DNB1168

Safety Manual

Rev 0.6 —2022/10/26

Document information

Info	Content
Title	Safety Manual for the DNB1168
Author(s)	Eric van Iersel, May Zhao
Role(s)	Functional Safety Architect
Department	Datang NXP Semiconductors
Keywords	

Revision history

Revision	Date	Description	Author
0.1	12/01/2022	First draft version	Eric van Iersel
0.2	18/01/2022	Proposed version	Eric van Iersel
0.3	04/02/2022	Update after first review	Eric van Iersel
0.4	21/02/2022	Update PMHF budget from 0.3 to 0.5 FIT in Table 7	Eric van Iersel
0.5	29/03/2022	Update after SGS-TÜV review - Updated document references in Table 3 - Added rationale about ASIL and FTTI to section 4.1.5 - Renamed TSR_xx to TLSR_xx in Table 6, Table 7 and Table 11 - Changed ID of external SM in Table 12 to be in line with ID used in FMEDA - Corrected DC of SM42 and SM43 in line with ISO 26262-5, D2.1.1	Eric van Iersel
0.6	26/10/2022	Added 6.12 and SM117 in table 12	May Zhao

Reviewer(s)

Name	Role	Location	Date	Signature (if required)
Marijn van Dongen	IC-Architect	Nijmegen		
Miranda Zhang	Safety Manager	Shanghai		
Joop van Lammeren	System Architect	Nijmegen		
Rene Hermanides	Application Engineer	Nijmegen		
Mark Kan	Application Engineer	Shanghai		

Approver(s)

Name	Role	Location	Date	Signature (if required)

1 Introduction

1.1 Document Information

For a component developed as Safety Element out of Context (SEooC), the necessary information from the safety related work products generated during the development is to be provided to the system integrator.

The Safety Manual provides all necessary assumptions of use to the system integrator, i.e.:

- Details of the assumed functional safety capabilities (ASIL capability, safe states, FTTI, technical safety requirements.), assumed use case(s).
- Assumed requirements from the user or integrator of the component.
- Safety process.

1.2 Purpose

This functional safety manual describes how to use the DNB1168 in the context of a safety related system, specifying the user's responsibilities for integration and operation of the DNB1168 in their system in order to reach the targeted safety integrity level.

The Safety Manual is intended to support engineering teams using DNB1168 as a safety element in their targeted functional safety relevant system with the objective to achieve functional safety up to ASIL D. The Safety Manual provides a set of minimum requirements that need to be fulfilled by the integrator for safe operation of the DNB1168 in a target system.

Following the requirements and the validity of the assumptions used to generate the requirements set out in the safety manual shall be used as the basis to meet the functional safety requirements for the purpose of the operation of the safety element under the integrator targeted system (context of use).

1.3 Scope

1.3.1 Application scope

The DNB1168 is a single cell supervisor chip capable of measuring the voltage (VM), impedance (ZM) and temperature (DTS) of an individual battery cell or logical cell, i.e. a group of cells in parallel. It can also balance the cell.

Since the development of DNB1168 is done based on a safety element out of context methodology, no specific battery management application is considered while deriving the functional safety requirements. Generic safety requirements are considered. This means there is no restriction in using DNB1168 for a specific battery management application scenario. However, the customer needs to evaluate and validate the assumptions on use and restrictions in use considered in this document before using it in an application specific safety context.

1.3.2 Document scope

1.3.2.1 Included

Included as part of the Safety Manual:

1. Documentation of assumed requirements including assumptions of use (SEooC development).
2. Assumptions related to the design external to the SEooC including external measures (HW and SW measures to be implemented by the user).
3. Description of ISO 26262 lifecycle tailored for the component development.
4. List of supporting safety documentation

   a. Shared.
   b. Not shared but open for audit.
5. Description of the safety architecture with an abstract description of functionalities.
6. Description of the component configuration and related HW and/or SW procedures to:
   a. Detection of failures.
   b. Control of a failure after its detection.
   c. Calibration parameters (and related procedures) that can influence the safety.
7. Description of Assumptions of Use (AoU) of the component with respect to its intended usage, including:
   a. component safe state.
   b. Assumptions on FTTI.
   c. External measures and interfaces.
8. Details of safety mechanisms.
   a. Integrated in the device and their availability and usage.
   b. Off-chip assumed safety mechanisms.
9. Production related instructions affecting safety.
   a. What is expected from integrator for system/item level production. Any precaution required in storage, handling, specially based on environmental effect on safety.

1.3.2.2 Not included

Not included in this Safety Manual, but shared through other documentation:

1. The description of safety analysis results at component level useful for the system integrator, (covered by safety analysis report) and the safety analysis result.
2. Description of fault models.
3. FIT calculation approach (information regarding the calculation of the base failure rate, methods used etc.).
4. Failure modes and failure rates considered in the safety analysis, their distribution, and diagnostic coverage offered from specific safety mechanisms.
5. HW architectural metrics (single-point fault and latent-fault metrics).

1.4 Component description

This safety manual is related to the DNB1168 single cell supervisor IC.

1.5 Applicable Functional Safety standards

The DNB1168 is intended for the automotive application domain and developed according the ISO 26262, second edition (2018) functional safety standard.

2 Description of ISO 26262 lifecycle used for the component development

2.1 Brief safety lifecycle description

In ISO 26262:2018 Vehicle Safety Systems are described in terms of items, systems, elements, components, hardware parts and software units. The products developed by Datang NXP Semiconductors (DNS) can be considered as component in the context of ISO 26262 and are made up of sub-blocks considered as Hardware (HW) parts. The component can then be further sub-divided into sub-parts or further still, as is required by architect to analyze the component for the purposes of Functional Safety.

A Safety Element out of Context (SEooC) is a safety-related element which is not developed for a specific item. This means, it is not developed in the context of a particular vehicle. Therefore, the DNS product development is completely decoupled from the development of an item or system.

The DNS products are developed as Safety Element out of Context (SEooC), as described in ISO 26262-10.9 ‘Safety element out of context’ and more specifically detailed in ISO 26262-10.9.2.3 ‘Development of a hardware component as a Safety element out of context’.

For the product development projects with HW only development, all the information needed to build the Hardware-Software Interface (HSI) is given in the Safety Manual [8] and HW Reference Manual [9].

Figure 1: ISO 26262:2018 process flow tailoring highlights the applicable parts from ISO 26262 relative to the SEooC development flows.

The project independent tailoring is also summarized in the Safety Plan [11] of the product in development as well as in the Safety Manual. The mapping between ISO 26262 work products and DNS deliverables can be found in the Safety Case [12]. This document provides a complete list of applicable ISO 26262 work products and the associated DNS deliverables.

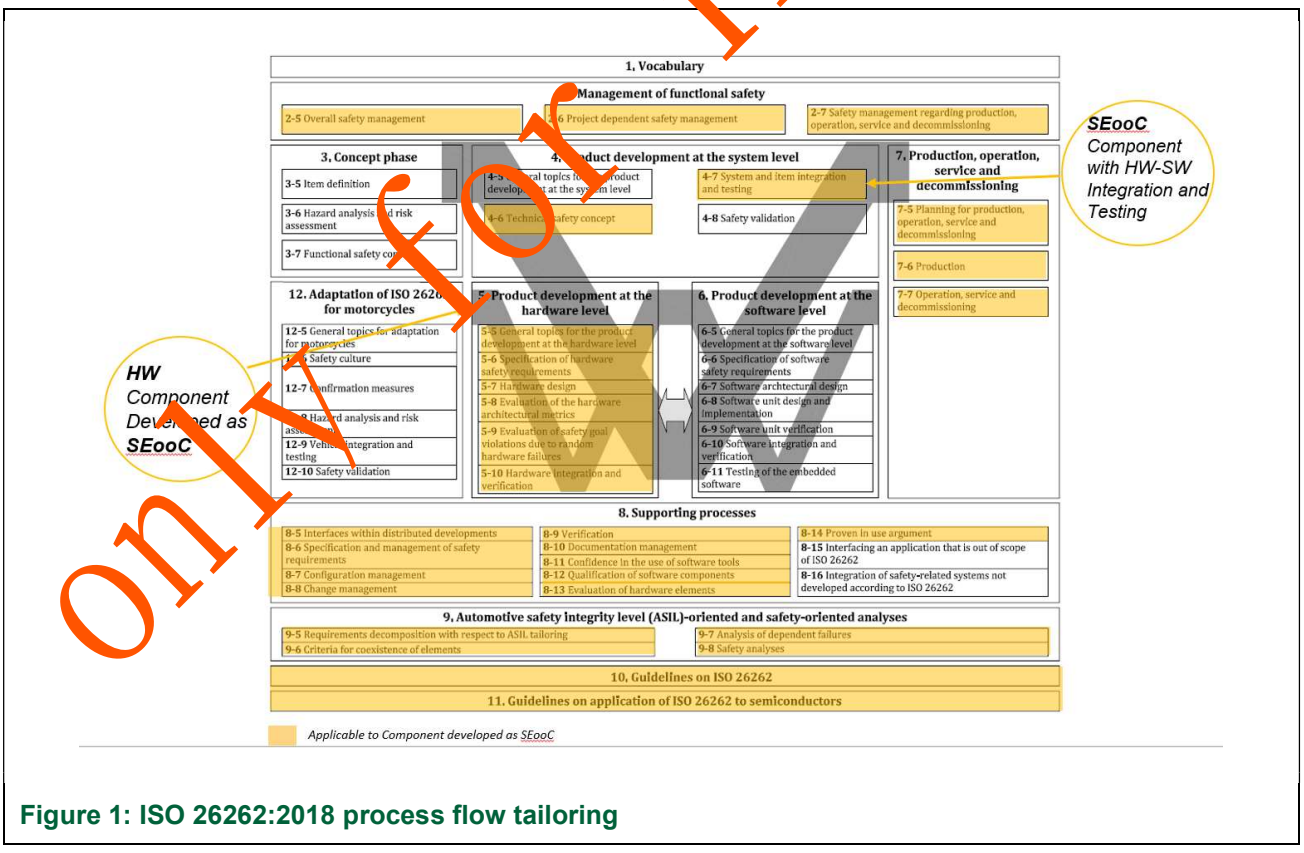

Figure 1: ISO 26262:2018 process flow tailoring

2.2 Tailored ISO 26262 life cycle applied at component level

Within DNS an approved product creation process with safety extension is defined with several gates and milestones, where in the objectives, input and deliverables are defined and checked. The product creation process is used as a guideline document for any project execution.

Within a development project, several gates/milestones are defined based on the governing product creation process, which divide the project up into manageable project phases. Within these project phases activities will be planned to generate several deliveries. Each of these deliveries will have their own maturity. It is related to the type of delivery, i.e. document, design, hardware, etc. based on the maturity model that is applied. The longer implementation phases are further sub-divided into different phases with defined milestones based on product maturity expectations. At the end of each planned phase, formal reviews and audits are conducted to make sure that the expected process compliance and product level maturity is in place.

The section below describes a basic overview of the project gates, objectives and key deliverables.

2.2.1 Development model

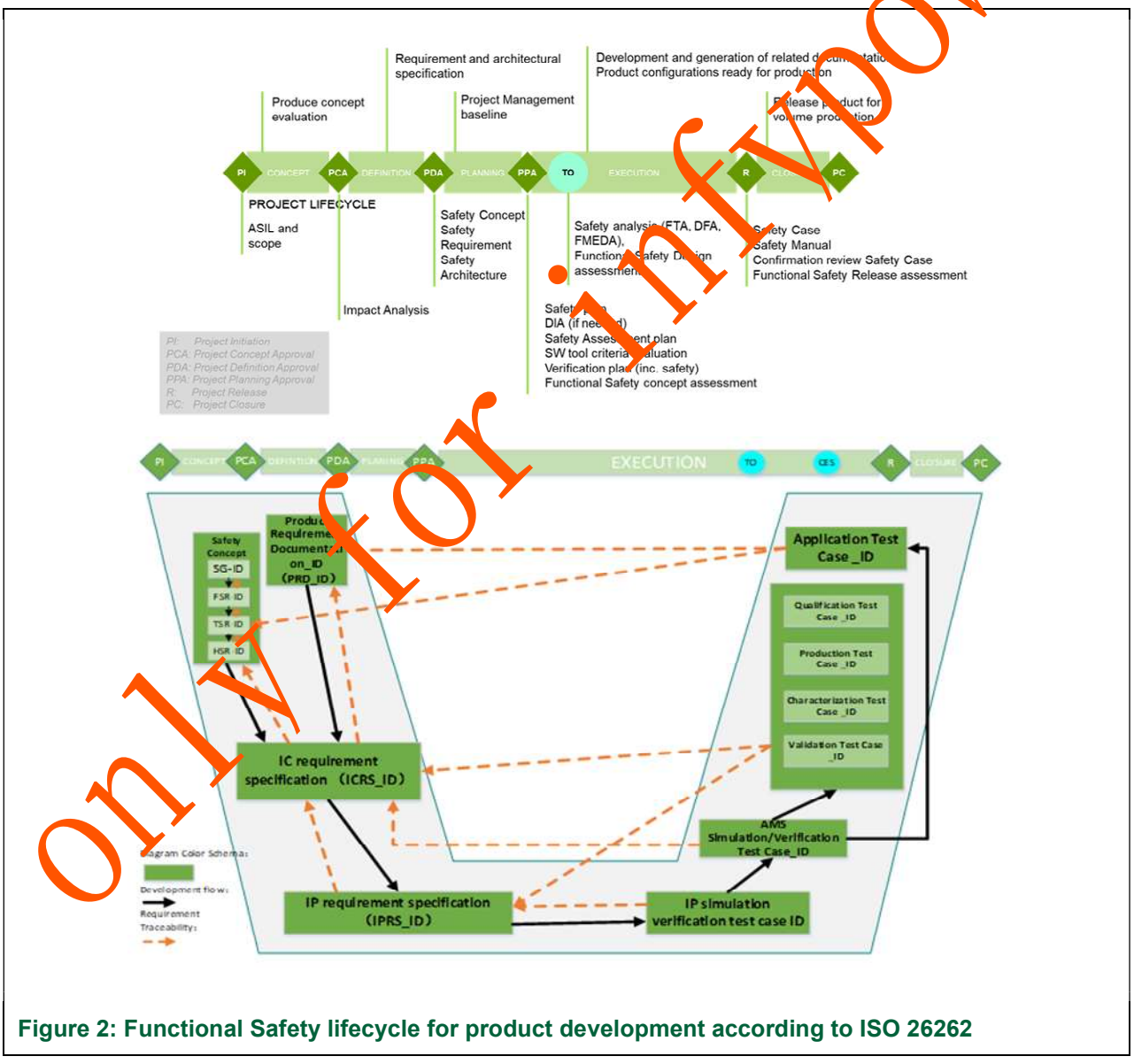

Figure 2: Functional Safety lifecycle for product development according to ISO 26262

2.2.2 Details of the tailoring per ISO 26262 parts

Table 1 : Tailoring applied during the HW component development

ISO26262 part	ISO26262 section	Topic of the part	Applicability	Justification or exceptions
1	All sections	Vocabulary	Applicable	-
2	All sections	Management of functional safety	Applicable	-
3	All sections	Concept phase	NOT applicable	-
4	All sections	Product development at system level	Partially Applicable	Applicable: • Technical Safety Concept (Ch. 6) • System and item integration and testing (Ch. 7)
5	All sections	Product development at Hardware level	Applicable	-
6	All sections	Product development at Software level	Not Applicable	-
7	All sections	Production and operation	Partially Applicable	No maintenance, no repairation and no decommissioning planned at IC level. The maintenance and repairation can be done only at system or vehicle level.
8	All sections	Supporting processes	Applicable	Interfaces with a distributed developments is not considered because the component development is a SEooC
9	All sections	ASIL-oriented and safety-oriented analysis	Partially Applicable	
10	All sections	Guideline on ISO 26262	Applicable	Informative part only.
11	All sections	Guidelines on application of ISO26262 to semiconductors	Applicable	Used as guideline.
12	All sections	Adaption of ISO26262 for motorcycles	Not Applicable	-

3 List of additional supporting documentations

3.1 Integration related documentations

A documentation set to assist safe integration of the component in the application context. Since not all such information is captured in a single safety manual, a list of additional documentations is provided that shall be considered by the integrator while integrating the component in their application context.

See Table 2 for a list of supporting documents that shall be used along with the safety manual to ensure functional safe use of the DNB1168 component.

Table 2 : List of additional supporting documents

Sr.no	Document description	Document objective	Document reference
1	Safety analysis results including results of safety verification	Hardware safety analysis summary report. Report of the effectiveness of the architecture of the component to cope with random hardware faults. Report of evaluation of safety goal violation due to random hardware failures; and results of analysis of dependent failures.	BBM1839_Safety_Analysis_Summary_r10_20211206.pdf
2	Base failure rate report	information regarding the calculation of the base failure rate, methods used etc.	BBM1839_Base_Failure_Rate_and_MTTF_Evaluation_v2.03_20211208.pdf

Sr.no	Document description	Document objective	Document reference
3	Confirmation measures report	The description of the functional safety assessment process. List of confirmation measures and description of the independency level. Summary of process for avoidance of systematic failures	S1N50001 report.pdf
4	Hardware-software interface specification	Required to support the IC safety mechanisms and to control failures after detection.	DNB11xx_software_development_manual_V1.1.pdf
5	DNB1168 Data sheet	Part of the data sheet is safety relevant, especially the specification limits and operational limits.	BBM1839_Datasheet_MRA3B_V1.06_0529.pdf
6	Silicon Note	A clear statement on the deficiencies of the component at release against the data sheet	Tbd, check with Rene

3.2 Reference documentations

Safety related documents generated during the development process that can be shared as reference documentation or audited to ensure process compliance.

Table 3 : Reference documents

Sr.no	Document name	Description	Document reference
1	Safety Analysis report	DNB1168 safety analysis summary report	BBM1839_Safety_Analysis_Summary_r13_20220301.pdf
2	FTA	Fault tree analysis of top level safety requirement	BBM1839_FTA_VM_v5_20211122.docx BBM1839_FTA_DTS_v4_20211122.docx BBM1839_FTA_ZM_v4_20211122.docx
3	DNB1168 DFMEA	Design FMEA for DNB1168 (including Pin FMEA)	BBM1839_DFMEA_V0.30_20220201.xlsx
4	FMEDA	Hardware metrics calculation	BBM1839_FMEDA_V0.28_20220329.xlsx
5	DFA	Dependent failure analysis	BBM1839_DFA_V1.2_20220104.xlsx
6	Fault Injection report	Fault injection report for DNB1168	BBM1839_Fault_injection_20220214.xlsx

4 Safety concept and safety architecture

4.1 DNB1168 overview

The DNB1168 is a single Li-ion cell supervisor IC capable of measuring the voltage (VM), impedance (ZM) and temperature (DTS) of an individual battery cell or logical cell, i.e. a group of cells in parallel. It can also balance the cell.

The DNB1168 was designed as a part of a single cell system architecture. It provides functionality for extensive monitoring of each individual (logical) battery cell in a battery management system.

Each logical battery cell (one or more battery cells in parallel) is connected to its own dedicated DNB1168 device. A pack controller ECU communicates with all DNB1168 devices via a daisy-chain string. For this reason, each DNB1168 can be placed very close to its battery cell. This topology has various advantages:

- The wiring can be significantly simplified. All connections between the cell and the DNB1168 are extremely short. Only the power connections between the cells and the communication wires are needed.
- Since the DNB1168 is so close to the cell, the temperature of the DNB1168 itself can be used as a cell temperature sensor without the need for an external device for temperature measurement.
- The impedance of each battery cell can be measured. By applying an excitation current at a chosen frequency, the battery voltage is modulated. By measuring the modulation, the complex impedance (real

and imaginary part) can be derived. The impedance is a direct measurement of the chemical properties of the cell.

- The customer has full flexibility on the number of battery cells in each power pack module.

The purpose of the pack controller is to use the BMS ICs to estimate battery parameters for each cell such as the State of Charge (SoC), State of Health (SoH) and State of Function (SoF). Each DNB1168 provides the following functions:

- Voltage measurement and Temperature measurement

  Basic functionality of a BMS device. These quantities are used to estimate the State of Charge (SoC).

- Impedance measurement

  Directly measure the chemical properties of the cell. Can be used for SoH estimation, but also to quickly detect internal temperature changes.

- Balancing

  After repeatedly charging and discharging the battery pack, some cells will be charged faster than others. This results in voltage differences between the cells. This is not desirable, because it will decrease the lifetime of the weak cells. For this reason, the pack controller will periodically apply balancing: it will discharge the strong cells until their voltage is equal to the voltage of the weakest cell in the pack.

- Communication

  Besides implementing the daisy-chain based communication protocol between DNB1168 devices, it is also possible to configure DNB1168 as an SPI interface. This mode is used to convert the SPI interface from the ECU into the dedicated DNB1168 communication interface. Note that communication is possible in two directions.

DNB1168 is considered as a 'sensor' device only: all the intelligence is in the pack controller. DNB1168 only responds to commands from the pack controller; it will not start any action by itself.

4.1.1 Functional block diagram

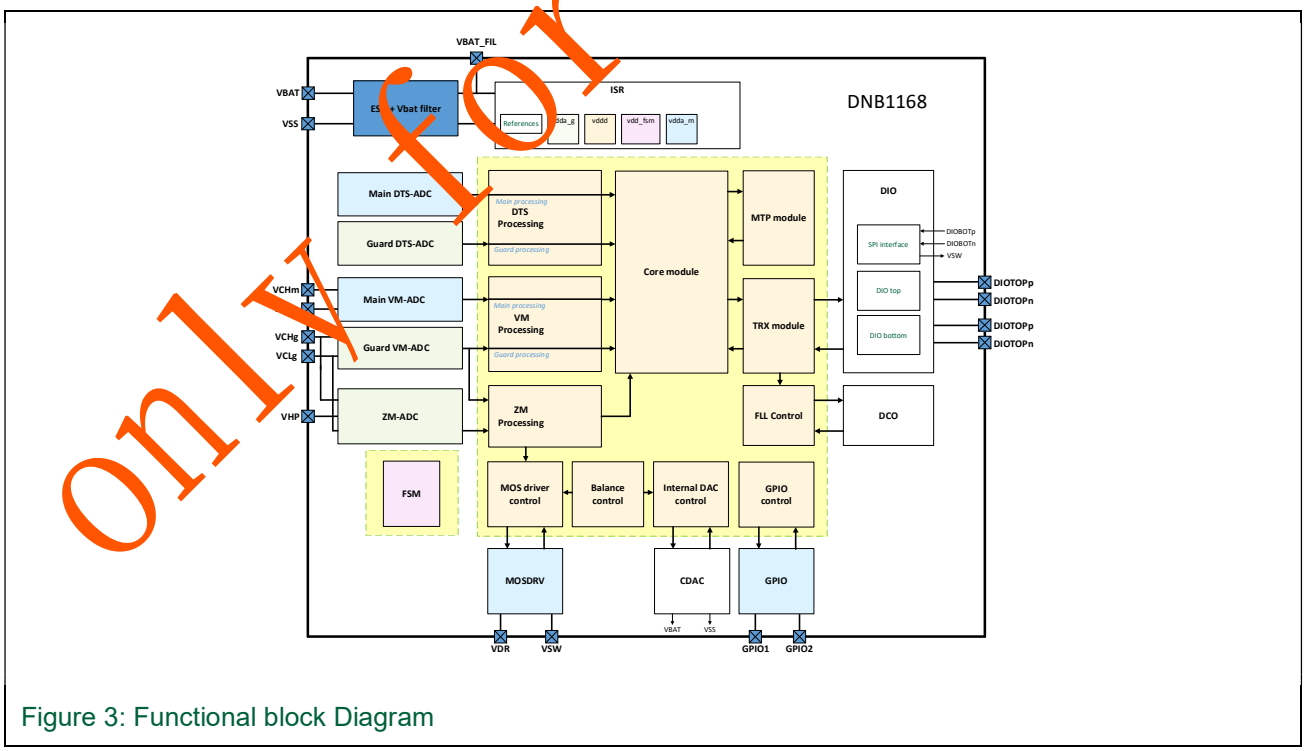

Figure 3: Functional block Diagram

4.1.2 Communication interface

The DNB1168 cell measurement information is communicated to the battery pack controller through a two-wire differential daisy chain, as shown in Figure 5. Each DNB1168 has a communication interface on both ends: top (DIOTOP) and bottom (DIOBOT/SPI).

The DNB1168 can be configured by the user in two different modes of operation:

- Measurement Mode (Figure 6) is active when the DNB1168 is powered up with the SPI_en pin connected to the ground. In this mode, the DNB1168 can be used to perform balancing and all the measurements (ZM, VM, DTS). It will utilize the differential DIO interface on both top and bottom ends in the chain.
- SPI Mode (Figure 4) is active when the DNB1168 is powered up with the SPI_en pin connected to the power supply. In this mode, the DNB1168 is used as an SPI to DIO converter. The SPI interface is active on the bottom end (DIOBOT) and the DIO interface is active on the top end (DIOTOP). The user still can measure the die temperature (DTS), however balancing and the voltage (VM) and the impedance (ZM) measurements are not available.

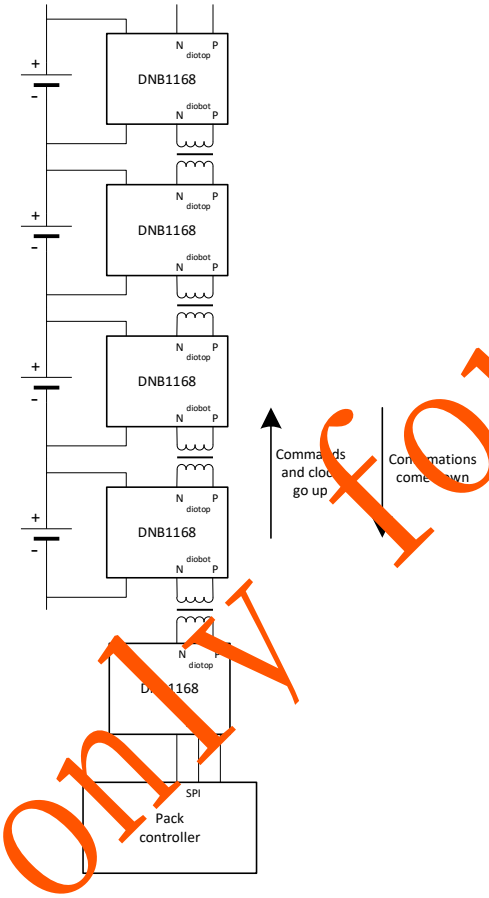

Figure 5: Daisy chain connection

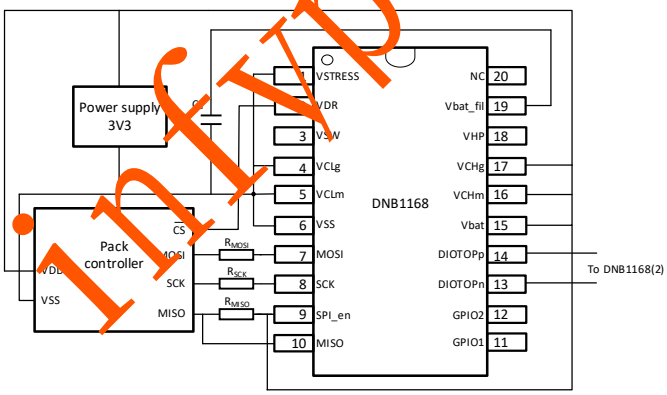

Figure 4: DNB1168 in SPI mode (SPI gateway)

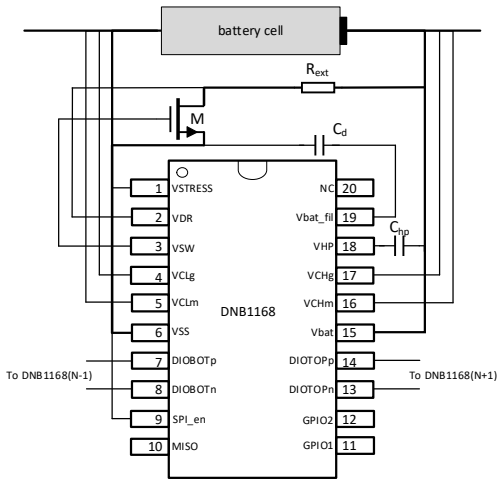

Figure 6: DNB1168 in measurement mode

4.1.3 Operating modes

DNB1168 has the following operating modes:

- Sleep Mode:

  All measurement and communication circuits are off, as well as the oscillator and all digital circuitry, except the Bus Activity Detector (BADET) and the Finite State Machine (FSM). The DNB1168 has no address and only checks for activity on the IOs. After initial power-up, the DNB1168 is in Sleep Mode and moves to Normal Mode upon reception of any valid command.

- Standby Mode:

  All measurement, communication circuits and the oscillator are off. All registers have their latest programmed values. The DNB1168 has an address and only checks for activity on the IOs.

- Normal Mode:

  All measurement and communication circuits are active. Impedance measurement and balancing can only be done in this mode. Guard measurement circuits are also active. Full diagnostics are available (e.g. comparison of redundant measurement samples).

- Self-test Mode:

  The Self-test Mode is used to check the safety mechanisms. These cannot be checked without interrupting the normal operation. When entering this mode, several error conditions are simulated by forcing certain conditions at the input of safety related comparators (for example fault forced on the input of the overvoltage comparator).

- Safe Mode:

  All measurement and communication circuits are active. Cell balancing is not available. Impedance measurement (ZM) is possible, however without the excitation current. The pack controller cannot change the mode to Safe Mode manually. This mode is triggered by a number of Service Request flags. For more information refer to Service request flags section 4.3.2.1.

- Sleep-Normal Mode:

  This is an intermediate state when the DNB1168 is waiting to go from Sleep to Normal Mode. It is triggered by activity on the communications lines while the DNB1168 is in Sleep Mode. The DNB1168 will move into Normal Mode only if a valid command is received. If not, then after 1.05 seconds it will return to Sleep Mode.

- Standby-Normal Mode:

  This is an intermediate state when the DNB1168 is waiting to go from Standby to Normal Mode. It is triggered by activity on the communications lines while the DNB1168 is in Standby Mode. The DNB1168 will move into Normal Mode only if a valid command is received. If not, then after 1.05 seconds it will return to Standby Mode.

4.1.4 Targeted applications

The DNB1168 features and safety requirements are derived from the needs of an automotive Battery Management System (BMS).

The BMS monitors and controls the battery pack. By measuring parameters such as battery voltage, temperature and current, the BMS is able to estimate some key battery metrics such as State of Charge, State of Health and State of Function. This Info is used to control the charging and discharging of the battery in a responsible fashion.

Some of the elements in a BMS based around single-cell monitoring include the single-cell supervisors (DNB1168), the pack controller ECU and the charge and discharge control circuitry.

Based on the information provided by the single-cell supervisors (DNB1168) as well as inputs from other parts of the car, the battery system will estimate the battery status parameters such as state of charge, state of health and state of function.

Figure 7 details one possible implementation of the BMS system, which will be used conceptually throughout this manual.

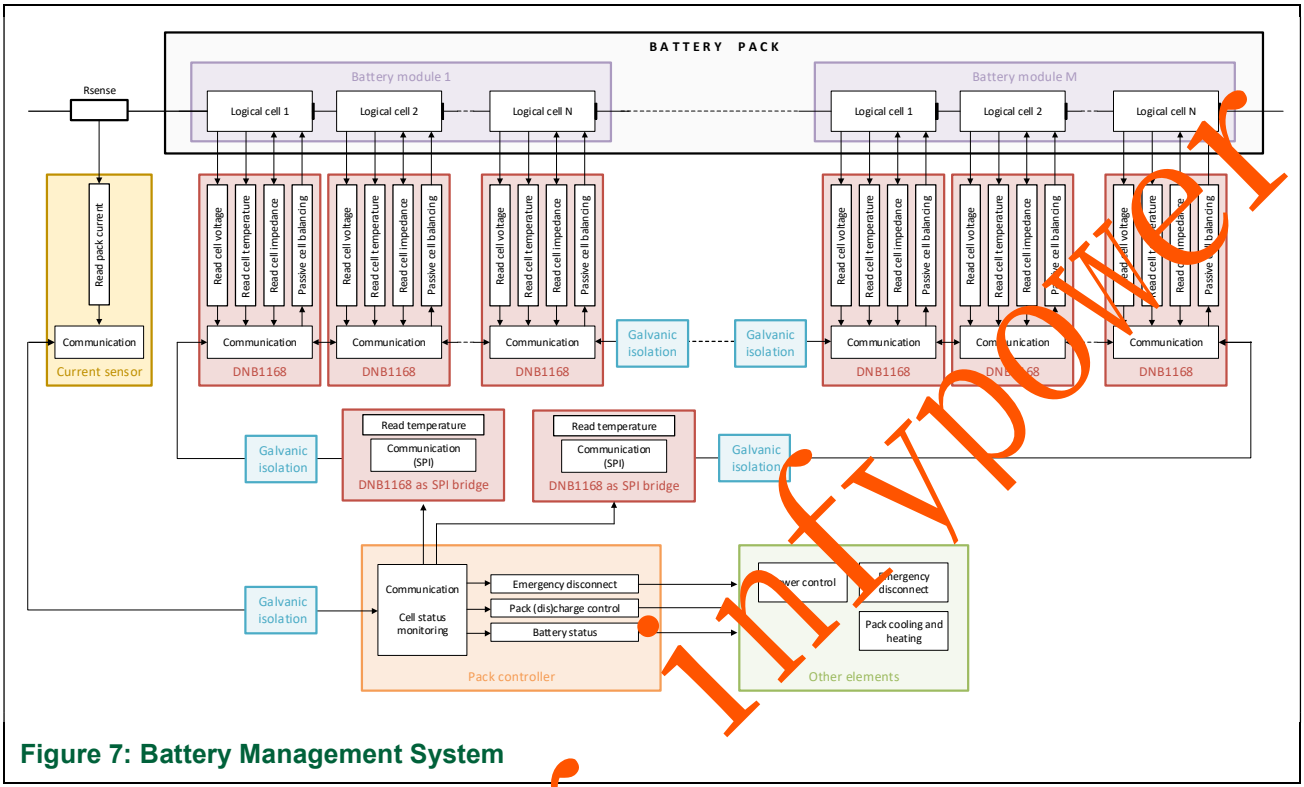

Figure 7: Battery Management System

4.1.5 Safety goals

The DNB1168 is targeted for Battery Management System application. Assumed hazard to be mitigated is thermal runaway of battery cells, caused by unintentional over-charging or over-discharging.

The assumed malfunctions as described below are potentially hazardous events of concern.

System malfunctions:

- Unintentional over-charging of battery cells with ASIL-D
- Unintentional over-discharging of battery cells with ASIL-D
- Undetected prewarning of thermal runaway in battery cells with ASIL-B
- Unintentional discharging of battery cell with ASIL-A

The assumed item Safety Goals and their ASIL are given in Table 4:

Table 4 : Assumed item Safety Goals

ID	Item Safety Goal	ASIL	Item Safe State	FTTI
SG_1	Prevent unintentional over-charging of battery cells	D	Stop battery charging / discharging and notify external system	400ms
SG_2	Prevent unintentional over-discharging of battery cells	D	Stop battery charging / discharging and notify external system	400ms
SG_3	Detect thermal runaway in the battery cell	B	Stop battery charging / discharging and notify external system	30s
SG_4	Prevent unintentional discharging of battery cell	A	Stop battery charging / discharging and notify external system	10min

The ASIL and FTTI values shown in Table 4 are assumptions based on industry requests and feedback.

The assumed ASIL-B for SG_3 in Table 4 is based on industry feedback. The detection of thermal runaway is an additional feature. The main goal is to prevent thermal runaway by prevention of over-charging and over-discharging of the battery cells with ASIL-D.

4.1.6 Architecture overview

The DNB1168 integrates redundant acquisition channels for cell voltage and temperature measurements. This includes redundant ADCs, signal processing, supplies/references and pinning.

Since the DNB1168 is thermically connected to the battery cells it is monitoring, the integrated redundant die temperature sensors are used for cell temperature measurements.

The DNB1168 measures the cell impedance based on a patented circuit technology using an external MOSFET for cell excitation.

Many monitors are included: supply monitoring, pin monitoring, timeouts, CRC etc.

4.1.7 Features overview

4.1.7.1 Functional feature overview

- Single battery cell management IC
- 2 independent cell voltage measurement channels
- 2 independent cell temperature measurement channels
- Low-ohmic cell electrochemical impedance spectroscopy (EIS)
- Cell balancing function (On-chip and external)
- Differential daisy chain communication
- Configurable as SPI transceiver
- Integrated Overvoltage and Undervoltage detection of battery cell
- Integrated Overtemperature and Undertemperature detection of battery cell
- Qualified for automotive applications according to AEC-Q100 grade 1

4.1.7.2 Safety feature overview

- Blackout / brownout detection on supply voltage
- Internal supplies voltage monitoring
- Internal redundant cell voltage and temperature comparison
- ADC Clipping detection
- Current monitor for internal DAC
- External MOSFET and resistor (VDR) monitoring
- Balancing and impedance measurement timeout watchdog
- Balancing Activity Reached Voltage Threshold
- Impedance measurement phase control clipping detection
- Oscillator control clipping detection
- Command CRC check
- Mismatch detection from sending SET commands twice
- ID check in each data frame
- Rolling sample counter for unique data detection for voltage, temperature and impedance measurement
- Auto standby (Timeout watchdog)
- CRC calculation over internal registers
- ECC protection for MTP data
- MTP Write Counter Error Flag and Lock Key protection
- MTP Header Self-Check
- Bitflip detection on internal Finite State Machines
- Broken pin detection on VBAT, VBAT_FIL, VSS and DIO pins
- GPIO1 / GPIO2 IO-Diagnostics
- Minimum and maximum die temperature detection
- Test/scan mode entry protection
- TCB/TPR toggling protection

4.2 DNB1168 safety concept and functional safety requirements

4.2.1 Assumed functional safety requirements

The following Functional safety requirements are assumed for the Battery Management System supporting the item Safety Goals.

Table 5 : Functional safety requirements

FSR-ID	Functional safety requirement	Supporting SG	ASIL	FTTI
FSR_1	The Battery Management System shall detect faults that cause unintended overcharging of battery cells	SG_1	D	300ms
FSR_2	The Battery Management System shall detect faults that cause unintended over-discharging of battery cells	SG_2	D	300ms
FSR_3	The Battery Management System shall detect thermal runaway of battery cells as early warning	SG_3	B	30s
FSR_4	The Battery Management System shall detect unintended battery cell discharging, to avoid empty battery	SG_4	A	7min
FSR_5	When fault is detected, Battery Management System shall turn-off the charge / discharge function and shall notify the external system	SG_1, SG_2, SG_3, SG_4.	D	10ms

4.2.2 Assumptions on use

- The target application assumed is an automotive Battery Management System.
- It is assumed that DNB1168 is a "Safety-related Element Out Of Context", thus the system requirements are not available in detail. Therefore, some assumptions are made on the "context of use" of the DNB1168 to derive the top level safety requirements of the DNB1168, based on assumptions for safety goals (at item level) and related ASIL.
- Each logic cell of the battery pack (one or more parallel battery cells) shall be connected to a dedicated single-cell supervisor IC (DNB1168).
- The pack controller ECU is communicating with all single-cell supervisors (DNB1168) using a bidirectional daisy-chain communication link.
- The interface between the pack controller and the daisy-chain communication link is handled by an SPI bridge IC that translates the SPI communication interface from the pack controller ECU into the DNB1168 custom daisy-chain protocol.
- Each single-cell supervisor (DNB1168) reports the voltage, temperature and impedance of the logic cell it is connected to when requested by the pack controller.
- Each single-cell supervisor (DNB1168) can apply passive charge balancing by discharging the logic cell when requested by the pack controller.
- DNB1168 is assumed to be a single-cell-supervisor element as part of an battery management system where the DNB1168 by itself does not directly take control/actions to mitigate an hazardous event on item level. Such control actions are assumed to be the responsibility of other parts of the system.
- Failing to produce and communicate accurate measurement results may violate the assumed Safety Goals.
- Assumed communication timeout mechanism of pack controller in case of communication fail.
- Assumed self-test sequence will be executed at key-off to detect latent faults.
- It is assumed that detection, prevention and handling of external component failure is the responsibility of the external system.

4.2.3 Device safety goals / toplevel safety requirements

- Since the DNB1168 is only a sensor element in the system, no Safety Goals can be specified at the device level. Only top level technical safety requirements can be assumed. See Table 6
- It is assumed that detection, prevention and handling of failure of components external to the DNB1168 is the responsibility of the external system.
- The DNB1168 shall use sampling rate for the voltage measurement that fits the assumed FTTI for the battery management system, if ASIL-D is targeted.
- A temperature measurement failure resulting in a higher measurement result than actual cell temperature, is also considered a safety issue allowing too much current to flow at low temperature causing dendrite growth leading to short circuit.
- The DNB1168 shall detect cell voltage measurement failure larger than +/- 15mV, supporting the item level safety goals SG_1 and SG_2 at ASIL-D with 0.5 FIT allocation for residual fault metric.
- The DNB1168 shall detect cell temperature measurement failure larger than +/- 6K, supporting the item level safety goals SG_1 and SG_2 at ASIL-D with 0.5 FIT allocation for residual fault metric.
- The DNB1168 shall detect cell impedance measurement failure larger than +/- 150µΩ, assuming 100mA DC excitation current for 1mΩ cell, to enable early warning on cell temperature, supporting the item level safety goal SG_3 at ASIL-B with 3 FIT allocation for residual fault metric.
- The DNB1168 shall detect unintended cell discharging, supporting the item level safety goal SG_4 at ASIL-A.

Above mentioned failures shall be detected within the Fault Detection Time Interval (FDTI). See Table 6.

Table 6 : Device safety goals / toplevel safety requirements

ID	Technical Safety Requirement	Relevant FSR ID	Supporting SG	ASIL	FDTI
TLSR_01	Shall detect a cell voltage measurement failure (larger than ±15 mV)	FSR_1, FSR_2	SG_1, SG_2	D	200ms
TLSR_04	Shall detect a cell temperature measurement failure (difference larger than ±6 K).	FSR_1, FSR_2	SG_1, SG_2	D	200ms
TLSR_07	Shall avoid a battery cell impedance measurement failure larger than ±150 µΩ, as input for early warning for thermal runaway detection of the battery cell (assumed 100mA DC excitation current for 1mΩ cell impedance).	FSR_3	SG_3	B	5s
TLSR_10	Shall detect unintended battery cell discharging due to balancing or impedance measurement	FSR_4	SG_4	A	6min

Note that the programmed sample rate of the voltage measurement is assumed to be <128ms when targeting ASIL-D.

4.2.4 Device hardware metric targets

Permanent faults are evaluated using SPFM and LFM. Transient faults are not evaluated for DNB1168, see base failure rate evaluation report. The base failure rate for permanent faults is derived from IEC/TR 62380.

The metrics in Table 7 are valid for the device safety goals / toplevel safety requirements of the DNB1168, as mentioned in Table 6.

Table 7 : Hardware metrics and PMHF for DNB1168

ID	Metric	Supporting SG	ASIL
TSR_18	SPFM ≥ 99% for TLSR_01	SG_1, SG_2	D
TSR_19	LFM ≥ 90% for TLSR_01	SG_1, SG_2	D
TSR_20	SPFM ≥ 99% for TLSR_04	SG_1, SG_2	D
TSR_21	LFM ≥ 90% for TLSR_04	SG_1, SG_2	D
TSR_22	SPFM ≥ 90% for TLSR_07	SG_3	B
TSR_23	LFM ≥ 60% for TLSR_07	SG_3	B
TSR_24	PMHF budget < 0.5 FIT for TLSR_01	SG_1	D
TSR_25	PMHF budget < 0.5 FIT for TLSR_04	SG_2	D
TSR_26	PMHF budget < 3 FIT for TLSR_07	SG_3	B

4.2.5 Assumptions on Fault Tolerant time interval (FTTI) and Multiple Point Fault Detection Interval (MPFDI)

Handling of failures on start-up, before enabling the system level safety function (for example, during system initialization or self-test). These errors are required to be handled before the system enables the safety function, or in a time shorter than the respective FTTI after enabling the safety function.

Handling of failures during runtime with repetitive supervision while the safety function is enabled. These errors are to be handled in a time shorter than the respective FTTI.

4.2.5.1 Single point fault tolerant time

The single-point fault tolerant time interval (FTTI) is the time span between a failure, that has the potential to give rise to a hazardous event and the time by which countermeasure action must be completed to prevent the hazardous event occurring. It is used to define the sum of worst case fault indication time and time for execution of corresponding countermeasures (reaction). Without any suitable functional safety mechanism, a hazard may appear after the FTTI elapsed.

The DNB1168 shall generate a safety flag to indicate a fault to the pack controller within the item FITI (Fault Indication Time Interval) when the defined fault(s) happen.

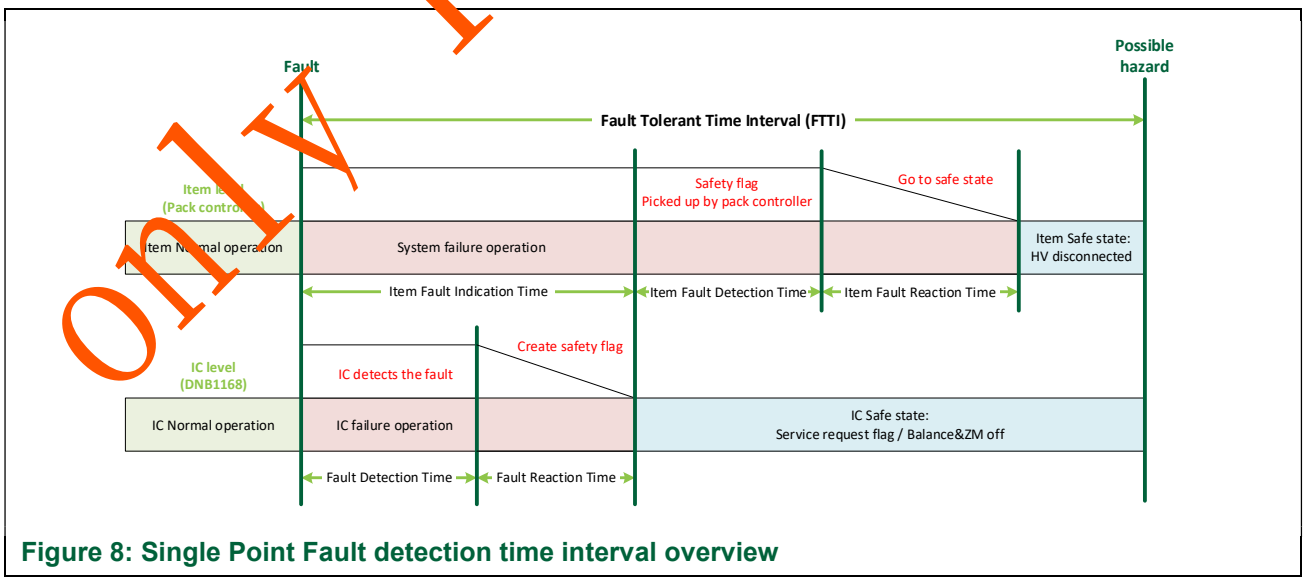

Figure 8: Single Point Fault detection time interval overview

Fault Indication Time is the time it takes from the occurrence of a fault to switching of the DNB1168 into IC safe state (raised Service Request flag and disabled ZM and Balancing functions).

Fault indication times for each safety mechanism are listed in Table 11.

4.2.5.2 Latent fault tolerant time

Latent fault only. DNB1168 will continue to produce valid measurements and therefore there is no Safety Goal violation. However, the item will detect that there is a latent fault after the self-test is executed.

Based on the application context, a worst case system Latent Fault Tolerant Time Interval (L-FTTI) of 4 hours is assumed for SG_1, SG_2, SG_3 and SG_4. It is assumed that a self-test sequence will be executed at key-off to detect latent faults.

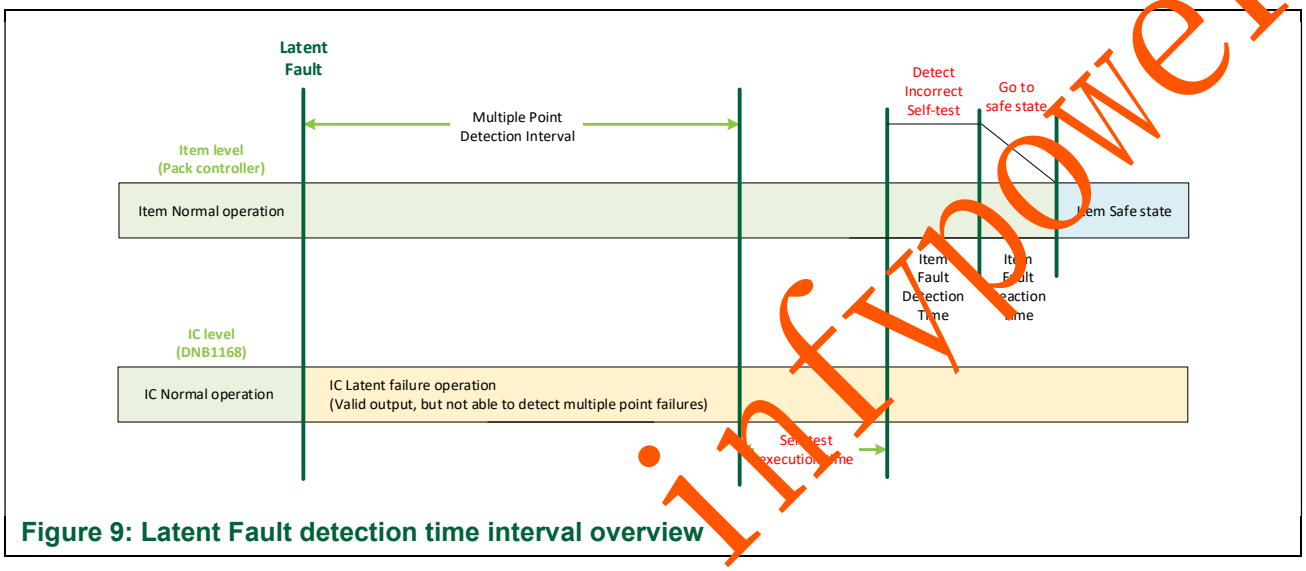

Figure 9: Latent Fault detection time interval overview

4.2.5.3 Multiple point fault tolerant time

Latent fault in combination with a Multiple Point Fault. The probability of this happening is very small (dual point fault).

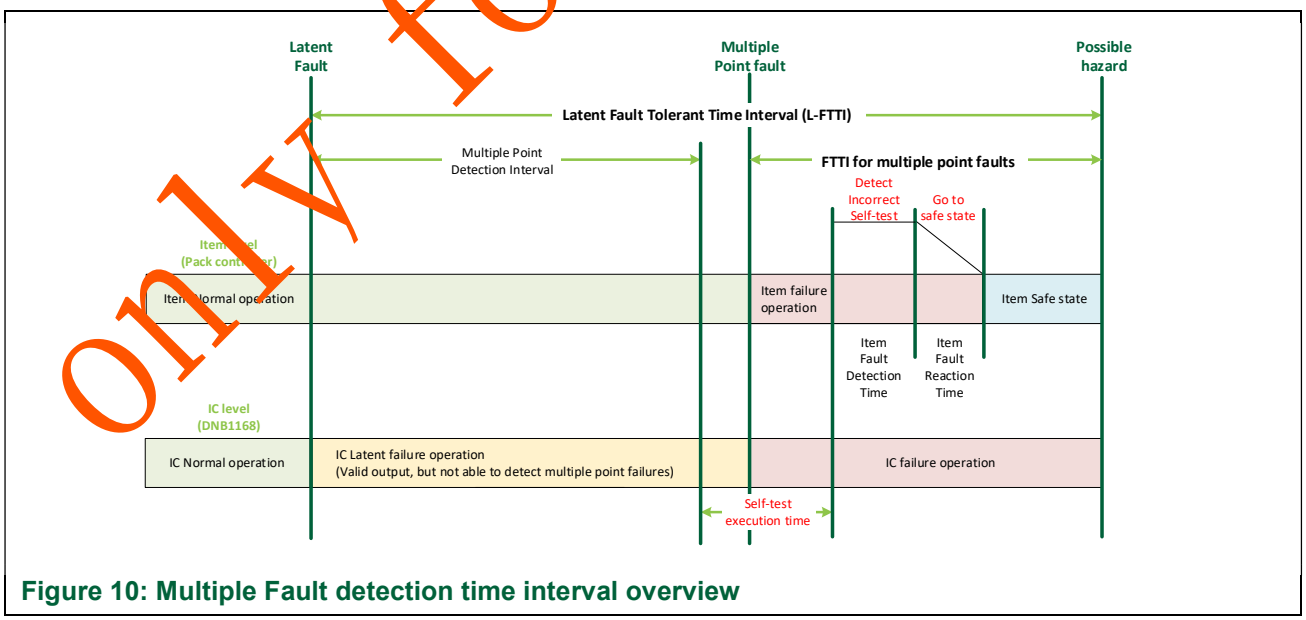

Figure 10: Multiple Fault detection time interval overview

4.2.6 Assumptions on component usage

- It is assumed that the DNB1168 is used within a specific mission profile.
- It is assumed that the DNB1168 is used in a battery management system in electric vehicles (EV), hybrid electric vehicles (HEV) or plug-in hybrid electric vehicles (PHEV).
- It is assumed that the DNB1168 is used in an application for which the mission profile is characterized by a lifetime of 15 years (131400 hrs).
- The mission profile shall be specified according to the vehicle status: driving, charging, preconditioning, on-grid parking, off-grid parking:

Table 8 : Assumed mission profile

		DNB1168 active functions			
Vehicle status	Hours	VM / DTS [hrs]	ZM [hrs]	Balancing [hrs]	Standby [hrs]
Driving	8000	8000	8000	0	0
Charging	30000	30000	30000	0	0
preconditioning	3000	3000	3000	0	0
On-grid parking	67000	7370	670	670	59630
Off-grid parking	23400	2574	234	2340	20826
Total	**131400**	**50944**	**41904**	**3010**	**80456**

Table 9 : Assumed temperature profile

	Distribution				
Air temp. [°C]	Driving [%]	Charging [%]	Preconditioning [%]	Off-grid parking [%]	On-grid parking [%]
-40	0	0	0	0	0
0	0	0	0	0	0
20	0	10	13	13	13
30	0	38	39	39	39
35	1	27	30	30	30
40	61	24	18	18	18
50	35	0	0	0	0
60	2	0	0	0	0
70	0	0	0	0	0
85	0	0	0	0	0
120	1	1	0	0	0

- It is assumed that the DNB1168 shall meet all the datasheet specifications after relevant qualification tests (following AEC-Q100 standard) to simulate the above mission profile are completed.
- It is assumed that the qualification tests will cover failures related to degradation of circuits over lifetime.

4.3 Safety architecture

4.3.1 Abstract description of the safety architecture

Figure 11 shows the functional safety block diagram of the DNB1168.

To achieve the ASIL-D rating for the voltage and temperature measurement, redundant acquisition channels for these functions are implemented. The redundant channels in DNB1168 are called ‘guard’ and ‘main’. For legacy naming reasons the primary acquisition channel is implemented in the ‘guard’ domain, while the secondary acquisition channel is in the ‘main’ domain.

Note that the redundant channel is not limited to the ADCs only. Also, all references, supplies and pins are completely redundant. The different domains are indicated in Figure 11 by means of color.

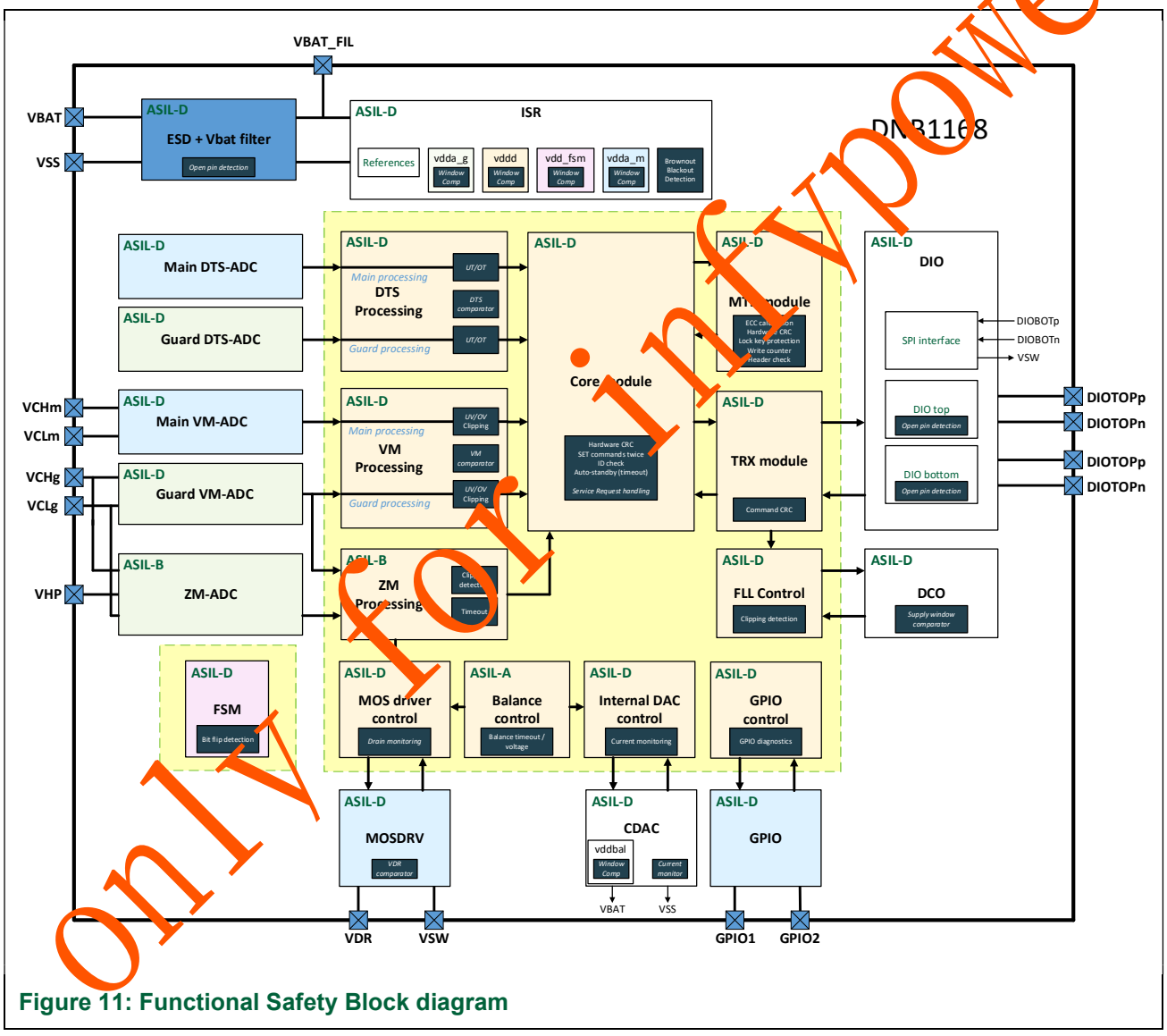

Figure 11: Functional Safety Block diagram

4.3.2 DNB1168 Safe state

The DNB1168 has 2 possible Safe States:

1. Alarm flagging to pack controller and degraded mode of operation

   Some Service Request error flags are 'Safety Flags' (see 4.3.2.2) that will cause the DNB1168 to enter a degraded mode of operation (Safe Mode) by disabling impedance measurement and cell balancing to avoid discharging the battery cell.

2. Alarm flagging to pack controller

   When a fault is detected by the DNB1168 that potentially will result in violation of a toplevel safety requirement, the measurement results can no longer be trusted and a Service Request error flag is sent to the pack controller via the daisy link.

4.3.2.1 Service Request flags

The DNB1168 is monitoring many internal features. Whenever it is detected that one of the features has a problem, a so-called Service Request Flag is raised. In Figure 12 an overview of all the Service Requests (SR) in DNB1168 is shown. The SrvReqData register contains individual SR-flags (grey colored), but also SR groups that are raised when one of the underlying flags (color coded) is raised. For example, the 'Openwire' bit from the SrvReqData register is raised if one of the bits in the 'BoardDiagnostics' register is raised.

SrvReqData	12h	Reserved	CmdErr	ClockErr	IntErr	GPIOErr	InvalidLockKey	OpenWire	ZM-ADCErr	Ba…nDo…n	CurrErr	LDO…oR	Temp-ADCErr	Cell-TempErr	VM-ADCErr	Cell-VoltErr	BrownOut	
VoltDiagnostics	13h	Reserved									…mMGdiff …ty flag	VM_Gclip	VM_Mclip	UVolt_G Safety flag	OVolt_G Safety flag	UVolt_M Safety flag	OVolt_M Safety flag	
TempDiagnostics	14h	Reserved								te…MG di… Safety flag	Reserved	MinDieTemp Safety flag	MaxDieTemp Safety flag	UTemp_G Safety flag	OTemp_G Safety flag	Reserved		
CurrDiagnostics	15h	Reserved											BalVoltLim	BalTmOut	ZMTmOut	VDRErr Safety flag	DAC-Err Safety flag	
ZMDiagnostics	16h	Reserved															ZMadc_clip	
BoardDiagnostics	17h	Reserved								DIOTOPp Safety flag	DIOTOPn Safety flag	DIOBOTp Safety flag	DIOBOTn Safety flag	Reserved		Resistor Safety flag	Vbat/Vss Safety flag	
ICDiagnostics	18h	Reserved		GPI…2OoR	GPIO1…oR	CRC_s…dw _DNS Safety flag	CRC_shdw _user	CRC_cmd Safety flag	MTP_wrt_cnt	MTP_ECC Safety flag	MTP_invalid	G_LDO_Dio	G_LDO_Ana	G_LDO_Dig	G_LDO_Pll	M_LDO_Ana	M_LDO_Bal	

Figure 12: Overview of the SR-flags in DNB1168

See Hardware-software interface specification referenced in Table 2 for a description of the Service Request handling in full detail.

When a SR-flag is raised, the DNB1168 typically will ignore the next command that is received and instead it will reply with a Service Request confirmation. This confirmation is sending the SrvReqData register. This allows the pack controller to know immediately which Service Request Flags were received without the need to send additional commands. Only the first command after an Service Request flag is raised might be ignored: all the next commands are handled normally.

It is critical that the pack controller confirms the reception of the Service Request flags. If the pack controller would have somehow missed the Service Request confirmation, it would be unaware of a potentially dangerous situation. Therefore, the pack controller is required to send a 'getData' command pointing to the register where the active Service Request flag was raised (e.g., the 'VoltDiagnostics' or 'ICDiagnostics' register).

Until the pack controller has issued the correct getData command, the reported Service Request flag remains 'pending' inside the DNB1168 and this will be reported with each following confirmation message. After all pending SR-flags are retrieved, the reporting will stop.

Retrieving an Service Request flag does not yet clear the Service Request flag inside the DNB1168. If the underlying problem would occur again, no new flag is sent out. Only after the pack controller issues the 'SetSrvReqMask' command, all active Service Request flags are cleared so the DNB1168 will send a new Service Request flag if the problem occurs again.

4.3.2.2 Safety Flags

Some of the Service Request flags in Figure 12 are labeled 'Safety Flags'. This means that if these Service Request flags are raised, the DNB1168 automatically transitions into Safe Mode, meaning that the excitation of the battery (via impedance measurement or cell balancing) is stopped. On top of that, the Service Request handling routine is started (see 4.3.2.1). For the non-safety flags only the Service Request handling routine is started and the DNB1168 does not transition into Safe Mode.

The DNB1168 will remain in Safe Mode until the pack controller changes the operation mode.

4.3.3 Self-test capabilities in DNB1168

The DNB1168 can be put in Self-test mode by the pack controller to detect latent faults.

- Based on the application context, a worst case system Latent Fault Tolerant Time Interval (L-FTTI) of 4 hours shall be used for SG_1, SG_2, SG_3 and SG_4.
- Assumed self-test sequence will be executed by pack controller at key-off to detect latent faults.

The Self-test Mode is used to check the safety mechanisms that cannot be checked without interrupting the normal operation. When entering this mode, several error conditions are simulated by forcing certain conditions at the input of safety related comparators (for example fault forced on the input of the overvoltage comparator).

Table 10 : self-test mechanisms in DNB1168

ID	Safety mechanism	Functional block allocation	Fault detection	Assumed diagnostic coverage for latent faults
ST3	Self-test of LDO VDDAm window comparator	ISR	Latent faults	60%
ST4	Self-test of LDO VDDD window comparator	ISR	Latent faults	60%
ST5	Self-test of LDO VDDAg window comparator	ISR	Latent faults	60%
ST6	Self-test of LDO VDDPLL window comparator	DCO	Latent faults	60%
ST7	Self-test of LDO VDDBAL window comparator	CDAC	Latent faults	60%
ST8	Self-test of LDO VDDFSM window comparator	ISR	Latent faults	60%
ST9	Self-test of VM comparator	VM processing	Latent faults	60%
ST12	Self-test of DTS comparator	DTS processing	Latent faults	60%
ST14	Self-test of VDD comparator	MOSDRV	Latent faults	60%
ST32	Self-test of VBAT open wire detector	Openwiredet	Latent faults	90%
ST33	Self-test of VSS open wire detector	Openwiredet	Latent faults	90%
ST34	Self-test of VBAT_FIL open wire detector	Openwiredet	Latent faults	99%
ST35	Self-test of DIO open wire detector	Openwiredet	Latent faults	90%
ST39	Self-test of GPIO1 diagnostics	GPIO	Latent faults	99%
ST40	Self-test of GPIO2 diagnostics	GPIO	Latent faults	99%

5 Details of safety mechanisms

5.1 Safety Mechanisms integrated in DNB1168

All safety mechanisms integrated in DNB1168 and considered as part of the safety analysis as summarized in the safety analysis report, are listed in Table 11. A detailed description of each safety mechanism is given in the sections below.

Table 11 : safety mechanisms in DNB1168

ID	Safety mechanism	Functional block allocation	Device safety goal allocation	Supporting SG	Fault indication time
SM1	Blackout detection	ISR	TLSR_01, TLSR_04, TLSR_07, TLSR_10	SG_1, SG_2, SG_3, SG_4	10us
SM2	Brownout detection	ISR	TLSR_01, TLSR_04, TLSR_07, TLSR_10	SG_1, SG_2, SG_3, SG_4	10us
SM3	VDDAm voltage monitoring	ISR	TLSR_01, TLSR_04	SG_1, SG_2	10ms
SM4	VDDD voltage monitoring	ISR	TLSR_01, TLSR_04, TLSR_07, TLSR_10	SG_1, SG_2, SG_3, SG_4	10ms
SM5	VDDAg voltage monitoring	ISR	TLSR_01, TLSR_04, TLSR_07	SG_1, SG_2, SG_3	10ms
SM6	VDDPLL voltage monitoring	DCO	TLSR_01, TLSR_04, TLSR_07, TLSR_10	SG_1, SG_2, SG_3, SG_4	10ms
SM7	VDDBAL voltage monitoring	CDAC	TLSR_10	SG_4	10ms
SM8	VDDFSM voltage monitoring	ISR	TLSR_01, TLSR_04, TLSR_07, TLSR_10	SG_1, SG_2, SG_3, SG_4	10ms
SM9	Redundant cell voltage comparison by DNB1168	VM processing	TLSR_01	SG_1, SG_2	150ms
SM10	VM-ADC Clipping detection	VM processing	TLSR_01	SG_1, SG_2	1ms
SM11	ZM-ADC Clipping detection	ZM processing	TLSR_07	SG_3	1ms
SM12	Redundant cell temperature comparison by DNB1168	DTS processing	TLSR_04	SG_1, SG_2	100ms
SM13	Current monitor for internal CDAC	CDAC	TLSR_10	SG_4	1ms
SM14	External MOSFET and resistor (VDR) monitoring	MOSDRV	TLSR_01, TLSR_07	SG_1, SG_2, SG_3	1ms
SM15	Balancing timeout watchdog	Balance	TLSR_10	SG_4	1ms
SM16	Balancing Activity Reached Voltage Threshold	Balance	TLSR_10	SG_4	1ms
SM17	Impedance timeout watchdog	ZM processing	TLSR_10	SG_4	1ms
SM18	Oscillator clipping detection	FLL	TLSR_01, TLSR_04, TLSR_07, TLSR_10	SG_1, SG_2, SG_3, SG_4	1ms
SM19	Command CRC check	TRX	TLSR_01, TLSR_04, TLSR_07, TLSR_10	SG_1, SG_2, SG_3, SG_4	1ms
SM20	ID check in each data frame	Core	TLSR_01, TLSR_04, TLSR_07, TLSR_10	SG_1, SG_2, SG_3, SG_4	NA
SM21	Rolling sample counter for unique data detection for voltage measurement	VM processing	TLSR_01	SG_1, SG_2	NA
SM22	Rolling sample counter for unique data detection for temperature measurement	DTS processing	TLSR_04	SG_1, SG_2	NA
SM23	Rolling sample counter for unique data detection for impedance measurement	ZM processing	TLSR_07	SG_3	NA
SM24	Auto standby (Timeout watchdog)	Core	TLSR_01, TLSR_04, TLSR_07, TLSR_10	SG_1, SG_2, SG_3, SG_4	5min
SM25	Mismatch detection from sending SET commands twice	Core	TLSR_01, TLSR_04, TLSR_07, TLSR_10	SG_1, SG_2, SG_3, SG_4	1s

ID	Safety mechanism	Functional block allocation	Device safety goal allocation	Supporting SG	Fault indication time
SM26	CRC calculation over command registers	Core	TLSR_01, TLSR_04, TLSR_07, TLSR_10	SG_1, SG_2, SG_3, SG_4	100ms
SM27	CRC calculation over user configurable shadow registers	MTP	TLSR_01, TLSR_04, TLSR_07, TLSR_10	SG_1, SG_2, SG_3, SG_4	100ms
SM28	CRC calculation over non-configurable shadow registers	MTP	TLSR_01, TLSR_04, TLSR_07, TLSR_10	SG_1, SG_2, SG_3, SG_4	100ms
SM30	ECC for MTP data. Redundant 6 bits /16bits	MTP	TLSR_01, TLSR_04, TLSR_07, TLSR_10	SG_1, SG_2, SG_3, SG_4	1ms
SM31	Finite State Machine bitflip detection	Core, CDAC, MOSDRV, VM processing, DTS processing, SRHandle, TRX	TLSR_01, TLSR_04, TLSR_07, TLSR_10	SG_1, SG_2, SG_3, SG_4	10us
SM32	Broken VBAT pin detection	Openwiredet	TLSR_01, TLSR_04, TLSR_07, TLSR_10	SG_1, SG_2, SG_3, SG_4	1ms
SM33	Broken VSS pin detection	Openwiredet	TLSR_01, TLSR_04, TLSR_07, TLSR_10	SG_1, SG_2, SG_3, SG_4	1ms
SM34	Broken VBAT_FIL pin detection	Openwiredet	TLSR_01, TLSR_04, TLSR_07, TLSR_10	SG_1, SG_2, SG_3, SG_4	1ms
SM35	Broken communication wire detection for the DIO pins	DIO	TLSR_01, TLSR_04, TLSR_07, TLSR_10	SG_1, SG_2, SG_3, SG_4	1ms
SM39	GPIO1 Diagnostics	GPIO	TLSR_01, TLSR_04, TLSR_07, TLSR_10	SG_1, SG_2, SG_3, SG_4	1ms
SM40	GPIO2 Diagnostics	GPIO	TLSR_01, TLSR_04, TLSR_07, TLSR_10	SG_1, SG_2, SG_3, SG_4	1ms
SM41	ZM phase control clipping detection	ZM processing	TLSR_07	SG_3	1ms
SM42	Maximum Temperature Detection	DTS processing	TLSR_01, TLSR_04, TLSR_07, TLSR_10	SG_1, SG_2, SG_3, SG_4	20ms
SM43	Minimum Temperature Detection	DTS processing	TLSR_01, TLSR_04, TLSR_07, TLSR_10	SG_1, SG_2, SG_3, SG_4	20ms
SM44	Lock key protection for MTP	MTP	TLSR_01, TLSR_04, TLSR_07, TLSR_10	SG_1, SG_2, SG_3, SG_4	NA
SM45	MTP Write Counter Error Flag	MTP	TLSR_01, TLSR_04, TLSR_07, TLSR_10	SG_1, SG_2, SG_3, SG_4	NA
SM46	MTP Header Self-Check	MTP	TLSR_01, TLSR_04, TLSR_07, TLSR_10	SG_1, SG_2, SG_3, SG_4	NA
SM47	Test/scan mode entry protection	Test	TLSR_01, TLSR_04, TLSR_07, TLSR_10	SG_1, SG_2, SG_3, SG_4	NA
SM48	TCB/TPR toggling protection	Test	TLSR_01, TLSR_04, TLSR_07, TLSR_10	SG_1, SG_2, SG_3, SG_4	NA

5.1.1.1 SM1: Blackout detection

- ASIL considered: ASIL D.
- Description:

  If the battery cell voltage is lower than 1.4V, the DNB1168 is reset to factory settings and placed in Sleep mode (see section 4.1.3). When the cell voltage is high enough to recover from the blackout state, the DNB1168 will send a service request flag to the pack controller via the daisy link.
- Allocation to functional block: ISR.
- Fault indication time: 10us.
- Assumed diagnostic coverage: 99% (ISO 26262-5:2018, D2.6.2).

- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  No self-test feature available.

5.1.1.2 SM2: Brownout detection

- ASIL considered: ASIL D.
- Description:

  If the battery cell voltage is lower than 1.8V, the analog part of the IC is switched off. The digital part remains powered and the DNB1168 retains its state. When the cell voltage is high enough to recover from the brownout state, the DNB1168 will send a service request flag to the pack controller via the daisy link.
- Allocation to functional block: ISR.
- Fault indication time: 10us.
- Assumed diagnostic coverage: 99% (ISO 26262-5:2018, D2.6.2).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  No self-test feature available.

5.1.1.3 SM3: VDDAm voltage monitoring

- ASIL considered: ASIL D.
- Description:

  A window comparator is used to monitor the VDDA_Main internal supply voltage for the cell voltage and temperature measurement main acquisition channel. When the supply monitor detects an error, the DNB1168 will send a service request flag to the pack controller via the daisy link.
- Allocation to functional block: ISR.
- Fault indication time: 10ms.
- Assumed diagnostic coverage: 99% (ISO 26262-5:2018, D2.6.2).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  ST3: The window comparator can be forced to present a flag. It can detect whether the comparators are functional, it cannot detect the accuracy of the window comparator. Self-test shall be initiated by the pack controller within the LFTTI (e.g. during key-off) to cover latent faults.

5.1.1.4 SM4: VDDD voltage monitoring

- ASIL considered: ASIL D.
- Description:

  A window comparator is used to monitor the VDDD internal supply voltage for digital circuits. The DNB1168 disables the CDAC and MOSFET driver and retain the state of the digital core when an output voltage range failure of the internal digital supply VDDD is detected. When the supply monitor detects an error, the DNB1168 will send a service request flag to the pack controller via the daisy link.

- Allocation to functional block: ISR
- Fault indication time: 10ms.
- Assumed diagnostic coverage: 99% (ISO 26262-5:2018, D2.6.2).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  ST4: The window comparator can be forced to present a flag. It can detect whether the comparators are functional, it cannot detect the accuracy of the window comparator. Self-test shall be initiated by the pack controller within the LFTTI (e.g. during key-off) to cover latent faults.

5.1.1.5 SM5: VDDAg voltage monitoring

- ASIL considered: ASIL D.
- Description:

  A window comparator is used to monitor the VDDA_Guard internal supply voltage for the cell voltage and temperature measurement guard acquisition channel. This supply voltage is also used for the cell impedance measurement. When the supply monitor detects an error, the DNB1168 will send a service request flag to the pack controller via the daisy link.
- Allocation to functional block: ISR.
- Fault indication time: 10ms.
- Assumed diagnostic coverage: 99% (ISO 26262-5:2018, D2.6.2).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  ST5: The window comparator can be forced to present a flag. It can detect whether the comparators are functional, it cannot detect the accuracy of the window comparator. Self-test shall be initiated by the pack controller within the LFTTI (e.g. during key-off) to cover latent faults.

5.1.1.6 SM6: VDDPLL voltage monitoring

- ASIL considered: ASIL D.
- Description:

  A window comparator is used to monitor the VDDPLL internal supply voltage for the clock generation circuits. The DNB1168 shall disable the CDAC and MOSFET driver and retain the state of the digital part when output voltage range failure of the internal digital supply VDDPLL is detected. Also, when the supply monitor detects an error, the DNB1168 will send a service request flag to the pack controller via the daisy link.
- Allocation to functional block: DCO.
- Fault indication time: 10ms.
- Assumed diagnostic coverage: 99% (ISO 26262-5:2018, D2.6.2).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  ST6: The window comparator can be forced to present a flag. It can detect whether the comparators are functional, it cannot detect the accuracy of the window comparator. Self-test shall be initiated by the pack controller within the LFTTI (e.g. during key-off) to cover latent faults.

5.1.1.7 SM7: VDDBAL voltage monitoring

- ASIL considered: ASIL D.
- Description:

  A window comparator is used to monitor the VDDBAL internal supply voltage for the CDAC. When the supply monitor detects an error, the DNB1168 will send a service request flag to the pack controller via the daisy link.
- Allocation to functional block: CDAC.
- Fault indication time: 10ms.
- Assumed diagnostic coverage: 99% (ISO 26262-5:2018, D2.6.2).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  ST7: The window comparator can be forced to present a flag. It can detect whether the comparators are functional, it cannot detect the accuracy of the window comparator. Self-test shall be initiated by the pack controller within the LFTTI (e.g. during key-off) to cover latent faults.

5.1.1.8 SM8: VDDFSM voltage monitoring

- ASIL considered: ASIL D.
- Description:

  A window comparator is used to monitor the VDDFSM internal supply voltage for the internal digital always-on circuitry. When the supply monitor detects an error, the DNB1168 will send a service request flag to the pack controller via the daisy link.
- Allocation to functional block: ISR.
- Fault indication time: 10ms.
- Assumed diagnostic coverage: 99% (ISO 26262-5:2018, D2.6.2).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  ST8: The window comparator can be forced to present a flag. It can detect whether the comparators are functional, it cannot detect the accuracy of the window comparator. Self-test shall be initiated by the pack controller within the LFTTI (e.g. during key-off) to cover latent faults.

5.1.1.9 SM9: Redundant cell voltage comparison by DNB1168

- ASIL considered: ASIL D.
- Description:

  The DNB1168 contains 2 independent voltage measurement paths (independent supply, references, ADC, digital filters and calibration). When the output differs by more than the threshold value (which is configurable and default 15mV), a service request flag is sent to the pack controller via the daisy link, and the DNB1168 shall disable cell impedance measurement and cell balancing. Since if the cell voltage measurement cannot be trusted, it shall be avoided to discharge the battery cell.
- Allocation to functional block: VM processing.
- Fault indication time: 150ms.
- Assumed diagnostic coverage: 99% (ISO 26262-5:2018, D2.1.2).
- Safety Mechanism always active, no triggering by BMS system required.

- Self-test feature:

  ST9: The digital VM comparator can be forced to present a flag. It can detect whether the comparator is functional. Self-test is initiated by the pack controller within the LFTTI (e.g. during key-off).

5.1.1.10 SM10: VM-ADC Clipping detection

- ASIL considered: ASIL D.
- Description:

  When the bitstream from the VM-ADC's is presenting too many consecutive 1's or 0's, a service request flag is raised and sent to the pack controller via the daisy link.
- Allocation to functional block: VM processing.
- Fault indication time: 1ms.
- Assumed diagnostic coverage: 99% (ISO 26262-5:2018, D2.4.4).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  No self-test feature available.

5.1.1.11 SM11: ZM-ADC Clipping detection

- ASIL considered: ASIL B.
- Description:

  When the bitstream from the ZM-ADC is presenting too many consecutive 1's or 0's, a service request flag is raised and sent to the pack controller via the daisy link.
- Allocation to functional block: ZM processing.
- Fault indication time: 1ms.
- Assumed diagnostic coverage: 99% (ISO 26262-5:2018, D2.4.4).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  No self-test feature available.

5.1.1.12 SM12: Redundant cell temperature comparison by DNB1168

- ASIL considered: ASIL D.
- Description:

  The DNB1168 contains 2 independent temperature sensors. When their output differs by more than the threshold value (which is configurable and default 6 degrees), a safety error flag is sent to the pack controller via the daisy link, and the DNB1168 shall disable cell impedance measurement and cell balancing. Since if the cell temperature measurement cannot be trusted, it shall be avoided to discharge the battery cell.
- Allocation to functional block: DTS processing.
- Fault indication time: 100ms.
- Assumed diagnostic coverage: 99% (ISO 26262-5:2018, D2.1.2).
- Safety Mechanism always active, no triggering by BMS system required.

- Self-test feature:

  ST12: The digital DTS comparator can be forced to present a flag. It can detect whether the comparator is functional. Self-test is initiated by the pack controller within the LFTTI (e.g. during key-off).

5.1.1.13 SM13: Current monitor for internal DAC

- ASIL considered: ASIL D.
- Description:

  Checks whether there is a DAC current when there should be one. When a fault is detected in the DAC current, the DNB1168 will send a service request flag to the pack controller via the daisy link and cell impedance measurement and cell balancing is disabled.
- Allocation to functional block: CDAC.
- Fault indication time: 1ms.
- Assumed diagnostic coverage: 99% (ISO 26262-5:2018, D2.9.1).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  No self-test feature available.

5.1.1.14 SM14: External MOSFET and resistor (VDR) monitoring

- ASIL considered: ASIL D.
- Description:

  The drain voltage of the external MOSFET is monitored at pin VDR. When the MOSFET is enabled, VDR must be pulled down. When the external MOSFET is disabled, VDR must be pulled up. When VDR is not behaving as expected, something is wrong with the external MOSFET and/or the external resistor, and a safety error flag is sent to the pack controller via the daisy link. Also, the DNB1168 will disable cell impedance measurement and cell balancing.
- Allocation to functional block: MOSDRV.
- Fault indication time: 1ms.
- Assumed diagnostic coverage: 99% (ISO 26262-5:2018, D2.9.1).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  ST14: The VDR comparator can be forced to present a flag. It can detect whether the comparator is functional. It cannot detect the accuracy of the comparator. Self-test is initiated by the pack controller within the LFTTI (e.g. during key-off).

5.1.1.15 SM15: Balancing timeout watchdog

- ASIL considered: ASIL A.
- Description:

  A timing watchdog checks whether battery cell balancing is enabled no longer than the time programmed by the pack controller. Balancing will be disabled if this watchdog timer is triggered and a service request flag is sent to the pack controller via the daisy link.
- Allocation to functional block: Balance

- Fault indication time: 1ms.
- Assumed diagnostic coverage: 60% (ISO 26262-5:2018, D2.1.1).
- Safety Mechanism shall be set by the pack controller by programming the time-out required. See 6.17.
- Self-test feature:

  No self-test feature available.

5.1.1.16 SM16: Balancing Activity Reached Voltage Threshold

- ASIL considered: ASIL A.
- Description:

  A voltage watchdog checks whether the battery cell voltage drops below a threshold set by the pack controller while balancing is enabled. When the voltage watchdog for the balancing triggers, the DNB1168 will send a service request flag to the pack controller via the daisy link.
- Allocation to functional block: Balance.
- Fault indication time: 1ms.
- Assumed diagnostic coverage: 60% (ISO 26262-5:2018, D2.4.5).
- Safety Mechanism shall be set by the pack controller by programming the threshold required. See 6.17.
- Self-test feature:

  No self-test feature available.

5.1.1.17 SM17: Impedance timeout watchdog

- ASIL considered: ASIL B.
- Description:

  A timing watchdog checks whether impedance measurement is enabled no longer than the time programmed by the pack controller. If the timing watchdog for the impedance measurement is triggered, the DNB1168 will send a service request flag to the pack controller via the daisy link.
- Allocation to functional block: ZM processing.
- Fault indication time: 1ms.
- Assumed diagnostic coverage: 60% (ISO 26262-5:2018, D2.1.1).
- Safety Mechanism shall be set by the pack controller by programming the time-out required. See 6.17.
- Self-test feature:

  No self-test feature available.

5.1.1.18 SM18: Oscillator clipping detection

- ASIL considered: ASIL D.
- Description:

  The DNB1168 contains a Frequency Locked Loop (FLL) controller that controls the frequency of the internal timing reference. The FLL uses the synchronization signal from the daisy chain communication link as reference. When the oscillator control setting is clipped to the maximum or minimum setting, a service flag is sent to the pack controller via the daisy link.
- Allocation to functional block: FLL.

- Fault indication time: 1ms.
- Assumed diagnostic coverage: 99% (ISO 26262-5:2018, D2.4.4).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  No self-test feature available.

5.1.1.19 SM19: Command CRC check

- ASIL considered: ASIL D.
- Description:

  A CRC check is calculated over the contents of each data frame received by the DNB1168. In case a fault is detected in the CRC of the received data, the DNB1168 ignores the command and sends back an 'invalid' confirmation via the daisy link to inform the pack. See 6.2.4.

  CRC-4, 0x9 (x^4+x+1), 28 bits data word -> Hamming distance 2
- Allocation to functional block: TRX.
- Fault indication time: 1ms.
- Assumed diagnostic coverage: 60% (ISO 26262-5:2018, D2.5.6a).

  Safety Mechanism always active, no triggering by BMS system required. It is assumed that the pack controller checks the CRC-error flagging in the confirmation messages sent by the DNB1168. See 6.2.4.
- Self-test feature:

  No self-test feature available.

5.1.1.20 SM20: ID check in each data frame

- ASIL considered: ASIL D.
- Description:

  All data sent over the daisy chain will contain an Identification number (ID). It is checked (both by the pack controller and by the DNB1168) whether the ID matches with the expected ID. See 6.1.
- Allocation to functional block: TRX.
- Fault indication time: not applicable.
- Assumed diagnostic coverage: 90% (ISO 26262-5:2018, D2.5.7).
- Safety Mechanism always active, no triggering by BMS system required. It is assumed that the pack controller checks the ID in the confirmation messages sent by the DNB1168. See 6.2.3.
- Self-test feature:

  No self-test feature available.

5.1.1.21 SM21: Rolling sample counter for unique data detection for voltage measurement

- ASIL considered: ASIL D.
- Description:

  To make sure that the data samples are not repeated or skipped, the DNB1168 maintains a Rolling Sample Counter (RSC) that is updated for each new measurement of the cell voltage. The 2-bits counter counts from zero to three and then starts again at zero.

- Allocation to functional block: VM processing.
- Fault indication time: not applicable.
- Assumed diagnostic coverage: 90% (ISO 26262-5:2018, D2.5.7).
- Safety Mechanism always active, no triggering by BMS system required. It is assumed that the pack controller checks the RSC in the confirmation messages sent by the DNB1168. See 6.2.4.
- Self-test feature:

  No self-test feature available.

5.1.1.22 SM22: Rolling sample counter for unique data detection for temperature measurement

- ASIL considered: ASIL D.
- Description:

  To make sure that the data samples are not repeated or skipped, the DNB1168 maintains a Rolling Sample Counter (RSC) that is updated for each new measurement of the cell temperature. The 2-bits counter counts from zero to three and then starts again at zero.
- Allocation to functional block: DTS processing.
- Fault indication time: not applicable.
- Assumed diagnostic coverage: 90% (ISO 26262-5:2018, D2.5.7).
- Safety Mechanism always active, no triggering by BMS system required. It is assumed that the pack controller checks the RSC in the confirmation messages sent by the DNB1168. See 6.2.4.
- Self-test feature:

  No self-test feature available.

5.1.1.23 SM23: Rolling sample counter for unique data detection for impedance measurement

- ASIL considered: ASIL B.
- Description:

  To make sure that the data samples are not repeated or skipped, the DNB1168 maintains a Rolling Sample Counter (RSC) that is updated for each new measurement of the cell impedance. The 2-bits counter counts from zero to three and then starts again at zero.
- Allocation to functional block: ZM processing.
- Fault indication time: not applicable.
- Assumed diagnostic coverage: 90% (ISO 26262-5:2018, D2.5.7).
- Safety Mechanism always active, no triggering by BMS system required. It is assumed that the pack controller checks the RSC in the confirmation messages sent by the DNB1168. See 6.2.4.
- Self-test feature:

  No self-test feature available.

5.1.1.24 SM24: Auto standby (Timeout watchdog)

- ASIL considered: ASIL D.
- Description:

  When no communication activity is detected by the DNB1168 for 5 minutes, it will automatically transition to standby mode. Internal (CDAC)/External (MOSFET) current sources will be switched

off when the DNB1168 goes into auto standby mode. This prevents a situation in which the current sources cannot be switched off when a DNB1168 device in the daisy chain closer to the pack controller is not responding.

- Allocation to functional block: Digital Core.
- Fault indication time: 5min.
- Assumed diagnostic coverage: 90% (ISO 26262-5:2018, D2.5.8).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  No self-test feature available.

5.1.1.25 SM25: Mismatch detection from sending SET commands twice

- ASIL considered: ASIL D.
- Description:

  The pack controller needs to send SET-commands twice within 1 second. If DNB1168 detects a difference between the 2 commands, this command shall be ignored and a service flag is sent to the pack controller via the daisy link.
- Allocation to functional block: Digital Core.
- Fault indication time: 1s.
- Assumed diagnostic coverage: 90% (ISO 26262-5:2018, D2.5.5).
- Safety Mechanism always active, no triggering by BMS system required. It is assumed that the pack controller inspects the error detection information in the confirmation messages sent by the DNB1168. See 6.2.4.
- Self-test feature:

  No self-test feature available.

5.1.1.26 SM26: CRC calculation over command registers

- ASIL considered: ASIL D.
- Description:

  Every 100ms a CRC is calculated by the DNB1168 over the contents of the command registers, and compared with the reference CRC result of the previous calculation. The result is stored in an output register which allows the pack controller to check consistency of the data. After the command registers contents are changed intentionally, the reference CRC is re-calculated immediately. In case of CRC error, a service flag is sent to the pack controller via the daisy link.

  CRC-16, 0xac9a, 208 bits data → Hamming distance 5
- Allocation to functional block: Digital Core.
- Fault indication time: 100ms.
- Assumed diagnostic coverage: 99% (ISO 26262-11:2018, 5.1.13.8).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  No self-test feature available.

5.1.1.27 SM27: CRC calculation over user configurable shadow registers

- ASIL considered: ASIL D.
- Description:

  At start-up the DNB1168 will copy the contents of the non-volatile memory (MTP) to shadow registers for fast access. A hardware CRC is calculated over the data stored in the user area of the MTP (including the MTP-write counter) after each MTP loading into the shadow registers and stored as a reference CRC. Every 100ms this CRC is recalculated to check consistency of the data in the shadow registers. In case of CRC error, a service flag is sent to the pack controller via the daisy link.

  CRC-16, 0xac9a, 192 bits data → Hamming distance 5
- Allocation to functional block: MTP.
- Fault indication time: 100ms.
- Assumed diagnostic coverage: 99% (ISO 26262-11:2018, 5.1.13.8).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  No self-test feature available.

5.1.1.28 SM28: CRC calculation over non-configurable shadow registers

- ASIL considered: ASIL D.
- Description:

  At start-up the DNB1168 will copy the contents of the non-volatile memory (MTP) to shadow registers for fast access. A hardware CRC is calculated over the data stored in DNS1168 area of the MTP and stored in the MTP as a reference CRC. Every 100ms the CRC is recalculated to check consistency of the data in the shadow registers. In case of CRC error, a service flag is sent to the pack controller via the daisy link and cell impedance measurement and cell balancing is disabled.

  CRC-16, 0xac9a, 688 bits data → Hamming distance 4
- Allocation to functional block: MTP.
- Fault indication time: 100ms.
- Assumed diagnostic coverage: 99% (ISO 26262-11:2018, 5.1.13.8).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  No self-test feature available.

5.1.1.29 SM30: ECC for MTP data.

- ASIL considered: ASIL D.
- Description:

  When the non-volatile memory (MTP) is copied to shadow registers upon startup, the contents is checked using an Error Correcting Code (ECC). All data stored in the MTP have ECC (error correction check) bits. If one bit flips, ECC will raise a service request flag to the pack controller via the daisy link and cell impedance measurement and cell balancing is disabled.

  Redundant 6 bits /16bits.
- Allocation to functional block: MTP.

- Fault indication time: 1ms.
- Assumed diagnostic coverage: 99% (ISO 26262-11:2018, 5.1.13.1).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  No self-test feature available.

5.1.1.30 SM31: Finite State Machine bitflip detection

- ASIL considered: ASIL D.
- Description:

  All FSMs in ASIL-D blocks uses special encoding of the states that allow for detection of a bitflip in the state registers. If a bitflip is detected in one of the FSMs, the DNS1168 sends a service request flag to the pack controller via the daisy link and cell impedance measurement and cell balancing is disabled.
- Allocation to functional block: Multiple.
- Fault indication time: 10us.
- Assumed diagnostic coverage: 99%
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  No self-test feature available.

5.1.1.31 SM32: Broken VBAT pin detection

- ASIL considered: ASIL D.
- Description:

  Open VBAT pin will lead to supply current through the VCHx pin ESD diodes. This will reduce cell voltage measurement accuracy and cause EMC issues. By monitoring the voltage over the ESD devices, a broken pin will be detected. The DNB1168 will raise a service request flag and disable cell impedance measurement and cell balancing when a broken VBAT pin is detected.
- Allocation to functional block: Openwiredet.
- Fault indication time: 1ms.
- Assumed diagnostic coverage: 99% (ISO 26262-5:2018, D2.4.4).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  ST32: The Open-wire comparator can be forced to present a flag. It can detect whether the comparator is functional. Self-test is initiated by the pack controller within the LFTTI (e.g. during key-off).

5.1.1.32 SM33: Broken VSS pin detection

- ASIL considered: ASIL D.
- Description:

  Open VSS pin will lead to supply current through the VCLx pin ESD diodes. This will reduce cell voltage measurement accuracy and cause EMC issues. By monitoring the voltage over the ESD

devices, a broken pin can be detected effectively. DNB1168 will raise a service request flag and disable cell impedance measurement and cell balancing when a broken VSS pin is detected.

- Allocation to functional block: Openwiredet.
- Fault indication time: 1ms.
- Assumed diagnostic coverage: 99% (ISO 26262-5:2018, D2.4.4).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  ST33: The Open-wire comparator can be forced to present a flag. It can detect whether the comparator is functional. Self-test is initiated by the pack controller within the LFTTI (e.g. during key-off).

5.1.1.33 SM34: Broken VBAT_FIL pin detection

- ASIL considered: ASIL D.
- Description:

  Open VBAT_FIL pin will result in supply filter not working. This will degrade EMC behavior of the DNB1168 (both emission and immunity). The DNB1168 will raise a service request flag and disable cell impedance measurement and cell balancing when a broken VBAT_FIL pin is detected.
- Allocation to functional block: Openwiredet.
- Fault indication time: 1ms.
- Assumed diagnostic coverage: 99% (ISO 26262-5:2018, D2.4.4).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  ST34: The Open-wire comparator can be forced to present a flag. It can detect whether the comparator is functional and reacts on the intended thresholds. Self-test is initiated by the pack controller within the LFTTI (e.g. during key-off).

5.1.1.34 SM35: Broken communication wire detection for the DIO pins

- ASIL considered: ASIL D.
- Description:

  The DIO pin diagnostics is synchronously demodulating the differential voltage on the DIO pins during the operation of the DIO pins. By monitoring this differential voltage, it is not only detecting open wires, but also short circuits to neighboring pins and short circuits to VBAT and VSS. The DIO diagnostic module works on either the DIOBOT or the DIOTOP, depending on the direction of communication. Broken DIO pins may effectively change the daisy chain bus from differential into a single ended bus, making the communication unreliable. DNB1168 will raise a Service Request flag and disable cell impedance measurement and cell balancing when a broken pin is detected.
- Allocation to functional block: DIO.
- Fault indication time: 1ms.
- Assumed diagnostic coverage: 99% (ISO 26262-5:2018, D2.4.4).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

ST35: The Open-wire comparator can be forced to present a flag. It can detect whether the comparator is functional. Self-test is initiated by the pack controller within the LFTTI (e.g. during key-off).

5.1.1.35 SM39: GPIO1 Diagnostics

- ASIL considered: ASIL D.
- Description:

  The GPIO1 diagnostics monitors the voltage at the GPIO1 when it is configured as an output stage. When the output is not within a certain window, it will send a service request flag to the pack controller via the daisy link.
- Allocation to functional block: GPIO.
- Fault indication time: 1ms.
- Assumed diagnostic coverage: 99% (ISO 26262-5:2018, D2.9.1).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  ST39: The GPIO1 comparator can be forced to present a flag. It can detect whether the comparator is functional. Self-test is initiated by the pack controller within the LFTTI (e.g. during key-off).

5.1.1.36 SM40: GPIO2 Diagnostics

- ASIL considered: ASIL D.
- Description:

  The GPIO2 diagnostics monitors the voltage at the GPIO2 when it is configured as an output stage. Needs to be ASIL D because it is also used to detect a pin fault that impacts the communication interface. When the output is not within a certain window, it will send a service request flag to the pack controller via the daisy link.
- Allocation to functional block: GPIO.
- Fault indication time: 1ms.
- Assumed diagnostic coverage: 99% (ISO 26262-5:2018, D2.9.1).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  ST40: The GPIO2 comparator can be forced to present a flag. It can detect whether the comparator is functional. Self-test is initiated by the pack controller within the LFTTI (e.g. during key-off).

5.1.1.37 SM41: ZM phase control clipping detection

- ASIL considered: ASIL B.
- Description:

  The phase compensation control loop for the MOSFET driver is used during the cell impedance measurement. When the phase control loop is out of range the phase of the impedance is incorrect. This can happen when the drive strength of the MOSFET driver becomes too low. This compensation circuit can control the delay of the MOSFET driver within a certain range. When this range is clipping, a service request will be send to the pack controller via the daisy link.
- Allocation to functional block: ZM processing.

- Fault indication time: 1ms.
- Assumed diagnostic coverage: 60% (ISO 26262-5:2018, D2.4.4).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  No self-test feature available.

5.1.1.38 SM42: Maximum Temperature Detection

- ASIL considered: ASIL D.
- Description:

  The result of the cell temperature measurement is used to detect whether the DNB1168 die temperature is higher than 125°C. If the die temperature goes out of range, a service request flag will be send to the pack controller via the daisy link and cell impedance measurement and cell balancing is disabled.
- Allocation to functional block: DTS processing.
- Fault indication time: 20ms.
- Assumed diagnostic coverage: 60% (ISO 26262-5:2018, D2.1.1).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  No self-test feature available.

5.1.1.39 SM43: Minimum Temperature Detection

- ASIL considered: ASIL D.
- Description:

  The result of the cell temperature measurement is used to detect whether the DNB1168 die temperature is lower than -40°C. If the die temperature goes out of range, a service request flag will be send to the pack controller via the daisy link and cell impedance measurement and cell balancing is disabled.
- Allocation to functional block: DTS processing.
- Fault indication time: 20ms.
- Assumed diagnostic coverage: 60% (ISO 26262-5:2018, D2.1.1).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  No self-test feature available.

5.1.1.40 SM44: Lock key protection for MTP

- ASIL considered: ASIL D.
- Description:

  A comparator is implemented for monitoring whether the pack controller provides the correct lock key before programming the MTP. This serves as a protection against unintended or unauthorized MTP programming. If 15 consecutive MTP write attempts are made with an incorrect key, the MTP

writing is disabled. If an MTP write attempt is made with an incorrect key, the DNB1168 will send a service request flag to the pack controller via the daisy link.

- Allocation to functional block: MTP
- Fault indication time: not applicable.
- Assumed diagnostic coverage: 99% (ISO 26262-5:2018, D2.1.2).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  No self-test feature available.

5.1.1.41 SM45: MTP Write Counter Error Flag

- ASIL considered: ASIL D.
- Description:

  The number of times the non-volatile memory (MTP) is programmed is counted by the MTP program counter. If the MTP program counter exceeds 200, the DNB1168 will send a service request flag to the pack controller via the daisy link. If the MTP program counter exceeds 255, the DNB1168 shall disable writing to the MTP.
- Allocation to functional block: MTP
- Fault indication time: not applicable.
- Assumed diagnostic coverage: 99% (ISO 26262-5:2018, D2.1.2).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  No self-test feature available.

5.1.1.42 SM46: MTP Header Self-Check

- ASIL considered: ASIL D.
- Description:

  For checking the validity of the non-volatile memory (MTP), the first row is written with 16'hAAAA. If the first row in MTP is found to be not equal to 16'hAAAA during read-out of the MTP, the DNB1168 will send a service request flag to the pack controller via the daisy link.
- Allocation to functional block: MTP
- Fault indication time: not applicable.
- Assumed diagnostic coverage: 99% (ISO 26262-11:2018, 5.1.13.3).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  Not applicable.

5.1.1.43 SM47: Test/scan mode entry protection

- ASIL considered: ASIL D.
- Description:

Global test related registers impact the mode of the DNB1168. If these registers would flip unintendedly, the DNB1168 would go into test mode, causing invalid behavior. By making these registers redundant, the DNB1168 is robust against unintended test mode entry.

- Allocation to functional block: Test.
- Fault indication time: not applicable.
- Assumed diagnostic coverage: 90% (ISO 26262-5:2018, D2.4.5).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  No self-test feature available.

5.1.1.44 SM48: TCB/TPR toggling protection

- ASIL considered: ASIL D.
- Description:

  Global test related registers control the multiplexers that switch between functional signals and test registers. If these signals would toggle unintendedly, the test registers would be used to control the modules, instead of the actual functional signals, leading to incorrect behavior. By making the registers for these global signals redundant, they are robust against bitflips.
- Allocation to functional block: Test.
- Fault indication time: not applicable.
- Assumed diagnostic coverage: 90% (ISO 26262-5:2018, D2.4.5).
- Safety Mechanism always active, no triggering by BMS system required.
- Self-test feature:

  No self-test feature available.

5.2 Safety mechanisms external to DNB1168

Captured under Assumptions of Use in Section 6.

6 Assumptions of use and external safety requirements

The following measures, shown in Table 12, are 'Assumptions of Use' (AoU) assumed in the Safety Analysis to be taken by the Battery Management System to avoid faults violating the item safety goals. The AoUs are requirements for the system integrator:

Table 12 : External safety mechanisms (assumptions of use)

ID	External Safety mechanism	Relevant FSR	Supporting SG
SM105	Assumed external system (pack controller) to execute CRC (see 6.2.1)	FSR_5	SG_1, SG_2, SG_3, SG_4.
SM100	Assumed external system (pack controller) to compare redundant battery cell voltage measurements (see 6.3.1)	FSR_1 FSR_2	SG_1, SG_2.

ID	External Safety mechanism	Relevant FSR	Supporting SG
SM101	Assumed external system (pack controller) to compare redundant battery cell temperature measurements (see 6.3.2)	FSR_1 FSR_2	SG_1, SG_2.
SM102	Assumed external system (pack controller) to have a communication timeout monitoring (see 6.2.2)	FSR_5	SG_1, SG_2, SG_3, SG_4.
SM103	Assumed external system (pack controller) to check the ID's in every transaction (see 6.2.3)	FSR_5	SG_1, SG_2, SG_3, SG_4.
SM104	Assumed the external system (pack controller) to inspect error detection information. (see 6.2.4)	FSR_5	SG_1, SG_2, SG_3, SG_4.
SM106	Assumed the external system (pack controller) to confirm that data is correctly written in the MTP (see 6.4)	FSR_5	SG_1, SG_2, SG_3, SG_4.
SM107	Assumed the external system (pack controller) to confirm that data correctly written in the command register (see 6.5)	FSR_5	SG_1, SG_2, SG_3, SG_4.
SM109	Assume external system (pack controller) to compare the temperatures of neighboring logical battery cells (see 6.6)	FSR_1 FSR_2	SG_1, SG_2.
SM110	Assume external system (pack controller) to check temperature increase when internal CDAC is enabled (see 6.7)	FSR_1 FSR_2	SG_1, SG_2.
SM111	Assumed external system (pack controller) to reverse the daisy chain communication direction in case of daisy chain communication fails. (see 6.2.5)	FSR_1 FSR_2 FSR_3 FSR_4	SG_1, SG_2, SG_3, SG_4.
SM112	It is assumed that the connection of the two redundant voltage measurement channels is realized using a 4-wire connection to the battery cell, with sufficient independence from each other and the power connections. (see 6.8)	FSR_1 FSR_2	SG_1, SG_2.
SM113	It is assumed that the maximum voltage difference between the VCL and VSS pins due to the routing on the PCB shall not exceed 10mV (see 6.9)	FSR_1 FSR_2	SG_1, SG_2.
SM114	It is assumed that the external MOSFET shall be the Nexperia PMV28UNEA transistor or equivalent type. (see 6.10)	FSR_3	SG_3
SM108	During Impedance measurement, the pack controller may change the gain_mode setting and will expect the results to remain equal. If the results change by a factor 4 or 16, the external bypass capacitor is defect. (see 6.11)	FSR_3	SG_3
SM115	Assume external system (pack controller) to compare the impedance of neighboring logical battery cells (see 6.12)	FSR_3	SG_3
SM116	Assume external system (pack controller) to execute self-tests (see 6.14)	FSR_1 FSR_2 FSR_3 FSR_4	SG_1, SG_2, SG_3, SG_4
SM117	Assume external system (pack controller) to send SetForcedError at least once every 6 mins.	FSR_4	SG_4

6.1 External hardware interface requirements and measures at system level

In the Battery Management System all DNB1168 devices are hardwired to their cells during assembly, and are connected to each other by means of a daisy chain (see Figure 7).

After initial power-up the DNB1168 moves into Sleep Mode and commands are send by the pack controller to initiate a set up according to the sequence below:

- Enumeration command: assign a unique ID to each DNB1168 in the daisy chain, starting with ID=1 and increasing it by one while moving to the next DNB1168.
- Initialization command: set up all DNB1168 devices.

Communication is initiated by the pack controller by sending commands up the chain to all DNB1168 devices. The DNB1168 will respond by sending confirmations back to the pack controller.

A transaction consists of three parts: Preamble, command, and confirmation. In between transactions there is a bus idle time to separate each individual transaction. All DNB1168 devices will forward the data received by the previous DNB1168 in the chain to the next DNB1168.

A transaction starts with a preamble (consisting of 60 zeros followed by 4 ones). The goal of the preamble is to synchronize the clocks of all the DNB1168 in the chain. Immediately after the preamble, a 32-bit command is sent. After the command, a continuous sequence of ones called the 'confirmation clock' is sent up the chain.

The purpose of the confirmation clock is to maintain a timing reference to keep the oscillators of all DNB1168 devices locked. During the confirmation clock the DNB1168 send back their confirmations to the pack controller.

Immediately after a command is received by a DNB1168, its own confirmation is sent back towards the pack controller. After the 32-bit confirmation has been sent out, the DNB1168 continues to pass through the confirmation received from the previous DNB1168.

6.1.1 Command structure

The 32-bit command structure is summarized in Table 13. It consists of the following fields:

- ID: used to address one or more DNB1168 devices in the chain.
- Command: This corresponds to one of the commands from the register map.
- Payload: This is the payload of the command that selects the parameters of each command, such as the actual mode the IC should transition to, which type of measurement should be returned, etc.
- CRC: The command contains a 4-bit CRC that is calculated over the entire 28-bit command that is in front of it. The polynomial used for the CRC calculation is 0x9 (x4+x+1).

Table 13 : Command structure

Commands (Pack controller to DNB1168)			
Header		Payload	CRC
ID [7:0]	CMD [4:0]	Payload [15:0]	CRC [3:0]

6.1.2 Confirmation structure

The 32-bit confirmation structure is summarized in Table 5. It is similar as the command:

- ID: Here the DNB1168 will insert its own ID. The pack controller is to check whether the confirmations come in with the expected ID.
- Acknowledgement nibble (ACK): this is a set of 4 bits used to reflect the internal status of the DNB1168.
- Payload: In the confirmation, the payload can contain the actual measurement data (in case of a getData command confirmation). If there is no data to return, the payload is copied form the command.
- CRC: The same implementation as for the command (see 6.1.1).

Table 14 : Confirmation structure

Confirmation (DNB1168 to Pack controller)			
Header		Payload	CRC
ID [7:0]	ACK [4:0]	Payload [15:0]	CRC [3:0]

The acknowledgement nibble (ACK) contains 4 bits for which the meaning depends on the context. If ACK [3] bit is not asserted, it means either something was wrong with the received command or something was wrong with the DNB1168 itself and it sends ServiceRequest information (see 4.3.2.1). In all these cases, the command was ignored by this DNB1168 device.

ACK [2] is used to indicate a pending service request (see 4.3.2.1). The command was executed, but it still informs the pack controller that there is an unconfirmed service request. ACK [1:0] are used in confirmations after a GET-command for the Rolling Sample Counter (RSC). The RSC is an overflowing counter that updates every time a new measurement comes available in DNB1168. This allows the pack controller to distinguish unique measurement samples.

SET-commands need to be sent twice within 1 second before they are executed. Furthermore, it is allowed to send GET commands between the 2 SET-commands. This reduces the chance to unintentionally change the register contents of the DNB1168 when a command is corrupted. For SET-commands ACK [1:0] are used to indicate whether the command was executed or not.

6.2 External safety mechanisms for communication

Assumptions on measures taken by the Battery Management System (BMS) pack controller to detect fails in the communication with the chain of DNB1168 devices.

6.2.1 SM105: External system to execute CRC

The pack controller is assumed to calculate a CRC over the contents of each received confirmation. When there is a mismatch with the received CRC (see 6.1.1 and 6.1.2), the pack controller cannot trust the contents of the confirmation.

CRC-4, 0x9 (x^4+x+1), 28 bits data word -> Hamming distance 2

6.2.2 SM102: External system to have a communication timeout monitoring

The pack controller is assumed to have a communication timeout mechanism to detect that the DNB1168 is not able to communicate. This is detected by the pack controller when not receiving a confirmation.

Timeout must be within the FTTI of the Battery Management System.

6.2.3 SM103: External system to check the ID's in every transaction

Each DNB1168 will be assigned an ID code by issuing the enumeration command by the pack controller. This ID is used for all transactions from and to the DNB1168 devices in the chain. See 6.1.1 and 6.1.2

The pack controller is assumed to check whether the values of the DNB1168 ID's are according to the expectations.

6.2.4 SM104: External system to inspect error detection information

The pack controller is assumed to inspect the ACK-nibble (see 6.1.2) of every confirmation from each DNB1168 device in the chain, and check the Rolling Sample Counter, Execution flag, CRC-error flag, Address-error flag and Service Request flag.

Table 15 : acknowledgement nibble specification

ACK [3]	ACK [2]	ACK [1]	ACK [0]	Comment
0	0	0	0	Illegal command (e.g. wrong register). Command was ignored
0	1	X	X	Received command has CRC error and was ignored
0	X	1	X	DNB1168 was not addressed; Command was ignored
0	X	X	1	DNB1168 Service Request. See 4.3.2.1 for details on when and how this confirmation is used. Command was ignored.
1	1	X	0	SET confirmation, command sent for the first time (and hence not executed). Pending Service Request (See 4.3.2.1).
1	1	X	1	SET confirmation, command sent for the second time (and hence executed). Pending Service Request (See 4.3.2.1).
1	0	X	0	SET confirmation, command sent for the first time (and hence not executed).
1	0	X	1	SET confirmation, command sent for the second time (and hence executed).
1	1	RSC [1:0]		GET confirmation. The RSC is the Rolling Sample Counter. Pending Service Request
1	0	RSC [1:0]		GET confirmation. The RSC is the Rolling Sample Counter.

6.2.5 SM111: External system to reverse the daisy chain communication direction

By default, the commands are sent up the chain from the bottom side to the top side of each DNB1168. However, as indicated in Figure 7, there can be a redundant communication path, which means that it is also allowed to send commands from the top side to the bottom side. Each DNB1168 must determine the communication direction upon waking up from Sleep or Standby mode.

The pack controller is assumed to reverse the daisy chain communication direction in case of detected communication fails. E.g. when the number of confirmations is less than the number of DNB1168 devices in the chain.

6.3 External safety mechanisms for redundant measurement comparison

The DNB1168 has 2 separate redundant and independent battery cell voltage and temperature measurement channels: ‘main’ and ‘guard’. If the measurement results of these 2 channels differs by more than 15mV a Service Request flag is raised.

Also, the measurement results of both channels are send to the pack controller. This enables the pack controller to compare the measurements as well, to safeguard against measurement errors.

6.3.1 SM100: External system to compare redundant battery cell voltage

The pack controller is assumed to check at least once within the system FTTI if the difference between the 2 independent voltage samples (‘main’ and ‘guard’) exceeds 15mV, complementary to the internal DNB1168 battery cell voltage comparison.

6.3.2 SM101: External system to compare redundant battery cell temperature

The pack controller is assumed to check at least once within the system FTTI if the difference between the 2 independent cell temperature samples (‘main’ and ‘guard’) exceeds 6K, complementary to the internal DNB1168 battery cell temperature comparison.

6.4 SM106: External system to confirm that data is correctly written in the MTP

The battery cell temperature measurement depends on the correct thermal resistance (Rth_{j-c}) value used for self-heating compensation. The Rth_{j-c} value is programmed into the MTP by the user, and copied into shadow registers at start-up.

The pack controller is assumed to read back the Rth_{j-c} shadow register content after programming to ensure that the MTP programming was successful.

6.5 SM107: External system to confirm that data correctly written in the Command register

If a SET command is not executed correctly, it will not be detected by the CRC since it will also not be updated correctly.

The pack controller is assumed to check the content of the Command register after each SET command using the SetRegBank instruction.

6.6 SM109: External system to compare temperatures of neighboring logical battery cells

It is assumed that the pack controller can detect temperature difference between neighboring battery cells.

The battery cell temperature is derived from the die temperature measurement by compensating for the self-heating of the DNB1168 based on the thermal resistivity towards the battery cell, as programmed in the MTP.

The pack controller shall compare the cell temperatures of neighboring logical cells. If the difference between neighboring cells exceeds a threshold, a problem with the self-heating compensation is detected:

- If case the current consumption of the DNB1168 is not constant/correct and hence the self-heating estimation used for both ‘main’ and ‘guard’ battery cell temperature measurement channels is not correct.
- Incorrect battery cell balance control can lead to unintended enabling of the CDAC, undetected by SM13. This causes incorrect self-heating estimation used for both ‘main’ and ‘guard’ battery cell temperature measurement channels.
- In general, self-heating compensation is not correct.

6.7 SM110: External system to check temperature increase when CDAC is enabled.

Check temperature increase when internal CDAC is enabled. This can confirm that the internal CDAC is sending out the correct and expected current. At the same time, it would also detect something is wrong in case the Rth of the IC is wrong (e.g. due to delamination) and the CDAC is correct

This can confirm that the internal CDAC is sending out the correct and expected current.

If there is CDAC monotonicity error, there is a severe impact on the accuracy of the CDAC, which will impact the capability of measuring the Rth sufficiently accurate in the application. This can reduce the accuracy of the cell temperature measurement. It can be detected by comparing the Rth between individual DNB1168 devices in the battery pack.

6.8 SM112: Connection of the two redundant voltage measurement channel inputs

It is assumed that the connection of the two redundant voltage measurement channels is compatible with the application note with sufficient independent from each other and the power connections, realized using a 4-wire kelvin connection to the battery cell.

Figure 13 demonstrates the approach of connecting the IC to the cell. It is essential to keep the forcing/power current (excitation current) away from the sensing lines. Any form of common impedance between these two lines will result in a measurement error.

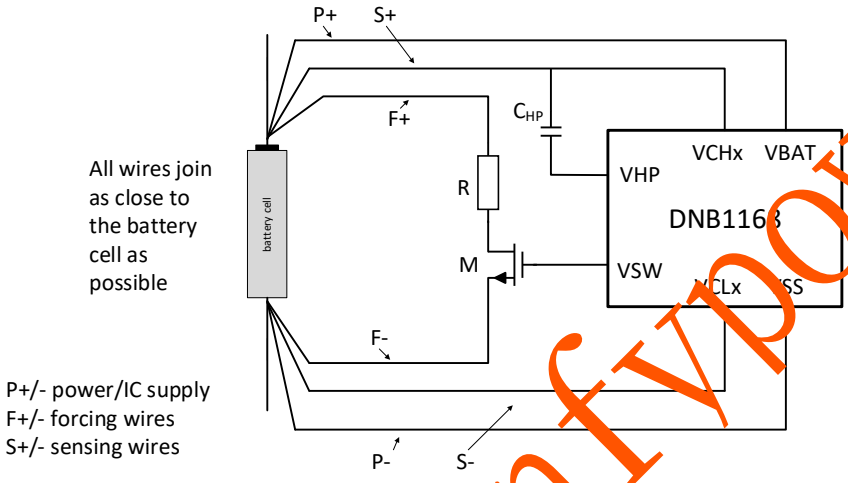

Figure 13: DNB1168 to battery cell wire connection

6.9 SM113: Maximum voltage difference between the VCL and VSS pins

Due to the routing on the PCB, the maximum voltage difference between the VCL and VSS pins shall not exceed 10mV.

6.10 SM114: External MOSFET

The external MOSFET shall be the Nexperia PMV28UNEA transistor or equivalent type.

6.11 SM108: Gain mode setting for impedance measurement.

Open VHP pin means the external bypass capacitor is not connected, effectively reducing the gain to 1 and generating an incorrect ZM result. Can be detected by bypass capacitor check

Between impedance measurements, the pack controller shall change the gain_mode setting and will expect the ZM results to remain equal. If the results change by a factor 4 or 16, the external bypass capacitor is defect. Note that the ZM result may clip during the charging time of the external bypass capacitor after the gain is changed.

6.12 SM117: External system to send SetForcedError at least once every 6 mins

When exteranl MOSFET is in use, it is assumed that pack controller send setForcedError command with VDRcomp =1, G_LDO_dig =1, and G_LDO_pll =1 at least once every 6 mins. if VSW and VDR is shorted, an VDRErr flag will keep low, but G_LDO_Pll and G_LDO_Dig will assert high. If VSW and VDR are not short (connected correctly without fault), VDRErr，G_LDO_Pll and G_LDO_Dig flag all will be high. After getting SR from pack controller, all these SR flag can be cleared by setForcedError command with VDRcomp = 0, G_LDO_dig =0, and G_LDO_pll =0.

6.13 SM115: External system to compare impedance of neighboring logical battery cells

It is assumed that the pack controller can detect impedance difference between neighboring battery cells.

The pack controller shall compare the cell impedances of neighboring logical cells. If the difference between neighboring cells exceeds a threshold, a problem with the impedance measurement accuracy is detected.

6.14 SM116: External system to execute self-test

It is assumed that the pack controller executes the self-test for all DNB1168 devices in the chain at each key-off event, to detect latent faults.

6.15 SM117: External system to send SetForcedError at least once every 6 mins

When external MOSFET is in use, it is assumed that pack controller send SetForcedError command with VDRcomp=1, at least once every 6 mins. If VSW and VDR is shorted, status register CurrDiagnostics[VDRErr] will keep low. If VSW and VDR are not short (connected correctly without fault), status register CurrDiagnostics[VDRErr] will be high. After pack controller getting SR, SR flag can be cleared by SetForcedError command with VDRcomp = 0.

6.16 Combination of Safety Mechanisms

The following Safety Mechanisms are combined to claim a high diagnostic coverage:

Table 16 : Combination of communication Safety Mechanisms

ID	Combination	Safety mechanism	ISO 26262	Diagnostic coverage
Smcomm	SM102 SM103 SM104	Combination of CRC, Counter and timeout	D.2.5.6a D.2.5.7 D.2.5.8	99%
SMvm	SM9 SM100	Combination of internal and external cell voltage comparison	D.2.1.2	99%
Smtemp	SM12 SM101	Combination of internal and external cell temperature comparison	D.2.1.2	99%

6.17 Hardware-software interface

See Hardware-software specification referenced in section 3.1, Table 2 for description of the interfaces required to support the DNB1168 safety mechanisms, and to control failures after detection.

7 Other general recommendations

Based on the assumed FDTI for the voltage measurement in Table 6, it is recommended not to use sample rate >128ms for VM when targeting ASIL-D.

DTS uses self-heating compensation based on the (fixed) supply current of the DNB1168. This supply current will be higher when cell balancing using the internal CDAC is active, resulting in incorrect self-heating compensation for the DTS measurement. It is recommended to first apply balancing on all even cells, while monitoring the temperature of the odd cells. If the temperature of one of the even cells starts to deviate significantly, the odd cells will also register this. After balancing on the even cells is finished, the odd cells are balanced, while the temperature of the even cells is measured.

8 Production related instructions affecting safety

8.1 Mounting the DNB1168

The temperature of the battery cell is calculated based on the die temperature of DNB1168 itself. This principle is possible because each DNB1168 is placed very close to the battery cell it is monitoring and therefore it can have a good thermal connection. This is illustrated in Figure 14.

The DNB1168 is assembled in a package with an exposed die pad, which means there is a good thermal connection (using wide metal only) directly to the die.

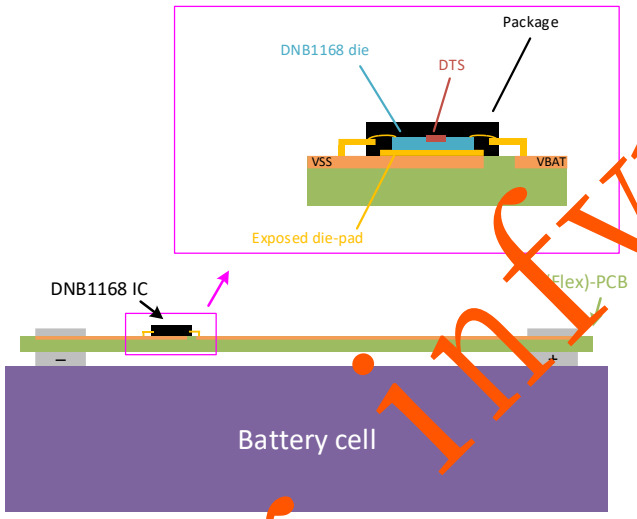

Figure 14: Principle of temperature measurement based on the die temperature of DNB1168

Although the DNB1168 is placed close to the battery with good thermal contact, all the circuits in the DNB1168 consume a (constant) current. Therefore, the internal power dissipation will cause self-heating resulting in a die temperature higher than the battery cell temperature. For an accurate battery cell temperature measurement it is necessary to compensate for this self-heating of the die.

The internal temperature sensors in the DNB1168 will have the same temperature as the exposed die pad. The self-heating is caused by the dissipation of the DNB1168 (Pdis) and the thermal resistance from die pad towards the battery cell (Rth). The temperature difference between the temperature sensors and the battery cell temperature is described as:

$\Delta T = Rth \times Pdis = Rth \times Vbat \times Ibat$

The current consumption of each DNB1168 is trimmed to 15mA. Assuming the Rth is known, the battery cell temperature can be accurately calculated from the die temperature since the cell voltage Vbat is available through the voltage measurement function of the DNB1168.

The Rth can be either estimated or measured in the application by measuring the die temperature increase under two different known values of Pdis. This is accurately achieved by enabling the internal CDAC that allows to increase Ibat with 200mA. This gives the following equation for Rth:

Rth = (Tdie1 – Tdie2) / ((Ibat1 – Ibat2) x Vbat).

Thermal resistance (Rth) between battery cell and DNB1168 is assumed to be typically 45K/W. Since the power consumption of the DNB1168 varies between roughly 30mW and 80mW, the impact of the self-heating is typically a few degrees.

Note that when the internal balancing CDAC is enabled, the assumed value for Ibat is not correct anymore and the cell temperature measurement will therefore not be correct anymore. One way around this problem is to first apply balancing on all even cells, while monitoring the temperature of the odd cells. If the temperature of one of the even cells starts to deviate significantly, the odd cells will also register this. After balancing on the even cells is finished, the odd cells are balanced, while the even cells measure the temperature.

9 Document information

9.1 References

Item	Description		DOC-ID
[1]	ISO 26262-1:2018	Road vehicles — Functional safety — Part 1: Vocabulary	
[2]	ISO 26262-2:2018	Road vehicles — Functional safety — Part 2: Management of functional safety	
[3]	ISO 26262-3:2018	Road vehicles — Functional safety — Part 3: Concept phase	
[4]	ISO 26262-4:2018	Road vehicles — Functional safety — Part 4: Product development at the system level	
[5]	ISO 26262-5:2018	Road vehicles — Functional safety — Part 5: Product development at the hardware level	
[6]	ISO 26262-6:2018	Road vehicles — Functional safety — Part 6: Product development at the software level	
[7]	ISO 26262-7:2018	Road vehicles — Functional safety — Part 7: Production and operation	
[8]	ISO 26262-8:2018	Road vehicles — Functional safety — Part 8: Supporting processes	
[9]	ISO 26262-9:2018	Road vehicles — Functional safety — Part 9: Automotive Safety Integrity Level (ASIL) oriented and safety-oriented analyses	
[10]	ISO 26262-10:2018	Guideline on ISO 26262	
[11]	ISO 26262-11:2018	Guidelines on application of ISO26262 to semiconductors	
[12]	ISO 26262-12:2018	Adaption of ISO26262 for motorcycles	
[13]	IEC/TR 62380	Reliability handbook - Universal model for reliability prediction of electronics components, PCBs and equipment	

9.2 Terms/Acronyms and Definitions

Acronym/ Terms	Definition
ASIL	Automotive Safety Integrity Level
SIL	Safety Integrity Level according to IEC61508
HW	Hardware
Functional Safety	Absence of unreasonable risk due to hazards caused by malfunctioning behaviour of E/E systems
Element	System or part of a system including components, hardware, software, hardware parts, and software units
Fault	Abnormal condition that can cause an element or an item to fail
Systematic fault	Fault whose failure is manifested in a deterministic way that can only be prevented by applying process or design measures
Hardware random fault	A hardware fault with a probabilistic distribution
Failure mode	Manner in which an element fails
Safety measure	activity or technical solution to avoid or control systematic failures and to detect random hardware failures or control random hardware failures, or mitigate their harmful effects
Hardware Architectural Metrics	Metrics for the assessment of the effectiveness of the hardware architecture with respect to safety Note: The single-point fault metric and the latent fault metric are the hardware architectural metrics.
Random Hardware Failure	Failure that can occur unpredictably during the lifetime of a hardware element and that follows a probability distribution

9.3 Abbreviations

BADET	Bus Activity Detector
SEooC	Safety Element out of Context
ASIL	Automotive Safety Integrity Level
FTTI	Fault Tolerant Time Interval
L-FTTI	Latent Fault Tolerant Time Interval
HW	Hardware

SW	Software
AoU	Assumptions of Use
FIT	Failure In Time
IC	Integrated Circuit
DNS	Datang NXP Semiconductors
PI	Project Initiation
PCA	Project Concept Approval
PDA	Project Definition Approval
PPA	Project Planning Approval
TO	Tape Out
CES	Customer Engineering Samples
R	Release
PC	Project Closed
FTA	Fault Tree Analysis
DFA	Dependent Fault Analysis
FMEDA	Failure Modes Effects and Diagnostic Analysis
SG	Safety Goal
FSR	Functional Safety Requirement
TSR	Technical Safety Requirement
TLSR	TopLevel Safety Requirement
HSR	Hardware Safety Requirement
PRD	Product Requirement Definition
ICRS	Integrated Circuit Requirement Specification
IPRS	Intellectual Property Requirement Specification
AMS	Analog Mixed Signal
FMEA	Failure Mode and Effects Analysis
ADC	Analog to Digital Converter
FSM	Finite State Machine
GPIO	General Purpose Input Output
ISR	Internal Reference and Supply
MTP	Multiple Time Programmable memory
ESD	Electro Static Discharge
FLL	Frequency Locked Loop
CDAC	Current Digital to Analog Converter
SPI	Serial Peripheral Interface
BMS	Battery Management System
ECU	Electronic Control Unit
MOSFET	Metal Oxide Semiconductor Field Effect Transistor
CRC	Cyclic Redundancy Check
EIS	Electrochemical Impedance Spectroscopy
AEC	Automotive Electronics Counsel
LDO	Low Drop Out voltage regulator
DCO	Digitally Controlled Oscillator
TCB	Test Control Block
TPR	Test Point Register
FDTI	Fault Detection Time Interval
SPFM	Single Point Fault Metric
LFM	Latent Fault Metric
PMHF	Probabilistic Metric of Hardware Failures
MPFDI	Multiple Point Fault Detection Interval
EV	Electric Vehicles
HEV	Hybrid Electric Vehicles
PHEV	Plug-in Hybrid Electric Vehicles
SR	Service Request
RSC	Rolling Sample Counter
ECC	Error Correcting Code
EMC	Electro Magnetic Compatibility

Legal Information

9.4 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, DATANG NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information.

In no event shall DATANG NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, DATANG NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of DATANG NXP Semiconductors.

Right to make changes — DATANG NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — DATANG NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an DATANG NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. DATANG NXP Semiconductors accepts no liability for inclusion and/or use of DATANG NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. DATANG NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using DATANGNXP Semiconductors products, and DATANG NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the DATANG NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

DATANG NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using DATANG NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). DATANG NXP does not accept any liability in this respect.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from national authorities.

9.5 Trademarks

Notice: All referenced brands, product names, service names and trademarks are property of their respective owners.

10 Index

No index entries found.

11 List of figures

12 List of tables