ISO 26262 Functional Safety Compliant BMS

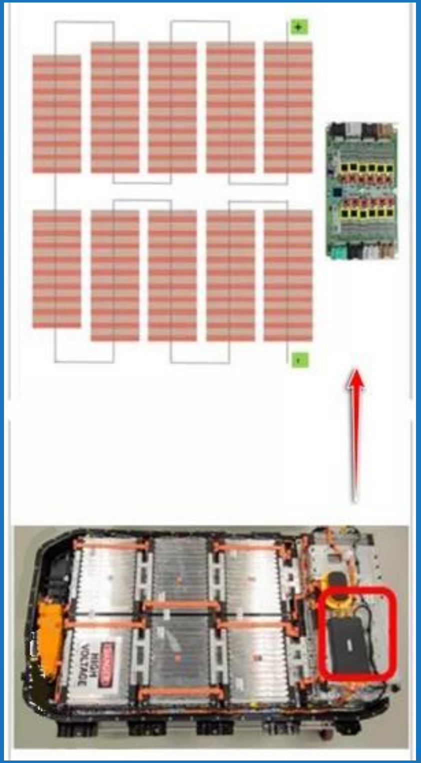
HKPC TechDive: Smart City – EV Technology
27 May 2020

Yiu Chi Wai
Consultant, Smart Electronics
Hong Kong Productivity Council

Battery Management System (BMS)

Main Features

• Cell Voltage Monitor	檢測單體電芯電壓
• Pre-charge Control	預充電控制
• SOC Calculation	SOC演算
• SOH Estimation	SOH估算
• SOP calculation	電池功率計算
• Charge Control	充電控制
• Discharge Control	放電控制
• Cell Balancing	電池單體均衡
• Thermal Management	熱管理
• Self Diagnostic	系統自我診斷



What is Functional Safety?

Absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E safety-related systems.

Scope of ISO 26262 for Automotive	
1st Edition 2011	2nd Edition 2018
Electrical / electronic (E/E) systems	Unchanged
Does not address electric shock, fire, radiation, toxicity, reactivity, corrosion, explosion, etc.	Unchanged
Mass produced vehicle mass up to 3,500 kg	Include motorcycles & commercial vehicles
Exclude special purpose vehicles	Exclude non-road going vehicles

China Counterpart: GB/T 34590-2017《道路车辆 功能安全》

Why ISO 26262?

Potential Legal Consequences

- ISO 26262 describes the SOTA in relation to functional safety during the lifecycle of safety-related systems comprised of E/E and software elements in vehicles that provide safety related functions.
- It is difficult to show evidence of compliance to SOTA without complying to ISO 26262, e.g. Toyota unintended acceleration 2013.

OEM Requirement

- All major European car makers;
- China Jeely, BAIC, SAIC, Great Wall, Nio, etc.

Self Improvement

- Minimise systematic failures;
- Improve reliability & robustness;
- Boost customer confidence.

Functional Safety In Various Industries

Medical
IEC 62304

Machinery
ISO 25119
IEC 62061
ISO 13849

Industrial Process
IEC 61511/3

Generic Safety Standard

IEC 61508

Automotive
ISO 26262

Railway
EN 50126/8/9

Aerospace
DO-178 8/C
DO - 254

Automotive Safety Integrity Level (ASIL)

ASIL (Automotive Safety Integrity Level)

One of four levels to specify the item's or element's necessary requirements of ISO 26262 and safety measures to apply for avoiding an unreasonable residual risk, with D representing the most stringent and A the least stringent level.

Limits for observable incident rate

ASIL	Observable incident rate
D	$< 10^{-9}$ /h
C	$< 10^{-8}$ /h
B	$< 10^{-8}$ /h
A	$< 10^{-7}$ /h

Targets for minimum service period of candidate

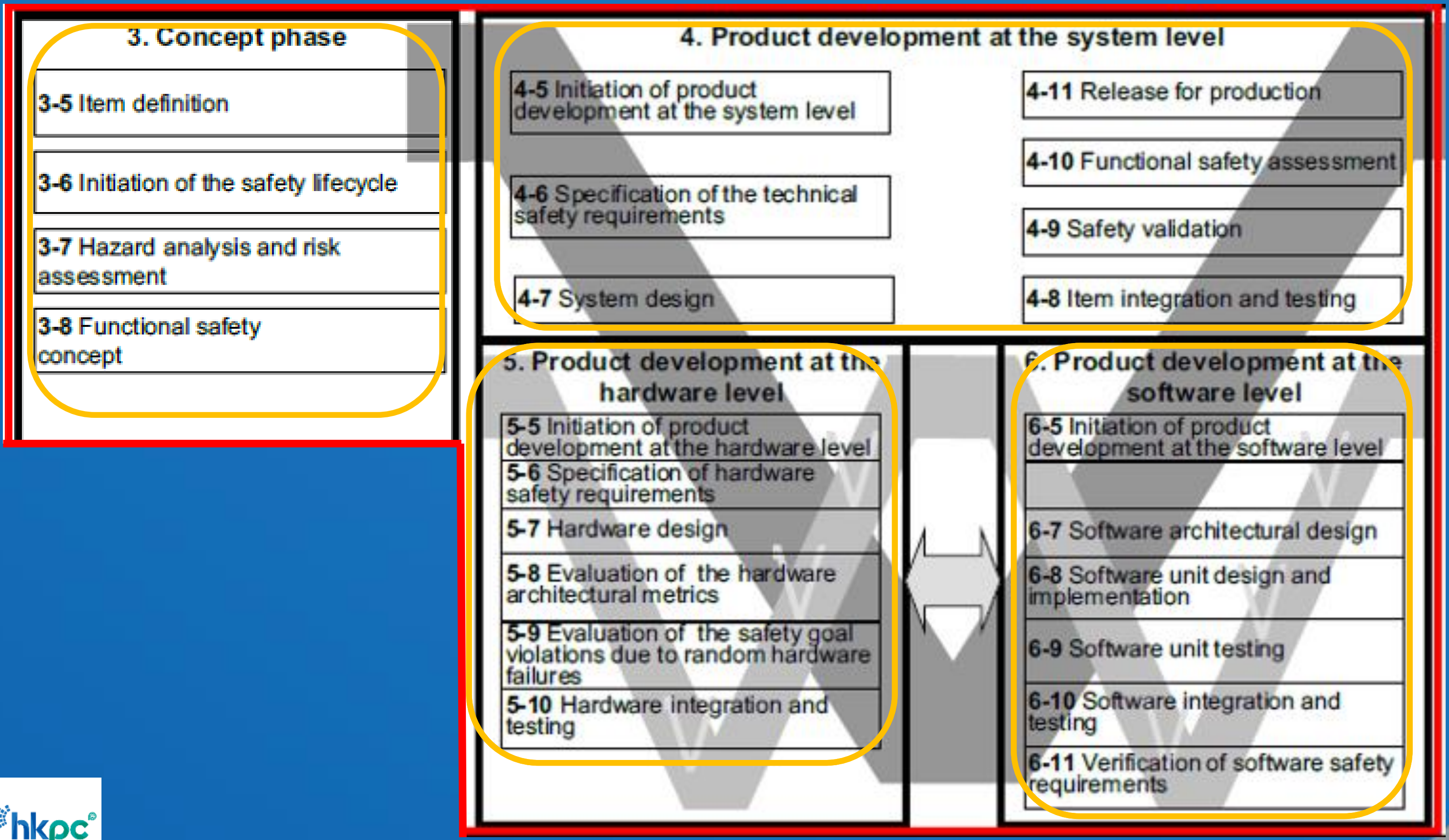
ASIL	Minimum service period without observable incident
D	1.2×10^{9} /h
C	1.2×10^{8} /h
B	1.2×10^{8} /h
A	1.2×10^{7} /h

Table 6 — Possible source for the derivation of the random hardware failure target values

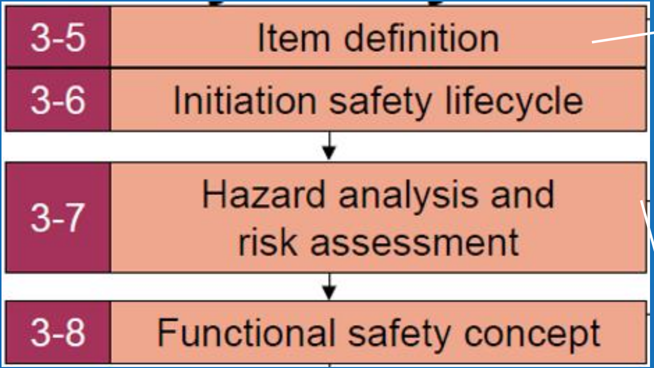
ASIL	Random hardware failure target values
D	$<10^{-8}\ h^{-1}$
C	$<10^{-7}\ h^{-1}$
B	$<10^{-7}\ h^{-1}$

NOTE The quantitative target values described in this table can be tailored as specified in 4.1 to fit specific uses of the item (e.g. if the item is able to violate the safety goal for durations longer than the typical use of a passenger car).

Functional Safety Lifecycle - Core



Concept Level



Objectives

1) To define and describe the item, its dependencies on, and interaction with, the environment and other items;

2) To support an adequate understanding of the item so that the activities in subsequent phases can be performed.

The objective of the hazard analysis and risk assessment (HARA) is to identify and to categorize the hazards that malfunctions in the item can trigger & to formulate the safety goals related to the Prevention or mitigation of the hazardous events, in order to avoid unreasonable risk.

Concept Level

HARA – Hazard Analysis & Risk Assessment

What can happen?

Table 1 — Classes of severity

	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

How often?

Table 2 — Classes of probability of exposure regarding operational situations

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

Can the driver control it?

Table 3 — Classes of controllability

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

Concept Level

HARA - Initial ASIL determination

Table 4 — ASIL determination

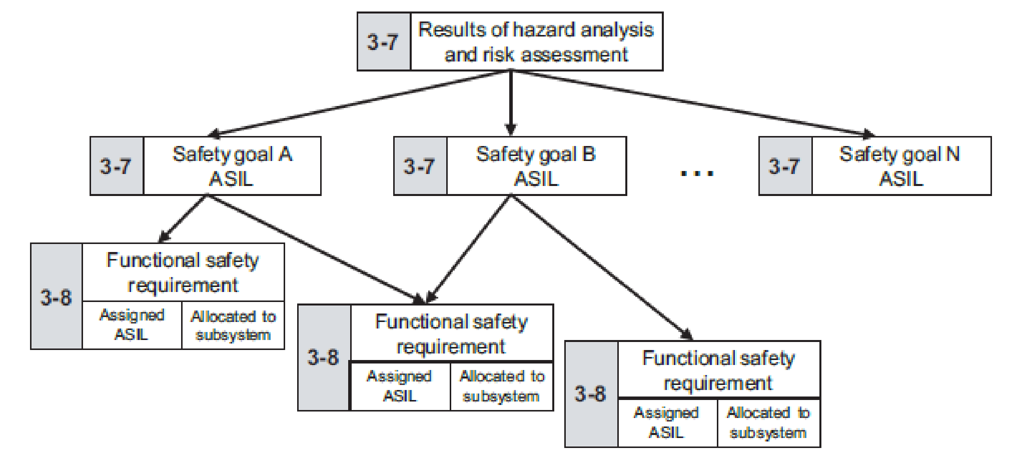
Severity class	Probability class	Controllability class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Concept Level

Safety Goals of BMS (as a result of HARA)

	Discharging	Charging	Monitoring	Balancing	Thermal Management	Exception Handling	Collision Protection	Maintenance & Service	Battery Protection
SG-001 Avoid over charging battery		X	|	X					X
~~SG-002 Avoid unintended cut off of DC/DC converter relay~~	~~X~~		~~X~~						
SG-003 Avoid unintended cut-off of main relay	X								
SG-004 Avoid over discharging battery	X			X					X
SG-005 Avoid incorrect cooling & heating operation	X	X			X				
SG-006 Avoid over temperature operation	X	X		X	X				
SG-007 Avoid over current operation	X	X		X					
SG-008 Assure to cut off all relays after collision	X						X		
SG-009 Avoid operation when there is a leakage current	X	X				X			

Concept Level



Functional Safety Concept

Objectives:

- Fault detection & mitigation;
- Transition to a safe state;
- Fault tolerance mechanisms;
- Driver warning;
- Arbitration logic from multiple requests.

Concept Level

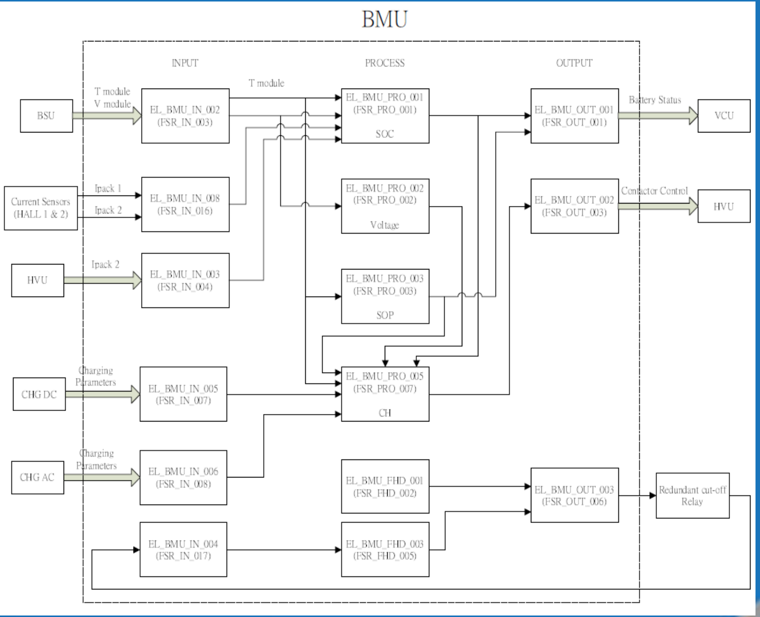
FSC Example:

Decomposition SG into FSR

SG-001 Avoid over charging battery

FSR	Description	ASIL	FTTI	Safety state	Verification criteria	Allocation to elements
FSR_IN_003	BMU shall receive correct module voltage & temperature signal from BSU via CAN	ASIL C	TBD - 1s	Restriction state(warning & power limit)		BMU CAN input capture (BSU-BMU) EL_BMU_IN_002
FSR_IN_004	BMU shall receive correct current, temperature & relay status from HVU	ASIL B	TBD - 1s	Restriction state (warning & power limit)		BMU CAN input capture (HVU-BMU) EL_BMU_IN_003
FSR_IN_007	BMU shall receive correct charging parameters from off-board charger	ASIL B	TBD - 1s	Restriction state(warning & power limit), cut-off state		BMU CAN input capture (CHGDC-BMU) EL_BMU_IN_005
FSR_IN_008	BMU shall receive correct charging parameters from on-board charger	ASIL B	TBD - 1s	Restriction state(warning & power limit), cut-off state		BMU CAN input capture (CHGAC-BMU) EL_BMU_IN_006
FSR_IN_005	BSU shall capture correct module voltage	ASIL B	TBD - 1s	Restriction state(warning & power limit), cut-off state		BSU cell voltage input capture function EL_BSU_IN_001
FSR_IN_006	BSU shall capture correct cell temperature signal	ASIL C	TBD - 1s	Restriction state(warning & power limit), cut-off		BSU cell voltage input capture function EL_BSU_IN_001

Safety Architecture



System Level

- ✓ Safety lifecycle steps for item system engineering
- ✓ ✓ Technical Safety Requirements (TSR)
- ✓ Technical Safety Concept including the System Design
- ✓ Steps for Integration and Testing
- ✓ Safety Validation and Functional Safety Assessment

Technical Safety Concept (TSC)

FSR ID	FSR Description / TSR ID	TSR Description	ASIL	Funcional Elements	Functional Elements Description	SW/HW	FSR ID
FSR_IN_001	BMU shall receive intended discharge request,speed,gear... from VCU via CAN		ASIL B	EL_BMU_IN_001	BMU CAN input capture function (VCU-BMU)		
	TSR_BMU_IN_001	BMU MCU shall capture discharging request from Motor control unit via vehicle CAN correctly	ASIL B	EL_BMU_IN_001	BMU CAN input capture function (VCU-BMU)	HW,SW	FSR_IN_001
	TSR_BMU_IN_002	BMU MCU shall get vehicle speed from VCU via vehicle CAN correctly	ASIL B	EL_BMU_IN_001	BMU CAN input capture function (VCU-BMU)	SW	FSR_IN_001
	TSR_BMU_IN_003	BMU MCU shall get gear position from VCU via vehicle CAN correctly	ASIL B	EL_BMU_IN_001	BMU CAN input capture function (VCU-BMU)	SW	FSR_IN_001
	TSR_BMU_IN_004	BMU shall get status information form VCU (error,motor status,dcdc status,ect...) via vehicle CAN correctly	ASIL B	EL_BMU_IN_001	BMU CAN input capture function (VCU-BMU)	SW	FSR_IN_001
	TSR_BMU_IN_005	BMU MCU shall get vehicle wakeup signal via vehicle CAN correctly	ASIL B	EL_BMU_IN_001	BMU CAN input capture function (VCU-BMU)	SW	FSR_IN_001
FSR_IN_002	BMU shall receive intended wakeup signal from VCU (HW)		ASIL B	EL_BMU_IN_004	BMU HW digital input capture function		
	TSR_BMU_IN_006	BMU_EL_IN_004 shall get wakeup signal from VCU via hard wire	ASIL B	EL_BMU_IN_004	BMU HW digital input capture function	HW,SW	FSR_IN_002
FSR_IN_003	BMU shall receive correct module voltage & temperature signal from BSU via CAN		ASIL C	EL_BMU_IN_002	BMU CAN input capture (internal CAN)		
	TSR_BMU_IN_007	BMU MCU shall get module voltage via BSU CAN correctly	ASIL C	EL_BMU_IN_002	BMU CAN input capture (internal CAN)	HW,SW	FSR_IN_003
	TSR_BMU_IN_008	BMU MCU shall get module temperature via BSU CAN correctly	ASIL C	EL_BMU_IN_002	BMU CAN input capture (internal CAN)	SW	FSR_IN_003

APAS 汽車科技研發中心 hkpc 生產力局

System Level

Safety Analyses

- Failure Mode and Effects Analysis (FMEA)
- Failure Mode, Effects, and Criticality Analysis (FMECA)

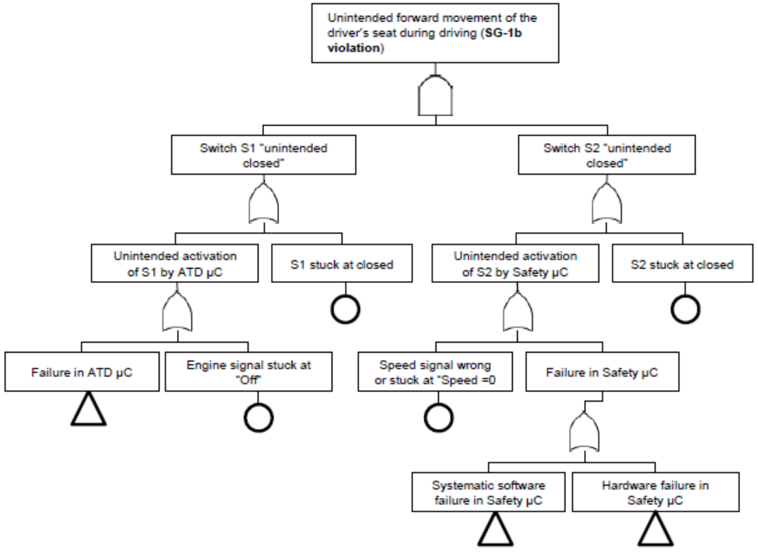
Inductive analysis:

FMEA, FMECA

Component	Effect		Causes (failure modes)		Measures		RPN
	Description	S	Description	O	Description	D	S*O*D
ATD µC	Unintended forward movement of driver's seat during parking or traffic light stops	10	Random hardware failures or systematic software faults in the ATD µC lead to an unintended activation of S1 and in combination with an unintended activation of S2 to an unintended activation of the seat motor and a forward movement of the driver's seat.	3	Current measures: - none – (To be addressed in ATD µC and in ATD µC SW development)	10	300
					New measures:		
Safety µC		10	Random hardware failures or systematic software faults in the Safety µC lead to an unintended activation of S2 and in combination with an unintended activation of S1 to an unintended activation of the seat motor and a forward movement of the driver's seat.	3	Current measures: - none – (To be addressed in Safety µC and in Safety µC SW development)	10	300
					New measures:		

Deductive analysis:

Fault Tree Analysis



Hardware Level

Types of Faults:
- Safe fault
- Multiple-point fault
- Latent fault
- Residual fault

Hardware Metrics:
- SPFM - Single-Point Fault Metric
- LFM - Latent Fault Metric
- PMHF - Probabilistic Metric for Hardware Failure

Failure rate: “λ”

Failure In Time (FIT): 1 FIT = 10^{-9} failures /h

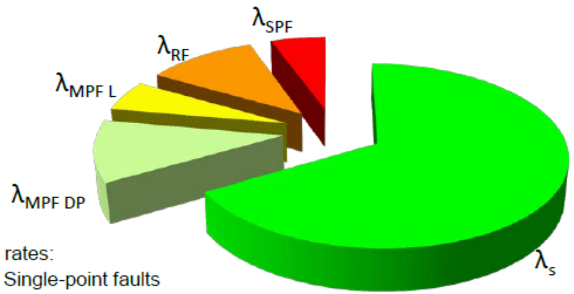
	Analysis of HW faults (-5, 7.4.3.2)	PMHF target values	SPFM target values	LFM target values
ASIL A				
ASIL B		10^{-7} per hour (100 FIT)	≥ 90 %	≥ 60 %
ASIL C	required	10^{-7} per hour (100 FIT)	≥ 97 %	≥ 80 %
ASIL D	required	10^{-8} per hour (10 FIT)	≥ 99 %	≥ 90 %

not required

recommended

required

$$PMHF = \lambda_{SPF} + \lambda_{RF} + \lambda_{SR} * \lambda_{DPFL} * T_{Lifetime}$$



Failure rates:

λ_{SPF}	Single-point faults
λ_{RF}	Residual faults
$\lambda_{MPF\ L}$	Multiple-point faults latent
$\lambda_{MPF\ DP}$	Multiple-point faults detected or perceived
λ_S	Safe faults

$$SPFM = \frac{\sum_{\text{Safety-related HW components}} (\lambda_{MPF} + \lambda_S)}{\sum_{\text{Safety-related HW components}} \lambda}$$

$$LFM = \frac{\sum_{\text{Safety-related HW components}} (\lambda_{MPF\ DP} + \lambda_S)}{\sum_{\text{Safety-related HW components}} (\lambda - \lambda_{SPF} - \lambda_{RF})}$$

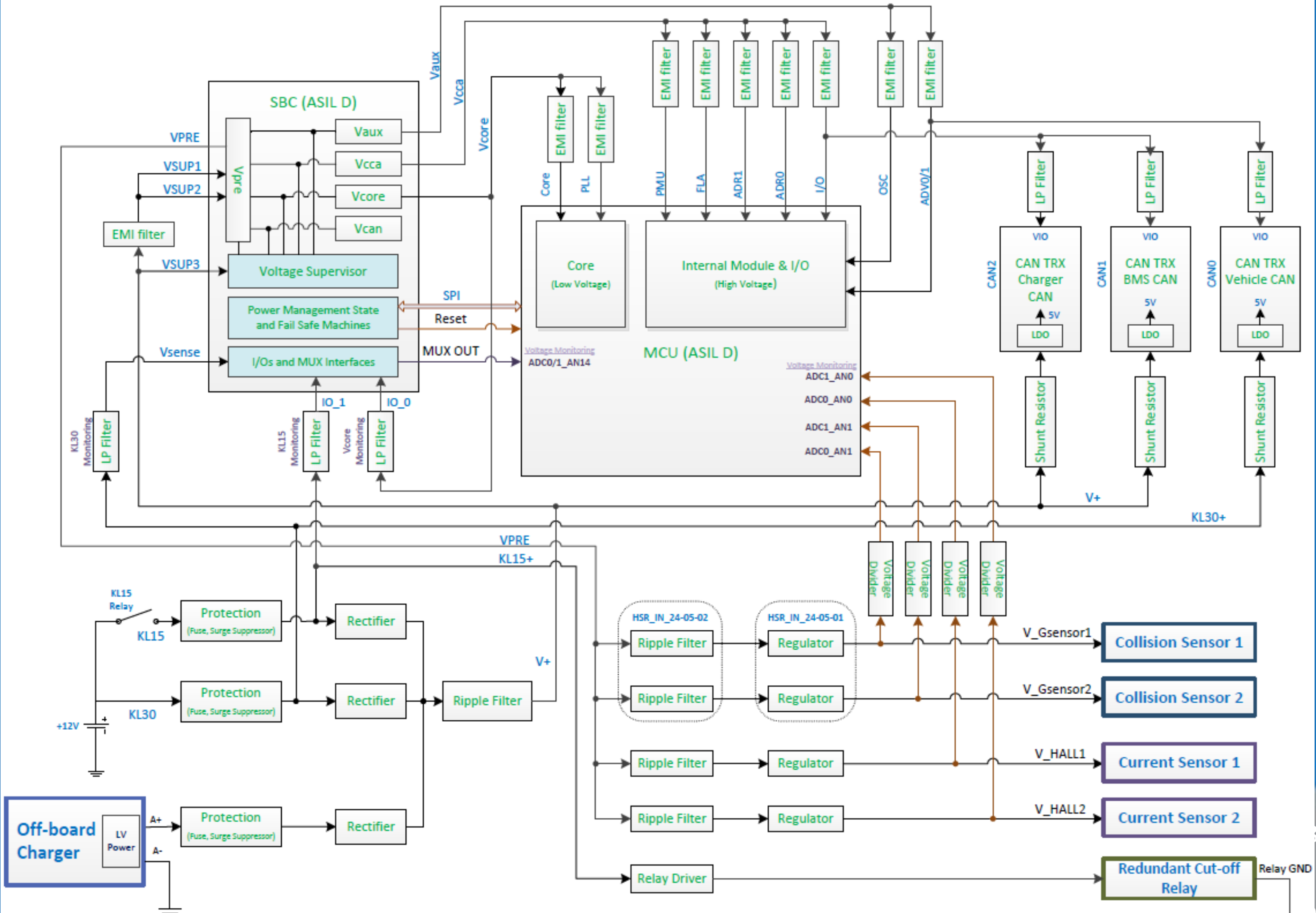
Hardware Level

- Safety lifecycle steps for item system engineering
- Technical Safety Requirements (TSR)
- Technical Safety Concept including the System Design
- Steps for Integration and Testing
- Safety Validation and Functional Safety Assessment

FSR ID	FSR Description		ASIL	Funcional Elements	Functional Elements Description	SW/HW	FSR ID
	TSR ID	TSR Description					
FSR_IN_001	BMU shall receive intended discharge request,speed,gear... from VCU via CAN		ASIL B	EL_BMU_IN_001	BMU CAN input capture function (VCU-BMU)		
	TSR_BMU_IN_001	BMU MCU shall capture discharging request from Motor control unit via vehicle CAN correctly	ASIL B	EL_BMU_IN_001	BMU CAN input capture function (VCU-BMU)	HW,SW	FSR_IN_001
	TSR_BMU_IN_002	BMU MCU shall get vehicle speed from VCU via vehicle CAN correctly	ASIL B	EL_BMU_IN_001	BMU CAN input capture function (VCU-BMU)	SW	FSR_IN_001
	TSR_BMU_IN_003	BMU MCU shall get gear position from VCU via vehicle CAN correctly	ASIL B	EL_BMU_IN_001	BMU CAN input capture function (VCU-BMU)	SW	FSR_IN_001
	TSR_BMU_IN_004	BMU shall get status information form VCU (error,motor status,dcdc status,ect...) via vehicle CAN correctly	ASIL B	EL_BMU_IN_001	BMU CAN input capture function (VCU-BMU)	SW	FSR_IN_001
	TSR_BMU_IN_005	BMU MCU shall get vehicle wakeup signal via vehicle CAN correctly	ASIL B	EL_BMU_IN_001	BMU CAN input capture function (VCU-BMU)	SW	FSR_IN_001
FSR_IN_002	BMU shall receive intended wakeup signal from VCU (HW)		ASIL B	EL_BMU_IN_004	BMU HW digital input capture function		
	TSR_BMU_IN_006	BMU_EL_IN_004 shall get wakeup signal from VCU via hard wire	ASIL B	EL_BMU_IN_004	BMU HW digital input capture function	HW,SW	FSR_IN_002
FSR_IN_003	BMU shall receive correct module voltage & temperature signal from BSU via CAN		ASIL C	EL_BMU_IN_002	BMU CAN input capture (internal CAN)		
	TSR_BMU_IN_007	BMU MCU shall get module voltage via BSU CAN correctly	ASIL C	EL_BMU_IN_002	BMU CAN input capture (internal CAN)	HW,SW	FSR_IN_003
	TSR_BMU_IN_008	BMU MCU shall get module temperature via BSU CAN correctly	ASIL C	EL_BMU_IN_002	BMU CAN input capture (internal CAN)	SW	FSR_IN_003

Hardware Level

Hardware Architecture



Power Supply Concept

Hardware Level

Example of Failure Mode Effect Diagnostic Analysis (FMEDA)

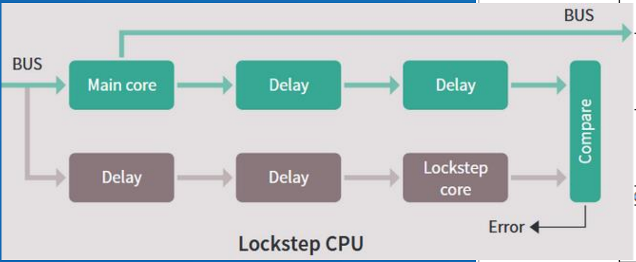
Failure Rates & Modes							Single Point Faults		
A	B	C	D	E	F	G	H	I	J
Type / function of HW part	ID	Failure rate	Failure rate	Safety or No Safety related?	Failure mode	Failure mode distribution	Potential to violate the SG in absense of Dangerous =1 Save = 0	Effect of the Failure Mode and argumentation SR/NR	Safety mechanism(s) ID
Text	ID	FIT	FIT	SR / NSR	Text	%	1 / 0	Text	Text
		λ							
Ceramic capacitor X7R dielectric 1uF 50V	C45	2.000000	2.000000	NSR	open	0.300000	0.000000	The VDD_HV_ADR0 voltage is not affected by open circuit.	
		2.000000		NSR	short	0.400000	0.000000	Through 100 ohm series resistance can prevent the power supply short circuit. Even if this fault power supply does not affect the operation due to double reading.	
		2.000000		NSR	0,5•C	0.150000	0.000000	The VDD_HV_ADR0 voltage is not affected by half value.	
		2.000000		NSR	2•C	0.150000	0.000000	The VDD_HV_ADR0 voltage is not affected by double values.	
Ceramic capacitor X7R dielectric 47nF 10% 50V	C43	2.000000	2.000000	NSR	open	0.300000	0.000000	The VDD_HV_ADR0 voltage is not affected by open circuit.	
		2.000000		NSR	short	0.400000	0.000000	Through 100 ohm series resistance can prevent the power supply short circuit. Even if this fault power supply does not affect the operation due to double reading.	
		2.000000		NSR	0,5•C	0.150000	0.000000	The VDD_HV_ADR0 voltage is not affected by half value.	
		2.000000		NSR	2•C	0.150000	0.000000	The VDD_HV_ADR0 voltage is not affected by double values.	
Ceramic capacitor X7R dielectric 10nF 50V	C44	2.000000	2.000000	NSR	open	0.300000	0.000000	The VDD_HV_ADR0 voltage is not affected by open circuit.	
		2.000000		NSR	short	0.400000	0.000000	Through 100 ohm series resistance can prevent the power supply short circuit. Even if this fault power supply does not affect the operation due to double reading.	
		2.000000		NSR	0,5•C	0.150000	0.000000	The VDD_HV_ADR0 voltage is not affected by half value.	
		2.000000		NSR	2•C	0.150000	0.000000	The VDD_HV_ADR0 voltage is not affected by double values.	
Ceramic capacitor X7R dielectric 1uF 50V	C48	2.000000	2.000000	NSR	open	0.300000	0.000000	The VDD_HV_ADR1 voltage is not affected by open circuit.	
		2.000000		NSR	short	0.400000	0.000000	Through 100 ohm series resistance can prevent the power supply short circuit. Even if this fault power supply does not affect the operation due to double reading.	
		2.000000		NSR	0,5•C	0.150000	0.000000	The VDD_HV_ADR1 voltage is not affected by half value.	
		2.000000		NSR	2•C	0.150000	0.000000	The VDD_HV_ADR1 voltage is not affected by double values.	

Hardware Level

Example of Failure Mode Effect Diagnostic Analysis (FMEDA)

Failure Rates & Modes							Multiple Point Faults			
A	B	C	D	E	F	G	Q	R	S	T
Type / function of HW part	ID	Failure rate	Failure rate	Safety or No Safety related?	Failure mode	Failure mode distribution	Effect of the Failure Mode	Safety mechanism(s) ID	Diagnostic coverage	MPF latent Failure rate.
										T=((C*G)-N)*P*(1-S)
Text	ID	FIT	FIT	SR / NSR	Text	%	Text	Text	%	FIT
		λ							FMC_MPF	$\lambda_{MPF\ L}$
Main MCU										
IC MCU 32 Bit 2.5MB Flash 384KB MPC5554P	U1	1000.000000	1000.000000	SR	Non-Volatile Memory - Flash (ISO 26262-5 D.1: Non-Volatile Memory)	0.200000	Leads to latent fault, when monitoring function is corrupted	Latent Fault Safety Mechanisms inside MCU. Refer to the FMEDA results from Vendor	0.990000	1.990000
		1000.000000		SR	Voltage Regulation and Distribution (ISO 26262-5 D.1: Power Supply)	0.200000	Leads to latent fault, when monitoring function is corrupted	SM281: MCU internal monitoring for latent faults (BIST)	0.990000	1.990000
		1000.000000		SR	Processing Units (ISO 26262-5 D.1: Processing Units)	0.200000	Leads to latent fault, when monitoring function is corrupted	SM281: MCU internal monitoring for latent faults (BIST)	0.990000	1.990000
		1000.000000		SR	Clock Generation and Distribution (ISO 26262-5 D.1: Clock)	0.200000	Leads to latent fault, when monitoring function is corrupted	SM281: MCU internal monitoring for latent faults (BIST)	0.990000	1.990000
		1000.000000		SR	Volatile Memory - System RAM (ISO 26262-5 D.1: Volatile Memory)	0.200000	Leads to latent fault, when monitoring function is corrupted	SM281: MCU internal monitoring for latent faults (BIST)	0.990000	1.990000
	C19	2.000000	2.000000	NSR	open	0.300000				0.000000
		2.000000		SR	short	0.400000	Leads to latent fault, when monitoring function is corrupted	SM281: MCU internal monitoring for latent faults (BIST)	0.990000	0.007920
		2.000000		NSR	0,5*C	0.150000				0.000000
		2.000000		NSR	2*C	0.150000				0.000000

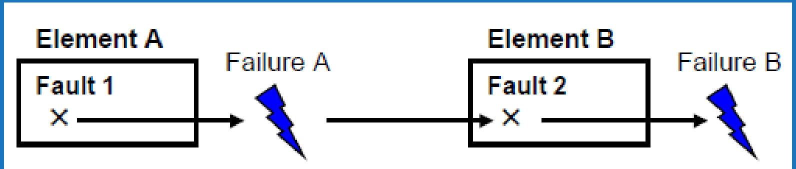
Multicore, Lock-step, ISO 26262 Certified MCU

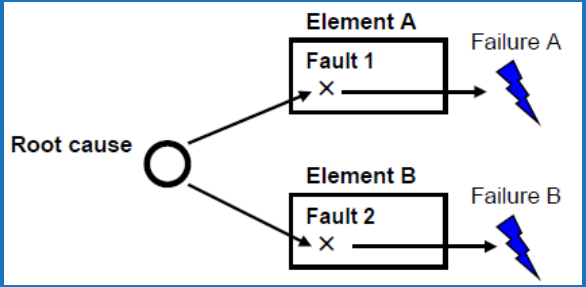


Software Level

SW Related Analyses

Dependent Failure Analysis to demonstrate
– **Freedom from interference**
Memory (Corrupted content, RW right assignment)
Timing (Loops, RTC, Control flow defect, etc)
Communication (Loss, delay, repetition, masquerade)
– **Independence between software components**

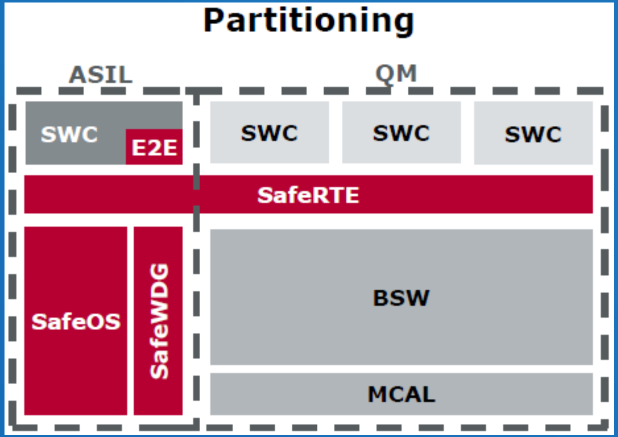




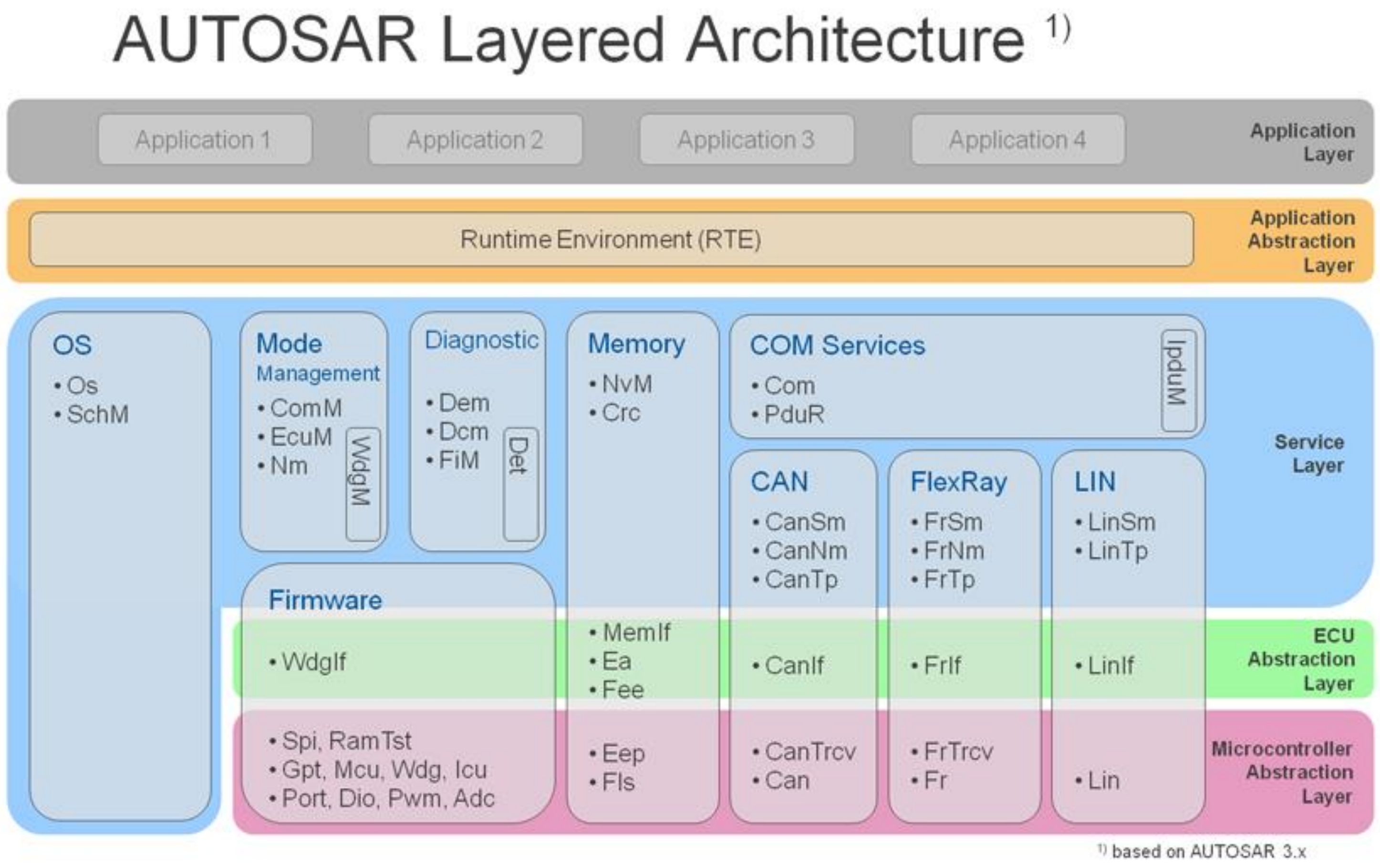
Divided into
– BSW (Basic Software);
– RTE (Run Time Environment);
– OS (Operating System);
– MCAL (MCU Abstraction Layer);
– ASW (Application Software);

Methods
– Deductive analysis (FTA etc.)
– Inductive analysis (FMEA etc.)

Other standards
– ASPICE, AUTOSAR, MISRA C, MISRA modeling guideline

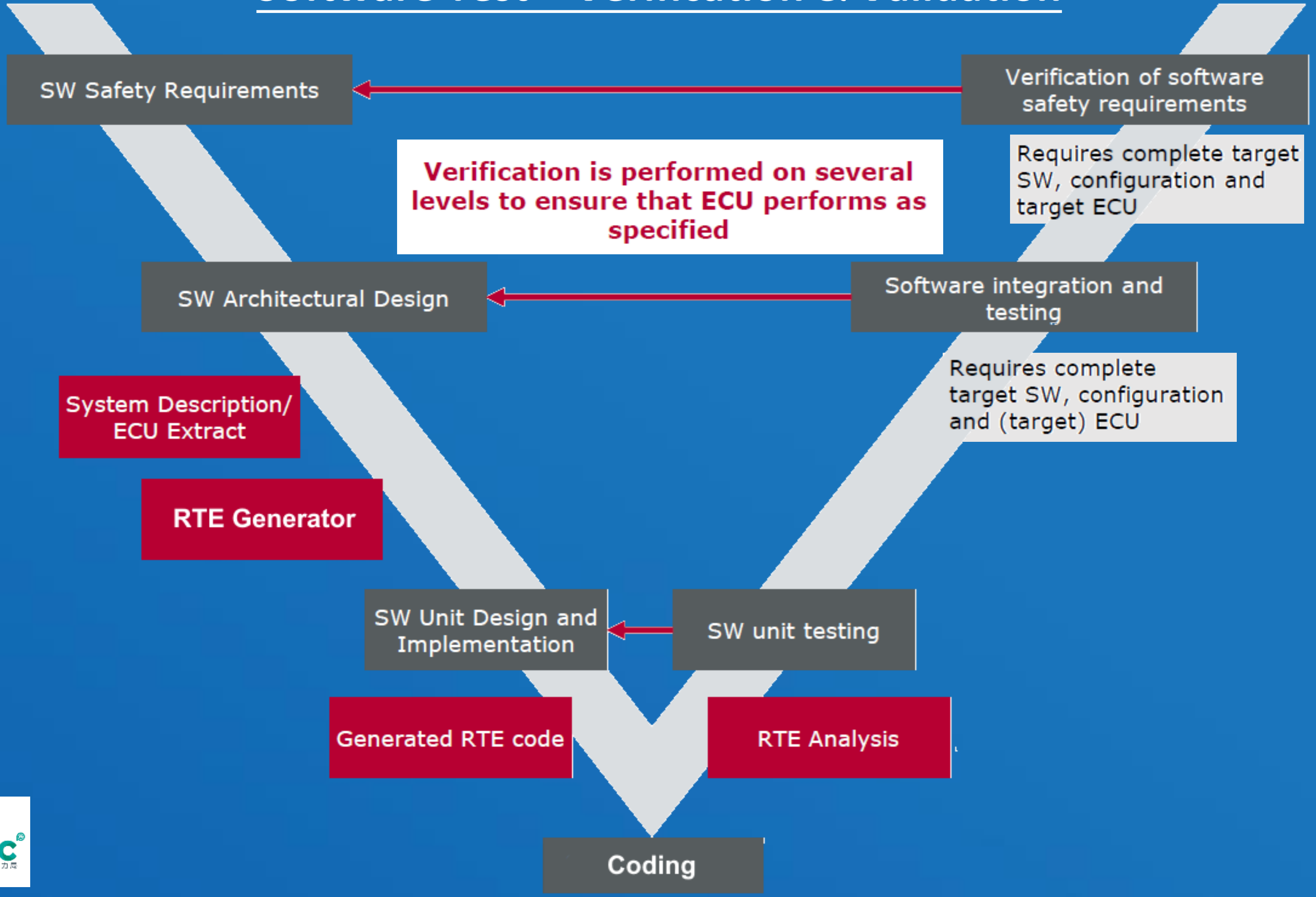


Software Level



Software Level

Software Test – Verification & Validation



Software Level

Software Unit Test

Methods For SW Unit Test

Methods	ASIL			
	A	B	C	D
Walk-through	++	+	n.a.	n.a.
Inspection	+	++	++	++
Semi-formal verification	+	+	++	++
Formal verification	n.a.	n.a.	+	+
Control flow analysis	+	+	++	++
Data flow analysis	+	+	++	++
Static code analysis	+	++	++	++
Semantic code analysis	+	+	+	+

Structural Coverage Metrics at SW Unit Level

Methods	ASIL			
	A	B	C	D
Statement coverage	++	++	+	+
Branch coverage	+	++	++	++
MC/DC	+	+	+	++

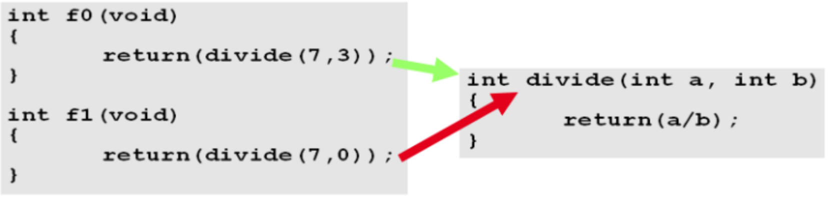
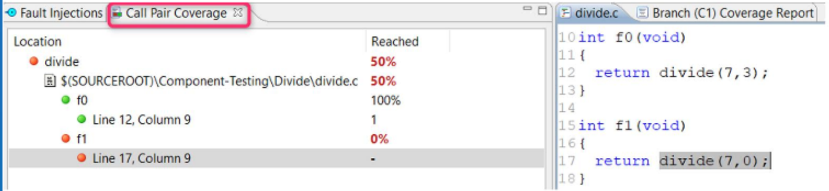


Fig. 1: The function divide() can be called from f0() and f1()



Software Level

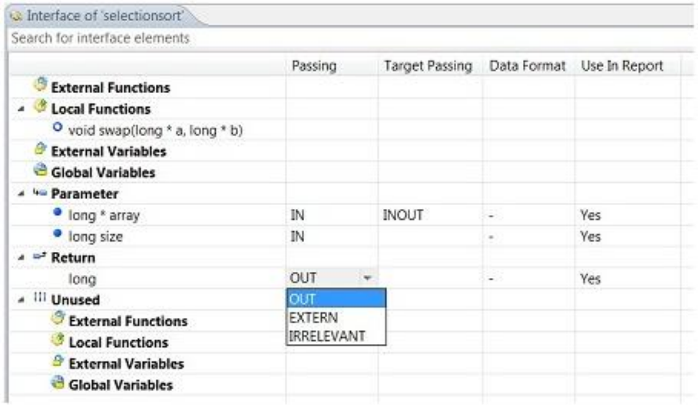
Software Integration Test

Methods For SW Integration Test

Methods	ASIL			
	A	B	C	D
Requirements-based test	++	++	++	++
Interface test	++	++	++	++
Fault injection test	+	+	++	++
Resource usage test	+	+	+	++
Back-to-back comparison test	+	+	++	++

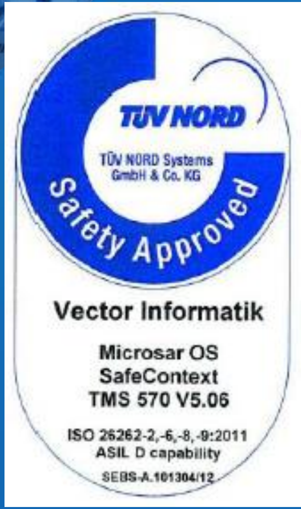
Deriving Test Cases at SW Integration Level

Methods	ASIL			
	A	B	C	D
Analysis of requirements	++	++	++	++
Generation and analysis of equivalence classes	+	++	++	++
Analysis of boundary values	+	++	++	++
Error guessing	+	+	+	+



Software Level

Software Tool Qualification



Qualification of software tools classified TCL3

Methods	ASIL			
	A	B	C	D
Increased confidence from use	++	++	+	+
Evaluation of the tool development process	++	++	+	+
Validation of the software tool	+	+	++	++
Development in accordance with a safety standard	+	+	++	++

Qualification of software tools classified TCL2

Methods	ASIL			
	A	B	C	D
Increased confidence from use	++	++	++	+
Evaluation of the tool development process	++	++	++	+
Validation of the software tool	+	+	+	++
Development in accordance with a safety standard	+	+	+	++

Challenges in Pursuit Of ISO 26262

- Work load: 70+ to 100+ work products;
- Multi-disciplined engineering;
- Training of engineers;
- Long time to compliance;
- Investment in tools;
- Management support

SGS TÜV SAAR
ASIL D READY
Functional Safety
www.sgs-tuev-saar.com

exida • CERTIFIED • ISO 26262 • ASIL D •

Market Opportunities of ISO 26262 ASIL C Compliant BMS by APAS

Enhance R&D capability & recognition. Capture potential OEM order .

Improve quality, reliability, safety & corporate image

Hybrid Energy Storage System For Electric Vehicles

(Ref.: ITP/025/12AP)

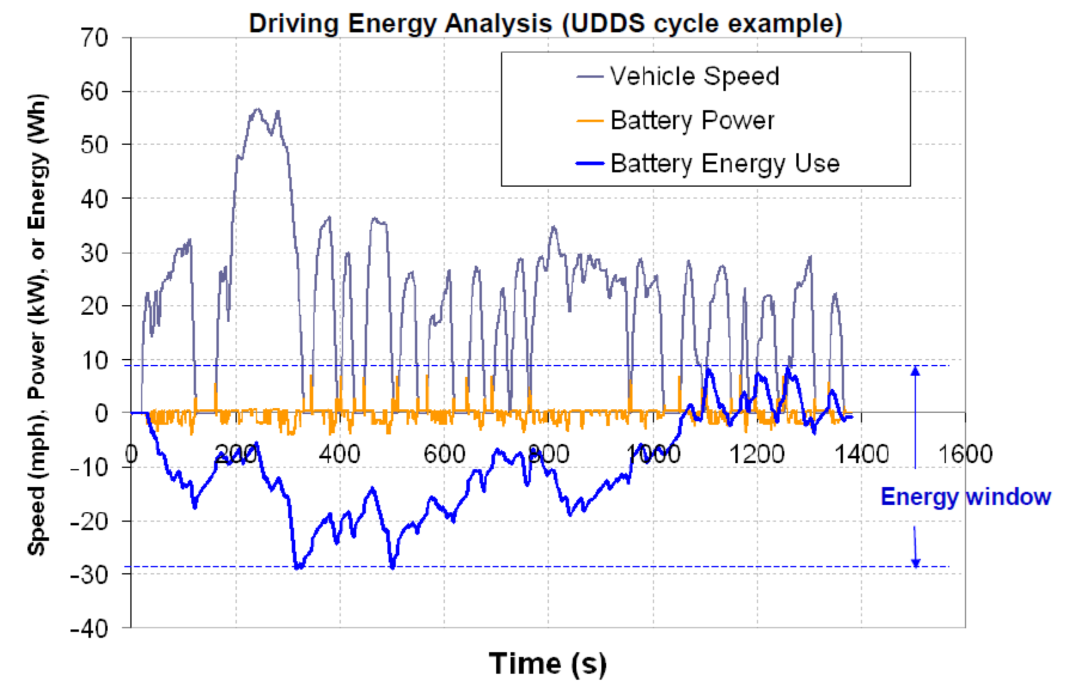
HKPC TechDive: Smart City – EV Technology
27 May 2020

Yiu Chi Wai
Consultant, Smart Electronics
Hong Kong Productivity Council

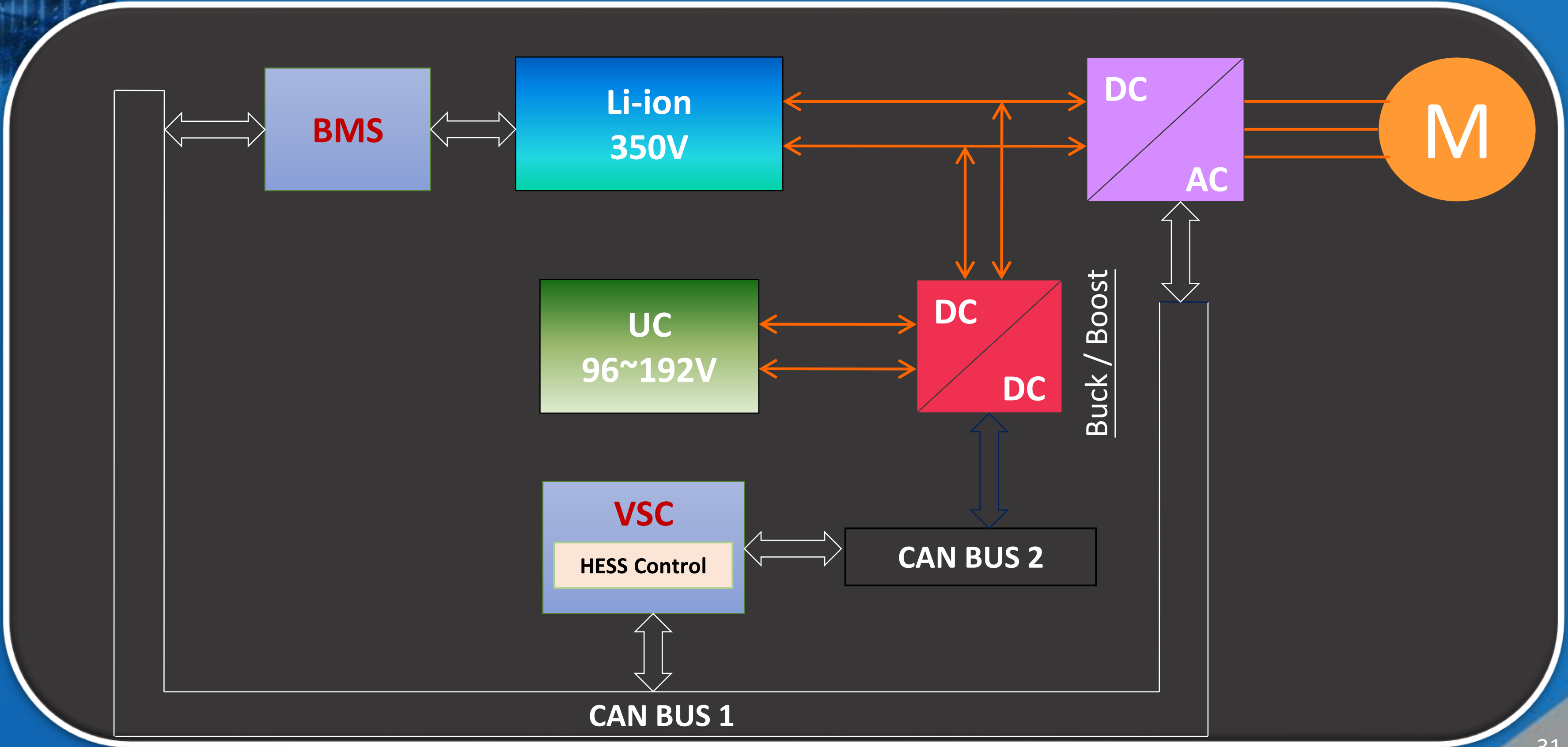
Urban Dynamometer Driving Schedule (UDDS) Battery Usage

Benefits of ultracapcitor & Li-ion hybrid:

- Elongate battery life;
- Increase instantaneous power – better acceleration



APAS HESS System Architecture



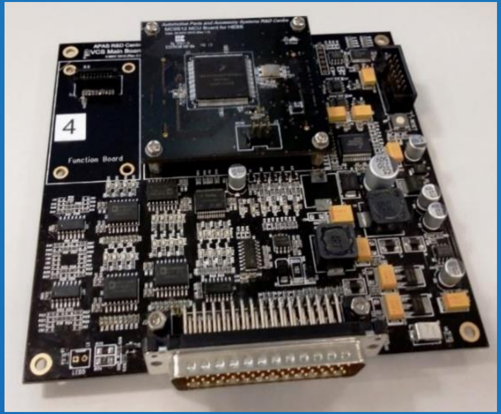
HESS Control Strategies

High SOC for startup & acceleration

Low SOC for regenerative braking

Ideal strategy should be adaptive to any drive cycles

Key Objectives for UC Development



Maximum converter input current

Maximum UC terminal voltage

UC voltage between U_{max} and U_{min}

UC SOC between 25% and 100%

Must conditions

Market Opportunities of APAS HESS System

Robust control software developed by Model Based Development (MBD)

Effectively extend battery life

Improve the available power of ESS for better vehicle performance

汽車科技研發中心

生產力局

Hong Kong Productivity Council
香港生產力促進局

HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong
香港九龍達之路78號生產力大樓
+852 2788 5678   www.hkpc.org

Automotive Platforms and Application Systems (APAS) R&D Centre
汽車科技研發中心

4/F, HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong
香港九龍達之路78號生產力大樓
+852 2788 5333 www.apas.hk