Functional safety (FuSa) concept for a traction inverter system

Guoliang Zhang
VEPCO Technologies, Inc.

VEPCO Introduction

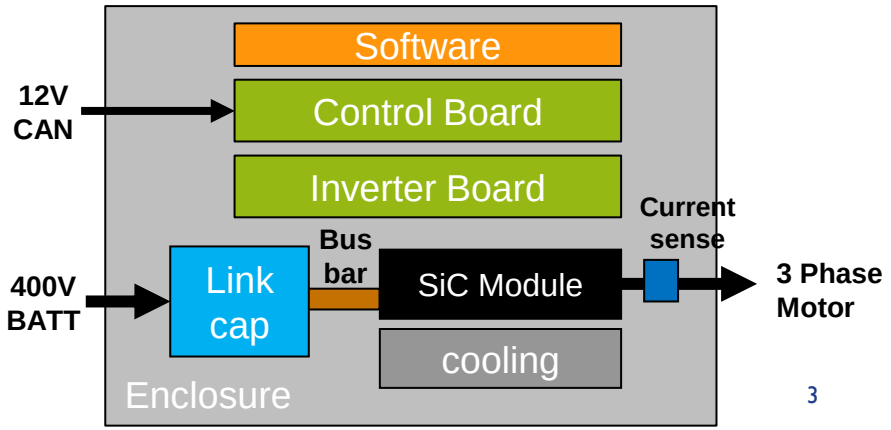
- NXP partner since 2018. Introduced functional safety inverters design with NXP in 2019
- Established in 2014, a southern California based R&D oriented engineering firm with field supports in Detroit, MI and China.
- 40+ years of combined experience in EV powertrain, charging infrastructure, battery management system.
- Focuses on vehicular electric power systems analysis, design, prototyping and testing to meet functional safety needs.

Partnership

- SiC/IGBT based Inverter Flatform for Motor Control

Partner	Responsibilities
VEPCO	• Traction Inverter design & HW/SW development • Verification & Validation testing • Prototyping and Manufacturing • System engineering & Integration
NXP	• Signal chain components and support • System enablement driver software • Basic safety case and software • SW development SDK • No 1 supplier of automotive power control
Wolfspeed A CREE COMPANY	• SiC Power Module • #1 supplier of SiC power devices
FE	• IGBT Power Module

Platform Electronics

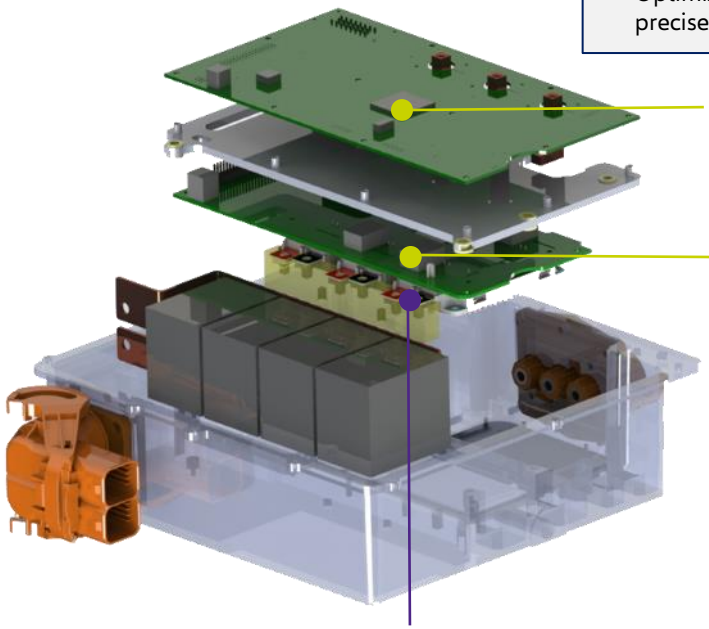


3

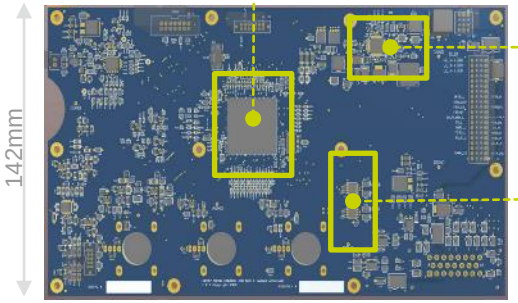
HPD form factor Inverter Overview

MPC5775E Motor Control MCU

- ±0.5° high accuracy software resolver
- ASIL-D functional safety support
- Optimized software libraries for precise motor drive control



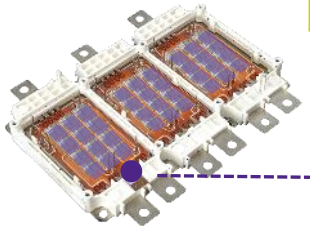
CONTROL BOARD



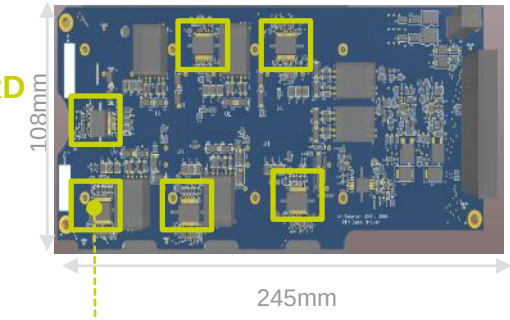
FS65xx System Basis Chip (SBC)

- Robust, reliable power management
- System safety monitoring and control for simplifying ASIL-D compliant design
- Scalable family for system optimization

POWER BOARD



CPM3-1200-0013A
[6pcs/switch, 36pcs/module]



GD3100 GATE DRIVER (x6)

GD31xx Isolated HV Gate Driver

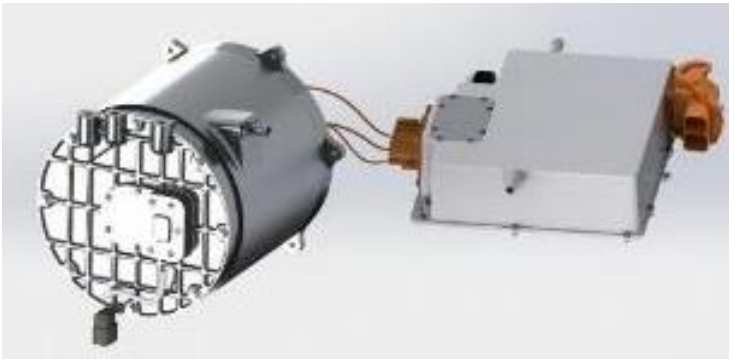
- Precise SIC/IGBT gate control
- < 2 µs short-circuit protection
- ±15A output drive current
- ASIL-D functional safety support

INDUSTRY STANDARD 6-in-1 STYLE MODULE
WOLFSPEED C3M SIC MOSFET: 1200V/600A 13mOhm

CONFIGURATIONS

3-in-1 Integrated eDrive
(Motor+Gearbox+Inverter)

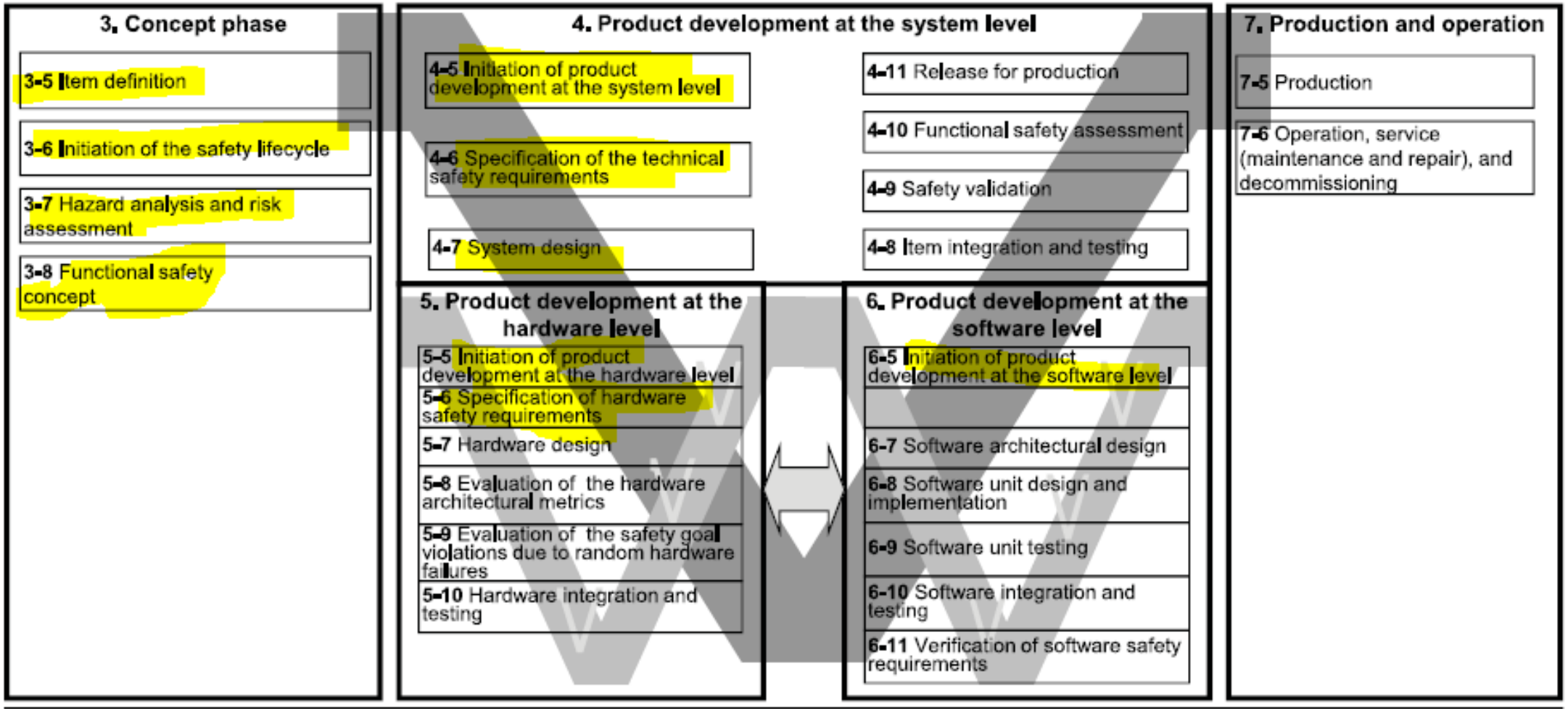
2-in-1 Integrated System
(Motor+Inverter)



Independent System
(Motor and/or Inverter)

Step by Step FuSa Concept for a Traction Inverter System

Coverage – what does the platform demonstrate



Terminologies

ASIL Allocation = Severity x (Exposure x Controllability)

Extent of harm to individual(s) that can occur in hazardous situation: Severity	Probability of exposure regarding operational situations: Exposure	Ability to avoid a specified harm through timely reactions: Controllability		
		C1 – SIMPLE	C2 – NORMAL	C3 – DIFFICULT
S1 - LIGHT	E1 (very low)	QM	QM	QM
	E2 (low)	QM	QM	QM
	E3 (medium)	QM	QM	A
	E4 (high)	QM	A	B
S2 – SEVERE	E1 (very low)	QM	QM	QM
	E2 (low)	QM	QM	A
	E3 (medium)	QM	A	B
	E4 (high)	A	B	C
S3 – FATAL	E1 (very low)	QM	QM	A
	E2 (low)	QM	A	B
	E3 (medium)	A	B	C
	E4 (high)	B	C	D

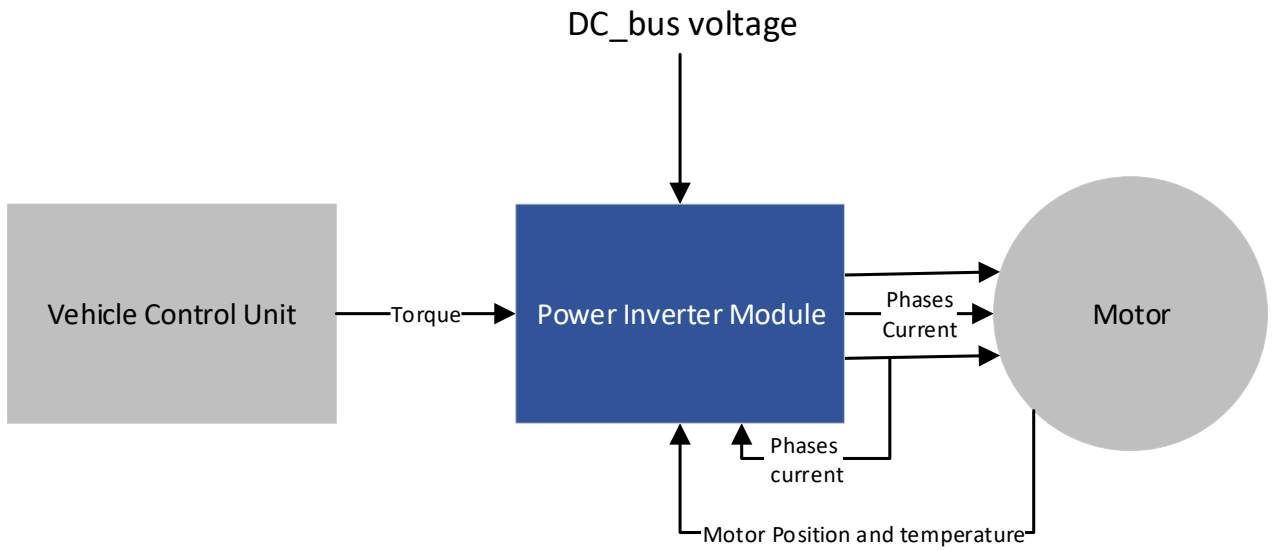
(QM: "quality managed" → no requirements from standard applied explicitly)

8

Step 1 Item definition

System description:

The power inverter controls energy conversion between an electric source (e.g. battery) and the mechanical shaft of the pmsm motor based on torque requested from Vehicle Control Unit (VCU).



Hazard analysis and risk assessment (HARA):

HAZ_01: Generate a torque without receiving request from VCU.

HAZ_02: Generate higher torque values as request from VCU.

HAZ_03: …

Safety Goal:

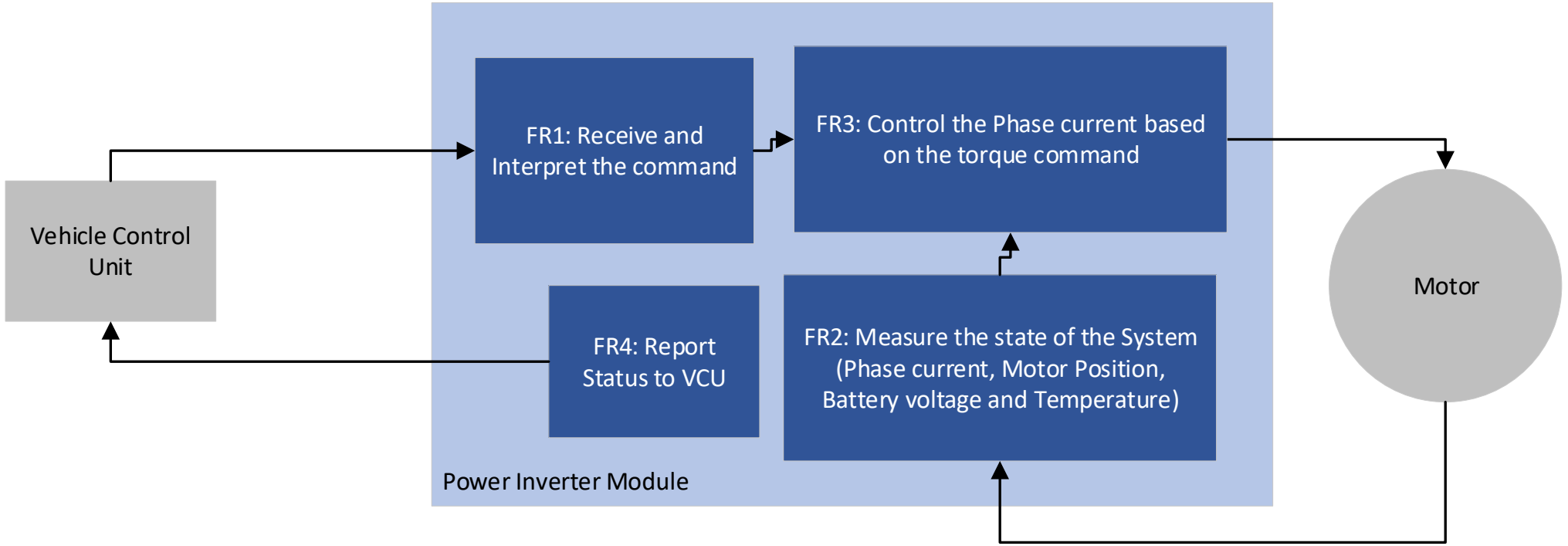
SG_01: Avoid generating torque that exceeds the commanded value from VCU (ASIL D) .

SG_02: Regnerative torque shall not cause the speed of the motor to the opposite commanded direction (ASIL D)

SG_03: … …

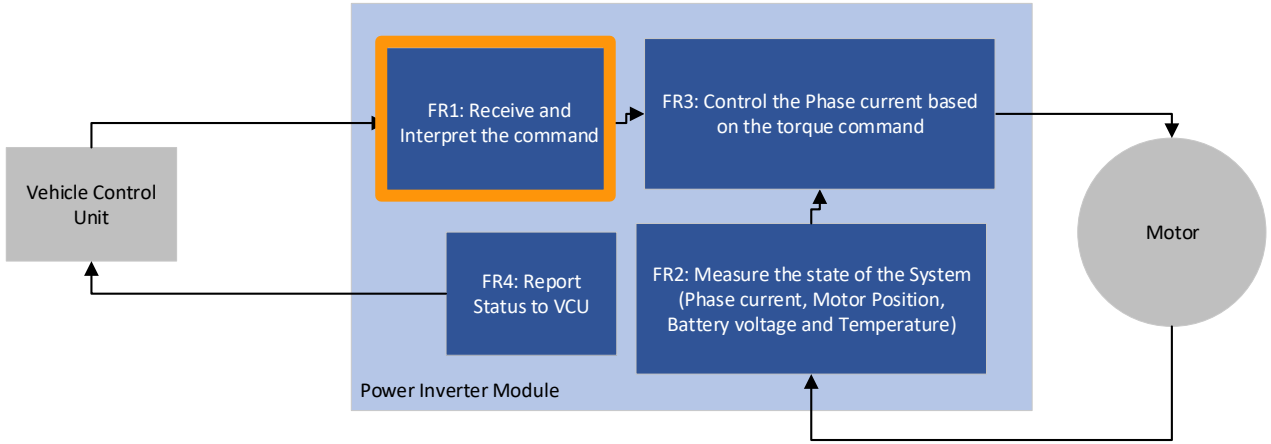
Step 2 Assumption and functional requirement

- Functional requirement: (What is the main function of our system?)



Step 3 Functional requirement to Functional Safety requirement

- Functional Safety requirement: (What are the system functions to guarantee we do not violate our Safety goals ?)



FR1: (Command) The Inverter shall receive and interpret the command from VCU.		System Safe State	FTTI	ASIL
FSR1.1	The Inverter shall not apply torque if no command have been received			D
FSR1.2	The Inverter shall not apply torque if the received command is incorrect			D
FSR1.3	The inverter shall deactivate torque based on a request from VCU			D
FSR1.4	The inverter shall limit the torque requested by VCU if the command is outside of plausible range.			D
FSR1.5	The inverter shall deactivate torque if the communication with VCU is interrupted			D

Step 4 Define System Safe state

$$Te=1.5(\lambda m.iq+(Ld-Lq)id.iq),$$

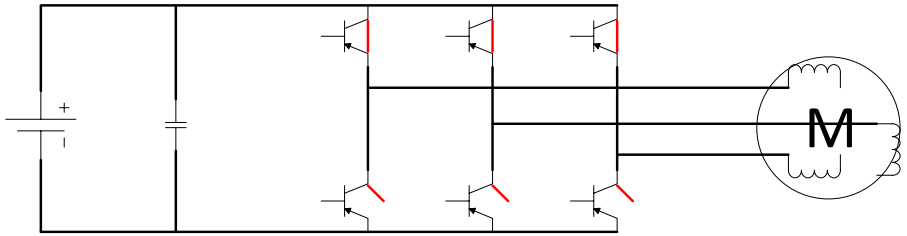
Safe State description for SG_01:

In the abnormal safe state, the electric motor shall achieve 0 torque output.

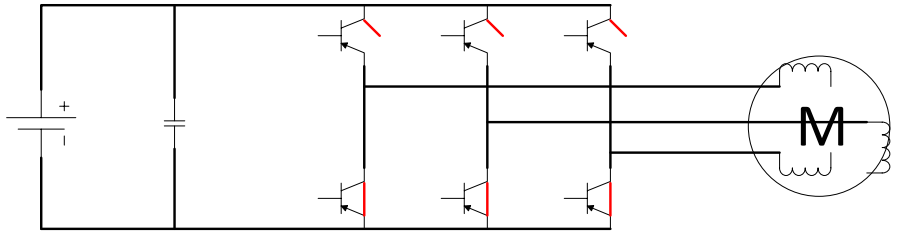
Option 1: The MCU can control Id and Iq to achieve 0 Torque => **Control Failsafe**

Option 2: We can control the state of the IGBT to achieve 0 Torque => **Logic Failsafe (with or without MCU)**

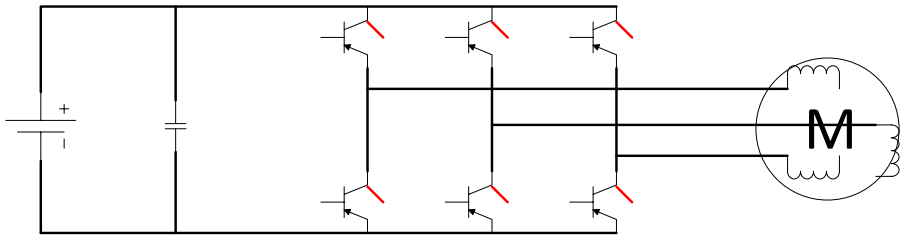
ID	Description
SS1	Normal Operation
SS2	Logic Failsafe
SS3	Control Failsafe (0 Torque control)
SS4	Send warning to VCU
SS5	Follow Safety Request from VCU



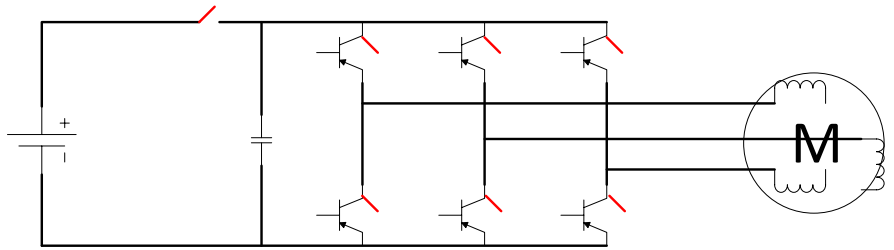
HS short Iq=0 Te=0



LS short Iq=0 Te=0



Te=0 only if BEMF <DC bus



Te=0 but needs action from VCU to open contactor

Step 5 Safety System Initiation

- High level HW block diagram
- Transient safe state : IGBT Fast protection with ASIL D gate driver
- Safe state logical connection
- MCU monitored by FS65
- Software architecture
- Sensing safety concept
  - Resolver
  - Current
- Monitoring and control of torque
- VCU command

Conclusion on Safety Concept Enablement platform

Safety concept
ASIL D gate driver to guarantee fast protection of IGBT
Safe state logical connection of FSBC, MCU and GD3100 safety IO to guarantee correct Safe state
MCU monitoring by FSBC to detect HW and SW fault
ASIL D Position sensing with independent eTPU resolver and eTPU diagnostic software
ASIL D Phase Current with 3 current senses
Software ASIL D decomposition to reduce software complexity (Execution and monitoring)
VCU command monitoring to guarantee integrity of communication

Safety Concept deliverables

Current status on safety