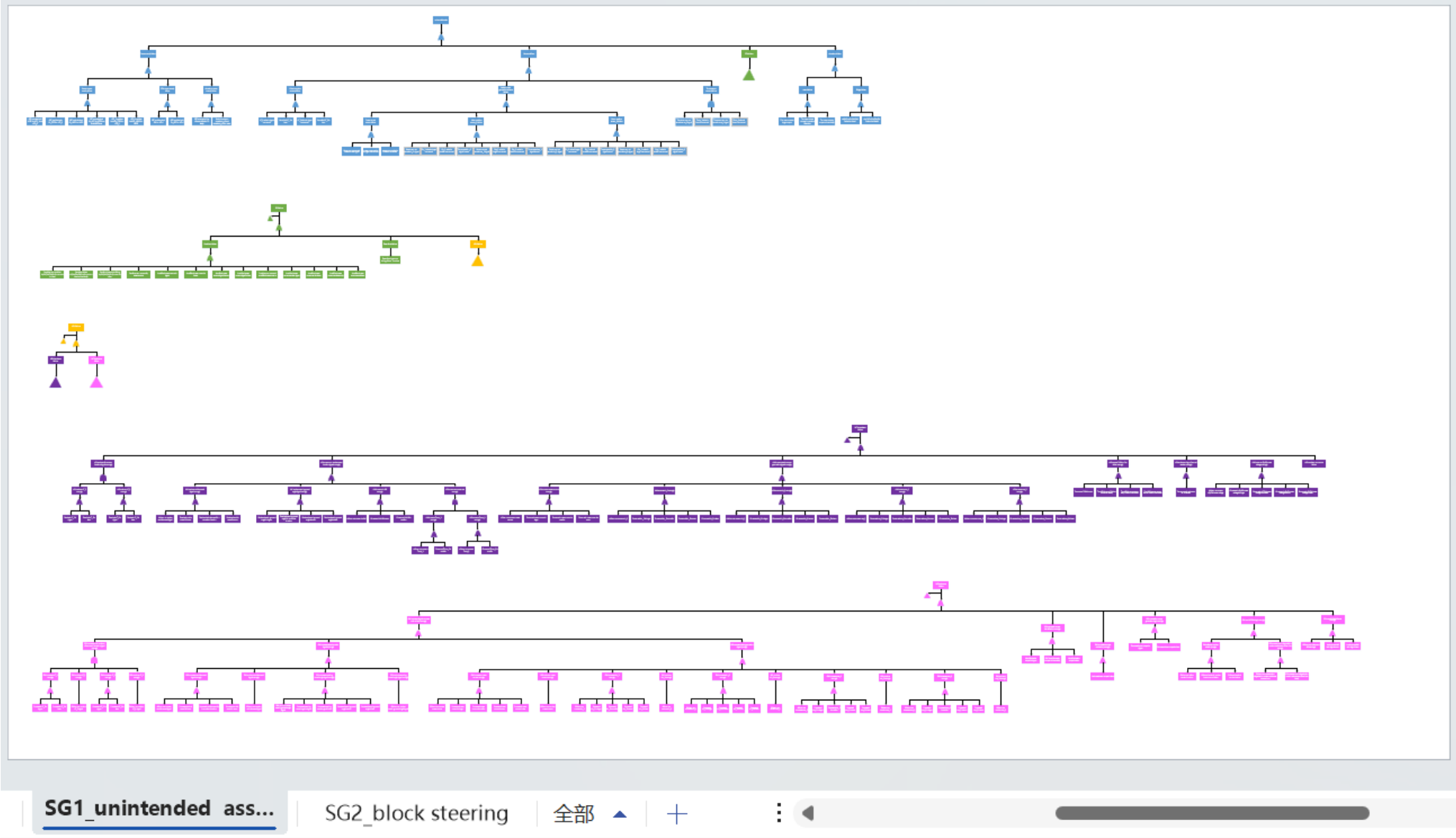
2c Malfunctions | 3 Hazard Analysis & Risk Assess | 4 Evaluation

2c Malfunctions | 3 Hazard Analysis & Risk Assess | 4 Evaluation | 5 Requirements | SEC | Calculation

Evaluation

Calculation

Steering by Wire / FuSa / FTA / example



Related Block	Related Block	Function description	HAZOP Key Word	refined Key Word	Specific Failure Mode	Effect	Violate safety goals	Safety Related?	Potential to violate the safety goal in absence of safety mechanisms	Is there any safety mechanism in place to control the failure modes of the signal	Failure mode that may lead to the violation of safety goal in combination with an another independent failure	Is there any safety mechanism to prevent the failure from latent
1. BAT _BlendingFilter												
		FuncDef_1:Obtain high-frequency hand torque BAT_HF_SWT	1)Signal too late or out of sequence.	Delay of information	The element obtains BAT_HF_SWT too late	The system can provide unintended assist	SG1	Yes	Yes	SM21	No	
				Incorrect sequence of information	The element obtains BAT_HF_SWT too late	The system can provide unintended assist	SG1	Yes	Yes	SM21	No	
				Blocking access to communication channel	The element obtains BAT_HF_SWT too late	The system can provide unintended assist	SG1	Yes	Yes	SM21	No	
				Blocking of execution	The element obtains BAT_HF_SWT too late	The system can provide unintended assist	SG1	Yes	Yes	SM21	No	
				Deadlocks	The element cannot obtain BAT_HF_SWT	The system can provide unintended assist or bolck steering	SG1、SG2	Yes	Yes	SM21	No	
				Livelocks	The element obtains BAT_HF_SWT too late	The system can provide unintended assist	SG1	Yes	Yes	SM21	No	
				Incorrect allocation of execution time	The element obtains BAT_HF_SWT too late	The system can provide unintended assist	SG1	Yes	Yes	SM21	No	
				Incorrect synchronization between software components	The element obtains BAT_HF_SWT too late	The system can provide unintended assist	SG1	Yes	Yes	SM21	No	
			2)Signal too early or out of sequence.	Incorrect sequence of information	The element obtains BAT_HF_SWT too early	No effect		No	No		No	
				Incorrect synchronization between soft□ware components	The element obtains BAT_HF_SWT too early	No effect		No	No		No	
			3)No signal	Blocking of execution	The element cannot obtain BAT_HF_SWT	No effect		No	No		No	
				Deadlocks	The element cannot obtain BAT_HF_SWT	No effect		No	No		No	
				Livelocks	The element cannot obtain BAT_HF_SWT	No effect		No	No		No	
				Incorrect synchronization between soft□ware components	The element cannot obtain BAT_HF_SWT	No effect		No	No		No	
			4)Signal value exceeds permitted range		The element obtains BAT_HF_SWT larger than actual	The system can provide unintended assist	SG1	Yes	Yes		No	
			5)Signal value falls bellows the permitted		The element obtains BAT_HF_SWT smaller than actual	No effect		No	No		No	
		FuncDef_2:Obtain low-frequency hand torque BAT_LF_SWT.	1)Signal too late or out of sequence.	Delay of information	The element obtains BAT_LF_SWT too late	The system can provide unintended assist	SG1	Yes	Yes	SM21	No	
				Incorrect sequence of information	The element obtains BAT_LF_SWT too late	The system can provide unintended assist	SG1	Yes	Yes	SM21	No	
				Blocking access to communication channel	The element obtains BAT_LF_SWT too late	The system can provide unintended assist	SG1	Yes	Yes	SM21	No	
				Blocking of execution	The element obtains BAT_LF_SWT too late	The system can provide unintended assist	SG1	Yes	Yes	SM21	No	
				Deadlocks	The element cannot obtain BAT_LF_SWT	The system can provide unintended assist or bolck steering	SG1、SG2	Yes	Yes	SM21	No	
				Livelocks	The element obtains BAT_LF_SWT too late	The system can provide unintended assist	SG1	Yes	Yes	SM21	No	
				Incorrect allocation of execution time	The element obtains BAT_LF_SWT too late	The system can provide unintended assist	SG1	Yes	Yes	SM21	No	
				Incorrect synchronization between software components	The element obtains BAT_LF_SWT too late	The system can provide unintended assist	SG1	Yes	Yes	SM21	No	
			2)Signal too early or out of sequence.	Incorrect sequence of information	The element obtains BAT_LF_SWT too early	No effect		No	No		No	
				Incorrect synchronization between soft□ware components	The element obtains BAT_LF_SWT too early	No effect		No	No		No	
			3)No signal	Blocking of execution	The element cannot obtain BAT_LF_SWT	No effect		No	No		No	
				Deadlocks	The element cannot obtain BAT_LF_SWT	No effect		No	No		No	
				Livelocks	The element cannot obtain BAT_LF_SWT	No effect		No	No		No	
				Incorrect synchronization between soft□ware components	The element cannot obtain BAT_LF_SWT	No effect		No	No		No	
			4)Signal value exceeds permitted range		The element obtains BAT_LF_SWT larger than actual	The system can provide unintended assist	SG1	Yes	Yes		No	
			5)Signal value falls bellows the permitted		The element obtains BAT_LF_SWT smaller than actual	No effect		No	No		No	
2. BAT_BoostCurve												
			1)Signal too late or out of sequence.	Delay of information	The element calculates BAT_LF_DMD too late	The system can provide unintended assist	SG1	Yes	Yes	SM21	No	
				Incorrect sequence of information	The element calculates BAT_LF_DMD too late	The system can provide unintended assist	SG1	Yes	Yes	SM21	No	
				Blocking access to communication channel	The element calculates BAT_LF_DMD too late	The system can provide unintended assist	SG1	Yes	Yes	SM21	No	
				Blocking of execution	The element calculates BAT_LF_DMD too late	The system can provide unintended assist	SG1	Yes	Yes	SM21	No	
				Deadlocks	The element cannot calculate BAT_LF_DMD	The system can provide unintended assist or bolck steering	SG1、SG2	Yes	Yes	SM21	No	

Cover | Safety Mechanism | System block Diagram | BAT FMEA | sys FMEA

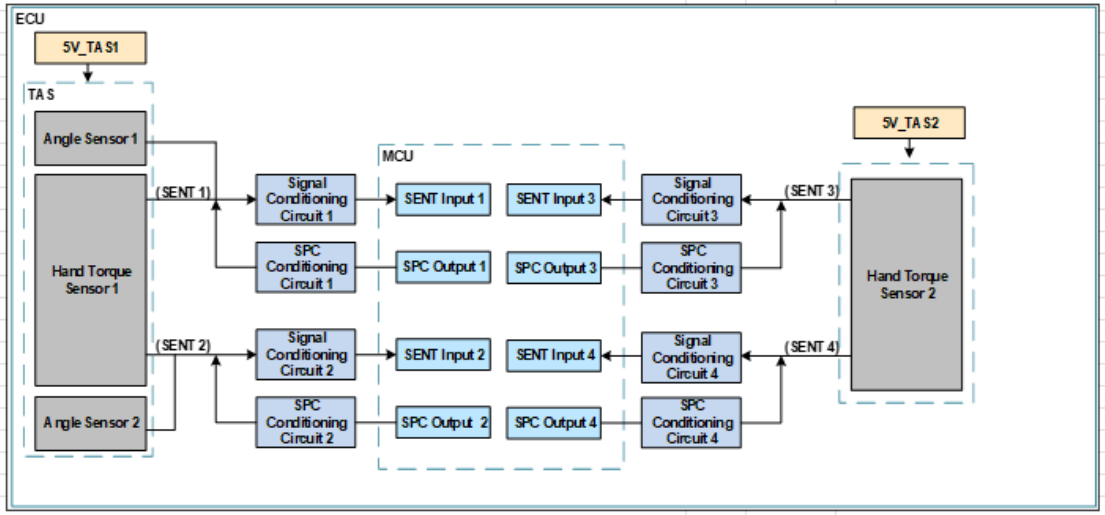
TSR ID	SG	Requirement	FTTI	ASIL	
TSR006	SG1	The system shall implement CRC check on HT_1 SENT communication every 5ms.	18ms	D	SW
TSR007	SG1	If the system detects CRC failed of SENT1 or SENT2, then the system shall confirm HT_1 CRC failure.	18ms	D	SW
TSR006	SG2	The system shall implement CRC check on HT_1 SENT communication every 5ms.	18ms	D	SW
TSR007	SG2	If the system detects CRC failed of SENT1 or SENT2, then the system shall confirm HT_1 CRC failure.	18ms	D	SW
TSR006	SG3	The system shall implement CRC check on HT_1 SENT communication every 5ms.	95ms	B	SW
TSR007	SG3	If the system detects CRC failed of SENT1 or SENT2, then the system shall confirm HT_1 CRC failure.	95ms	B	SW
TSR006	SG4	The system shall implement CRC check on HT_1 SENT communication every 5ms.	95ms	B	SW
TSR007	SG4	If the system detects CRC failed of SENT1 or SENT2, then the system shall confirm HT_1 CRC failure.	95ms	B	SW

SSR from TSR006, TSR007 and TSR008

SSR ID	Allocated to	Requirement	FTTI	ASIL	ASW/BSW
SSR021	E2EXf	The software shall check SENT1 CRC fault every 1 ms.	18ms	D	BSW
SSR022	E2EXf	If SENT1 CRC fault detected, then the software shall set: SENT1 CRC fault flag = 1 Else SENT1 CRC fault flag = 0	18ms	D	BSW
SSR023	E2EXf	The software shall detect SENT1 CRC fault flag every 10 ms.	18ms	D	BSW
SSR024	E2EXf	If the software detect: SENT1 CRC fault flag = 1 then the software shall set: SENT1 CRC fault counter+1	18ms	D	BSW
SSR025	E2EXf	If the software detects: SENT1 CRC fault flag = 0 then the software shall set: SENT1 CRC fault counter-1	18ms	D	BSW
SSR026	E2EXf	If the software detects: SENT1 CRC fault counter = 10 then the software shall set: SENT1 CRC failure flag=1. (0 ≤ counter ≤ 40)	18ms	D	BSW
SSR033	E2EXf	The software shall check SENT2 CRC fault every 1ms.	18ms	D	BSW
SSR034	E2EXf	If SENT2 CRC fault detected, then the software shall set: SENT2 CRC fault flag = 1 Else SENT2 CRC fault flag = 0	18ms	D	BSW
SSR035	E2EXf	The software shall detect SENT2 CRC fault flag every 10ms.	18ms	D	BSW
SSR036	E2EXf	If the software detect: SENT2 CRC fault flag = 1 then the software shall set: SENT2 CRC fault counter+1	18ms	D	BSW
SSR037	E2EXf	If the software detects: SENT2 CRC fault flag = 0 then the software shall set: SENT2 CRC fault counter-1	18ms	D	BSW
SSR038	E2EXf	If the software detects: SENT2 CRC fault counter = 10 then the software shall set: SENT2 CRC failure flag=1.(0 ≤ counter ≤ 40)	18ms	D	BSW
SSR045	E2EXf	If the software detects SENT1 CRC failure flag = 1 or SENT2 CRC failure flag = 1, then the software shall confirm HT_1 CRC failure.	18ms	D	BSW

1. Hand Torque and Angle Sensor Module

TSR ID	TSR Description	ASIL	FTTI	Allocation
TSR001	The system shall use two hand torque sensors to measure the driver hand torque. One is called HT_1, the other is called HT_2. HT_1 has two signals, called SENT1 and SENT2. HT_2 has two signals, called SENT3 and SENT4. (Resolution:0.02Nm, Accuracy:±0.1Nm, Range: ±12Nm)	QM	18ms	HW
TSR002	The type of hand torque sensors shall be SPC.	QM	18ms	HW
TSR194	The system shall use two angle sensors to measure steering wheel angle. One is called ANG_1, the other is called ANG_2. (Resolution: TBD, Accuracy: TBD, Range: TBD)	QM	18ms	HW
TSR195	The type of hand angle sensors shall be SPC.	QM	18ms	HW



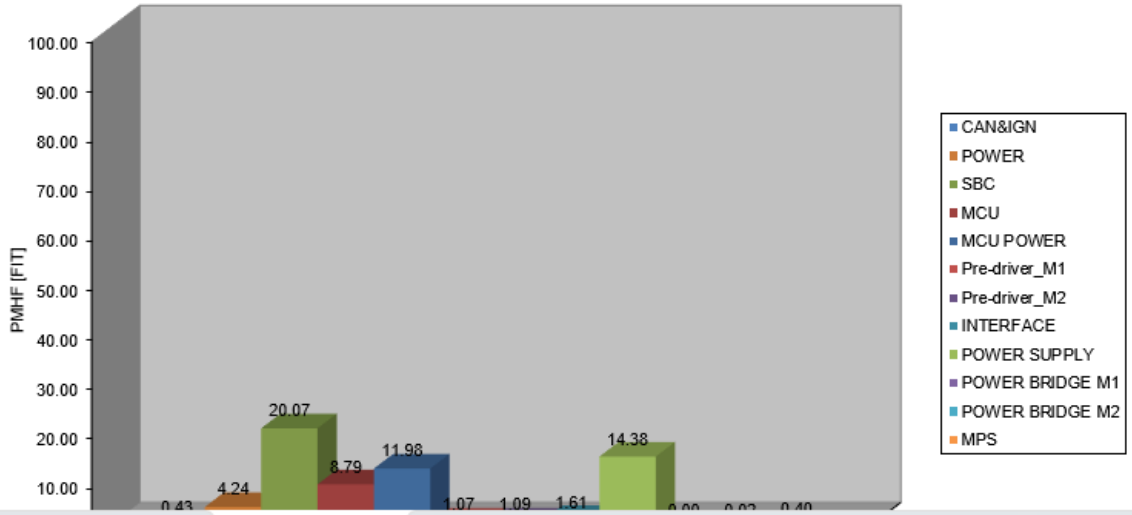
ID	Hardware Safety Requirement	ASIL	FTTI	Allocation	Safe State	Acceptance
HSR001	Operating supply voltage 1: Min. 4.5V, Typ. 5.0V, Max. 5.5V	QM	18ms	5V_TAS1	No assistance	5V_TAS1 voltage 4.5 ~ 5.5V
HSR002	Operating supply voltage 2: Min. 4.5V, Typ. 5.0V, Max. 5.5V	QM	18ms	5V_TAS2	No assistance	5V_TAS2 voltage 4.5 ~ 5.5V
HSR003	The Hand Torque Sensor 1 provides SENT_1 and SENT_2	QM	NA	Hand Torque Sensor 1	NA	NA
HSR004	The Hand Torque Sensor 2 provides SENT_3 and SENT_4	QM	NA	Hand Torque Sensor 2	NA	NA
HSR005	HT channels is digital with a SENT based protocol (SPC).	QM	18ms	Hand Torque Sensor 1,Hand Torque Sensor 2	4/4 TAS channels failure: no assist 3/4 TAS channels failure: no assist 2/4 TAS1 channels failure: no assist TAS1 and TAS2 rangecheck and	Decode correctly

Cover Sheet | Reference | HSR

Safety Goal	ASIL Level
SG3: EPS shall not Lost assist.	ASIL B

Functional Block Summary

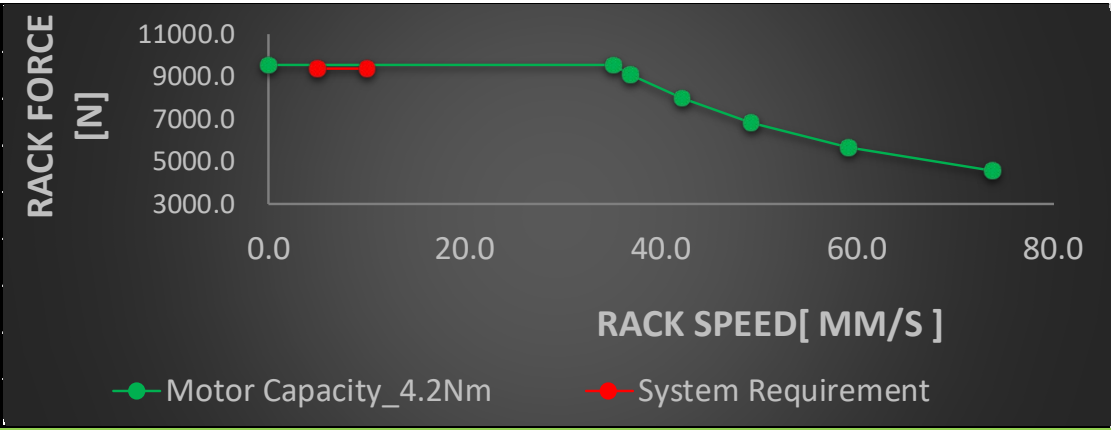
Functional Block	λ_{SR} [FIT]	λ_{SPF} [FIT]	λ_{RF} [FIT]	$\lambda_{MPF,latent}$ [FIT]	PMHF [FIT]		SPFM		LFM	
CAN&IGN	63.62	0.00	0.43	0.43	0.43	ASIL D	99.32%	ASIL D	99.33%	ASIL D
POWER	89.24	4.19	0.05	0.74	4.24	ASIL D	95.25%	ASIL B	99.13%	ASIL D
SBC	156.29	19.21	0.86	1.25	20.07	ASIL C	87.16%	ASIL A	99.08%	ASIL D
MCU	5774.68	0.00	7.98	14.37	8.79	ASIL D	99.86%	ASIL D	99.75%	ASIL D
MCU POWER	46.69	11.68	0.30	0.31	11.98	ASIL C	74.34%	ASIL A	99.11%	ASIL D
Pre-driver_M1	144.76	0.00	1.07	3.65	1.07	ASIL D	99.26%	ASIL D	97.46%	ASIL D
Pre-driver_M2	145.83	0.00	1.08	0.00	1.09	ASIL D	99.26%	ASIL D	97.48%	ASIL D
INTERFACE	332.70	0.00	1.61	2.03	1.61	ASIL D	99.52%	ASIL D	99.39%	ASIL D
POWER SUPPLY	44.49	0.00	0.00	0.00	14.38	ASIL C	67.69%	ASIL A	100.00%	ASIL D
POWER BRIDGE M1	77.68	0.00	0.00	0.56	0.00	ASIL D	100.00%	ASIL D	99.28%	ASIL D
POWER BRIDGE M2	77.68	0.00	0.02	0.58	0.02	ASIL D	99.97%	ASIL D	99.25%	ASIL D
MPS	85.53	0.00	0.40	0.80	0.40	ASIL D	99.53%	ASIL D	99.06%	ASIL D
Total Value	**7039.19**	**35.08**	**13.82**	**24.71**	**64.09**	**ASIL C**	**99.31%**	**ASIL D**	**99.65%**	**ASIL D**



Summary | SN29500 Constants | IEC61709 FMD | BOM | BOM_2 | CAN&IGN | POWER | SBC | MCU

02 Proposal for Robo-Bus

1. Customer Information		
1.1	Customer	XXXX
1.2	Platform	TBD
1.3	Vchicle Type	TBD
1.4	Drive Type	TBD
1.6	Rack Force(N)	9400
1.7	Rack Travel(mm)	100
1.9	R/P efficient	0.9
1.10	C-Factor（mm/rev）	44.3



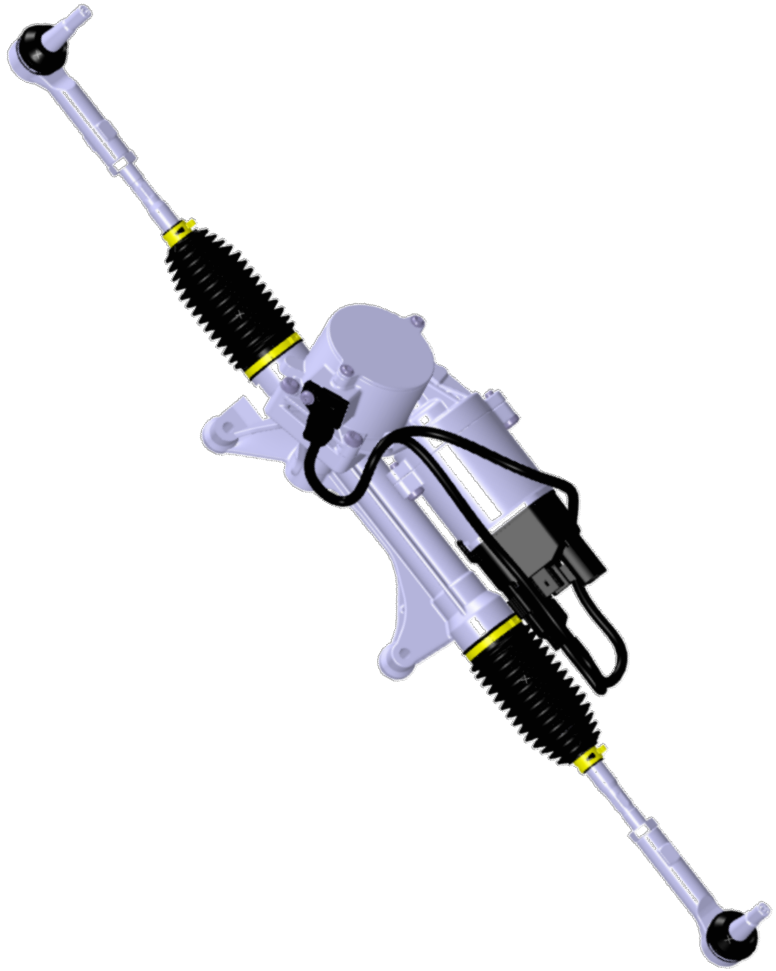
2. SBW RWA Assistance Requirement

Condition		Rack Force Percentage	Rack Force (N)	Rack Speed (mm/s)
1	Auto Parking1	100%	9400	5
2	Auto Parking2	100%	9400	10

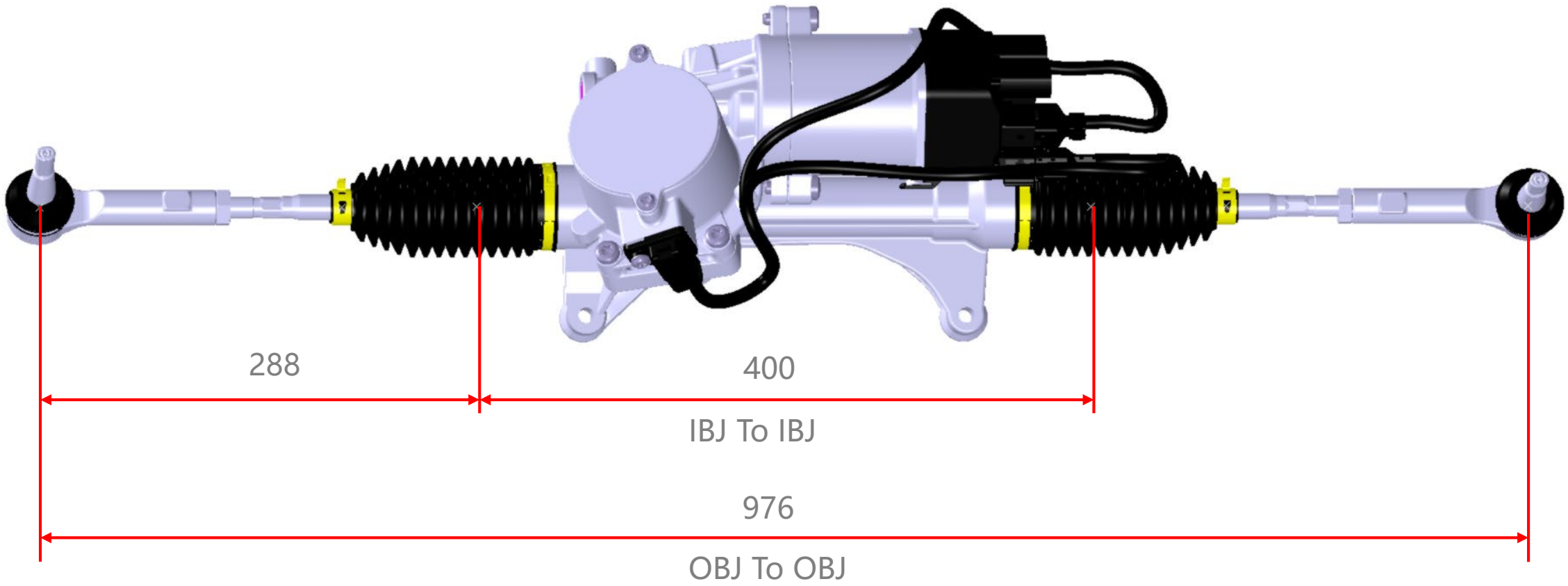
3.Motor Capacity

Torque Output (Nm)	Motor Speed （rpm）	Power （W）	Rack Foce （N）	Max. Rack Speed (mm/s)
4.2	0	0	9570	0.0
4.2	1000	440	9570	35.2
4	1050	440	9114	36.9
3.5	1200	440	7975	42.2
3	1400	440	6836	49.2
2.5	1680	440	5696	59.1
2	2100	440	4557	73.8

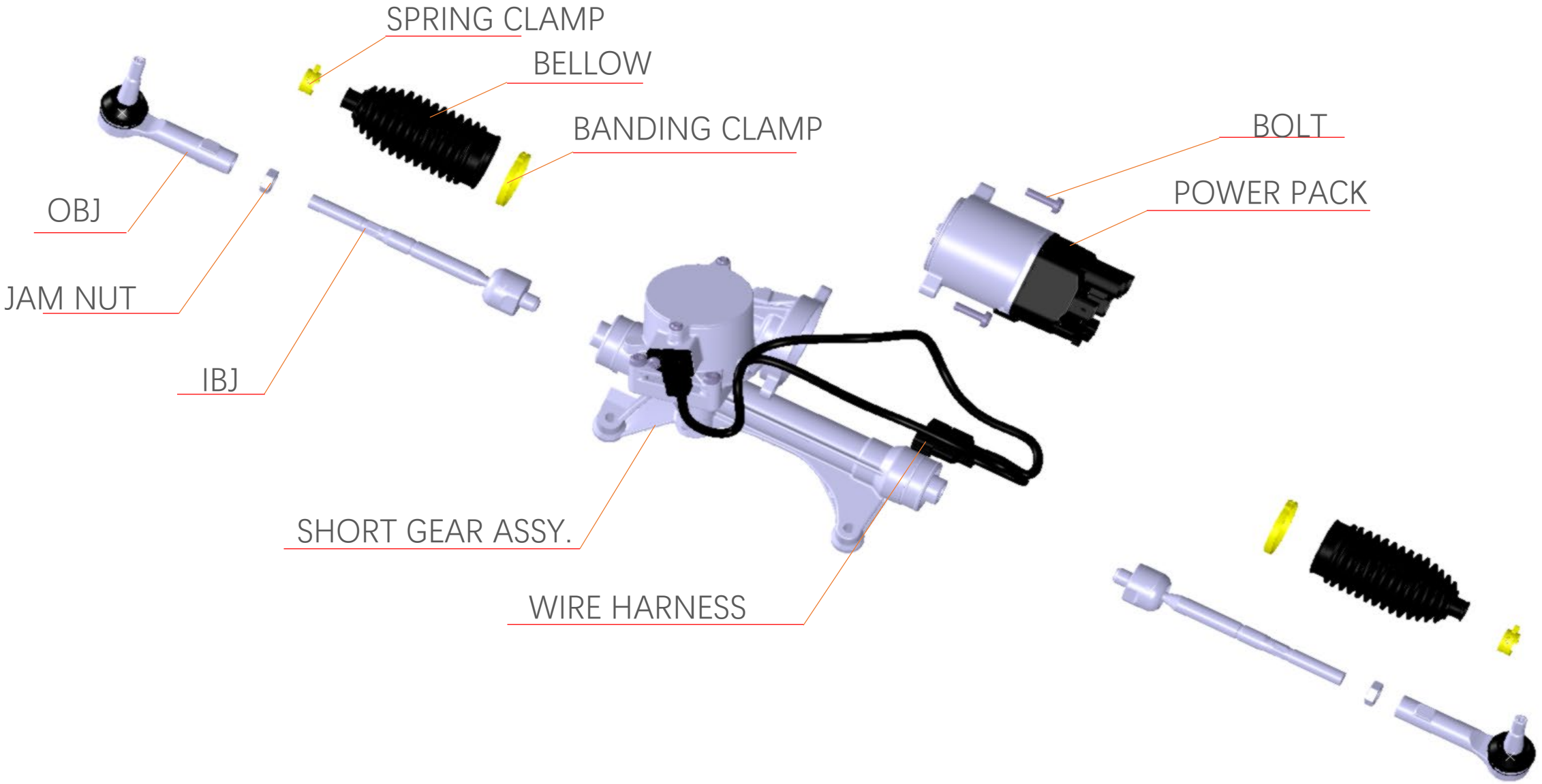
Steering by Wire / RWA / system parameters



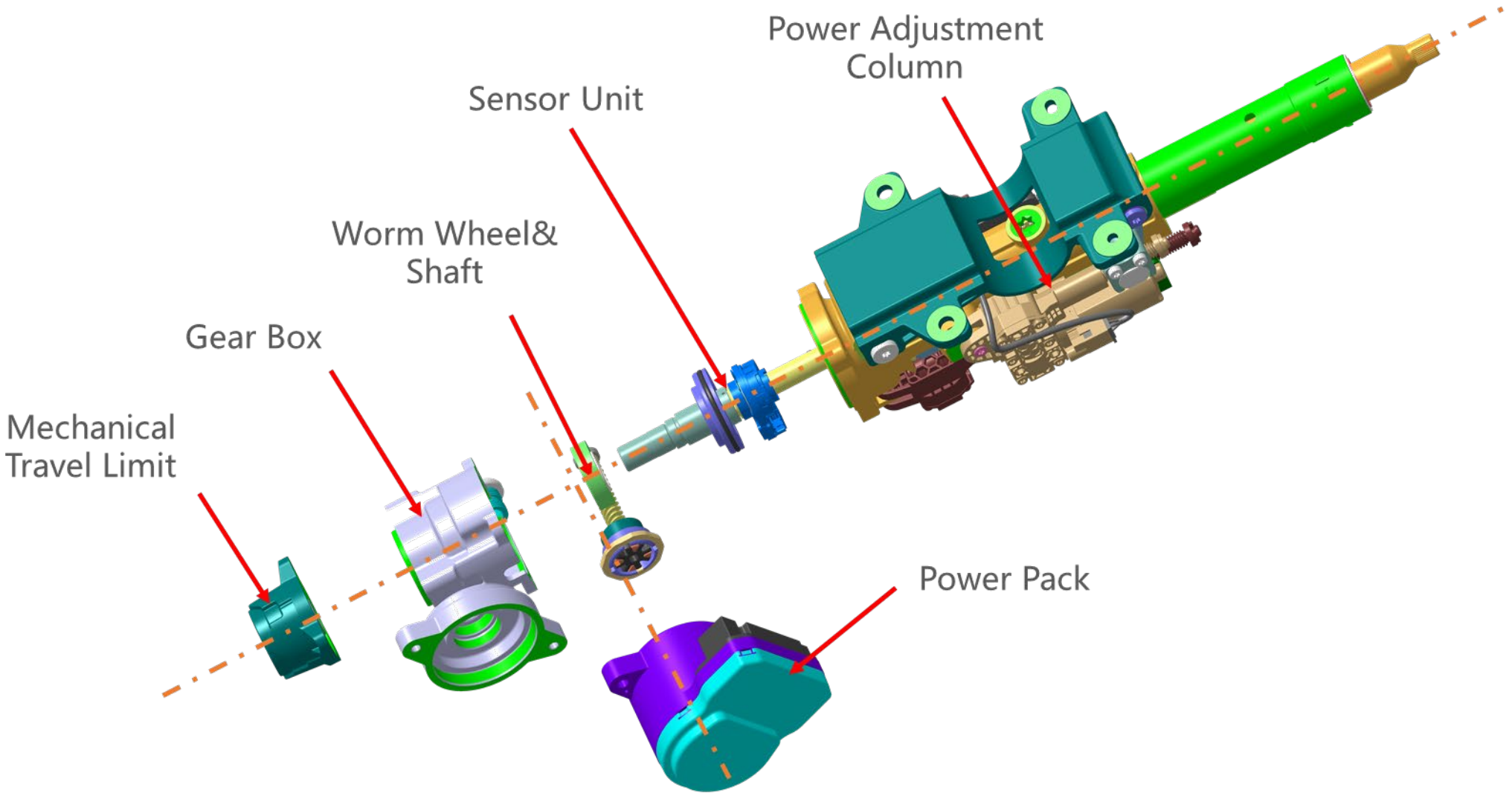
Item	Value
Motor Type	PMSM _ Double Winding
Motor Torque	4.2Nm
ECU Current	80A Max
Function Safety	Fit10 (Full Redundant)
Gear Reduction	Worm Wheel & Worm Shaft
Sensor Type	Inductive Hella 4T+2A
Gear Ratio	21:1
R/P C-Factor	44.3mm/rev
Rack Travel	100mm
IBJ to IBJ distance	400mm
OBJ to OBJ distance	976mm
IP Level	IP69K
Weight	9.8kg


288
400
IBJ To IBJ
976
OBJ To OBJ

Steering by Wire / RWA / product explode view



Item	Value
Motor Type	PMSM _ Double Winding
Motor Torque	3.5Nm
ECU Current	80A Max
Function Safety	Fit10 (Full Redundant)
Gear Reduction	Worm Wheel & Worm Shaft
Sensor Type	Inductive Hella 4T+2A
Gear Ratio	21:1
Telescope Travel Range	+30 ~ -120mm+
Telescope Speed	20mm/s
Tilt Travel Range	-26mm ~ +26mm
Tilt Speed	10mm/s
Mechanical Travel Limit Range	-510° ~ +510°
MTL strength	150Nm


Power Adjustment Column
Sensor Unit
Worm Wheel& Shaft
Gear Box
Mechanical Travel Limit
Power Pack

YouTube Link, JIYU-Chassis-By-Wire:

www.shanghaijiyu.com