

Electrification – Functional Safety Backbone Solutions to Attach with S32

David Lopez

Segment Manager Functional Safety SBC
Safety Power Management Product Line

October 2018 | AMF-AUT-T3351



SECURE CONNECTIONS
FOR A SMARTER WORLD

Agenda

- Multi-PMIC Solutions
- Powertrain & Vehicle Dynamics: Solutions
- Safety Proven
- Portfolio Scalability
- Electrification Robustness
- System Solutions
- Next Generation FS-SBCs

Global Megatrends

NXP to Lead This Industry Transformation

Autonomy



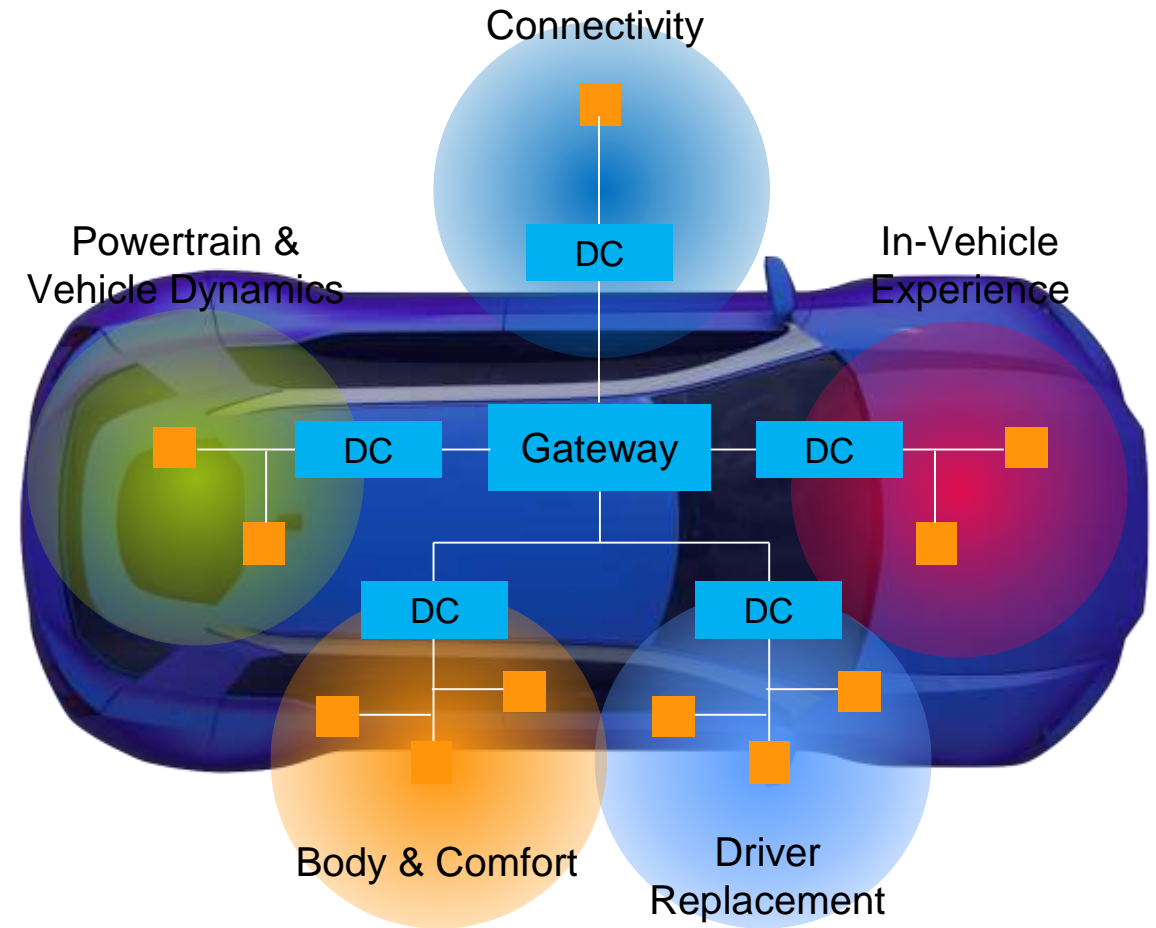
Electrification



Connectivity



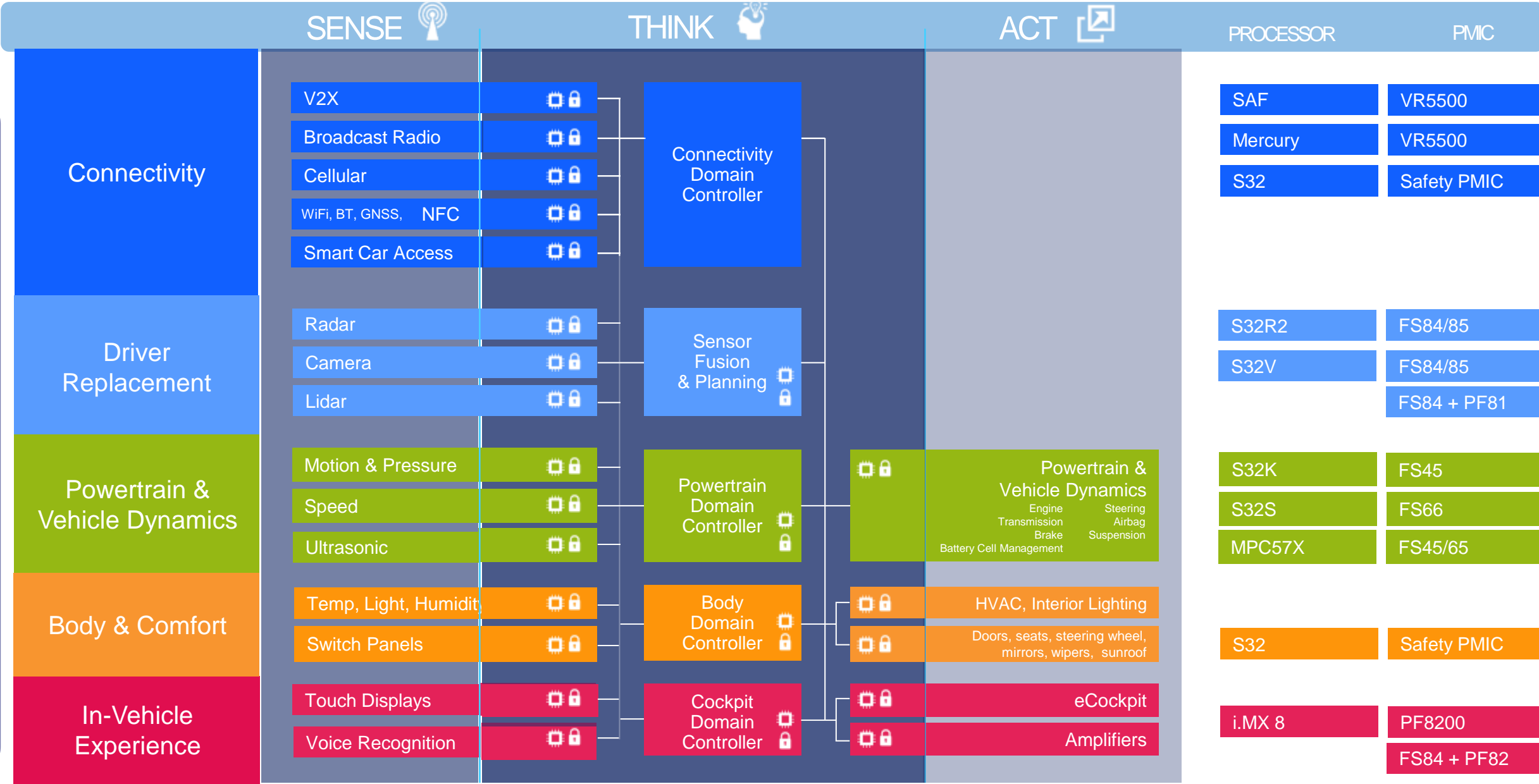
Domain-Based Architecture



One Processor = One Safety PMIC



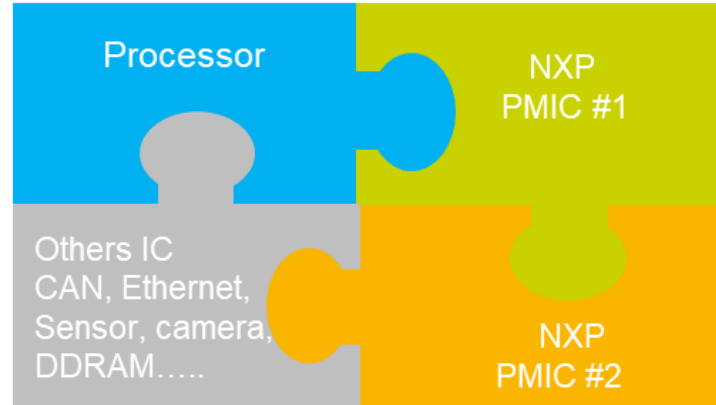
Gateways & Networks



► **BENEFITS: PMIC DESIGNED & VALIDATED WITH PROCESSOR | COMMON REFERENCE DESIGN | SOFTWARE**



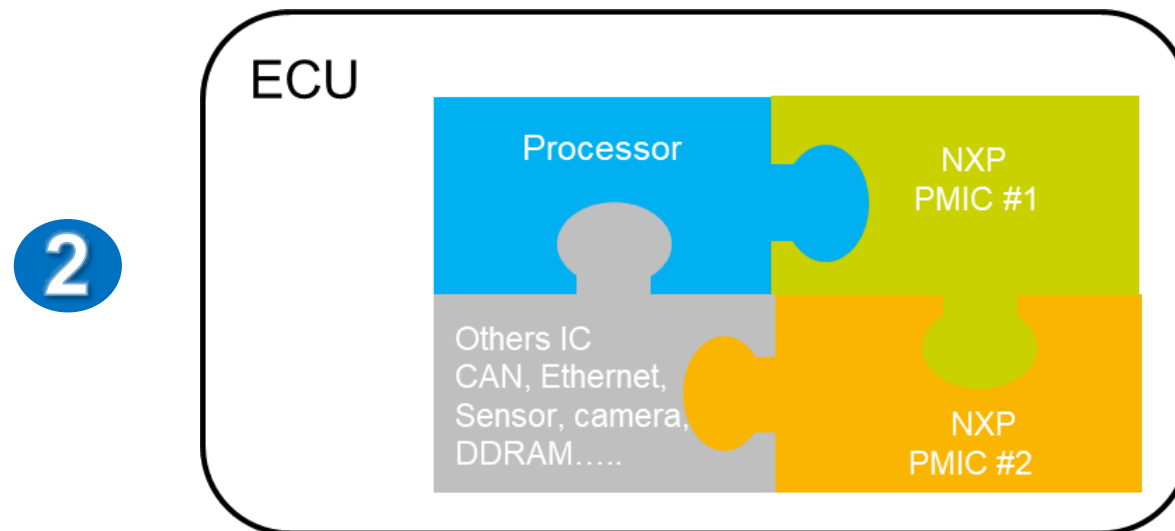
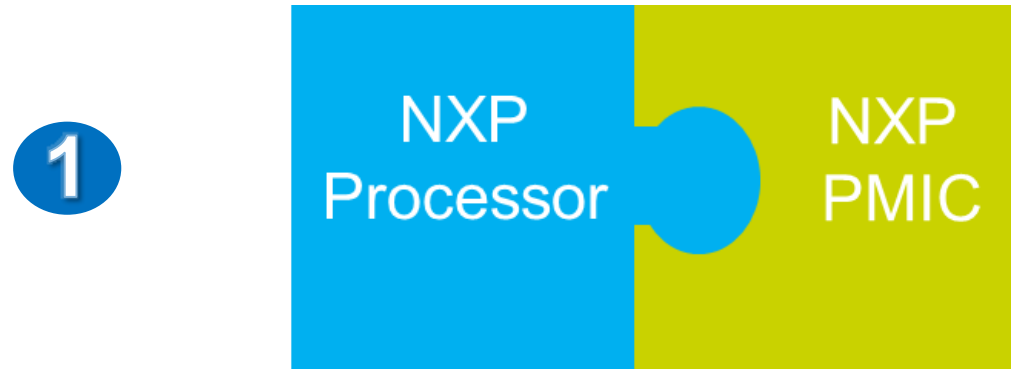
Multi-PMIC Solutions for System Power and Safety



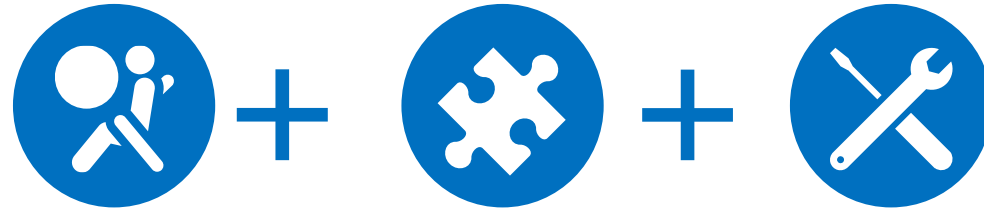
NXP's next generation power management: Simplicity of safety power management IC family



Automotive Safety Power Management Solutions Strategy



NXP Safety PMIC's DNA



Safety
Feature

IP Block
Strategy

Device
Flexibility

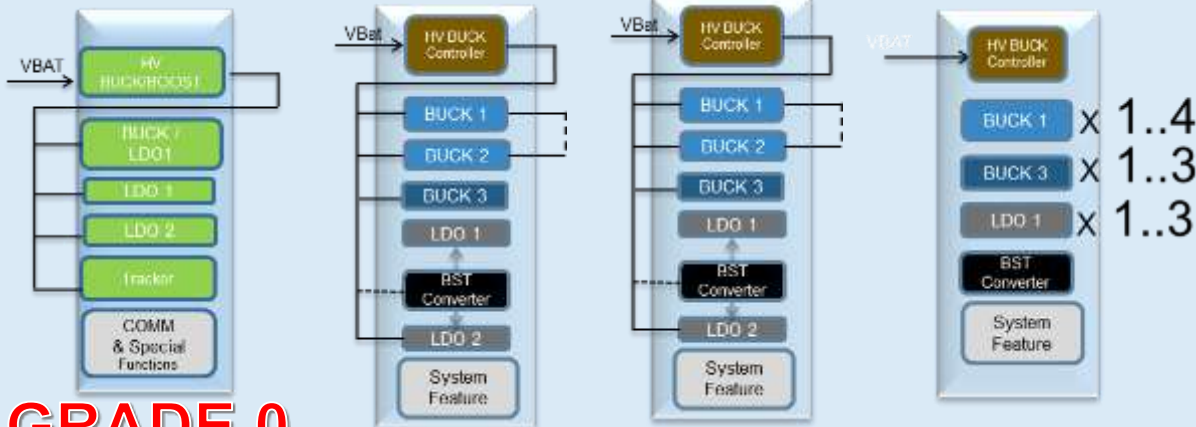
Automotive Safety PMIC 12V/24 Battery Connected

FS45/6500

FS84/85x0

FS6600

Next FS Series



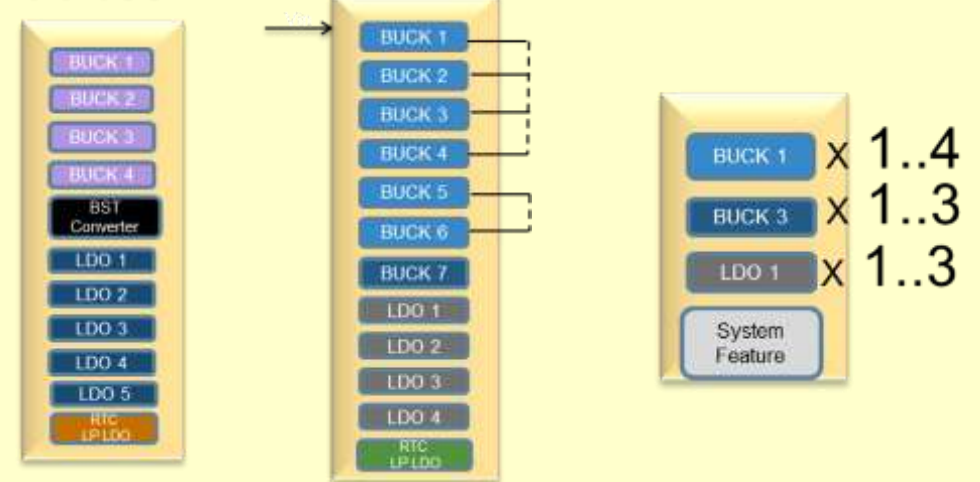
GRADE 0

Automotive Safety PMIC <5V LOW Vin Connected

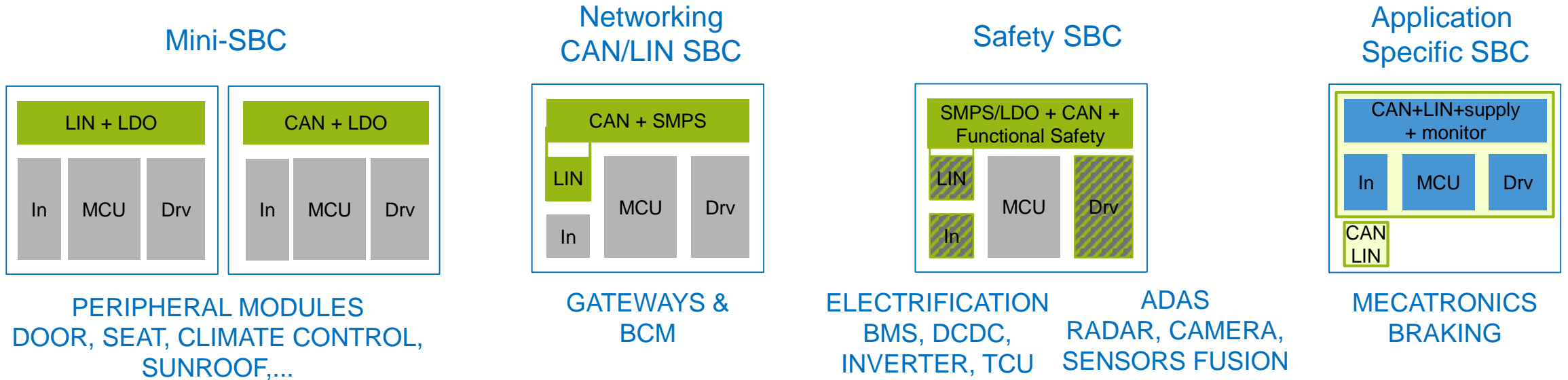
PF100

PF81/8200

Next PF Series



System Basis Chip Integrates Power and System Level Features



Simplifying the System

Improving Space, Quality & Overall Cost
Leverage NXP in-vehicle networking expertise

Safe & Scalable SBC Solutions

System Power Solution

System Differentiation with High Performance MCUs
Attach Strategy and Functional Safety

Powertrain & Vehicle Dynamics

 SENSE

 THINK

 ACT

Powertrain &
Vehicle
Dynamics



Motion & Pressure



Speed



Ultrasonic









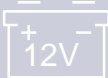













Powertrain
Domain
Controller



Powertrain &
Vehicle Dynamics

Engine Steering
Transmission Airbag
Brake Suspension
Battery Cell Management

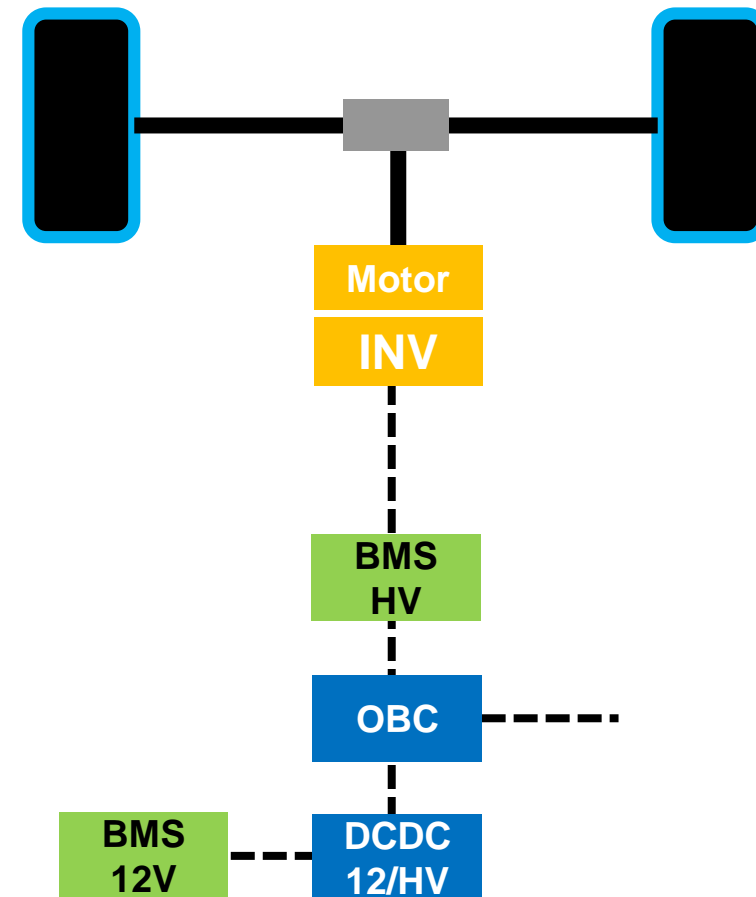
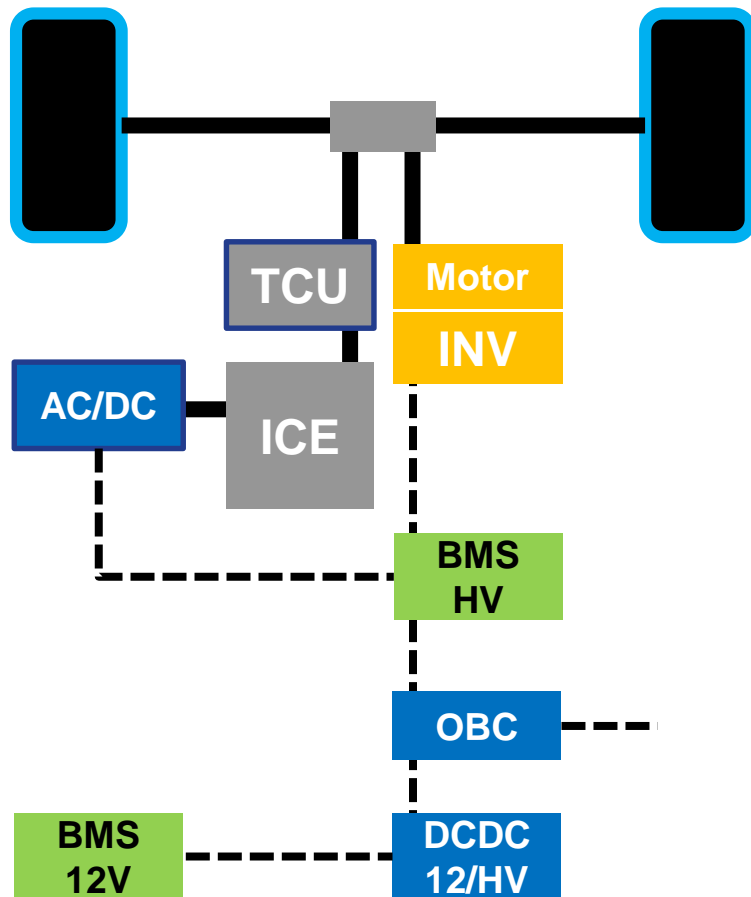
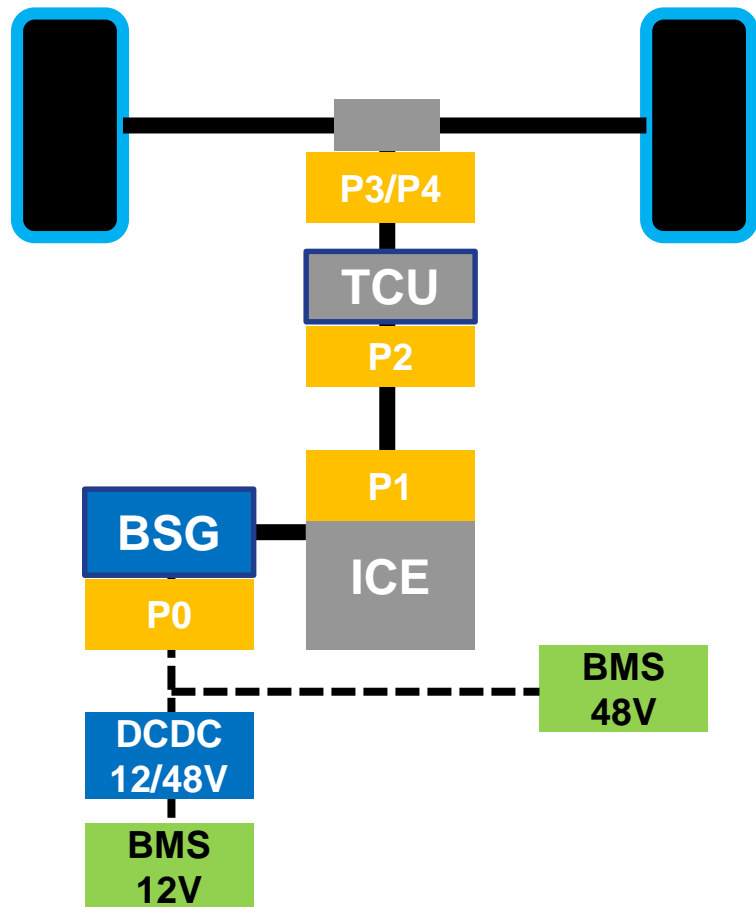
Vehicle Electrification: Diversity Of Approaches

Common Name	Combustion Engine (ICE)	Mild Hybrid (M-HEV)	Full Hybrid (F-HEV)	Plug-in Hybrid (P-HEV)	Range Extended EV (RE-BEV)	Pure Electric Vehicle (BEV)
Example	Ford Mustang 	Honda Insight 	Toyota Prius 	FCA Pacifica 	BMW i.3 	Nissan Leaf 
Combustion Engine	● ● ● ●	● ● ● ●	● ● ●	● ● ●	● ●	
Battery System						
Mains Charging	-	-	-			
Electric Traction	-	 10 – 20 kW	 15 – 60 kW	 40 – 80 kW	 40 – 80 kW	 > 80 kW

ICE & Mild Hybrid Drive by Engine

Full & Plug In Hybrid Drive by Engine & Motor

Battery Electric Vehicle Drive Motor

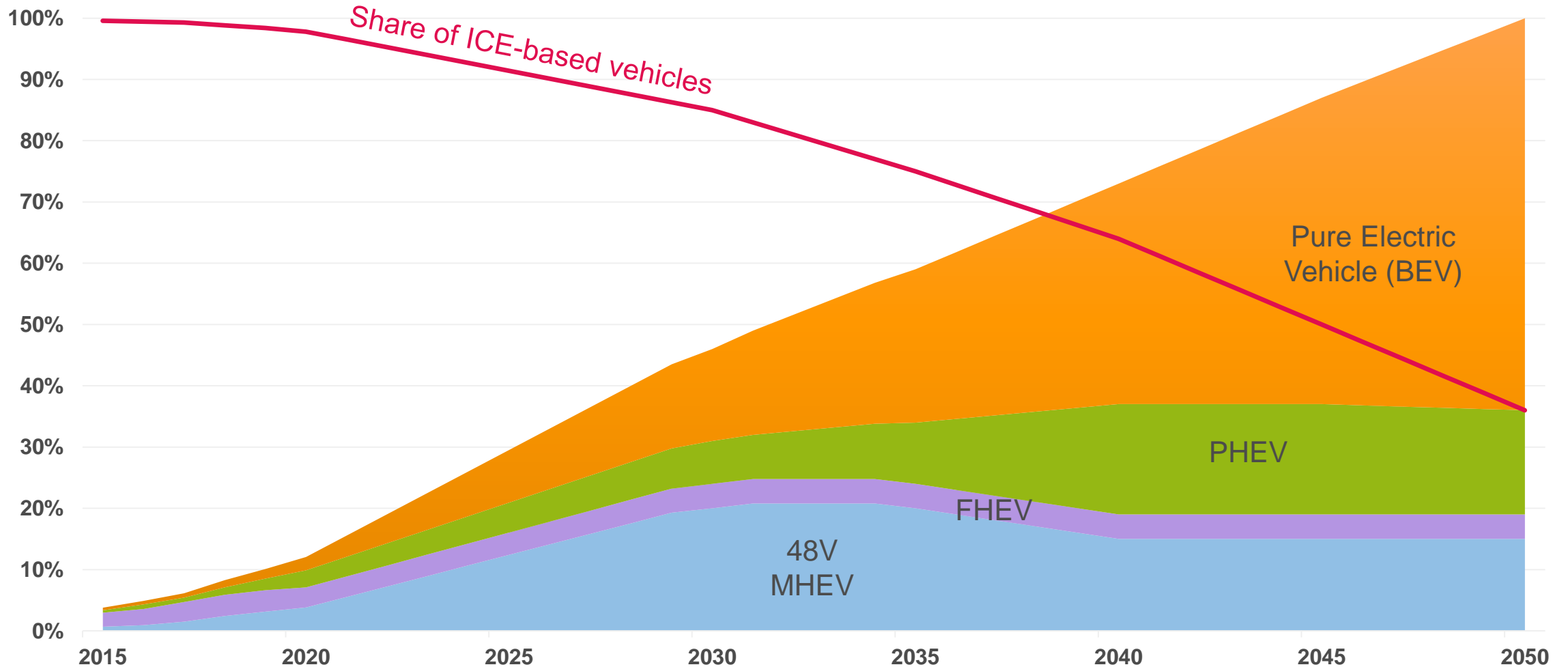


Actuation

Conversion

Storage

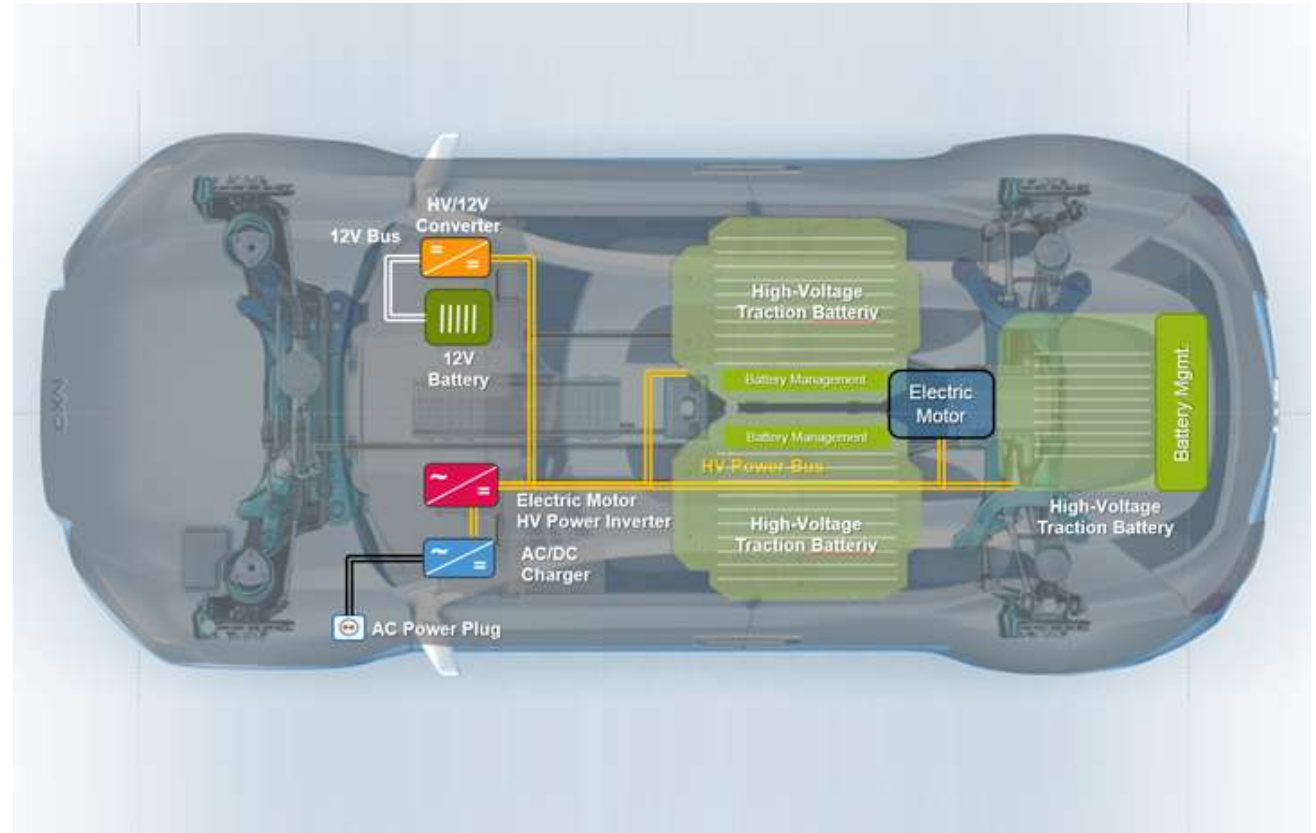
xEV Long Term Market Forecast



SOURCE: STRATEGY ANALYTICS, EVERCORE, NXP CMI

Efficient Powertrain and Energy Management

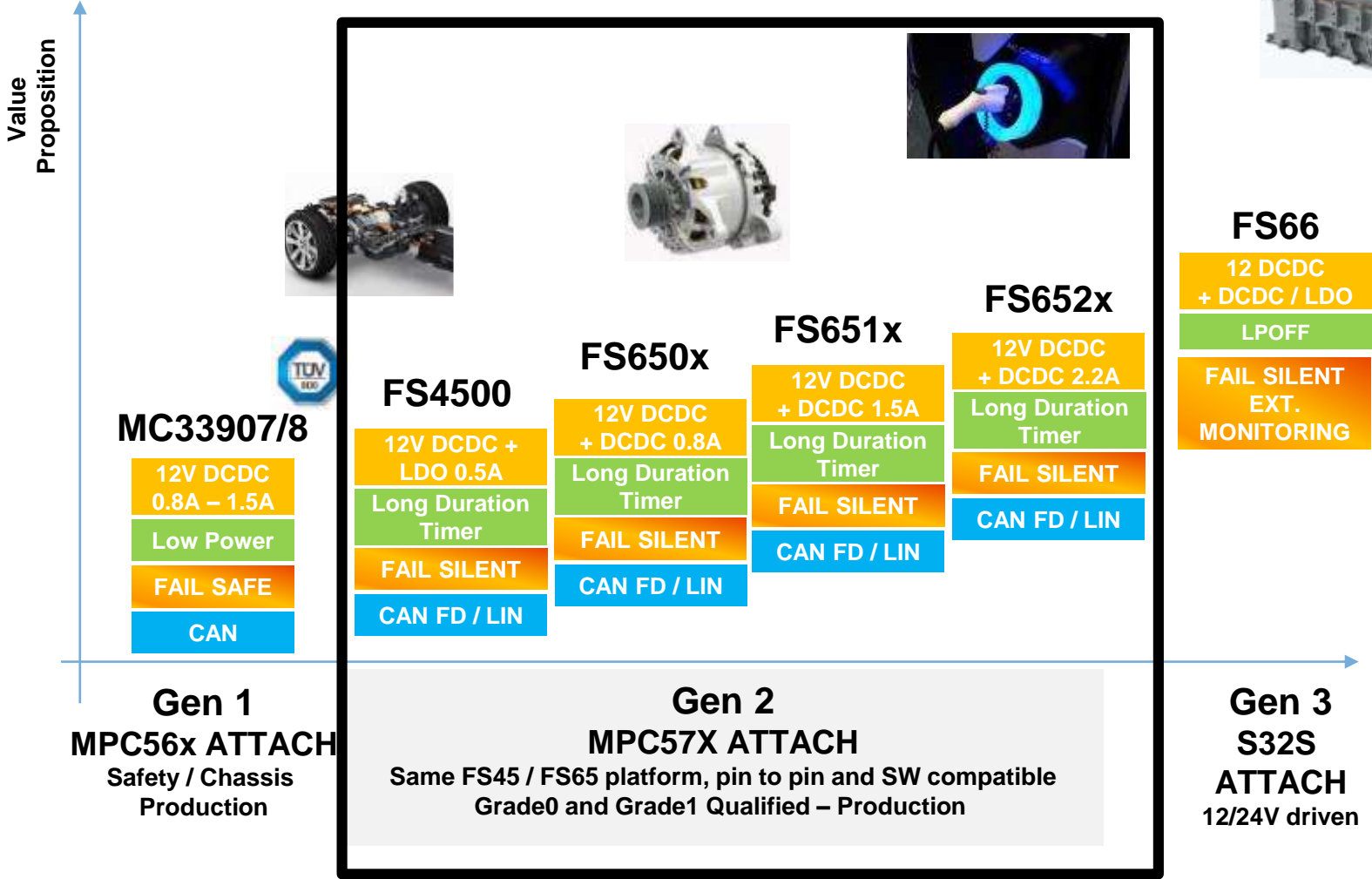
Major xEV Components	MCU	SBC	COMM	Driver	AFE
Motor control, inverter, HCU	●	●	●	●	■
DC/DC voltage domain converter	●	●	●		■
On-board charger AC/DC converter	●	●	●		■
Battery management system	●	●	●	●	
48V eMachine (BSG, ISG, HVAC)	●	●	●		





Energy Storage – Conversion – Actuation

Electrification & General Purpose Safety Power Management



Secured & Safe System Solutions

- ISO26262 architecture (TUV SUD proven)
- Functional robustness (non ISO pulse, EMC, HTOL)
- Security (SM transition and Power Gate)

High Efficient Solutions

- Target 12 V, 24 V, 48V (application note)
- DCDC & LDO architecture (Vpre + Vcore)
- Ultra low power modes (low Iq, long dur. timer)

Safety Simplified Solutions

- ISO26262 ready documentation
- System validation test (eFAST)
- Global ecosystem (incl HW & SW)



NXP® POWER SBC APPLICATION EXAMPLES

8 Drive Train—Safety & Chassis

Transmission, Transfer Case – ASIL **D**
FS650x with other MCU

7 Drive Train—Safety & Chassis

Suspension/Dumping – ASIL **C**
FS65 with other MCU

6 Drive Train—Safety & Chassis

Electric Power Steering with Fail Safe & Fail Operational strategies - FS65 or FS45 with MPC5744P – ASIL **D**

5 Drive Train—Safety & Chassis

Engine Management Unit – ASIL **B**
FS651x with MPC5777C

4 Drive Train—Electrification

Hybrid Vehicle Controller – ASIL **D** FS66 with S32S2

3 Drive Train—Electrification

Inverter, DC-DC converter - ASIL **D** FS650x or FS45
Vepco high-voltage inverter RD - ASIL **D**
MPC5775 with FS651x & GD3100

1 ADAS-Gateway

Bluebox development platform- ASIL **D**
S32V234, S32R27, LS2084A + FS65

2 ADAS—Vision

Data Fusion – ASIL **D**
(Autonomous Drive) FS652x attach with MPC5777C or other MCU

3 ADAS—Radar

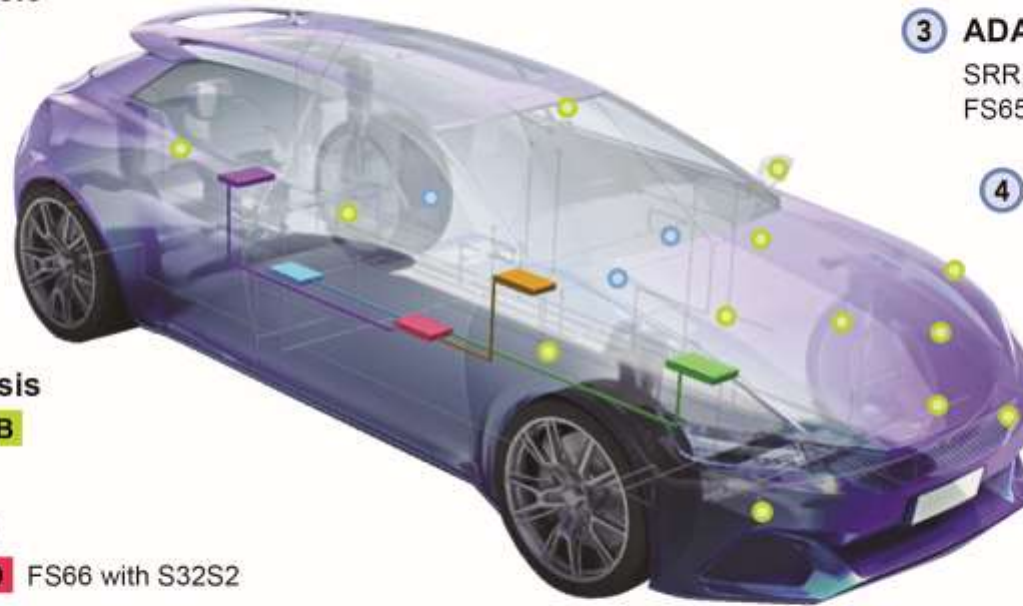
SRR, MRR, LRR – ASIL **D**
FS652x with S32R2

4 ADAS—Camera Sensor

-S32V + FS85 + PF82 – ASIL **B**

5 ADAS—ACC

Adaptive Cruise Control – ASIL **C**
FS652x with MPC5744P



1 Drive Train—Electrification

Battery Management (12 V, 48 V, HV) FS650x with MPC5744P & MC33771 – ASIL **C**
NewTec RD: S32K with FS45 – ASIL **C**
MPC577x with FS650x – ASIL **D**

2 Drive Train—Electrification

Electric Motor (Alteno Starter, eAxel drive...) – ASIL **C** FS45

ASIL **QM** **A** **B** **C** **D**



Electrification FSBC NXP Designs: Where & Why?

> 60 customers, 16 Applications

55% DW in Energy Actuation in Inverter, TCU

30% DW in Energy Storage in BMS

14% in Energy Conversion in DCDC and BSG

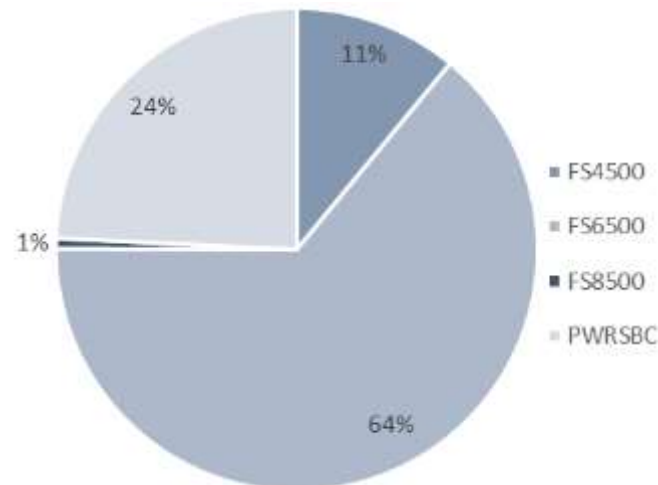
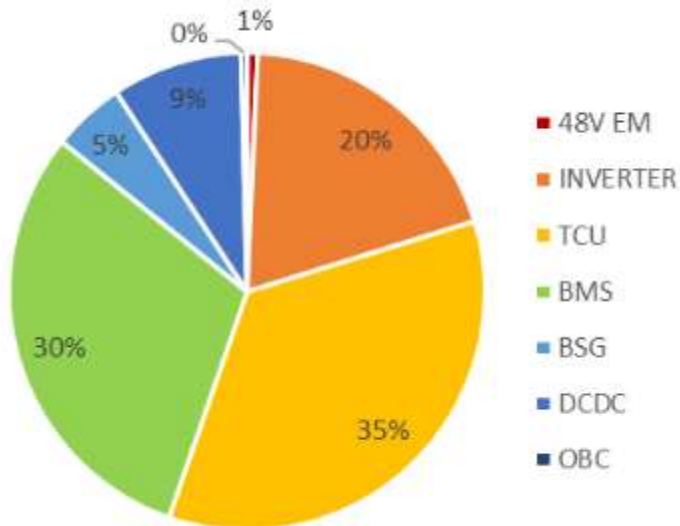
24% DW w 1st Generation FSBC PowerSBC (MC33907, 33908)

75% DW w 2nd Generation FSBC FS45 and FS65

First DW with FS85 and FS66 on 24V BMS and Inverter

FSBC Driving factors

- SAFETY PROVEN**
 - MCU agnostic
 - Self independent Monitoring
 - Fail Silent (3 generations)
- FAMILY SCALABILITY**
 - Pay what is needed
 - Pin to pin & SW scalable
 - Power & System Segmentation
- SYSTEM BASE SOLUTIONS**
 - Low Power Strategy (LDT)
 - Trackers & 1% Accuracy
 - Grade 0 capability (Robustness)



Safety Proven



Reduce Risk: Track and Understand Failures

Car OEM

SET SYSTEM **RISK CRITICITY** (HAZARD ANALYSIS) ASIL A, B, C or D
DEFINE **SAFETY GOALS**

Tier1 &
Silicon

IMPLEMENT MEASURES TO REDUCE RISK OF FAILURE
DIFFERENT TYPE OF FAILURES



Avoid **SYSTEMATIC FAILURES**
during development

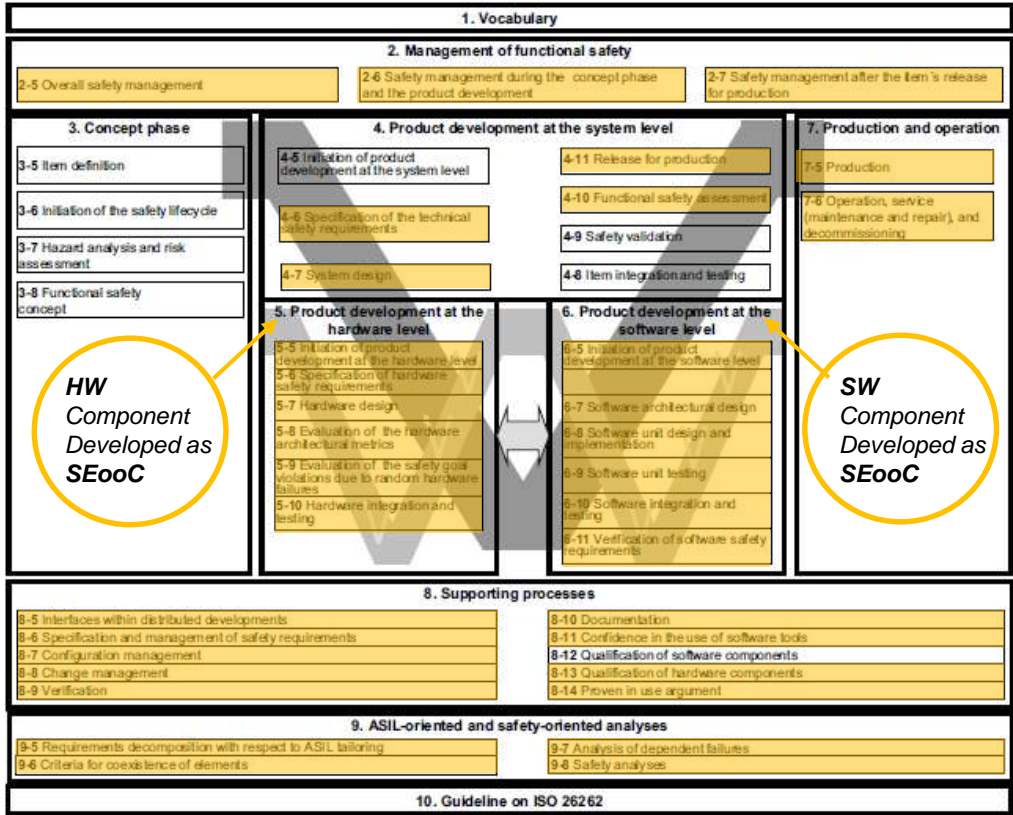
- Process
- Safety management
- Best practices
- Lessons learned
- Verification & validation



Avoid **RANDOM FAILURES**
during operation

- System safe state
- Safety architecture
- Quantitative & qualitative analysis
- Documentation

Functional Safety - Vmodel & Responsibility



Applicable to Component developed as SEooC

Reference ISO 26262-10:2012

NXP focuses on **Safety Element Out Of Context (SeooC)**

OEM

- Item definition
- Hazard analysis and risk assessment
- Safety Goals
- Functional Safety Concept

Safety Manual Safety Analysis ↑ ↓ Safety Requirements DIA

Tier 1

- Technical Safety Concept
- Technical Safety Architecture
- ASIL Classification of Functions
- HW / SW design

Safety Manual Safety Analysis ↑ ↓ Safety Requirements DIA

Tier 2 Supplier - NXP

- HW / SW “products”

Product Safety Mechanisms
(implemented in offering, described in Safety Manual, quantified/qualified by Safety Analysis)

Development Process & Methods

ISO 26262

QUALITY

NXP Auto BCaM7 Process Fully Compliant with ISO 26262: 2011



NPI PROJECT LIFECYCLE

- QM or ASILx

- Impact Analysis

- Safety concept
- Safety reqs.
- Safety archi.

- Safety analysis (FTA, DFA, FMEDA)
- Confirmation review Safety Analysis
- **Functional Safety assessment 2**

- Safety plan
- DIA (if needed)
- Safety Assessment plan
- SW tool criteria Eval.
- Verification Plan (inc. safety)
- **Confirmation review Safety Plan**
- **Confirmation review SW tools**
- **Functional Safety assessment 1**

- **Safety assessment 3**
- **Confirmation review Safety case**

FUNCTIONAL SAFETY

Automotive Processes	ISO 9001	ISO 14001	ISO 45001	ISO 26262	ISO 9001:2015	ISO 14001:2015	ISO 45001:2018	Doc ID	Status
Automotive Functional Safety Management Procedure	x	x	x	x	x	x	x	DOC-25809	"update"
Automotive Functional Safety Analysis Procedure	x	x	x	x	x	x	x	DOC-25810	"update"
Automotive Functional Safety Assessment Procedure	x	x	x	x	x	x	x	DOC-25811	"update"
Automotive Functional Safety Test Compliance Procedure	x	x	x	x	x	x	x	DOC-25812	"update"
Templates & Deliverables									
Automotive Expert Training for Safety	x	x	x	x	x	x	x	DOC-25841	
Automotive Fault Injection Software	x	x	x	x	x	x	x	DOC-25842	
Automotive Development Processes									
Automotive Confirmation Measure Report Template	x	x	x	x	x	x	x	DOC-25824	"update"
Automotive Confirmation Review Safety Analysis Template	x	x	x	x	x	x	x	DOC-25813	"update"
Automotive Confirmation Review Safety Plan Template	x	x	x	x	x	x	x	DOC-25814	"update"
Automotive Confirmation Review Safety Case Template	x	x	x	x	x	x	x	DOC-25815	"update"
Automotive Confirmation Review SW Tool Criteria Evaluation Template	x	x	x	x	x	x	x	DOC-25816	"update"
Automotive Safety Assessment Support Template	x	x	x	x	x	x	x	DOC-25817	"update"

AUTOMOTIVE BCAM 7.0 V3.1

NOTE: Enovia is up and running again. ALL links with "DOC-" are accessible.

Automotive Processes	Doc ID
Automotive Research and Development Process	DOC-25802
Automotive Research and Development Manual	DOC-25803
Automotive Role Descriptions Procedure	DOC-25804
Product Creation Processes	
Automotive Communication Package Phase 1	DOC-25821
Automotive Communication Package Phase 2	DOC-25822
Automotive Master Checklist (AMC)	DOC-25823
Automotive Master Checklist (AMC)	DOC-25824
Automotive Deliverables	DOC-25825
Automotive Transition Table	DOC-25826
Automotive BCAM 7.0 Expert Training	DOC-25827



NXP ISO 26262 INNOVATIONS

Lessons Learned and Continuous Improvement

Product Requirement Mgt

- OEM workshops
- Lessons learned
- System Safety Goal Translation
- **Fail Operational analysis and solutions**

Product Definition

- Doors (SoC & IP)
- Standardized Fail Safe State Machine
- Common chassis safety platform
- **Safety Behavioral Model**

Product Architectures

- Fail Safe (qualified, certified)
- Fail Silent (qualified, certified)
- **Fault Tolerant Systems**



Customer Support

- Documentation (FMEDA, SM)
- Reference Design & AN
- SW Production ready
- **System Solutions (RADAR, ...)**

System Validation

- eFAST : OEM Non ISO Pulse
- HW Fault Injection Test
- FS65 Safety Behavioral Model
- **FIT verification through Model**



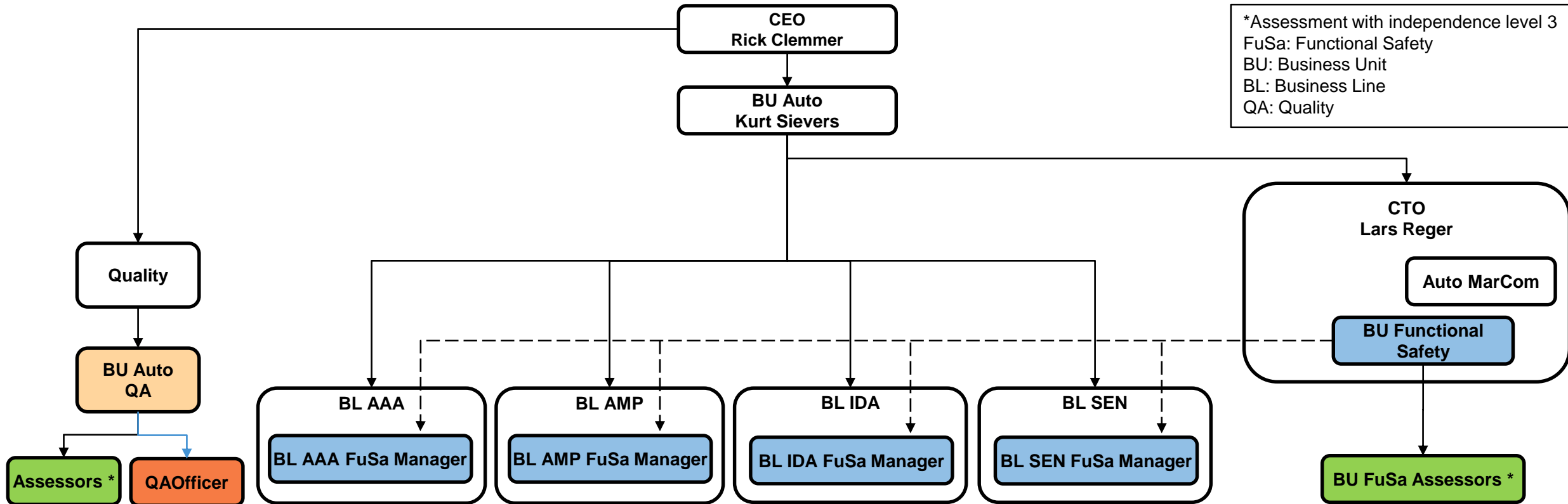
Verification

- Automated Traceability Matrix (NPI360)
- Virtual Test
- Fault Injection Simulation

- available
- **planned**



Automotive Functional Safety – Organization Setup



SafeAssure Community

Customer support for Functional Safety



SafeAssure Community

Public Space for knowledge distribution and industry-wide news
[here](#)

SafeAssure NDA

Private NDA space for customer to access safety documentation
[here](#)

Support

Safety Expert Group composed of Safety Managers and Architects, Field and Application Engineers



Self Sufficient

Community users find answers to their questions and safety documentation requests



Reduce Risk: Track & Understand Failures

Car OEM

SET SYSTEM **RISK CRITICITY** (HAZARD ANALYSIS) ASIL A, B, C or D
DEFINE **SAFETY GOALS**

Tier1 &
Silicon

IMPLEMENT MEASURES TO REDUCE RISK OF FAILURE
DIFFERENT TYPE OF FAILURES



Avoid **SYSTEMATIC FAILURES**
during development

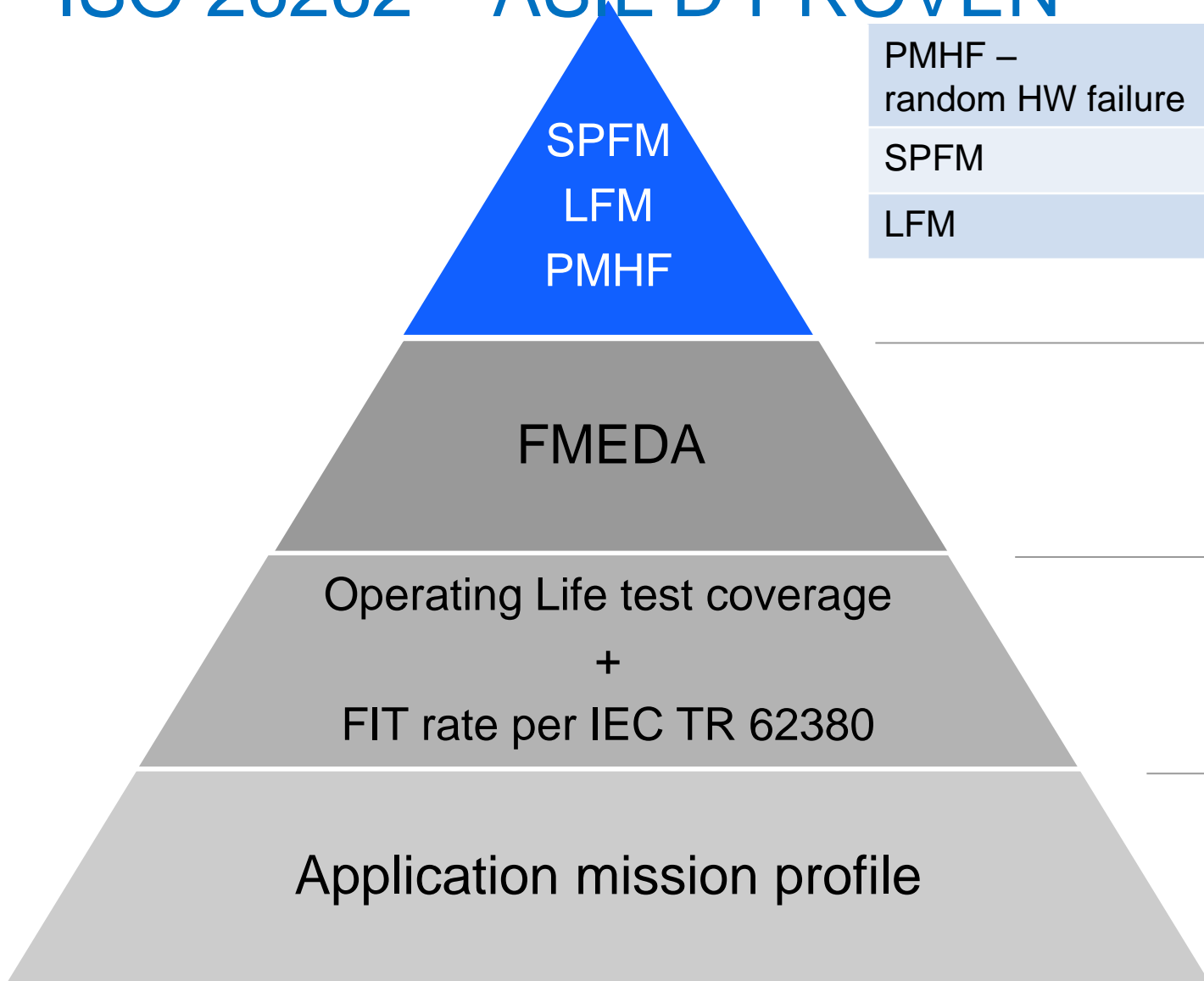
- Process
- Safety management
- Best practices
- Lessons learned
- Verification & validation



Avoid **RANDOM FAILURES**
during operation

- System safe state
- Safety architecture
- Quantitative & qualitative analysis
- Documentation

ISO 26262 – ASIL D PROVEN



	ASIL B	ASIL C	ASIL D	FS45/65
PMHF – random HW failure	$<10^{-7}$	$<10^{-7}$	$<10^{-8}$	$0.721 \cdot 10^{-9}$
SPFM	$>90\%$	$>97\%$	$>99\%$	99.3%
LFM	$>60\%$	$>80\%$	$>90\%$	96.9%

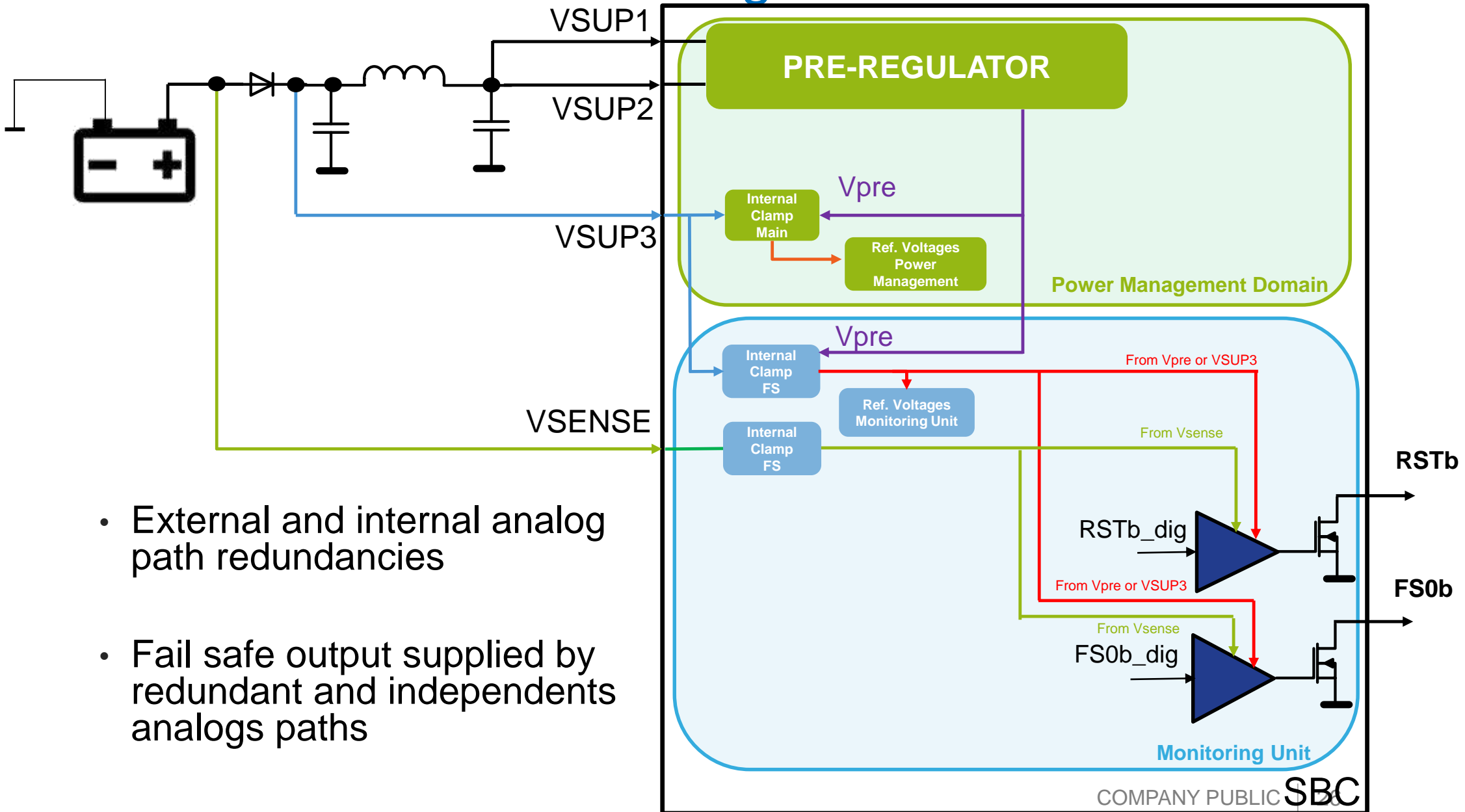
SafeAssure

NXP – Robustness and Safety

Customer

External and Internal Analog Paths

■ Power Management Domain
■ Monitoring Unit



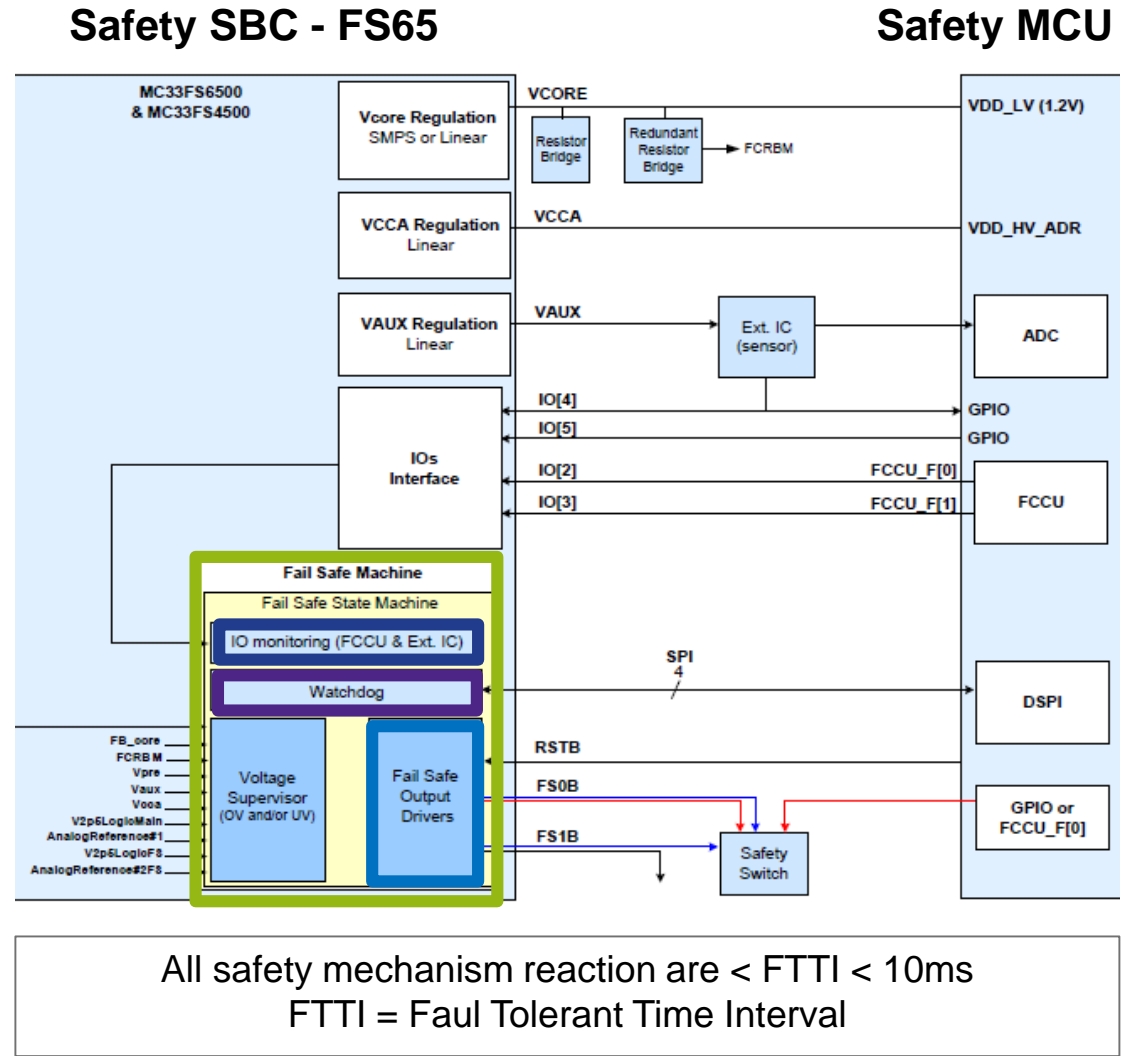
- External and internal analog path redundancies
- Fail safe output supplied by redundant and independent analogs paths

MCU + FSBC Fit for ASIL D Backbone

HW & SW added values for fail silent requirements

- Independent Fail Safe State Machine**
- Physical & Electrical independence to fit for ASILD
 - Power Management Monitoring Unit (UV / OV)
 - Analog & Digital Built In Self Test to minimize Latent Faults
 - Own Reference & Supply to Reduce Common Cause Failure

- Advanced Watchdog**
- Challenger
 - Replace external MCU Monitoring



- HW Redundancy**
- Vcore external Monitoring

- MCU Monitoring**
- FCCU : Fault Collection Control Unit
 - Monitor Dual Core Lock Step Modes MCUs

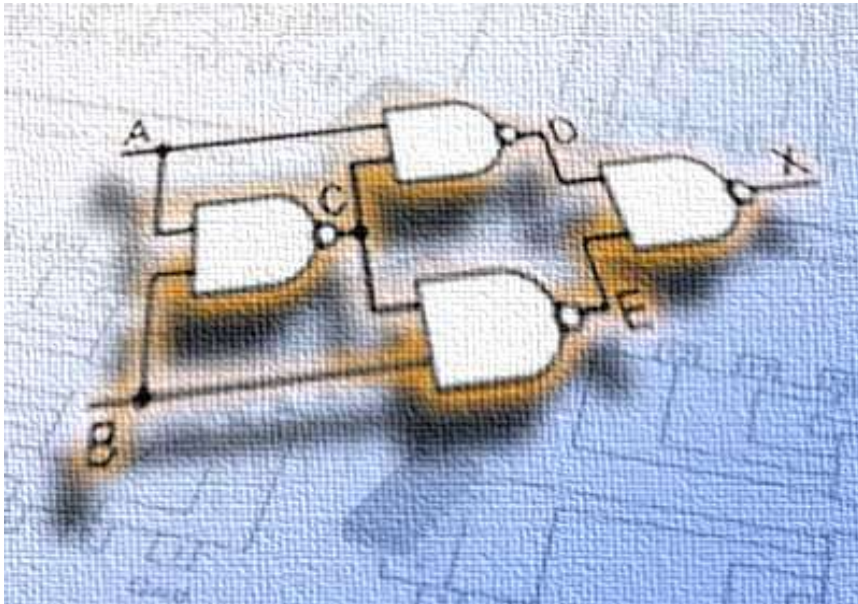
- RSTb – Fail Silent Mode**
- Configurable RSTb activation giving more system availability

- Fail Safe Pin (FS0b) :**
- Redundant System Fail Safe enabler
 - Second Fail Safe pin to assert safety path with configurable delay after failure

Digital Architecture Of Monitoring Unit

Several mechanisms are implemented to avoid a bad interpretation of a bit flip (SEU):

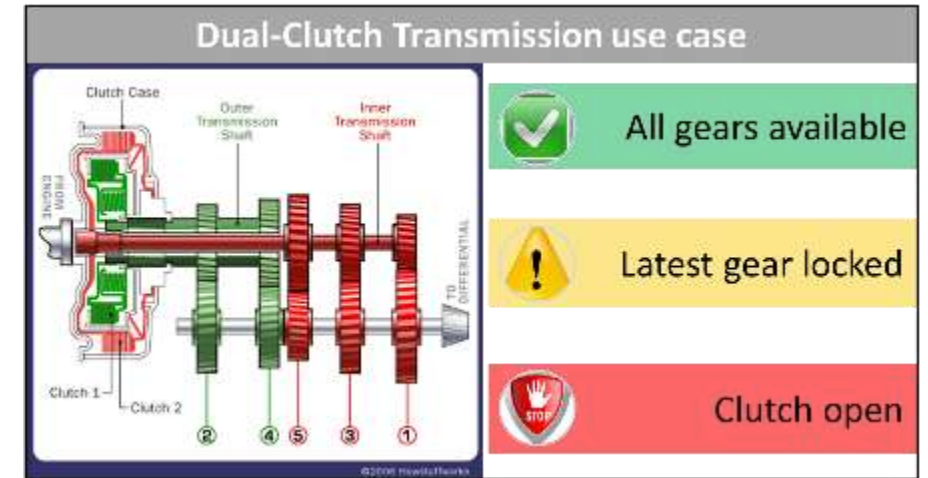
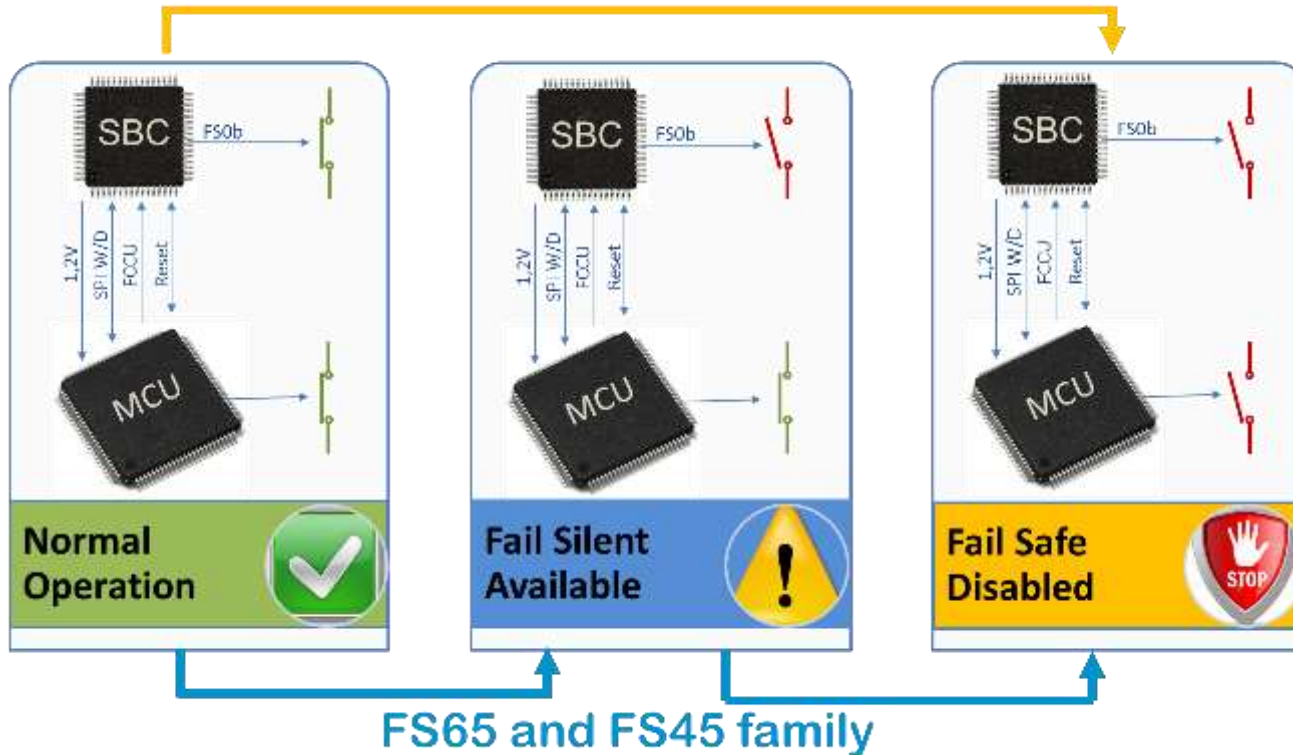
- Triplication of safety registers with majority voter (e.g. WD period duration)
- Design structure to avoid erratic activation of safety outputs (e.g. FS0b)
- ECC for fuse
- Detection and correction of 1-bit flip (SPI registers of Monitoring Unit)
- Detection of 2-bits flips (SPI registers of Monitoring Unit)
- LBIST to reduce Latent Fault



Dependability: Safety vs Availability

Qualitative Analysis – Enabling Fail Silent Operations

MC33907 & MC33908

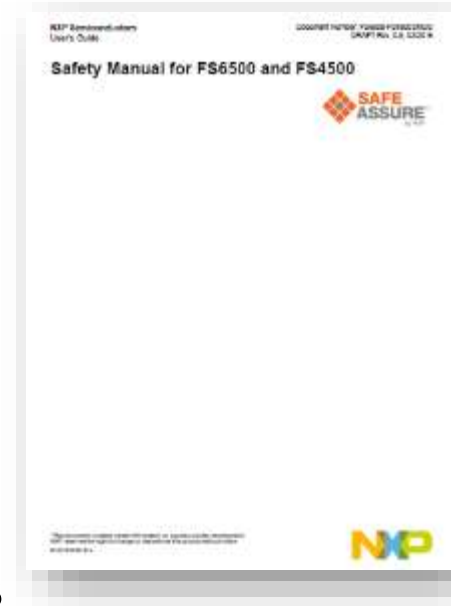


1. **CONFIGURABLE RESET** at SAFE STATE activation to enable **MCU Diagnostic**.
2. **CONFIGURABLE SAFE STATE**, independently for each failure with **2nd Fail Safe output**.
3. **HIGH AVAILABILITY** : No **MCU shutdown** in case of multiple failures.
4. **SMART DEGRADED MODE** : Application is failing with **safe and available** operation

Safety SBC Documentation

SafeAssure – Safety Manual

- Integration of the SBC in a functional safety relevant application
- HW and SW guidelines for the system integrator
- Assumptions of use



SafeAssure – Dynamic FMEDA

Failure Mode	Category	SPF	LF	PMHF	Other Metrics
...

- ASIL metrics (SPF, LF, PMHF)
- FIT RATES
- System Assumptions
- Safety functions and safety mechanisms

SafeAssure – Fault Injection Test report

- Linked to FMEDA
- Validation and verification of the good implementation of all the Safety Mechanisms
- FTTI verification

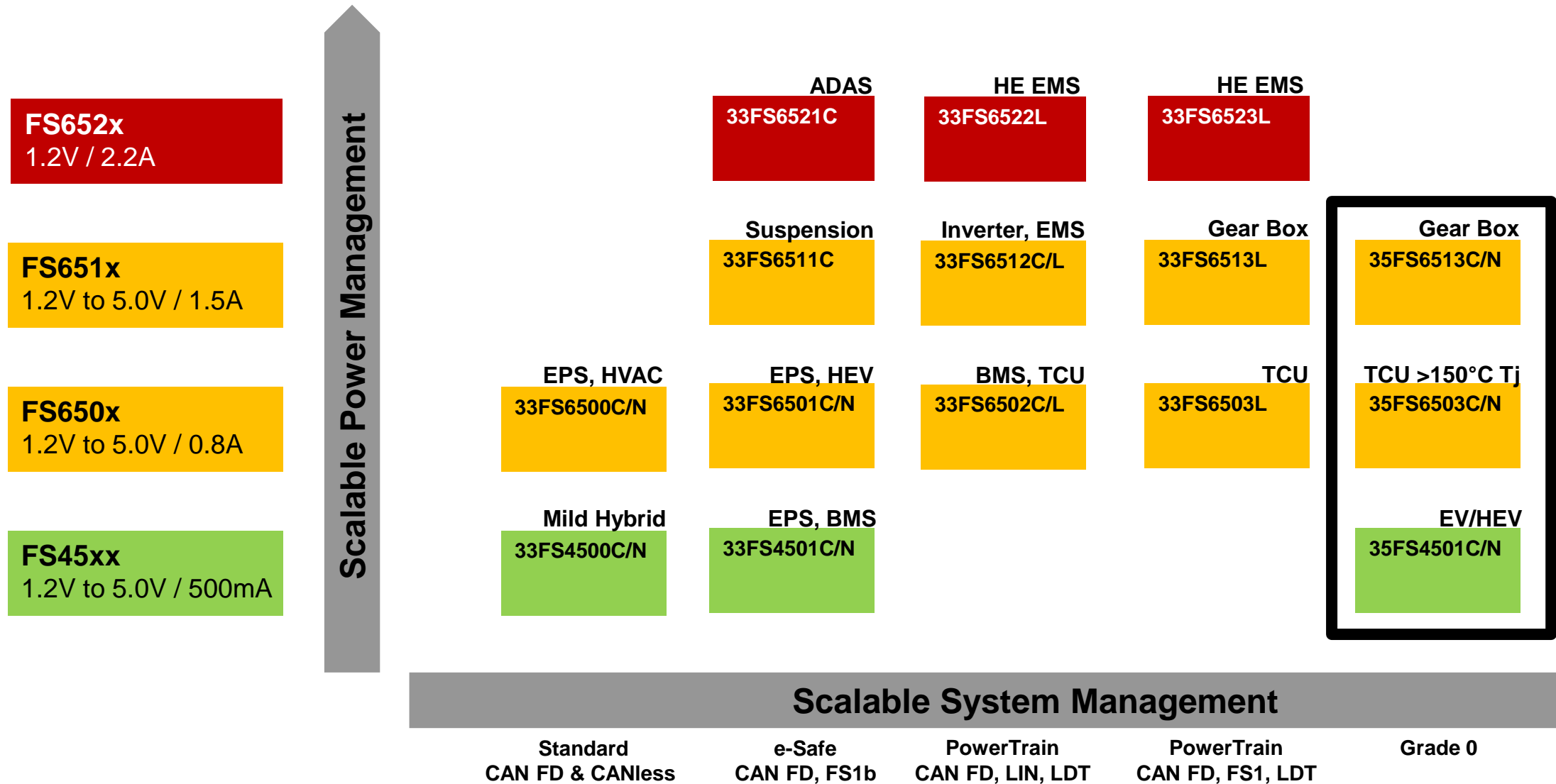
Item ID	Failure ID	Failure Mode	Failure Rate	Failure Type	Failure Mechanism	Failure Mode	Failure Rate	Failure Type	Failure Mechanism
1	FS6500_001



Portfolio Scalability



FS65/45 Family – SCALABLE Functional Safety SBC Solutions



FS65x: ASIL D Safety SBC

MPC57xx Attach Solution used in ASIL D systems (TCU, Inverter, EPS)

✓ GRADE 0
✓ GRADE 1
QUALIFIED



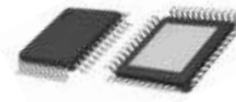
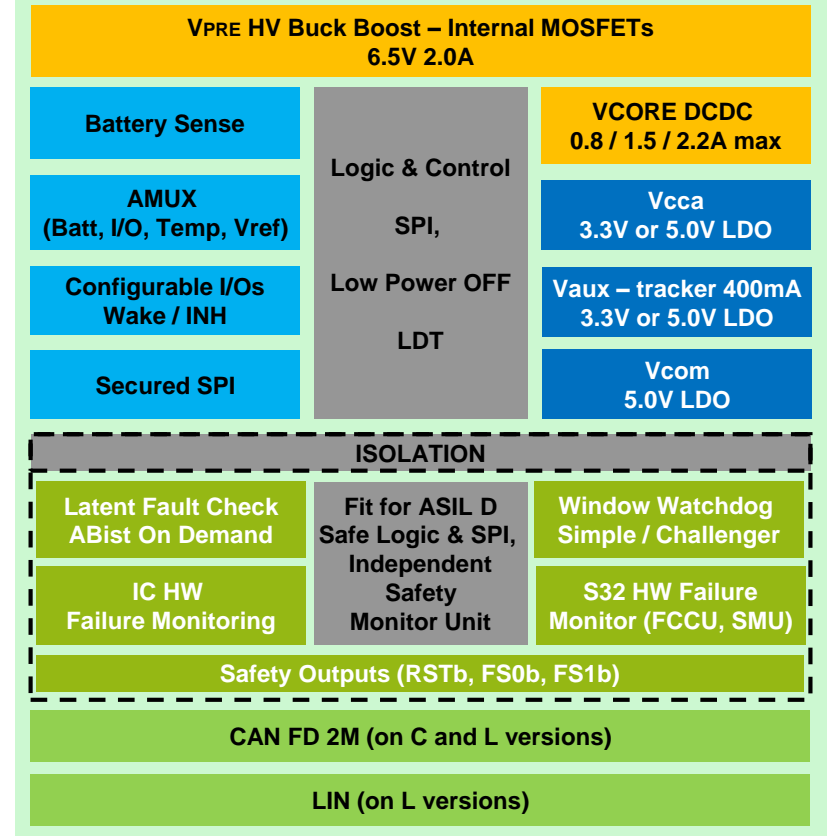
Power Management Solution

- Input supply up to 40V DC
- **HV BUCK/BOOST**, 6.5V, 2.0A DC, 440kHz Asynch. With integrated MOSFETs
- **VCORE : DCDC** with adjustable Vcore 1.0V to 5.0V
 - Part Number selection for Max Current : 0.8A (FS650x) or 1.5A (FS651x) or 2.2A (FS652x)
- **VCCA LDO 3.3V or 5V**, 100mA / 1% or 300mA 3%
- **VAUX TRACKER 3.3V or 5V**, 400mA, with 10mV offset
- **VCOM LDO 5V**, 100mA
- **LOW POWER OFF MODE**, with Wake up by I/Os, CAN/LIN, and 30µA Low Quiescent current

Safety & System Features

- **Fail Silent – Configurable State Machine** with Independent Safety Monitoring Unit
- Control via 32 bits SPI (including CRC)
- Low Power OFF Mode with Low Quiescent current : 30µA
 - Wake up via dedicated pins, CAN, LIN
 - Long Duration Timer (LDT) feature – counter from few secs up to 6 months
- AMUX: Battery, Internal Safety critical voltages, Precise Vref and Temperature
- CAN FD 2M PHY and LIN
- Several Part Numbers pin to pin compatible with optional FS1b, LDT, CAN, LIN

FS65xx Functional Block Diagram



Samples : Now
PPAP : Now
Package : LQFP48eP

FS450x: ASIL D Safety SBC

S32Kx Attach Solution used in ASIL C/D systems (BMS with Newtec)

✓ GRADE 0
✓ GRADE 1
QUALIFIED



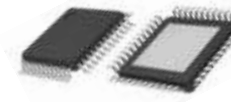
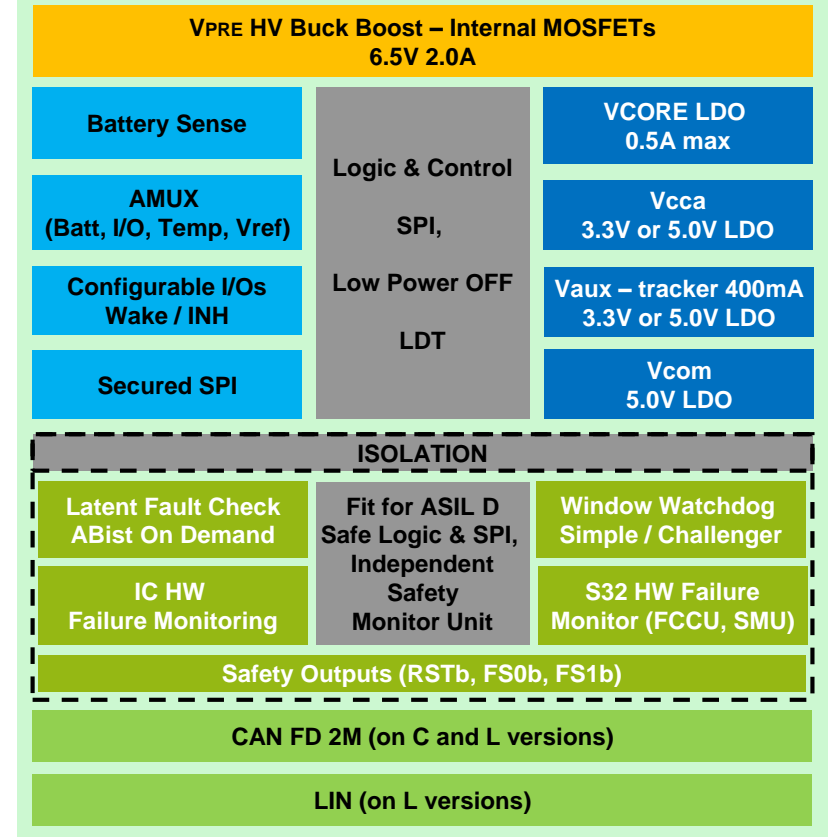
Power Management Solution

- Input supply up to 40V DC
- **HV BUCK/BOOST**, 6.5V, 2.0A DC, 440kHz Asynch. With integrated MOSFETs
- **VCORE : LDO** adjustable 1.0V to 5.0V, 0.5A max
- **VCCA LDO 3.3V or 5V**, 100mA / 1% or 300mA 3%
- **VAUX TRACKER 3.3V or 5V**, 400mA, with 10mV offset
- **VCOM LDO 5V**, 100mA
- **LOW POWER OFF MODE**, with Wake up by I/Os, CAN/LIN, and 30µA Low Quiescent current

Safety & System Features

- **Fail Silent – Configurable State Machine** with Independent Safety Monitoring Unit
- Control via 32 bits SPI (including CRC)
- Low Power OFF Mode with Low Quiescent current : 30µA
 - Wake up via dedicated pins, CAN, LIN
 - Long Duration Timer (LDT) feature – counter from few secs up to 6 months
- AMUX: Battery, Internal Safety critical voltages, Precise Vref and Temperature
- CAN FD 2M PHY and LIN
- Several Part Numbers pin to pin compatible with optional FS1b, LDT, CAN, LIN

FS450x Functional Block Diagram



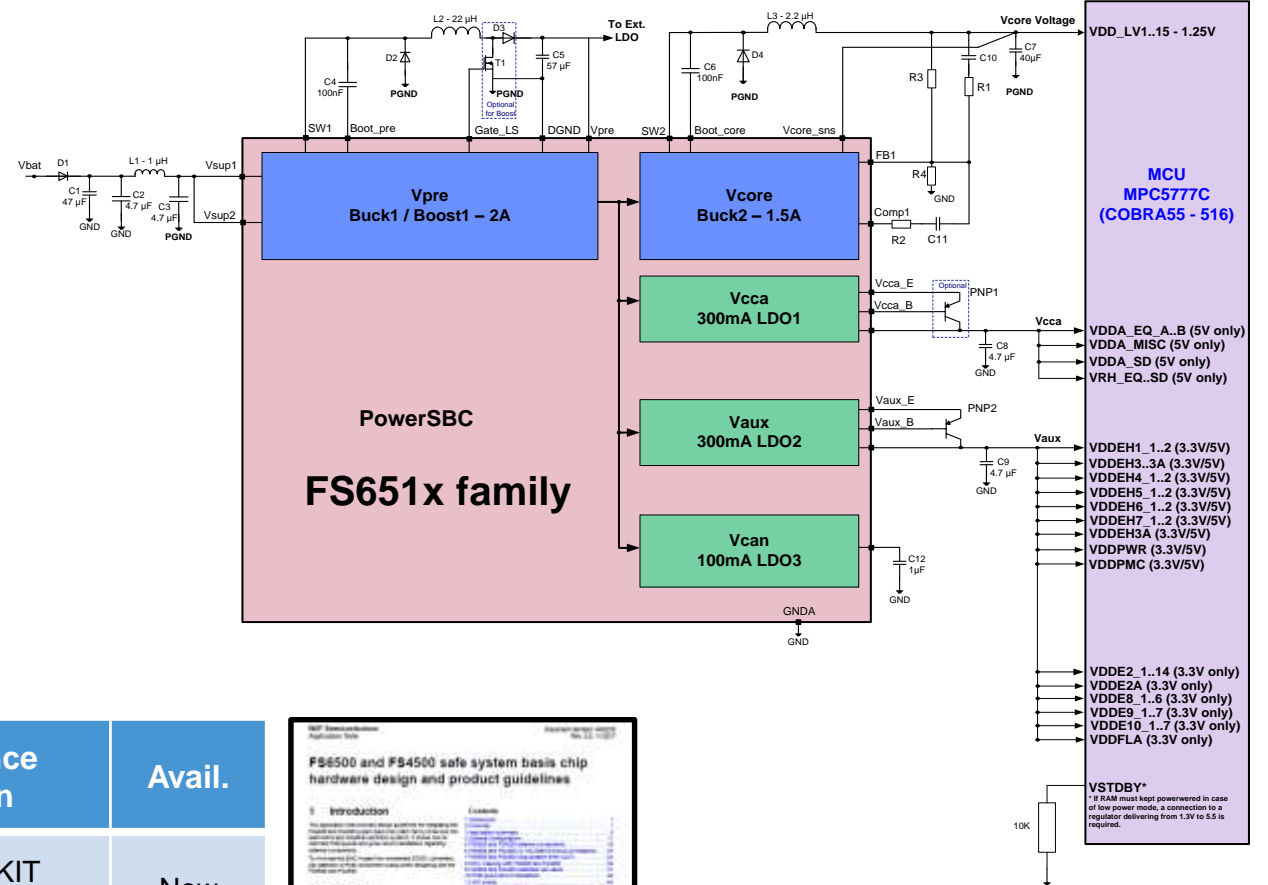
Samples : Now
PPAP : Now
Package : LQFP48eP

Attaching FS45/65 to NXP Safety MCU

FROM AN5238

FS45 & FS65 Power Management Values

- ✓ **Scalability** : Pin Compatible Solutions
- ✓ **Power Flexibility**
 - ✓ FS450x : 0.5A Vcore (LDO)
 - ✓ FS650X : 0.8A Vcore (DCDC)
 - ✓ FS651X : 1.5A Vcore (DCDC)
 - ✓ FS652X : 2.2A Vcore (DCDC)
- ✓ **Availability** :
 - ✓ Configurable Buck / Buck Boost Vpre
 - ✓ Min Vsupply : 2.7V – LV124 compliant
 - ✓ Max Vsupply : 36V



Auto MCU Part Number	Applications	ASIL level	Safety SBC Attach	Reference Design	Avail.
MPC5744P	HEV, Motor ctrl EPS	D	FS650X	SAFETYKIT MICROSYS	Now
MPC5775E	Inverter	C/D	FS651X	ASIL D INVERTER On going	Now
S32K1	Safety General Purpose	B to C	FS450x	BMS ASIL C NEWTEC	Now

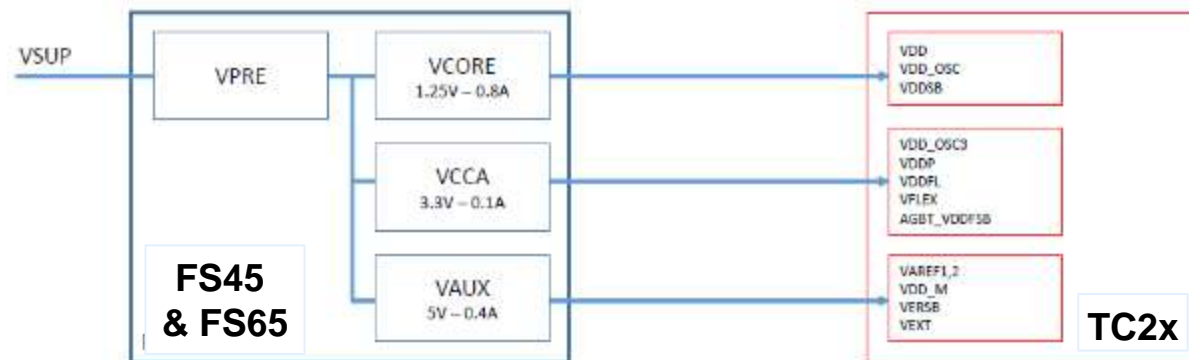


Attaching FS45/65 to AURIX Safety MCU

FROM AN5238

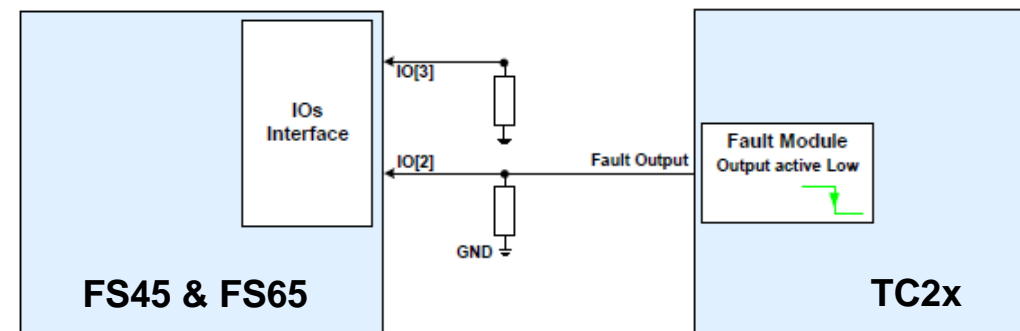
Power Management

- FS6500 can power Aurix MCU. Below power tree proposal described in AN5238 is not the only one, and can be adjusted depending on application need.
- Proven solution in production at multiple Tier 1 & Disty.



Safety Monitoring

- FS6500 can monitor AURIX Safety Monitoring Unit (SMU) output thru IO_2:3 safety input pins with below connections described in the Safety Manual.

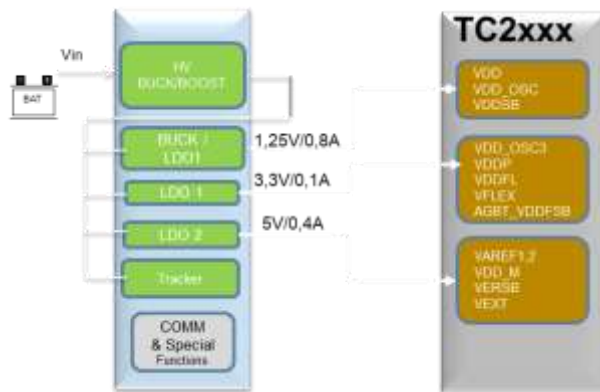


NXP Safety PMIC Solution Attached to NON NXP Processor

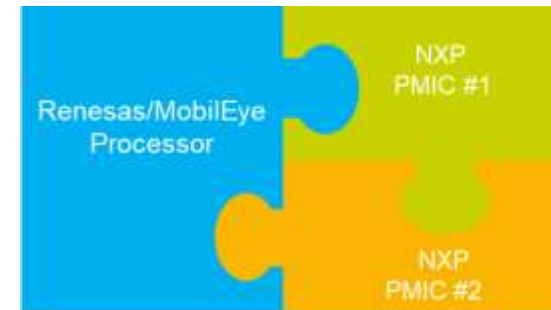
NXP Safety PMIC is ideal solution to achieve ASIL D Level



AURIX	Example of NXP PMIC solution
	MC33907
TC2/3X	FS6500
	FS8500



NXP Safety PMIC solution for Renesas & MobilEye Soc



MobilEye	Example of NXP PMIC solution
EyeQ4	PF8100
EyeQ5 EyeQ5Mid	PF Series As One Box System

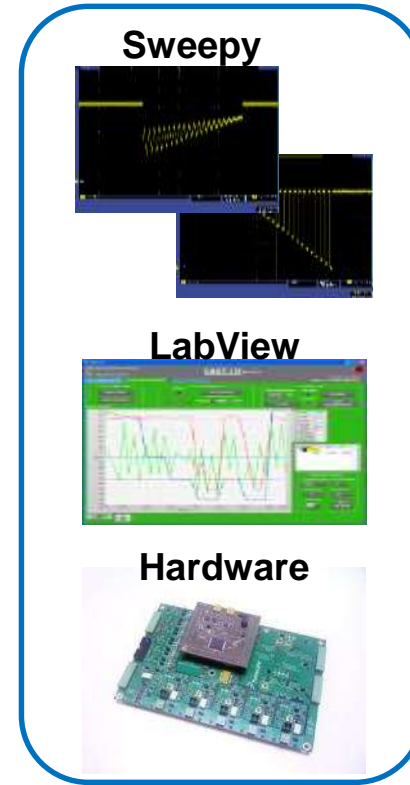
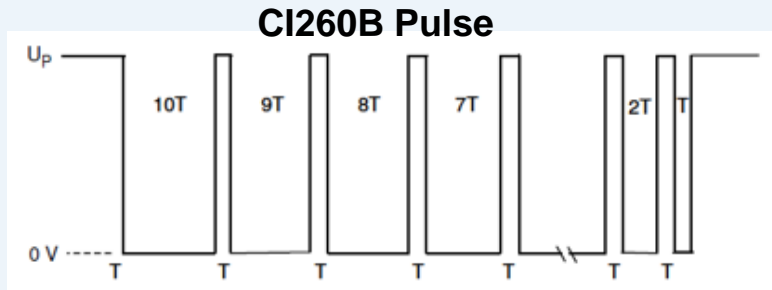
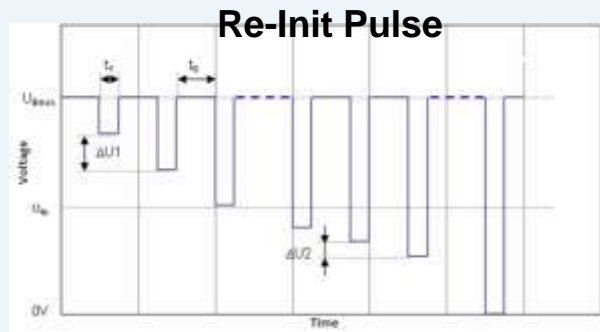
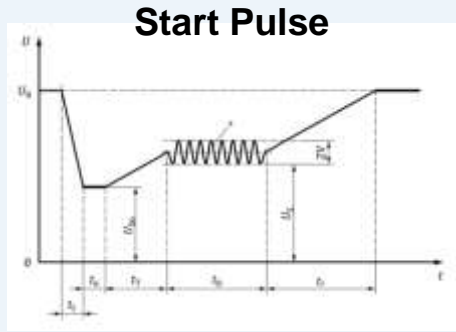
Renesas	Example of NXP PMIC solution
RH850	FS65
R-CAR	PF Series As One Box System

Electrification Robustness



Functional Robustness

AUTOMATED BATTERY TEST VALIDATION PLATFORM

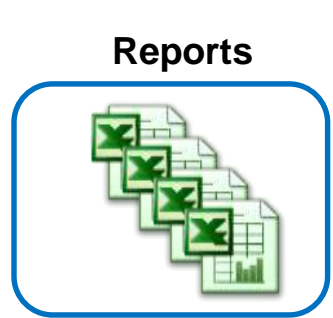
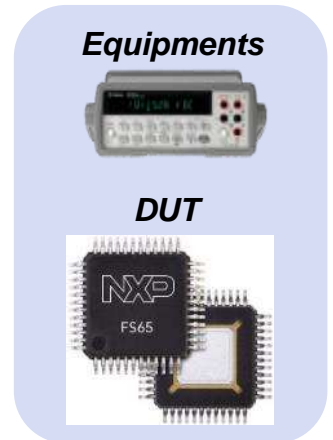


Control & Monitoring

Configuration & Results

UNIQUE

Automated Execution



BENEFITS – EXTENDED VALIDATION

Car OEMs PULSES - Database

INCREASE USE CASE Coverage - Break the limit. (x10)

ACCELERATE VALIDATION – Reduce validation by 4

ISO26262 COMPLIANT - Full Traceability

MULTIPURPOSE - Non-ISO, Funct. Validation

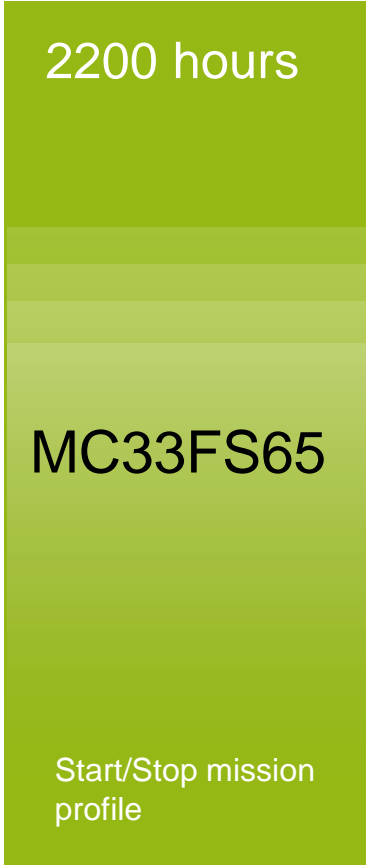
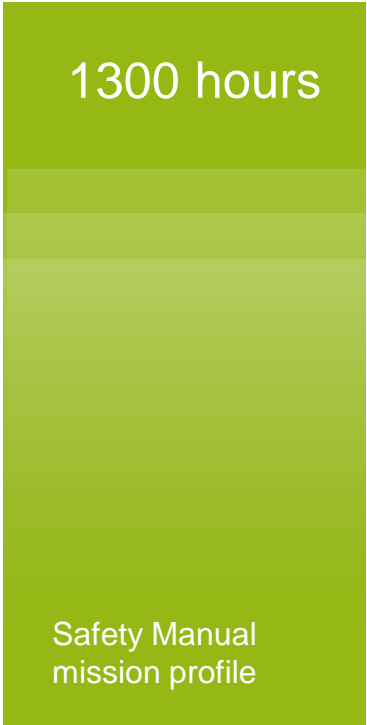
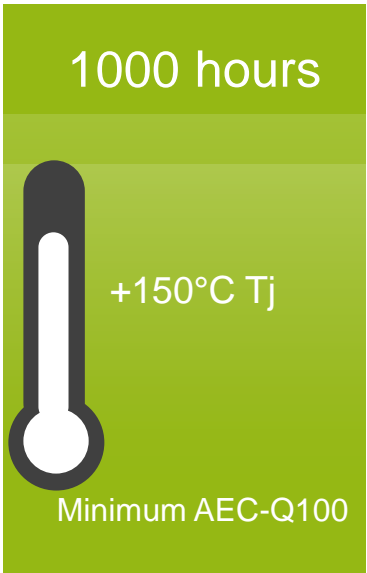
FS45/65 Reaching Extended Automotive Qualification

UNIQUE ASIL-D device Grade 0 qualified

Grade 0

Grade 1

ROBUSTNESS



System Solutions

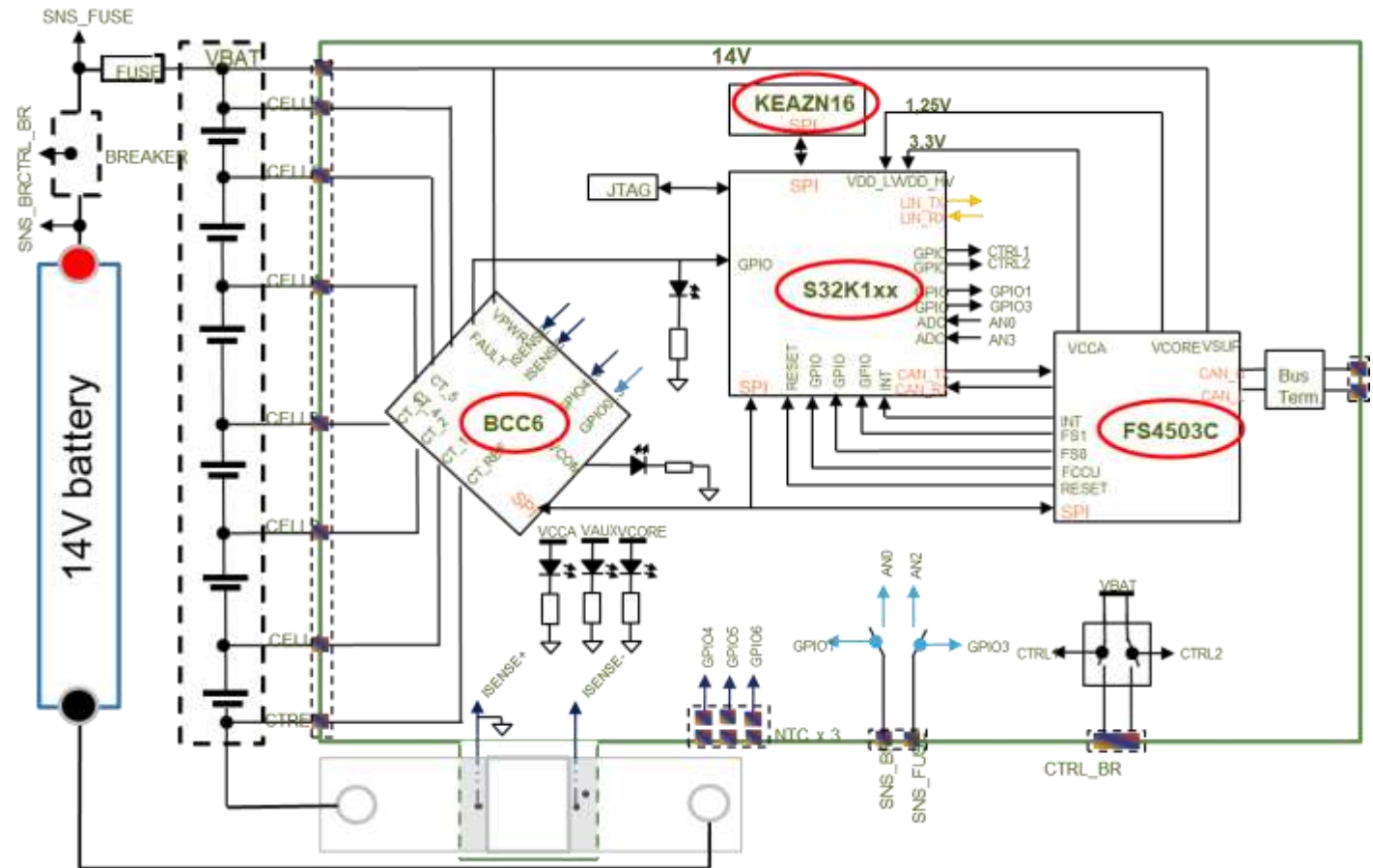


Mastering xEV Power: ePowertrain Solutions

Major xEV Components

	MCU	SBC	COMM	Driver	AFE
Battery management system	S32K	FS45	TJA104x	eSwitch	BCC6x
Motor control, inverter, HCU	5775E	FS65	TJA104x	GD3100	Software resolver
48V eMachine (BSG, ISG, HVAC)	S32Kx	FS45 UJA116x	TJA14xx		
DC/DC voltage domain converter	S32K+		TJA104x		
On-board charger AC/DC converter	S32K+		TJA104x		

Low Cost ASIL C Battery Management System



FS45/65 – System Solutions for Electrification

Enabling ASIL D Fail Silent Operations, Simplify Design and Reduce System cost

FIT FOR ASIL-D APPLICATIONS

- SPM>90%, LT>99%, PHMF<10⁻⁸
- Analog & Digital Safety Mechanisms to fit for ASILD
- All safety mechanism reaction are < FTTI < 10ms

FAIL SILENT MODE

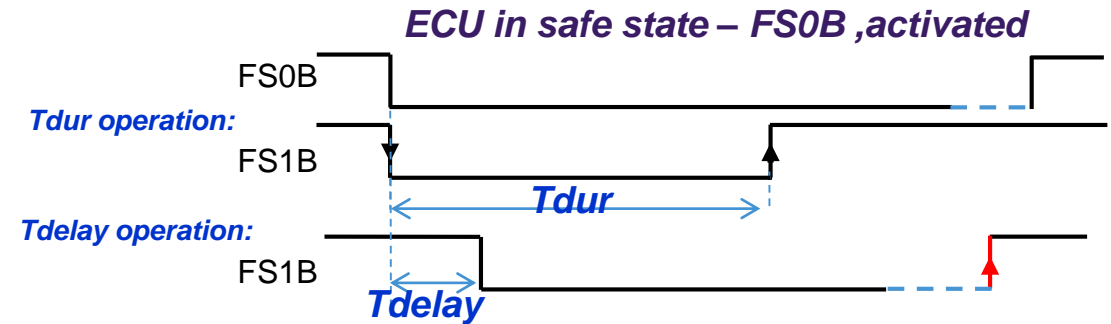


- OPTIONAL RESET at SAFE STATE to enable MCU Diag
- CONFIGURABLE SAFE STATE, independently for each failure
- SYSTEM AVAILABILITY : No MCU shutdown after multiple failures
- SMART DEGRADED MODE : safe and available operation

LONG DURATION TIMER

- Internal SBC Counter from few sec to 6 months
- Active in Run and Low Power Operations
- Measure time during Parking Mode (Low Power)
- Measure time during BMS Operation (Run)
- Optional Cyclic Wake Up (every week)

REDUNDANT FAIL SAFE PIN (FS0B & FS1B)



- T duration OPERATION : Inhibit CAN during T_{dur} duration
- T delay OPERATION : Safe delay of BMS load desactivation

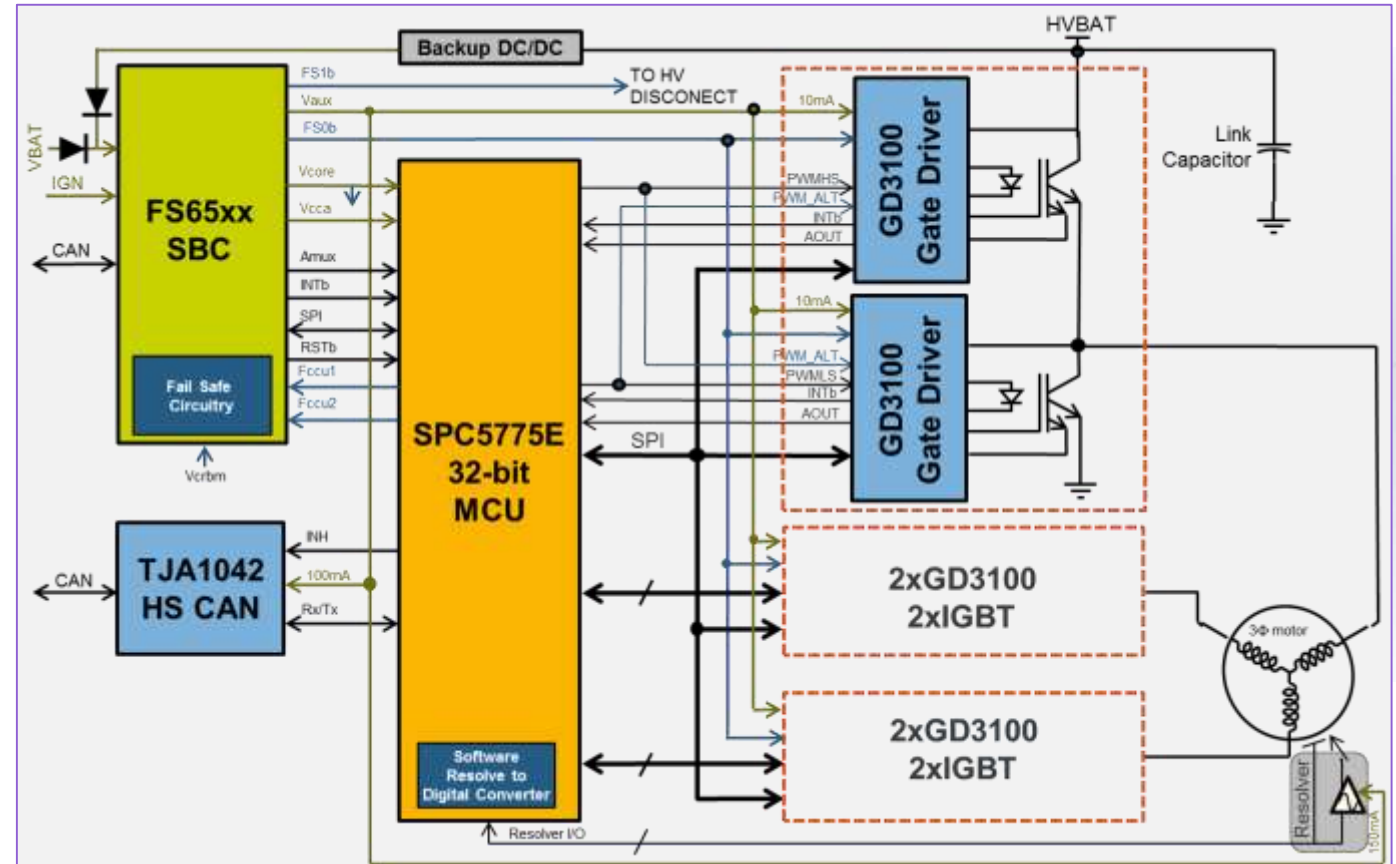
Mastering xEV Power: ePowertrain Solutions



Major xEV Components

	MCU	SBC	COMM	Driver	AFE
Battery management system	5775B	FS65	TJA104x	eSwitch	BCC77x
Motor control, inverter, HCU	5775E	FS65	TJA104x	GD3100	Software resolver
48V eMachine (BSG, ISG, HVAC)	S32Kx	FS45 UJA116x	TJA14xx		
DC/DC voltage domain converter	S32K+		TJA104x		
On-board charger AC/DC converter	S32K+		TJA104x		

Traction Motor Power Inverter Solution

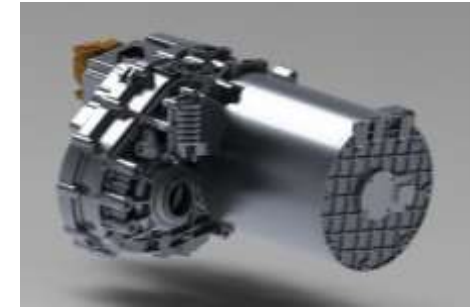


VEPCO PIM Support and Engineering Services



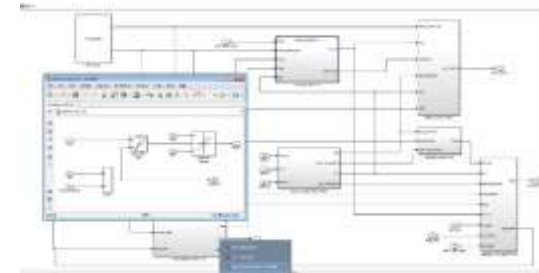
Power Inverter Platform (PIM)

- Apply **NXP hardware, software and toolchains** to vehicle motor control
- **Setup and training** on the use of PIM
- Introduction on **safety** concept of the PIM



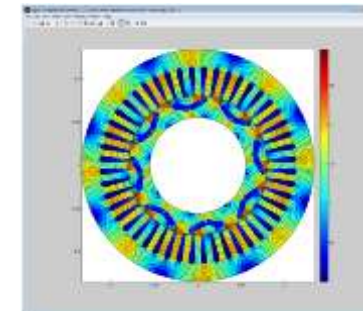
Customization and advanced support:

- Advance PIM design principle to **different vehicle architecture and topology** needs
- Participate customer's **packaging design** and integration analysis
- Premium support over design of complete **eDrivetrain system**
- Facilitate customer ISO 26262 **functional safety** related activities in system design, development, validation and integration cycle
- Work with agencies on design and development process **certification**



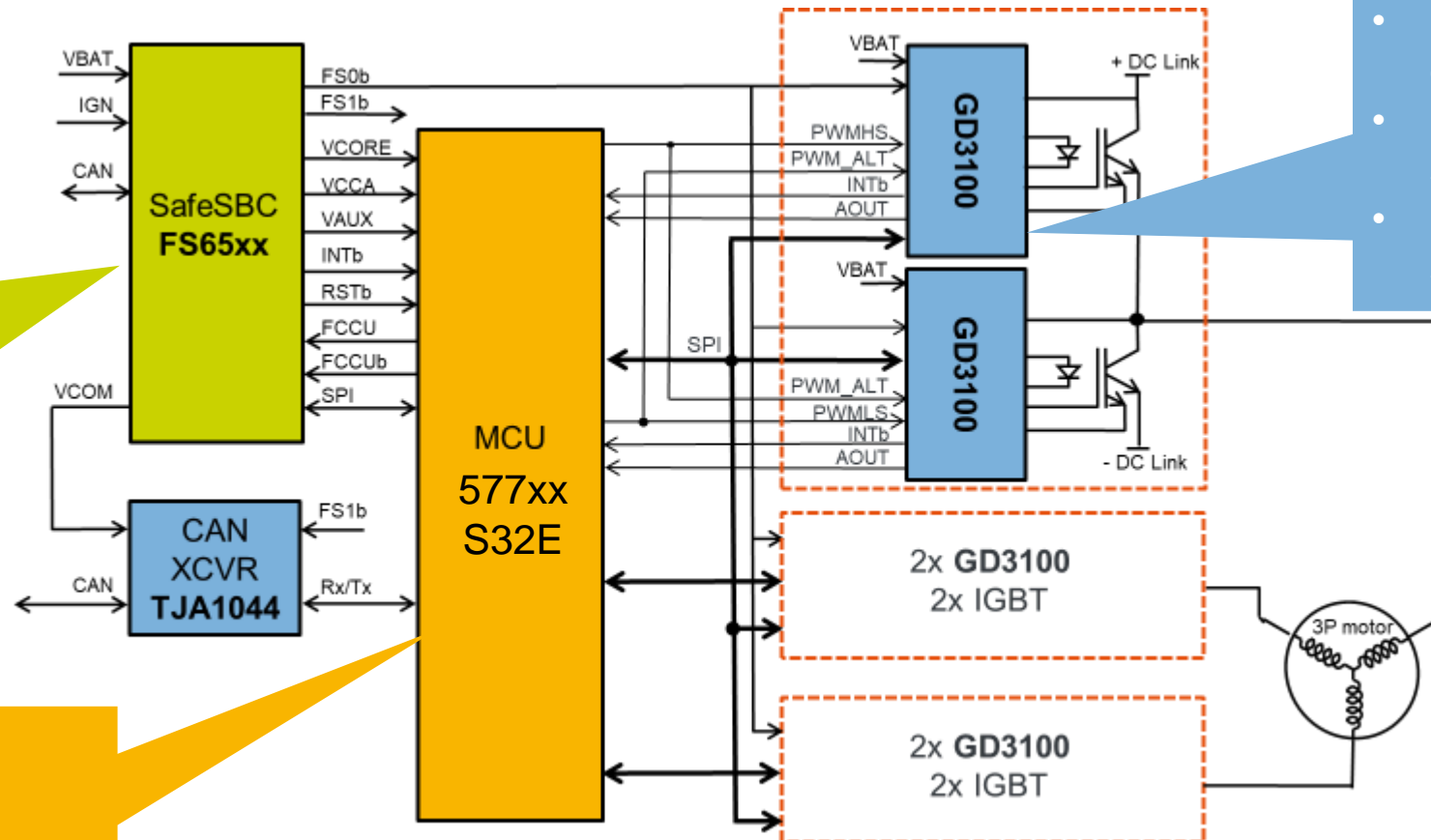
Value-added services:

- **Calibration** and tools integration
- Application level **integration** with advanced auto **code generation** tools
- Engineering software and **tools**
- Dyno and Hardware-in-the-loop **testing**



Example of Solution : Inverter/Traction Motor Control System

- Independence (Phys & Elect) for ASILD
- UV / OV monitoring
- Fail Safe State Machine
- Analog & Digital BIST
- Challenger watchdog



- Fast short circuit protection
- High speed over current protection
- Integrated temp sense
- Integrated galvanic signal isolation

- Multi-core, ASIL-D MCU
- Programmable MC timers
- Software resolver
- Rich on-chip resources – communications, timer, ADC etc

NXP Offer Standard Offer and New Offer

ASIL D components



NXP ASIL-D components are developed accordingly to the ISO26262 standard SEooC

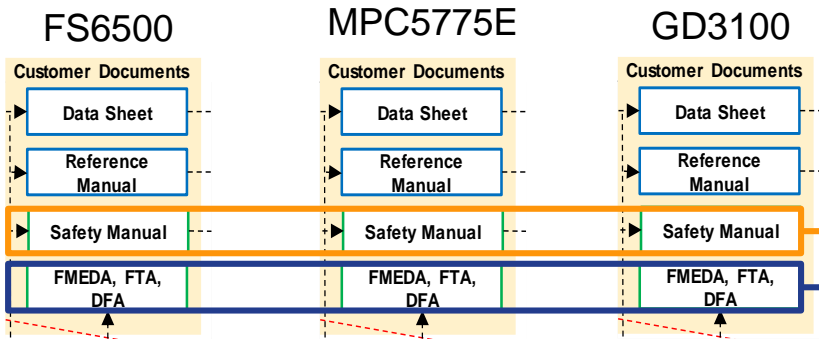
1. Vocabulary		
2. Management of functional safety		
2.6 Overall safety management	2.4 Safety management during the concept phase and the product development	2.7 Safety management after the item is released for production
3. Concept phase		
3.5 Item definition	3.6 Initiation of the safety lifecycle	3.7 Hazard analysis and risk assessment
3.8 Functional safety concept	3.9 Safety validation	3.10 Production
4. Product development at the system level		
4.1 Allocation of product development at the system level	4.2 Specification of the technical requirements	4.3 System design
4.4 System design	4.5 Product development at the hardware level	4.6 Product development at the software level
4.7 Release for production	4.8 Safety validation	4.9 Term integration and testing
5. Production and operation		
5.1 Production	5.2 Operation, service (maintenance and repair) and decommissioning	
6. Supporting processes		
6.1 Requirements management	6.2 Configuration management	6.3 Verification
6.4 Change management	6.5 Validation	6.6 ASIL-oriented and safety-oriented analyses
6.7 Requirements decomposition with respect to ASIL, safety	6.8 Compliance for construction elements	6.9 Analysis of concurrent behavior
6.10 Safety analysis		
7. Guideline on ISO 26262		

Applicable to Component developed as SEooC Reference ISO 26262-10:2012

System safety enablement

- 1- Example of components safety mechanisms and safety concept
- 2- How to attach components together to meet system safety goal
- 3- Propose methodology for new customer
- 4- How to use NXP safety collateral (FMEDA, FTA, DFA).

Current status



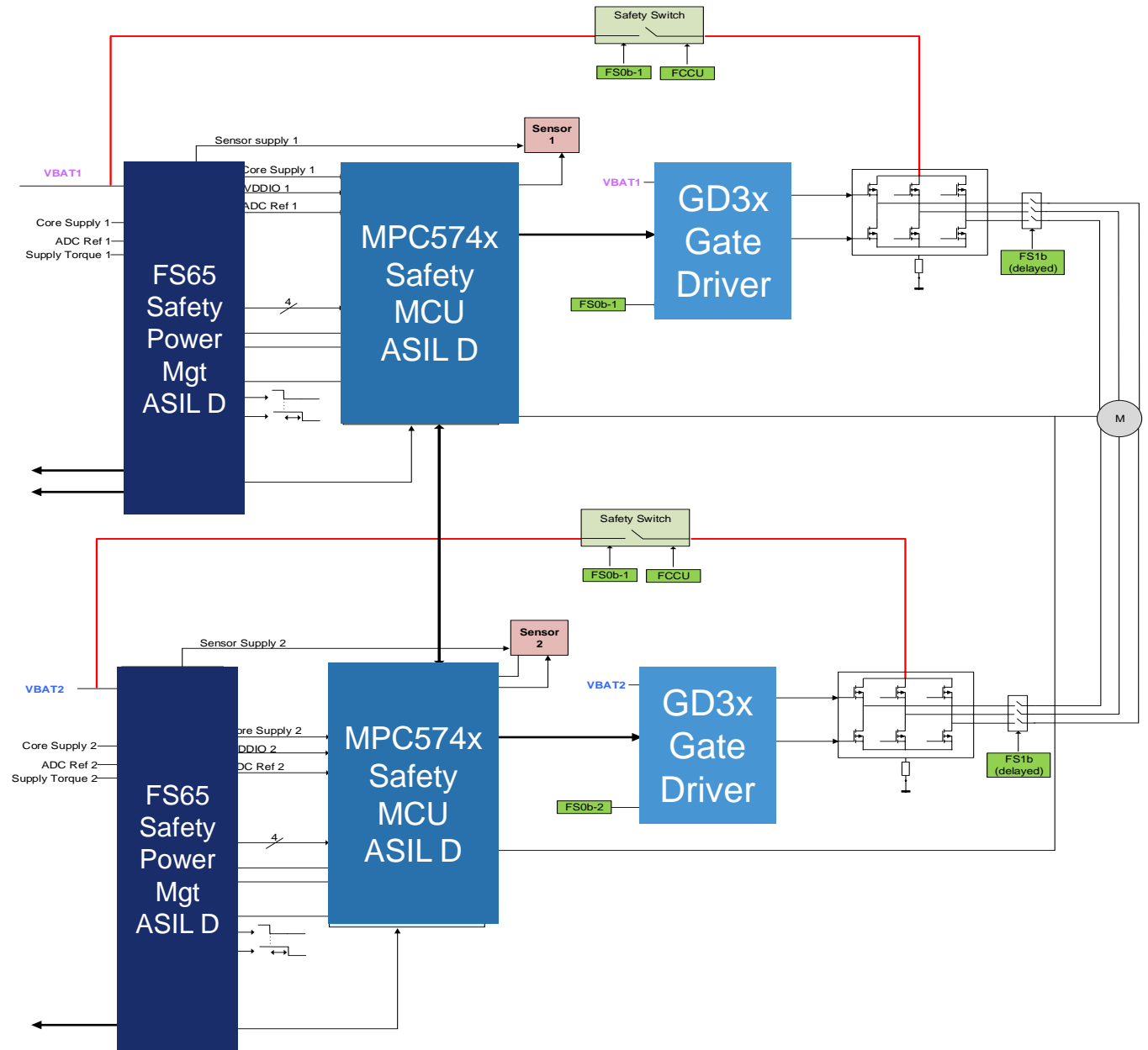
Customers can keep a fast time to market, without compromising on functional safety.

But the safety analysis is not 100% complete. It is the OEM, T1 or partner responsibility for adapting the platform for production.



Motor Control Fail Operational Architecture

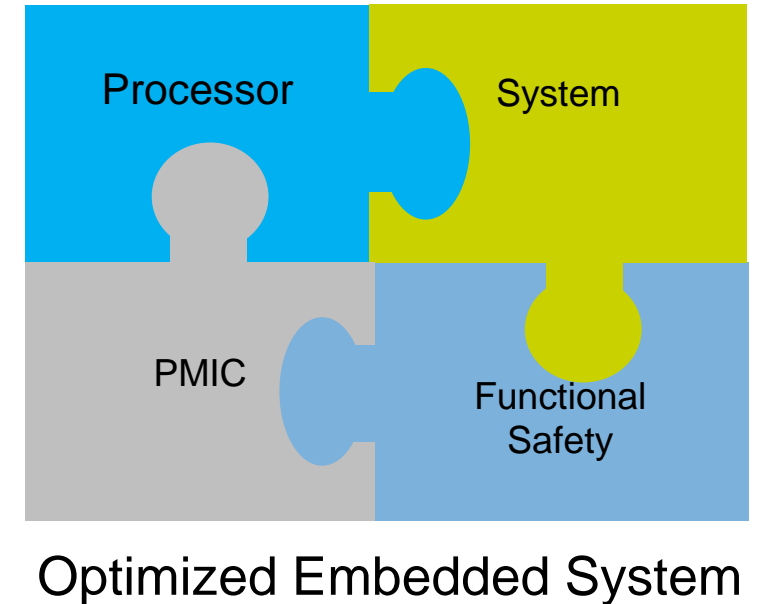
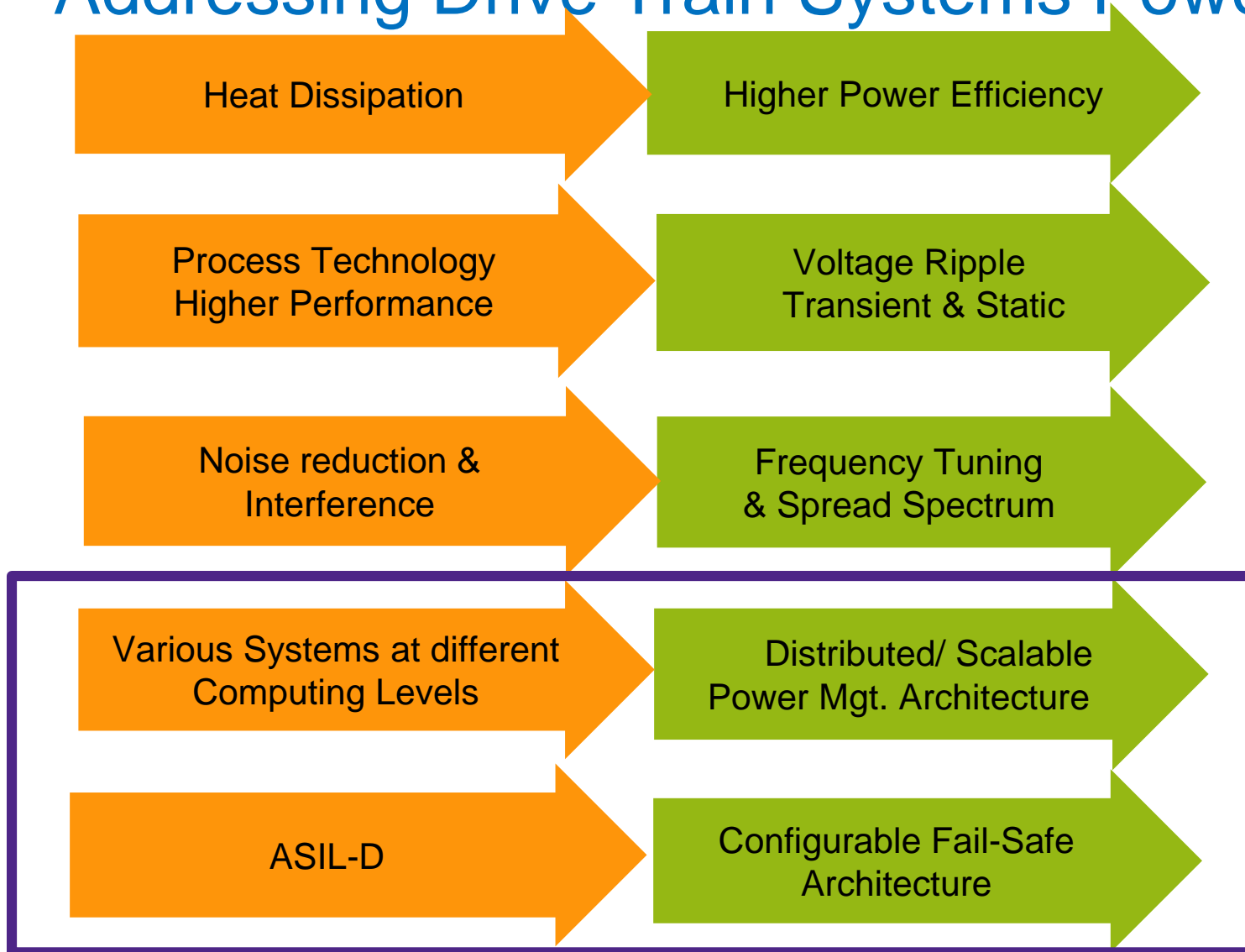
- SAE standards require new fail operational architecture
- Guarantees full/ degraded operation of a function
- Full safety analysis needed to eliminate common cause failures



Next Generation FSBCs

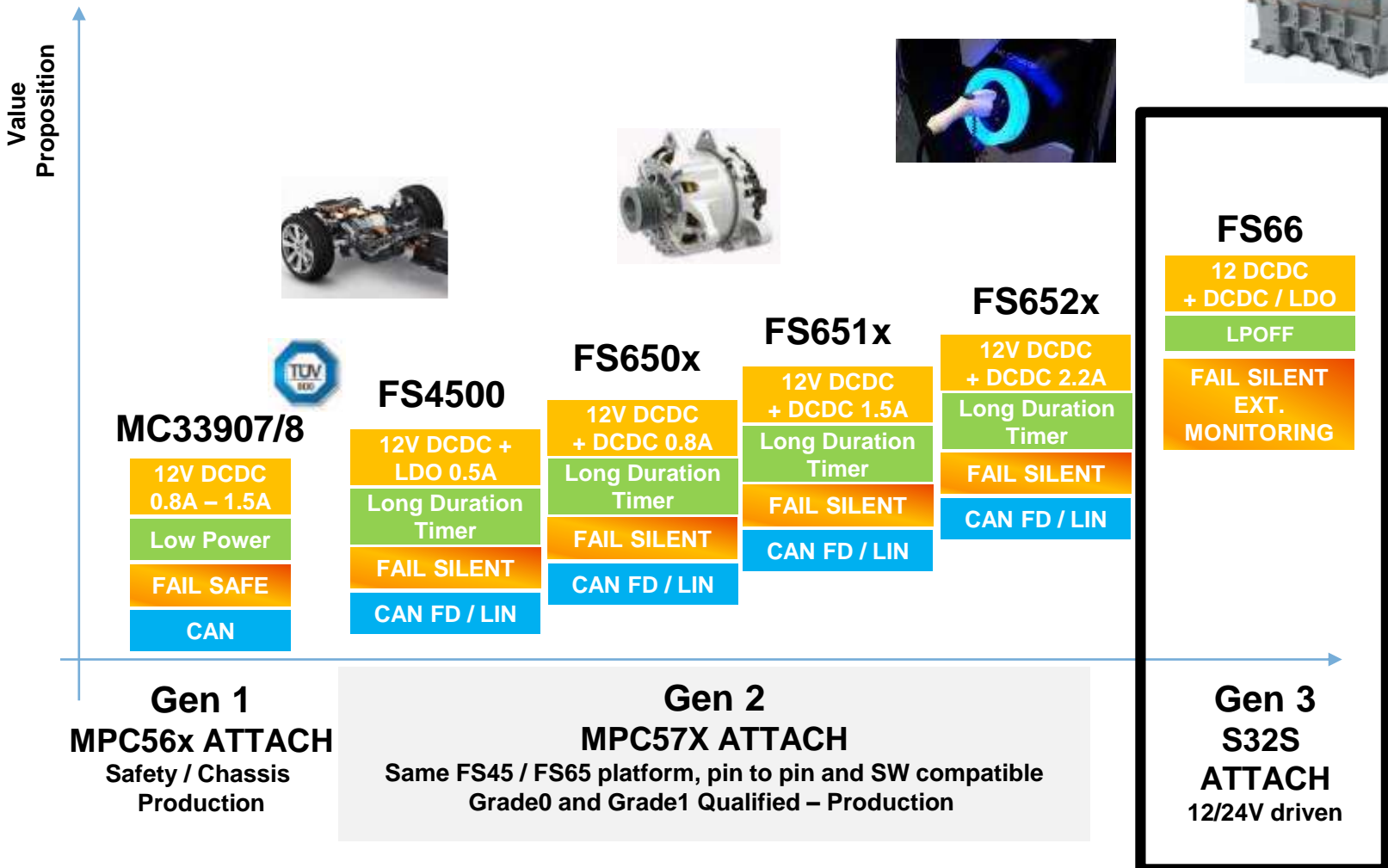


Addressing Drive Train Systems Power Supply Challenges



ENERGY STORAGE – CONVERSION – ACTUATION

Electrification & General Purpose Safety Power Management



Secured & Safe System Solutions

- ISO26262 architecture (TUV SUD proven)
- Functional robustness (non ISO pulse, EMC, HTOL)
- Security (SM transition and Power Gate)

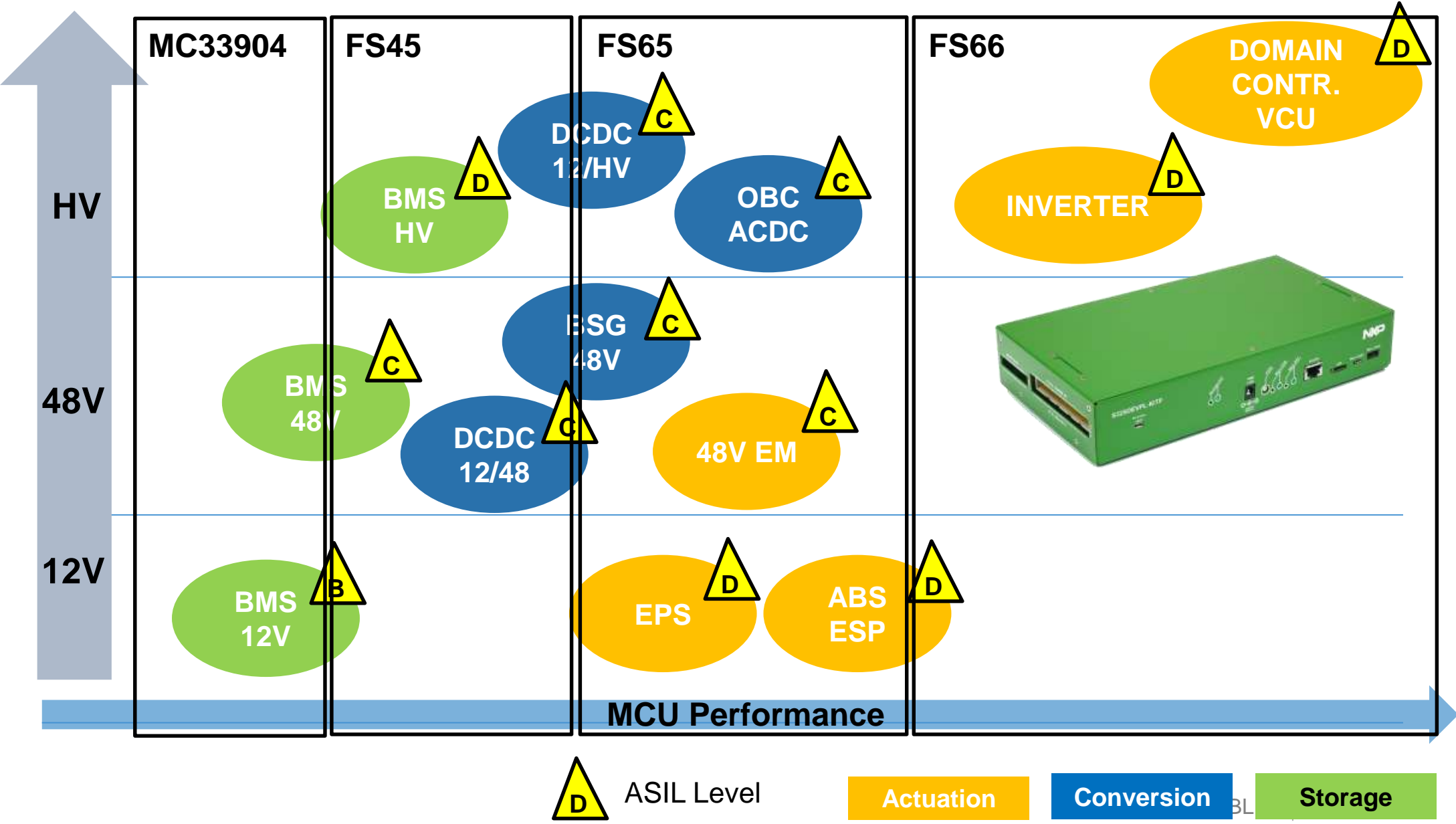
High Efficient Solutions

- Target 12 V, 24 V, 48V (application note)
- DCDC & LDO architecture (Vpre + Vcore)
- Ultra low power modes (low Iq, long dur. timer)

Safety Simplified Solutions

- ISO26262 ready documentation
- System validation test (eFAST)
- Global ecosystem (incl HW & SW)

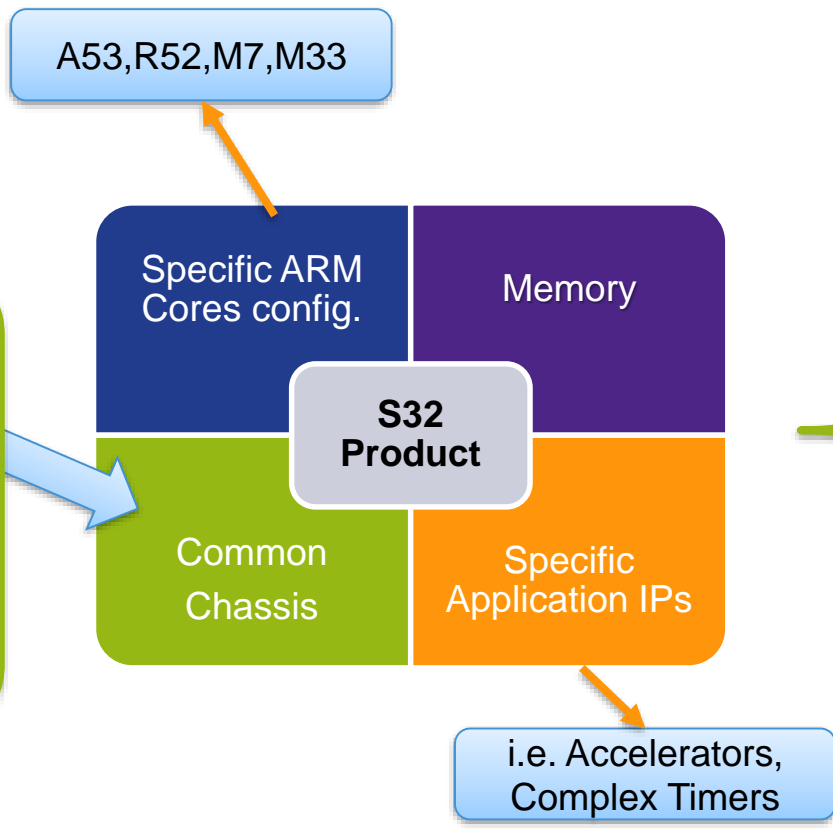
Electrification Market Mapping



Common Chassis: A Common HW and SW Platform

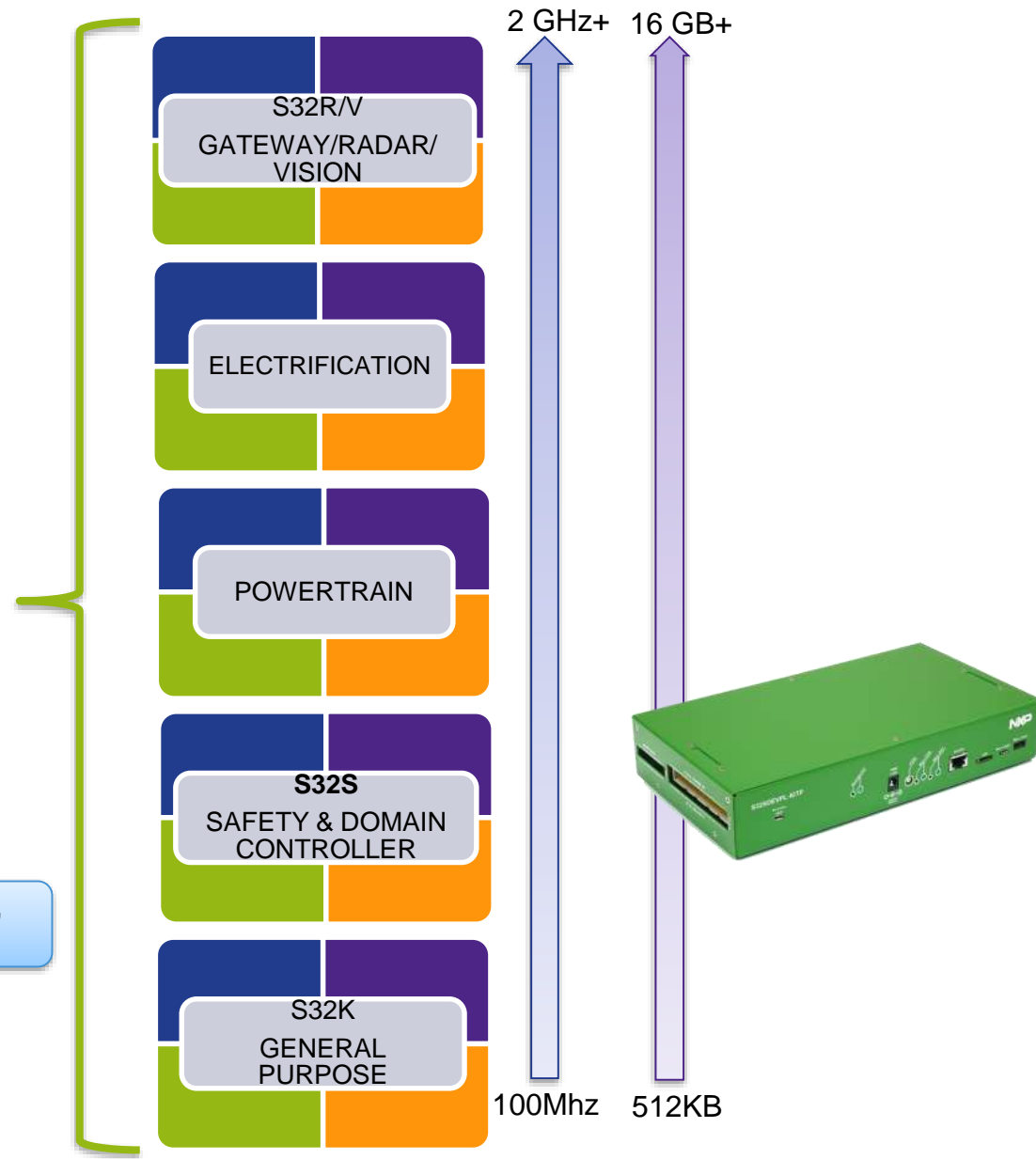
Common Chassis

- Boot & Debug
- Security
- Safety
- Base Peripheral Set
- Clock, Reset, Power
- Interconnection

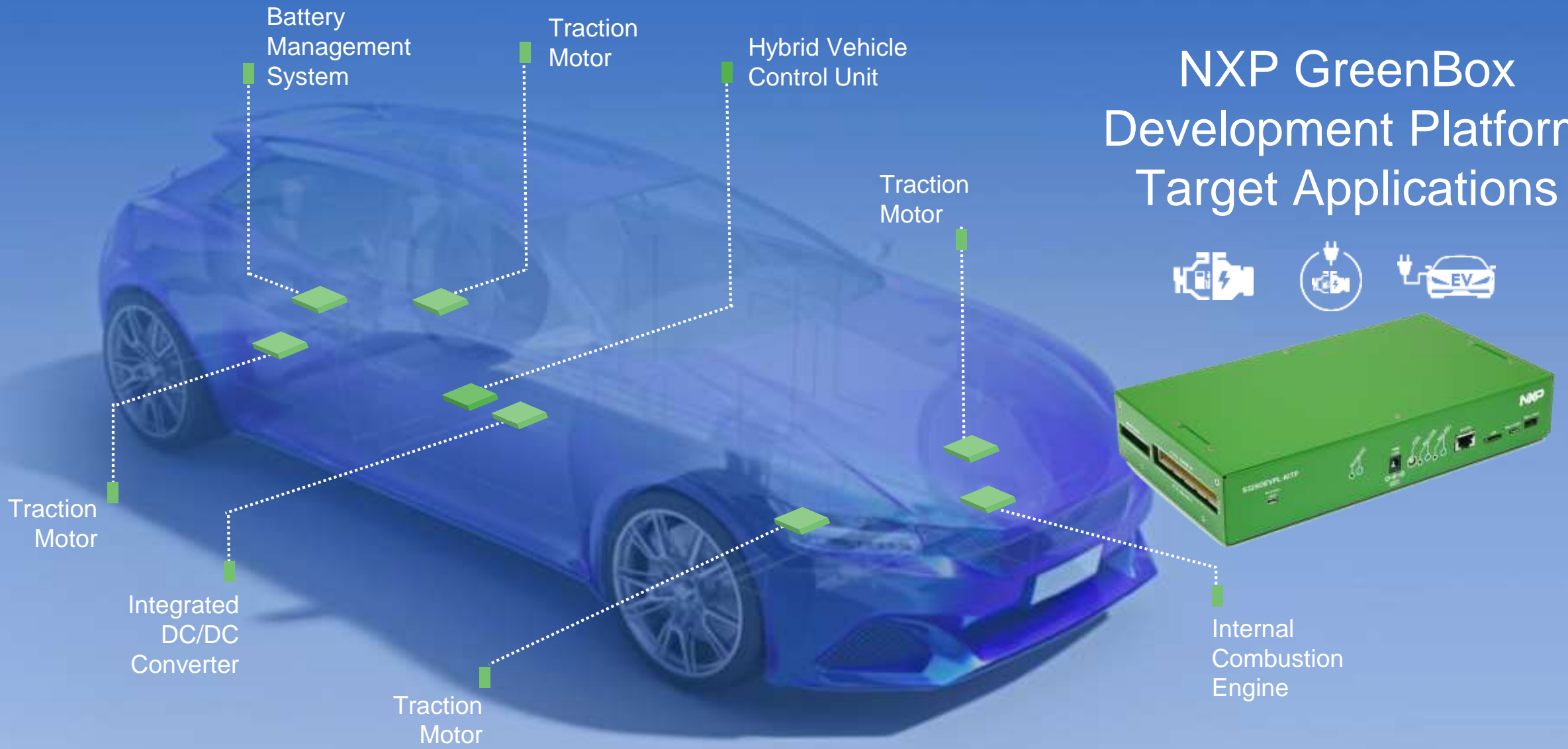


A53,R52,M7,M33

i.e. Accelerators, Complex Timers

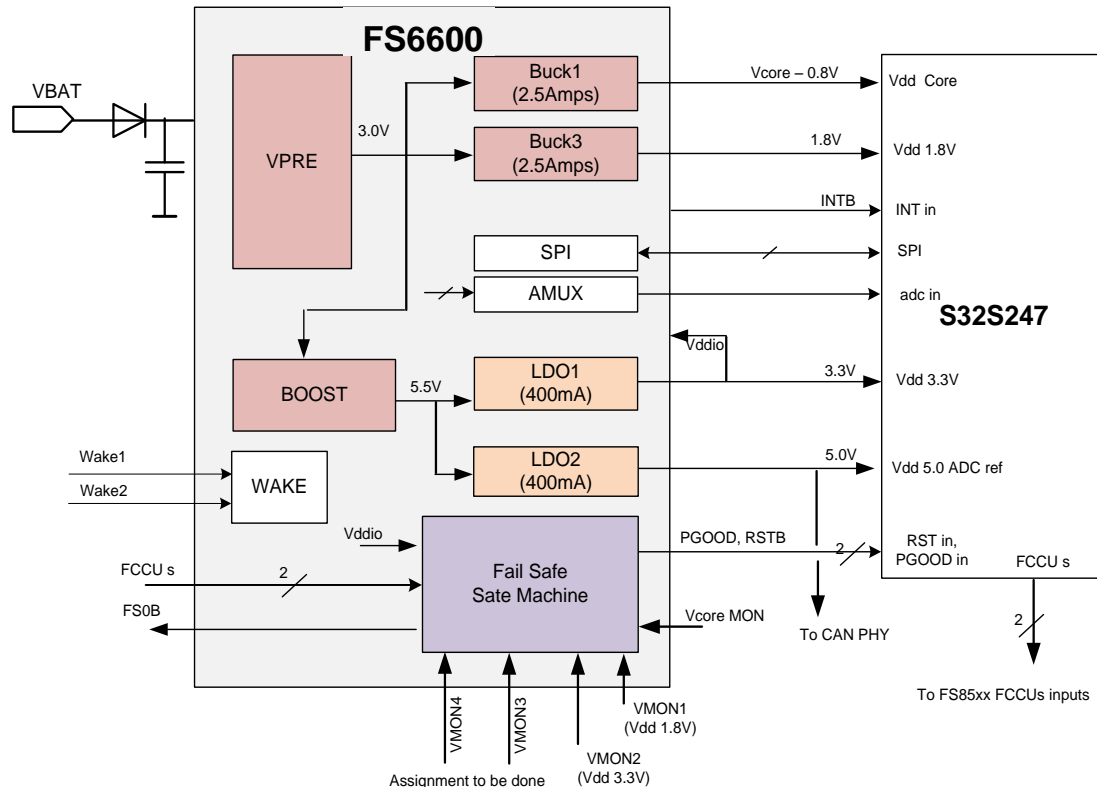


NXP GreenBox Development Platform Target Applications



S32S2 + FS6600 – Value Proposition

FS8530 Derivative for Drivetrain Market



- **NXP system solution** : integrated Safety Power Management solutions to support High Performance applications requiring S32Sx MCUs.
- **Simplify your ISO 26262 development** : designed to support up to ASIL-D level with combined architecture and documentation
- **Fault tolerant system** : Innovative Fail Silent and Fault Recovery Modes
- **High-Performance energy usage** : Synchronous DC-DC Converter Architecture with High Efficiency and Lower Power Dissipation.
- **BOM optimized** : Programmable Switching frequency up to 3MHz, for cost and space savings
- Configurable High Precision Monitoring
- **Accelerate your development** : Ready to use platform combining HW, SW and Documentation.
- **Platform available end 2018**

FS6600 – S32S2 Attach ASIL-D SBC

FS85 Derivative for Drive Train Domain Controller



Power Management

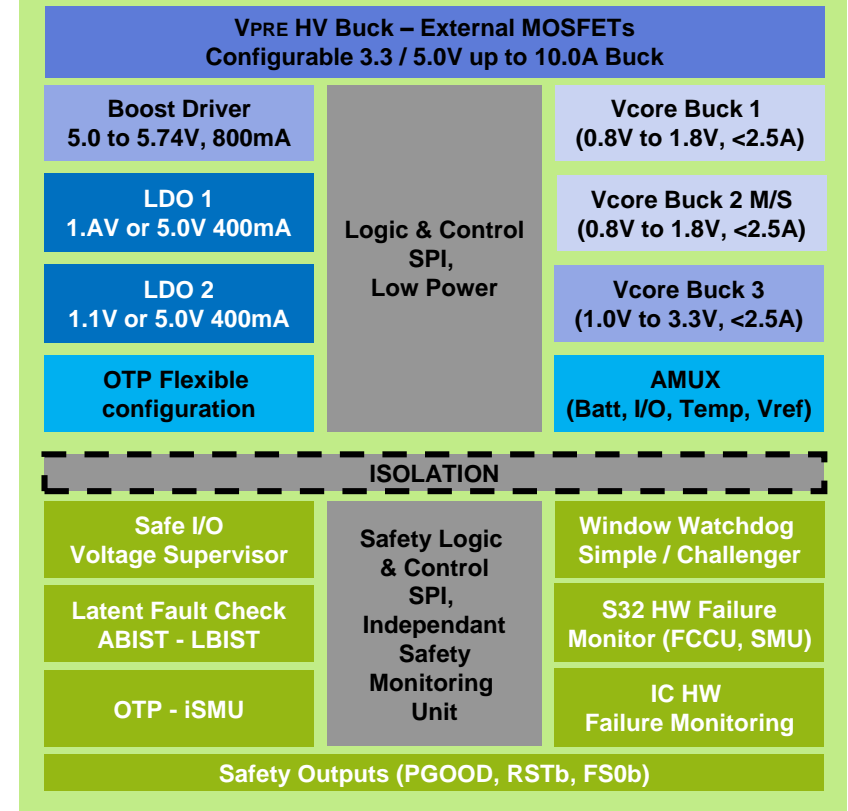
- Input supply up to 60V – 12V and 24V systems
- **HVBUCK** , adjustable 3.3V to 5V, scalable output current up to 10A
 - Synchronous Buck, 300kHz to 2.5MHz, ext. MOS
- **BUCK1+2**, multiphase, adjustable 0.8V to 1.8V, up to 5A DC max
 - Synchronous Buck, up to 3MHz, int. MOS
- **BUCK3**, adjustable 1.0V to 3.3V, up to 2.5A DC max
 - Synchronous Buck, up to 3MHz, int. MOS
- **BOOST** 5V to 5.74V, up to 800mA DC- 1.5A peak, int. MOS
- **LDO1/2**, configurable 1.1V to 5V, up to 400mA
- Synchronization signal for dual device operation / Power GOOD output

System Features

- Independent Safety Monitoring Unit
- Control via 32 bits SPI (including CRC).
- Low Power Mode : <10µA in LPOFF, wake up via dedicated pins
- AMUX: Battery, Internal Safety critical voltages, Precise Vref and Temperature
- Emulation and Programming capability offered in Engineering mode only : Voltage, frequency, phase shift, PW sequencing.
- EMC optimization : Spread Spectrum, Vpre Slew Rate control



FS6600 Functional Block Diagram



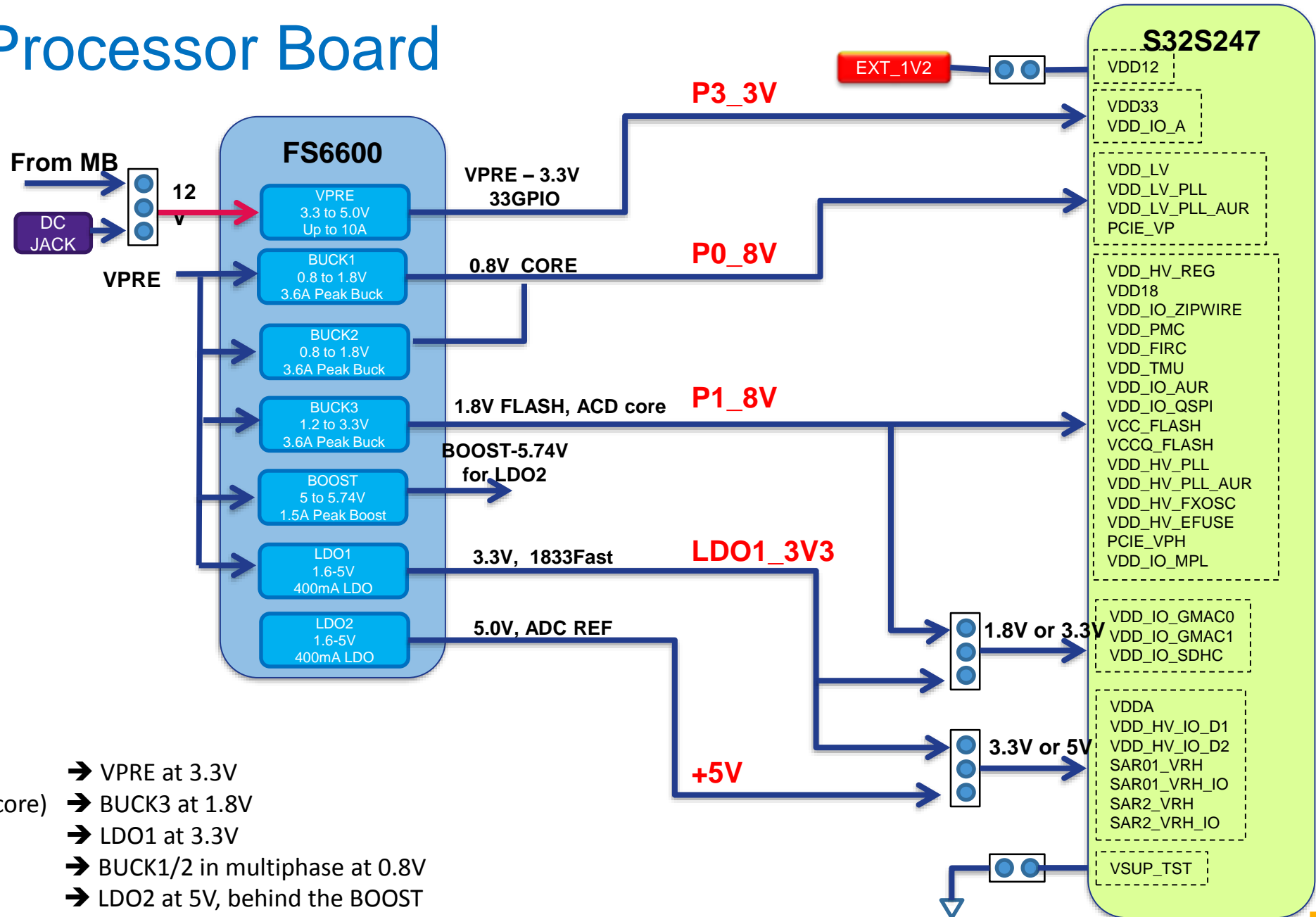
Reference silicon available now

FS66 Samples : Now

FS66 PPAP : Q1 2019

S32S247 Processor Board

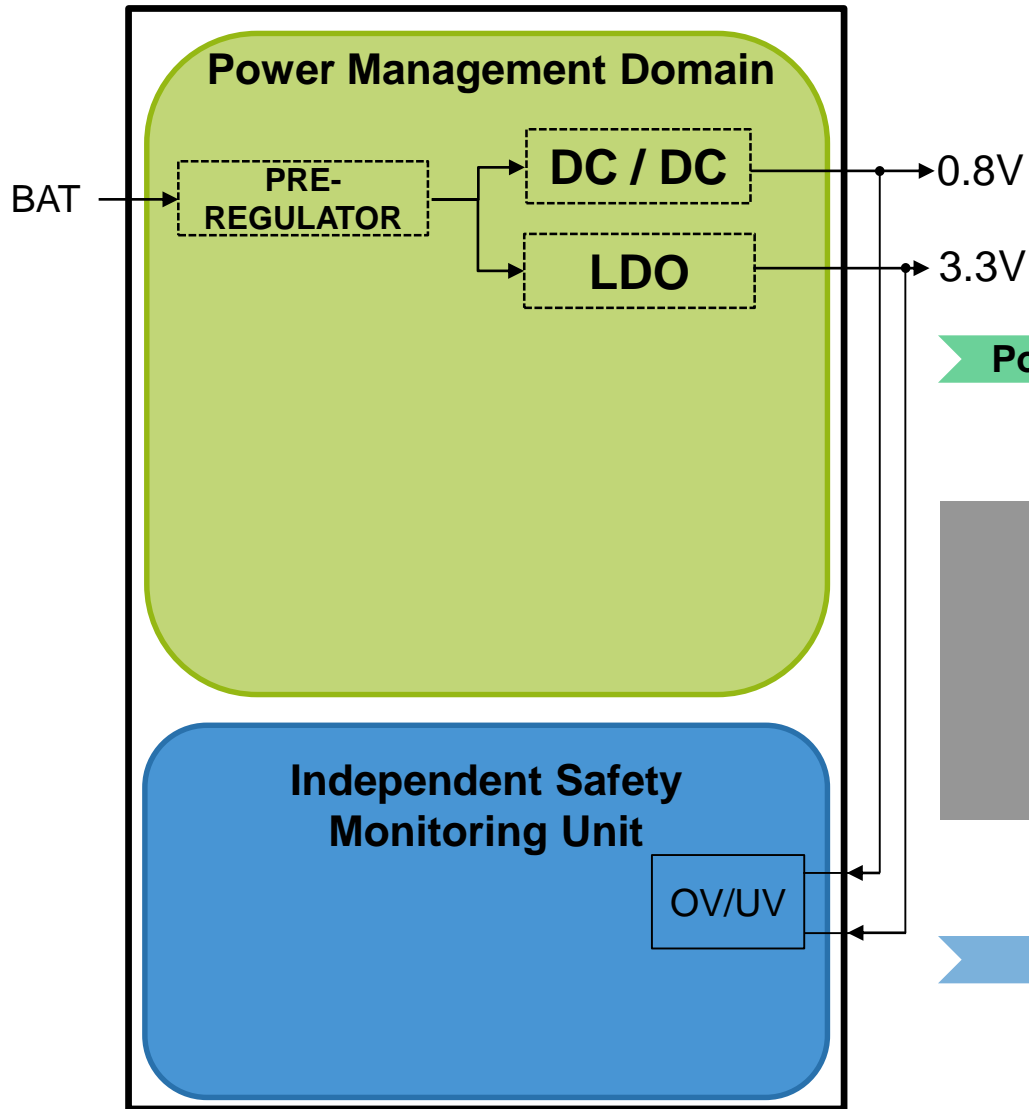
Power Tree



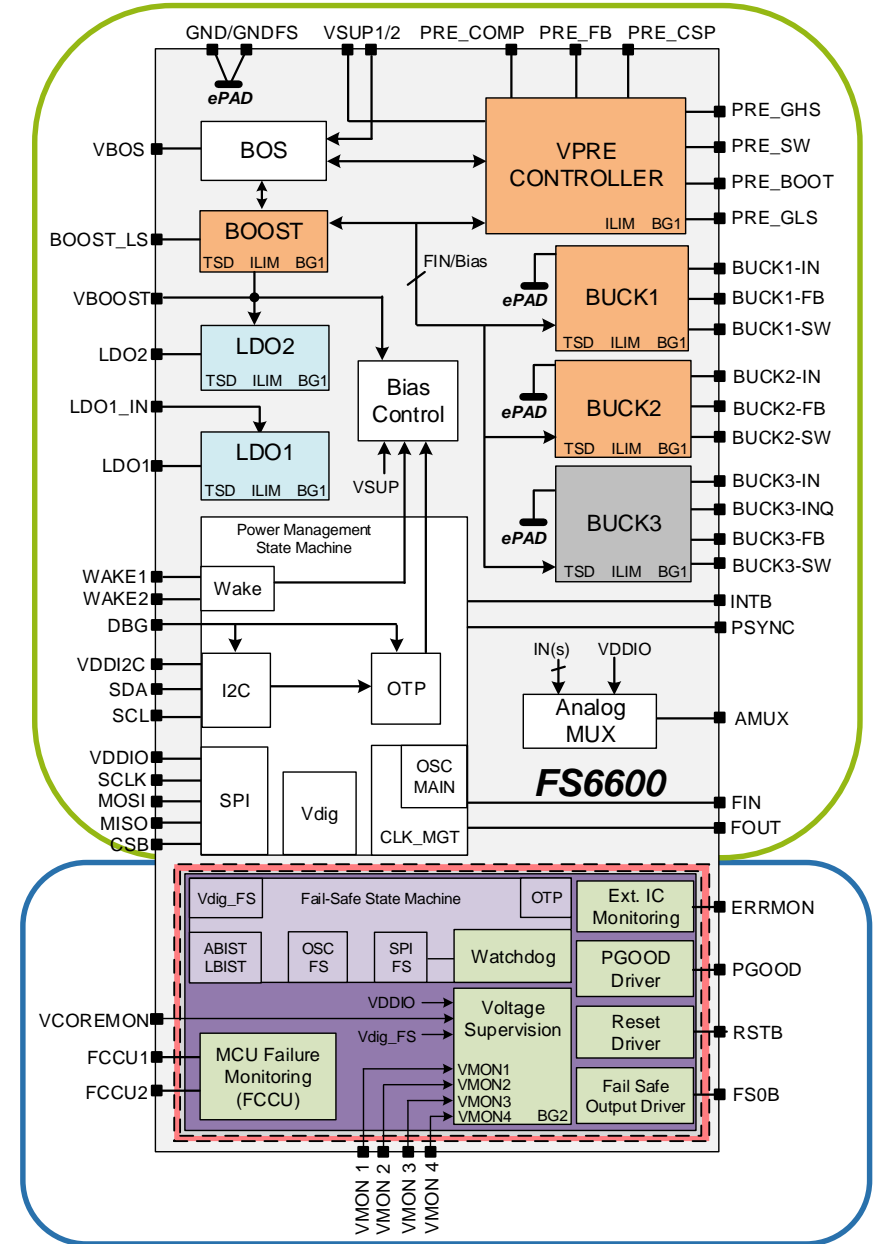
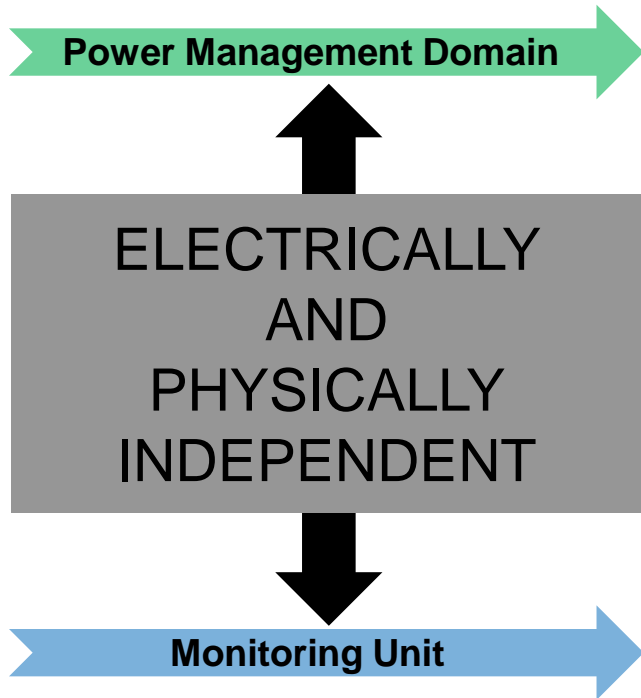
Power up sequence:

- 3.3V (3.3V IO) → VPRE at 3.3V
- 1.8V (Flash, ACD core) → BUCK3 at 1.8V
- 3.3V (1833 IO) → LDO1 at 3.3V
- 0.8V (16FFC core) → BUCK1/2 in multiphase at 0.8V
- 5V → LDO2 at 5V, behind the BOOST at 5.74V, to be quiet supply for ADC reference

Architecture Concept



Simplified Integrated Power Supply Architecture



FS66 Architecture Concept

All safety mechanism reaction are $< \text{FTTI} < 10\text{ms}$
 FTTI = Fault Tolerant Time Interval

Independent & configurable Fail Safe State Machine

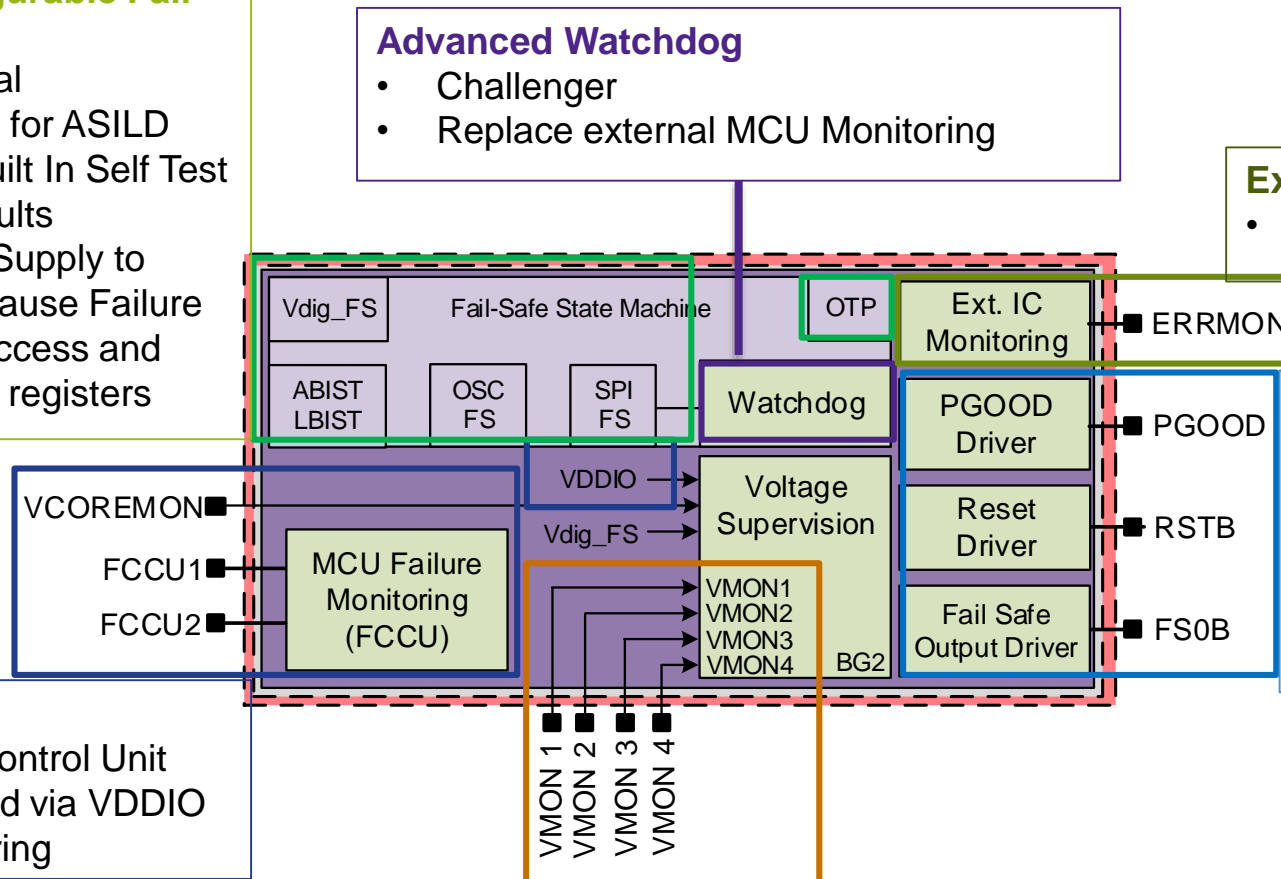
- Physical & Electrical independence to fit for ASILD
- Analog & Digital Built In Self Test to detect Latent Faults
- Own Reference & Supply to reduce Common Cause Failure
- SPI with CRC To access and configure Fail-Safe registers

Advanced Watchdog

- Challenger
- Replace external MCU Monitoring

External IC Monitoring

- Input pin to monitor external IC



Fail Safe Output

- 3 safety output with configurable reaction
- Safety output to transition the system in safe state (FS0b)

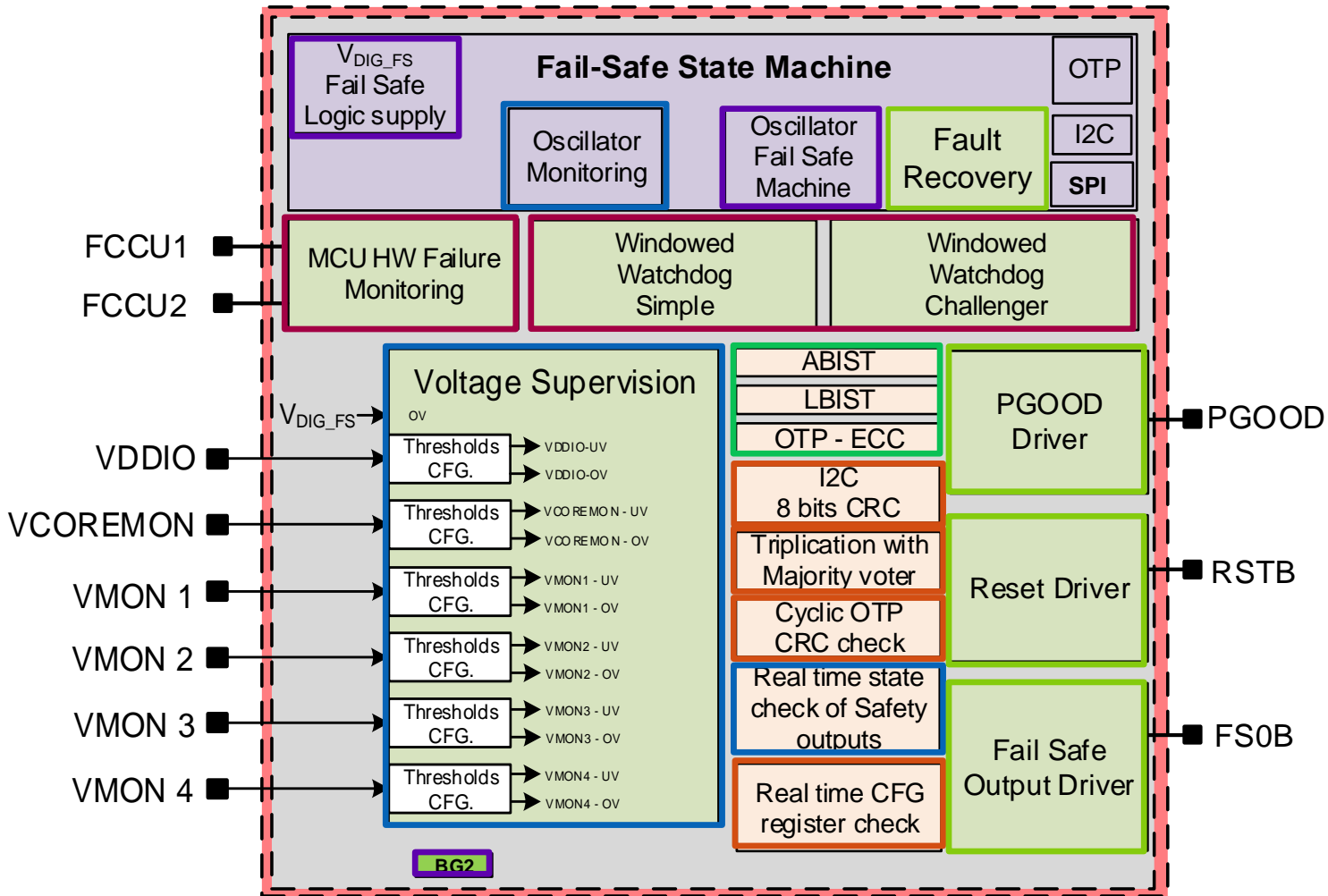
MCU Monitoring

- FCCU : Fault Collection Control Unit
- MCU I/O voltage monitored via VDDIO
- MCU core voltage monitoring

Voltage Monitoring

- Voltage supervisor monitoring of internal references and safety related regulators

Independent Safety Monitoring Unit



Summary



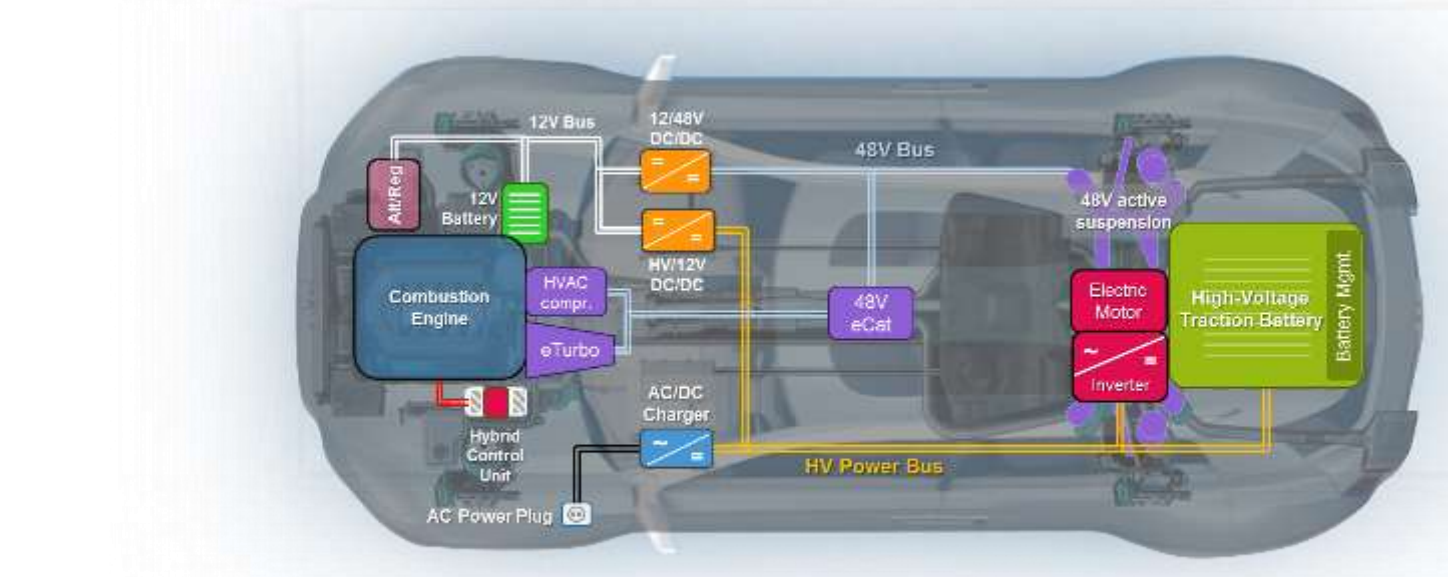
NXP Safety Backbone Solutions for Drivetrain Electrification

MCU	Attach	Reference
S32S24x	FS6600	Green Box
S32K1x	FS450x	Yes
MPC574x	FS650x	Yes
MPC577x	FS651x	Yes

48V eMachine
MPC574x + FS651x

VCU – Domain Control
S32S2x + FS66x

BMS - Battery Controller
12V S32K1 + FS45
HV MPC577x+FS65



AC/DC converter
MPC574x + FS650x

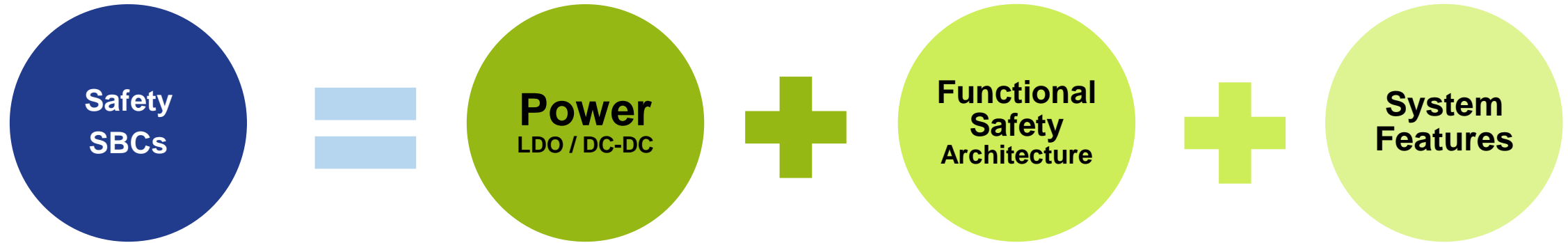
Motor control, inverter, HCU
MPC577x+FS65

DC/DC Converter
MPC574x + FS650x

Safety System Basis Chip



- FOCUS ASIL B/D SYSTEMS TO POWER SAFETY MCU
- SCALABLE AND SAFE PORTFOLIO FOR DRIVETRAIN ELECTRIFICATION AND ADAS MARKETS



SBC	Package	Voltage	Current	MCU Attach	Safety Features	System Features	SOP
FS650x FS45xx	LQFP48EP	DC/DC 6.5V DC/DC 0.9-5V or LDO 0.9-5V LDO 3.3/5V	2.0A 0.8/1.5/2.2A or 0.5A 100/300mA	MPC574x MPC577x S32K1 Other safety MCUs	ASIL D. Fail Silent. FS0 /FS1 safe delay.FCCU Watchdog challenger	Vcore DC/DC FS65 or LDO FS45. Grade 1 & 0. LDTimer. 30µA low power mode. Tracker. CAN/LIN/no PHY options	Released
FS85xx FS84xx FS6600	QFN56EP	DC/DC 3.3/5.0V DC/DC 0.8/1.8V DC/DC 1.0/3.3V LDO 1.1/5.0V	10A (ext.) 2.5/5.0A 2.5A 2x 400mA	S32R2 Radar S32V2 Vision S32S2 Safety Other safety MCUs	ASIL D: FS85, FS66. ASIL B: FS84. Fail Silent. FS0. W/D challenger. FCCU	12 & 24V systems. Frequency synch. Config Power Up/Down. Static Voltage Scaling. SPI/I ² C. External PMIC synchronization	Q2 2019





Summary

- Automotive Market moving to electrification after 2020
- NXP has a global portfolio of solutions to support Electrification market (MCU, FSBC, PHY, GD, BCC)
- FSBC has strong market presence in Electrification
 - Energy Conversion : DCDC 48/12, DCDC HV/12, BSG
 - Energy Storage : BMS12V, BMS48V, BMSHV
 - Energy Actuation : HV Inverter, 48V EM, TCU
- Main reasons of market acceptance are
 - Safety concept to help achieving ASIL D and Robustness
 - Portfolio Scalability and System Solution
- Next Generation MCU + FSBC provide
 - Computing, power and safety scalability offer
 - Safety innovations
 - Simplified and ready to use ecosystem

Other Sessions of Interest

WEDNESDAY

Session Code	Title	Presenter	CoPresenters	Duration	Room	Start Time
AMF-AUT-T3352	Automotive—Safety Power Management Solutions for Car Electrification and ADAS	David Lopez	Vincent Lagardelle	2	Galilee (Main Floor)	9:00 AM
AMF-AUT-T3402	Attach PMIC Offerings for NXP's Next-Generation Gateway Processors	Vincent Lagardelle	David Lopez	1	Galilee (Main Floor)	11:00 AM

Join our Community



Public community for NXP power management solutions, it addresses:

- Solutions to power i.MX, MPC, S32, LS and LX processors
- Support for Functional safety related items
- EMC considerations in power management



<https://community.nxp.com/community/Power-Management?tid=community>



SECURE CONNECTIONS
FOR A SMARTER WORLD

www.nxp.com