

DMC5 – Inverter safety unit (ISU) Handout

Version 1.0



1	INTRODUCTION	3
2	IMPORTANT SAFETY INSTRUCTIONS	3
3	INVERTER SAFETY UNIT (ISU).....	4
3.1	Architecture and overall concept in vehicles	4
3.2	What means ISU and why is it necessary?	4
3.3	Operation of the ISU	4
3.4	Characteristics and function of the ISU	5
3.5	Why is the ISU only optional?	5
4	BLOCK DIAGRAM.....	6
5	RESPONSIBILITIES FOR ENSURING THE SAFETY	7

Version	Datum	Name	Kommentar
1.0	01.12.2011	Holger Schmidt	neues Dokument

1 Introduction

The Inverter Safety Unit (ISU) is an optional integrable safety module of the inverter DMC5 and offers the possibility for intrinsically safe operation.

This document describes the concept and the functionality of the ISU and shows possibilities for custom development to reach the necessary safety requirements for the overall system.

2 Important safety instructions

- For all vehicles, which participates in public transport according to the country specific traffic regulations, is recommended urgently to develop the safety concept in attendance to the current ISO26262.
- BRUSA Elektronik AG only ensures the inverter-safety itself – not the safety for the overall system the inverter is integrated in.
- The ISU was developed according the ISO26262 as a SEooC (Safety Element Out Of Context). In this manner that assumptions were made about safety objectives of the overall system.
- The integrator* himself is responsible for the overall safety concept.
- As long as the safety system of the vehicle does not correspond to ASIL-C and no verification has been carried out by a certified institute, it is highly recommend to install an emergency button, to stop the car in emergency situations any time!
- During development phase it is recommend to access to the vehicle only for trained persons, which are instructed in the special dangers of electric vehicles.

* persons or companies, which integrates the inverter into a vehicle-system and placing it into circulation.

3 Inverter Safety Unit (ISU)

3.1 Architecture and overall concept in vehicles

By integrating an electric drive train into a vehicle there has to be done fundamental considerations regarding measures of the vehicle architecture, to monitor conditions and to reach a safe state by appropriate acting on components.

3.2 What means ISU and why is it necessary?

The ISU is considered as the primary safety device. By using an electric drive train there's usually no power-flow interruption, so the safety of the drive train has to be guaranteed in different ways. The torque generated by the motor has to be safe and controllable in any situations. The ISU controls the generated torque anytime and shuts down the inverter if an error occurs.

The control-side of the ISU must be designed by considering all possible faults and dangers. The ISU has to operate fail-safe anytime and brings the vehicle in a safe state if the ISU itself has a malfunction. The following failures can occur by the motor:

- Too much recuperation
- Unexpected vehicle movements
- Incorrect signed vehicle movements

3.3 Operation of the ISU

The ISU controls the phase current and phase voltage of the motor. With this data the ISU calculates the torque continuously (estimated torque), which will be compared with the desired torque. In case of a violation of certain configurable rules and limits the inverter assumes an error and shuts down immediately.

For shutting down the inverter and bring the vehicle in a safe state the following shutdown-paths are possible:

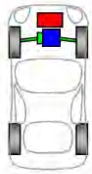

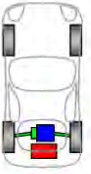
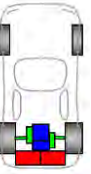

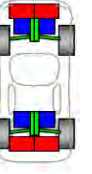
- Clamp 15
- Clamp 30
- Pin ExtAW1 + ExtAW2

The output-signals *ENA OUT1* und *ENA OUT2* can be used for shutdown any other components (e.g. connection to HV-supply). The block diagram in chapter 4 shows the ways of communication between the individual drive components and clarifies the statements.

3.4 Characteristics and function of the ISU

Different drive-train-concepts requiring different measures to reach the needed safety in the vehicle. Especially the use of two drives on one axis (without mechanical coupling) requires an enormous effort to ensure the safety. According to BRUSA Elektronik AG this constellation already requires ASIL-D, which must be guaranteed by the overall system.

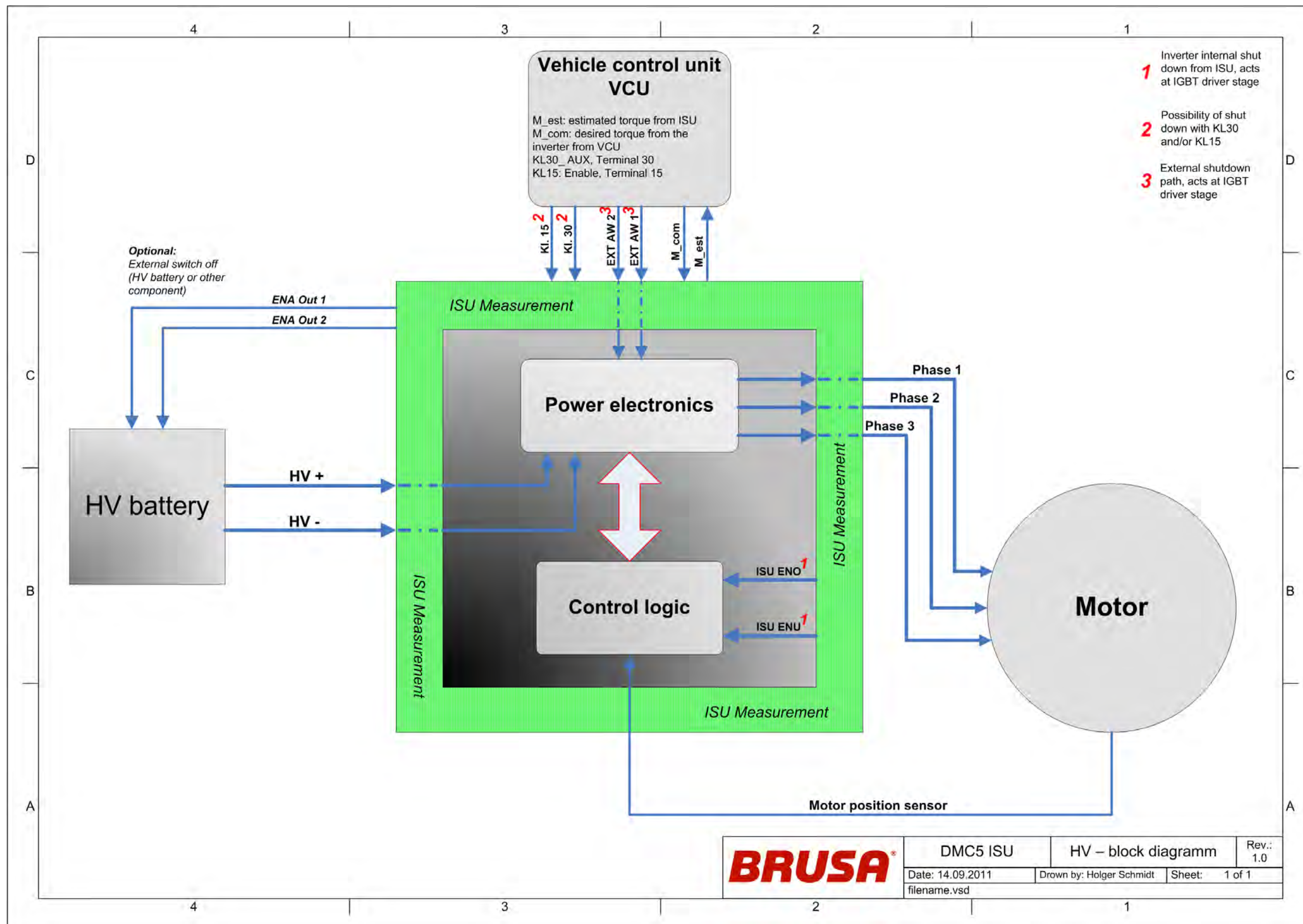
The following table shows an overview about possible drive concepts:

Front-wheel drive single and double		Rear-wheel drive single and double		Four-wheel drive single and double	
					

3.5 Why is the ISU only optional?

Basically, the hardware of the inverter is designed to facilitate the achievement of ASIL C. Due the different customer requirements and integration of different variants in vehicles it is not possible to develop a comprehensive ISU, which covers all these requirements. This was explained in previous chapters.

4 Block diagram

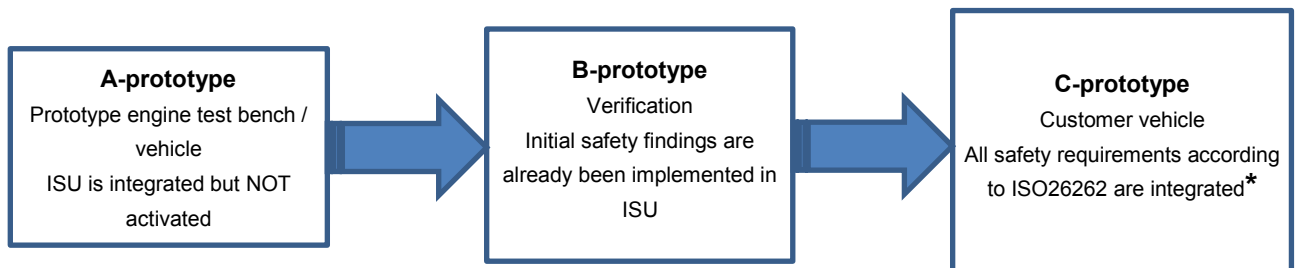


5 Responsibilities for ensuring the safety

Basically it is important to know, that the integrator is responsible for installation of components in any over-all-concepts. This applies installations in vehicles and also installations in test-stands. Details can be found in section 10 of the current ISO26262.

BRUSA Elektronik AG will be assistance for the Implementation of safety requirements and will work generally supportive. Thus, parallel to the development of the pattern stands the security measures could be gradually introduced.

The following illustration shows a possible way of development:



*** To reach the required automotive safety level (ASIL-C or ASIL-D), a customer-specific project must be started. For evaluation of the overall-system it is advisable to consult a certified body (e.g. TÜV).**