UM11163

Safety manual for the HB2000

Rev. 6.0 — 12 November 2018 Safety manual

1 Document purpose and scope

1.1 Purpose

This functional safety manual discusses the integration, operation, and use of the HB2000 device in the context of a safety-related system. It is intended to support system engineers in reaching the targeted safety integrity level for the application, using HB2000's available features and any additional diagnostic coverages provided by system hardware or software.

1.2 Scope

The safety manual provides a set of requirements and practices for safe operation of an element, considered in a given context of use. To this end, the safety manual provides necessary assumptions of use and details for the HB2000: ASIL capability, FTTI, technical safety requirements, use cases, etc.

The contents of the functional safety manual are defined by the following:

- Safety context and safety concept, established during the development of the HB2000 IC
- Safety analysis results, including information about element failures and their distribution, failure rate calculations, diagnostic coverages, etc.
- Additional safety measures to be implemented by the integrator to ensure safe operation

1.3 Content

The safety manual includes the following:

- Description of assumptions surrounding the use of the IC (e.g. safety goals, safe state, fault tolerant time interval, etc.)
- Descriptions of the element's safety architecture and functional safety features
- Technical requirements for safety mechanisms within the component
- Technical requirements for safety mechanisms external to the component
- References to supplemental supporting safety documentation
- General information on the HB2000 features and functionality

2 ISO 26262 life cycle and customer responsibility

2.1 Tailored lifecycle description

The HB2000 is a component (a non-system element) in the sense of ISO 26262, comprised of many internal hardware blocks. Therefore, the HB2000 project follows a tailored “Safety Element out of Context” (SEooC) life cycle.

Along with the hardware part, usual documentation (data sheet including electrical parameters) and safety related documentation (safety manual, FMEDA) are provided to parties who integrate the HB2000 into systems.

Figure 1 provides detail of the specific tailoring of the safety life cycle applicable for the HB2000 development.

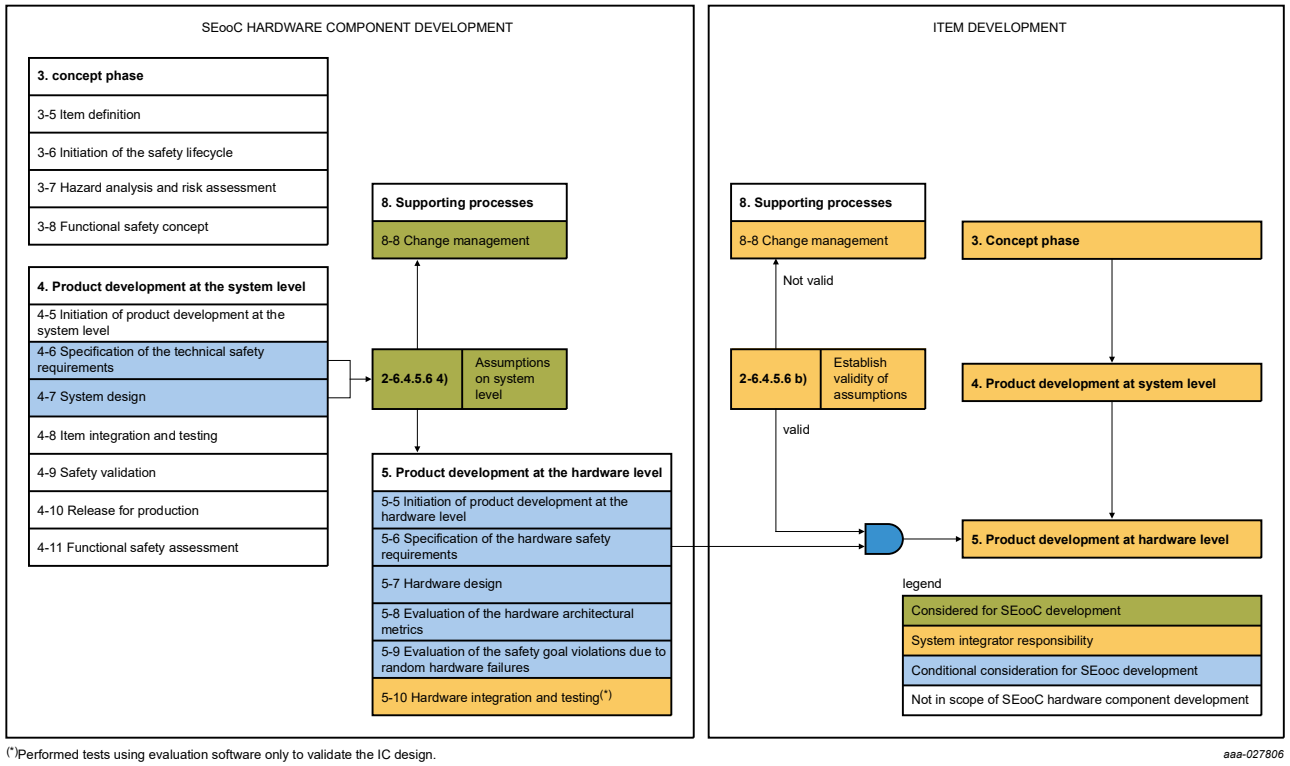

Figure 1. Tailored lifecycle description

2.2 Customer responsibility

In a context of customer applications, this is a list of required customer tasks under the responsibility of that customer. The list is delivered as an example and is not exhaustive. In case of questions, the customer should contact a local NXP representative.

- Use of the latest HB2000 documentation revision (data sheet, safety manual, FMEDA, application notes, errata, etc. per the documentation list provided in Section 2.4 "Supporting documents")
- Other or additional safety requirements might have to be considered depending of the target application and required standard (for example, IEC 61508, IEC 61784, and so on)

- Verify the application mission profile is well covered by the HB2000 devices. See Section 4.5 "Assumed operating conditions".
- Compare system requirements versus HB2000 requirements and make sure there are no deviations
- Establish validity of assumptions at the system level considered in Section 4.4 "System level assumptions"
  - Verify the fault tolerant time interval of the HB2000 is under the system FTTI specified as in Section 4.7 "Assumptions on failure handling"
  - Verify the violation of the HB2000 technical assumptions in Section 4.6.1 "Technical assumptions"
  - Verify the safe state considerations
- Perform safety analysis at the system level, taking into account the safety analysis provided for the HB2000 per the assumptions in Section 4 "Assumptions on use"
- Perform a dependent fault analysis at the system level
- Validate the device and system response as expected in the application, both under normal conditions and in case of error conditions
- Consider and verify single point failures and latent failures at the system level
- Consider and verify systematic errors during development
- Verify the effectiveness of diagnostics at the system level
- Perform fault injection tests and validate safety mechanisms
- The installation of the device at the module level is the responsibility of the customer. However, NXP gives recommendations on NXP packages during printed circuit board (PCB) assembly. This document serves only as a guideline to help users develop a specific solution. Actual experience and development efforts are still required to optimize the assembly process and application design per individual device requirements, industry standards such as IPC and JEDEC, and prevalent practices in the user assembly environment.

2.3 Component safety analysis

In distributed development, the user(s) integrating the NXP component need to perform safety analysis at the application/system level. Under the customer application/system, those results are aggregated with those other elements, components, or subsystems, under the application's safety architecture. The customer's application/system-level safety analysis and metric values are the sole responsibility of the customer, and may be tailored to varying safety integrity levels.

The HB2000 is developed as a "Safety-related Element Out of Context" (SEooC), so some system requirements are not available in detail. Therefore, some assumptions are made regarding the "context of use" of the HB2000. It is assumed the user is generally familiar with both the NXP device and the ISO 26262 standard.

2.4 Supporting documents

The system integrator should utilize the supporting documents in Table 1 mentioned throughout this manual for safe integration of the HB2000 device.

Table 1. List of documents

Document name	Description	Link
ISO 26262	ISO 26262 road vehicles - Functional safety, November 2011	—
HB2000 data sheet	Data sheet: 10 A H-bridge, SPI programmable brushed DC motor driver, latest revision	https://www.nxp.com/docs/en/data-sheet/MC33HB2000.pdf
HB200x safety context	Safety context for HB200x	Contact sales representative
HB200x safety concept	Safety concept for HB200x	Contact sales representative
PFMEA	Pin FMEA for HB200x	Accessible via secure Docstore server
Safety analysis report	HB200x safety analysis summary report	
FTA	Fault tree analysis	
HB200x_Block_DFMEA	Design FMEA for HB200x	
FMEDA	Hardware metrics calculation	
DFA	Dependent fault analysis	
Fault injection report	Fault injection report for HB200x	
PPAP	Production part approval process documentation release for the HB2000, latest revision	Contact sales representative

3 General information

3.1 Applicable part numbers and packages

- HB2000 is a single H-bridge motor driver IC, used in various automotive (throttle, gas valve control) and industrial applications. The complete part number and packaging options are:
- MC33HB2000EK (HSOP-32)
- MC33HB2000FK (HQFN-32)
- MC33HB2000ES (HVQFN-28)

3.2 Product features

The HB2000 has been developed using SMARTMOS monolithic H-bridge power IC, enhanced with SPI configurability and diagnostic capabilities. It is designed primarily for DC motor or servo motor control applications within the specified current and voltage limits.

The HB2000 is able to control inductive loads with peak currents greater than 10 A. The nominal continuous average load current is 3.0 A. A current mirror output provides an analog feedback signal proportional to the load current. This part is designed to specifically address the ISO 26262 safety requirements. Figure 2 shows the functional block diagram of the device.

Features:

- Advanced diagnostic reporting via a serial peripheral interface (SPI): charge pump undervoltage, overvoltage, and undervoltage on VPWR, short to ground and short to VPWR for each output, open load, temperature warning and overtemperature shutdown

- Thermal management: excellent thermal resistance of < 1.0 °C/W between junction and case (exposed pad)
- Eight selectable slew rates via the SPI: 0.25 V/µs to more than 16 V/µs for EMI and thermal performance optimization
- Four selectable current limits via the SPI: 5.4/7.0/8.8/10.7 A covering a wide range of applications
- Can be operated without SPI with default slew rate of 2.0 V/µs and a 7.0 A current limit threshold
- Highly accurate real-time current feedback through a current mirror output signal with less than 5.0 % error
- Drives inductive loads in a full H-bridge or half-bridge configuration
- Overvoltage protection places the load in high-side recirculation (braking) mode with notification in H-bridge mode
- Wide operating range: 5.0 V to 28 V operation
- Low $R_{DS(on)}$ integrated MOSFETs: maximum of 235 mΩ (T_J = 150 °C) for each MOSFET
- Internal protection for overtemperature, undervoltage, and short-circuit by signaling the error condition and disabling the outputs
- I/O pins can withstand up to 36 V

3.3 Functional block diagram

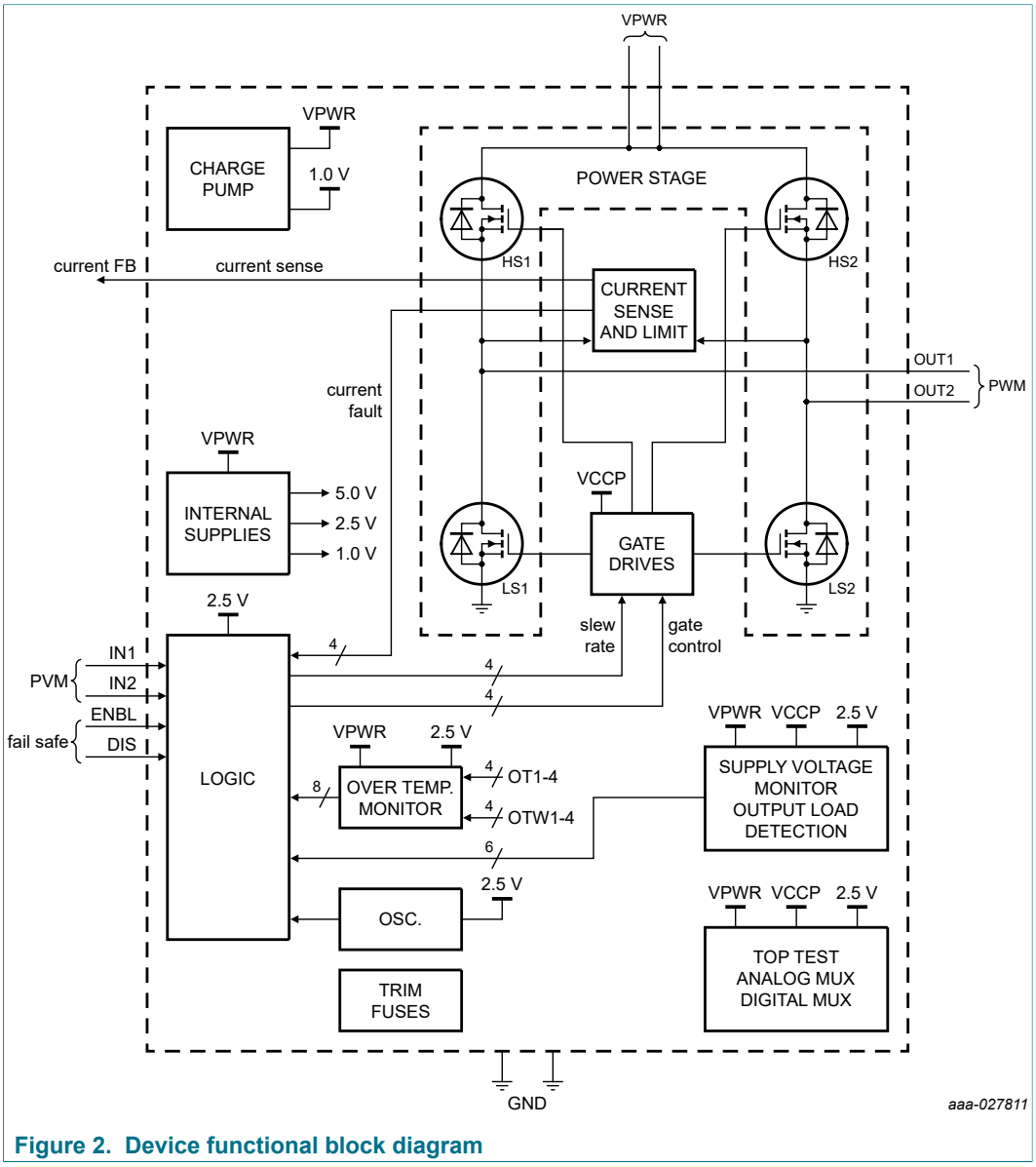

Figure 2. Device functional block diagram

4 Assumptions on use

4.1 Target application

The HB2000 features and safety requirements are derived from the needs of an automotive electronic throttle control (ETC) system. Figure 3 details one possible implementation of the system, which will be used conceptually throughout this manual.

In the application, the HB2000 needs to receive PWM signals and fail-safe control logic as inputs, drive a motor in full-bridge configuration, and report current (analog) and fault indication (digital) to the system MCU.

4.2 Target ASIL

It is assumed herein that the application is required to meet ASIL D safety metrics. The assumed system hazards, system safety goals, and safe states are described in detail in Section 4.3 "System safety goals" (all assumptions).

The device safety concept and safety requirements are discussed in Section 4.6 "Device safety concept and safety requirements".

4.3 System safety goals

SA248: Assumed system safety goals

The HB2000 is targeted for electronic throttle control application. The throttle controls air flow into the engine, controlling engine power output, which ultimately results in drive torque to the wheels. The assumed malfunctions as described below are potentially hazardous events of concern.

SA262: System malfunctions

- SA263: MF01 Loss of position control of the throttle ASIL D
- SA264: MF02 Loss of feedback creating unstable control of the system ASIL B
- SA265: MF03 Unintended acceleration ASIL D
- SA266: MF04 Unintended deceleration ASIL A

The assumed safety goals and their ASIL levels are given in Table 2.

Table 2. Assumed system safety goals

Safety goal	ASIL	Safe state
Maintain stable engine speed control	B	Minimum engine speed
Maintain acceleration control as requested	D	Minimum engine torque

4.4 System level assumptions

SA234: The target application assumed is vehicle engine throttle control system.

SA236: It is assumed that HB2000 is a "Safety-related Element Out Of Context", thus the system requirements are not available in detail. Therefore, some assumptions are done on the "context of use" of the HB2000.

SA237: It is assumed that the position command is translated by the MCU into a PWM command, which is transmitted to the HB2000. The HB2000 returns a current FB, which corresponds to the motor torque. It is assumed that the motor position is input to the MCU via the position feedback. The MCU maintains the motor torque until the position feedback matches the position command.

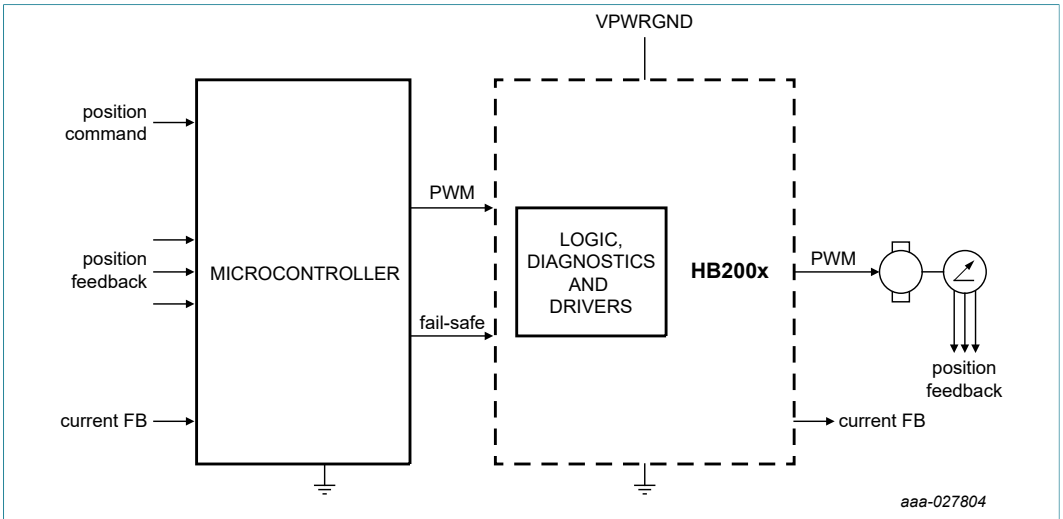

Figure 3. HB2000 interface with microcontroller in the context of safety

SA240: Figure 3 shows an assumed high level implementation of the HB2000 interfacing with the microcontroller in the context of safety.

SA242: Assumed use case is to provide a means of engine speed control during idle, acceleration, and cruising, by providing torque control on the throttle.

SA244: It is assumed that the HB2000 is part of the safety architecture of the vehicle. Based on the assumptions described, the HB2000 will fulfill the following functions within the application. These functions are assumed to be the safety goals on the component level for the HB2000.

SA245: It is assumed that HB2000 is a hardware interface between the MCU and the throttle control motor. It is assumed to provide control signals to the motor as long as the system parameters do not exceed the safe operating window of operation.

SA246: It is assumed that HB2000 will inhibit operation of the throttle control motor when operating conditions exceed the safe operating window of the component and report a warning back to the MCU.

SA247: It is assumed that in case the MCU does not respond to control inputs, fail-safe inputs provided by the HB2000 that allow an external safety hardware to bring the system to a safe state.

SA298: It is assumed that the HB2000 is used in combination with other devices in the application (MCU, other Analog IC), which overlap functionality and diagnostics of the HB2000 to achieve the desired system ASIL goals.

SA511: It is assumed that all ASIL QM(D) goals meet random failure rates compliant with an ASIL D system. All other faults will be covered by system level monitoring and diagnostics.

SA299: It is assumed that there is a spring return mechanism in the throttle control valve to bring it to a closed position upon motor load de-energization.

SA300: It is assumed that there is a position sensor available in the system to feedback the throttle position to the MCU.

4.5 Assumed operating conditions

SA301: It is assumed that the HB2000 is used within a specific mission profile.

SA302: It is assumed that the HB2000 is used in an application for which the mission profile is the following (or less aggressive):

Mission parameters	Mission profile
FTTI	10 ms
Lifetime (T_{life})	10 years
Total operating hours	6000 hours

SA316: Assumed mission profile:

Device type	Ambient temperature (°C)	Percentage of total operating hours (%)
Packaged device	−40	6
	25	21
	58	35
	72	19
	81	10
	95	3
	100	2
	109	2
	125	1

SA359: It is assumed that the HB2000 shall meet all the data sheet specifications after relevant qualification tests (following AEC-Q100 standard) to simulate the above mission profile are completed.

SA360: It is assumed that the qualification tests will cover failures related to degradation of circuits over lifetime.

4.6 Device safety concept and safety requirements

4.6.1 Technical assumptions

SA406: It is assumed that HB2000 is used in automotive applications where fail-safe reaction is expected. The HB2000 is only supporting the system level fail-safe requests.

SA407: It is assumed that HB2000 is used in an application for which the mission profile is previously defined for ambient temperature. The device temperature profile will be derived based on performance defined in the product specification.

SA408: It is assumed that the HB2000 is used in an application for which the battery voltage never exceeds the maximum ratings of the HB2000 (40 V). Above this voltage, the HB2000 run the risk of being destructed and the safety requirements are not satisfied anymore.

SA409: It is assumed that the HB2000 is used in combination with other devices in the application (MCU, other analog IC).

SA410: It is assumed that the number of simultaneous faults is restricted to 1.

SA411: It is assumed that the number of simultaneous pin disconnections (pin lift on the PCB) is restricted to 1.

SA412: It is assumed that the exposed pad of the package cannot be disconnected from the PCB due to its large size.

SA413: It is assumed that the short-circuit between PCB tracks is not considered in the HB2000 (diagnostic, countermeasures).

SA414: It is assumed that external component disconnection is not considered in the HB2000 except for load connection between Out1 and Out2 (diagnostic, countermeasures).

SA415: It is assumed that the voltage and ground signal level integrity is guaranteed by the system.

4.6.2 Device safety goals

Table 3. Device safety goal

Safety goal ID	Safety goal	ASIL	FTTI (ms)	Safe state
SG01	Provide PWM output control as directed by inputs	B(D)	1	Shutdown outputs
SG02	Report load current within system-defined accuracy and response times	QM(D)	1	N/A
SG03	Monitor device system parameters	B(D)	1	Shutdown outputs and report fault to system

4.7 Assumptions on failure handling

Failure handling can be split into two categories:

- Handling of failures on start-up, before enabling the system level safety function (for example, during system initialization). 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.

4.7.1 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 counteraction 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.

- SA286: Fault tolerant time interval for the system is assumed to be 10 ms.
- SA289: The minimum number of random hardware faults causing the loss of correct operation is assumed to be 1.
- SA290: Hardware fault tolerance mechanism (HFT) is assumed to be 0 for the HB2000.

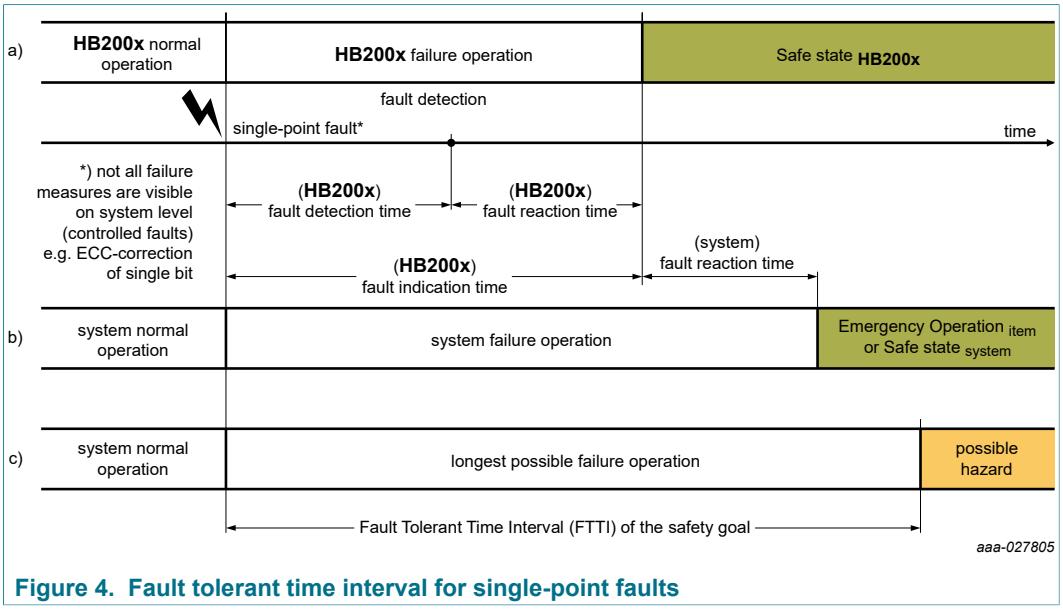

Figure 4. Fault tolerant time interval for single-point faults

Fault indication times for each safety mechanism are listed in Section 5.2.2 "Safety mechanisms".

4.7.2 Fault indication time

Fault indication time is the time it takes from the occurrence of a fault to switching into device safe state (for example, indication of that failure by asserting the fail-safe output pins).

Fault indication time of the HB2000 is the time required to notify an observer about the failure external to the device. This includes the time from detection of the fault in the chip to FS_B going low. It is the time needed to activate fail-safe outputs when the internal command is sent from digital and activates the analog drivers.

SA287: The assumed HB2000 response time interval is less than 1.0 ms.

4.7.3 Multiple point

The multiple point detection interval is the maximum time used for the HB2000 safety analysis.

SA292: A driving cycle or trip time, that is the time of operation of the system without a power-on reset, is assumed to be a maximum of 12 hours. This time is assumed to be the latent fault tolerant time interval (L_FTTI).

SA440: It is assumed that the system always performs a power-up/power-down within the latent fault tolerant time interval.

SA294: It is assumed the multiple point detection interval is less than one drive cycle.

SA295: It is assumed that the HB2000 is used in applications where the maximum "driving cycle" (the time of operation without a power-on reset of the state machine of the HB2000) or trip time is 12 hours.

SA296: It is assumed that for any other driving cycles, the system integrator shall deeply analyze the risks taking into account the inherent behavior of the HB2000.

4.8 Assumed metrics requirements

4.8.1 System architecture metrics requirements

SA362: Safety metrics follow ISO 26262 according to defined ASIL for assumed safety goals.

SA363: The evaluation of the effectiveness of the architecture demonstrates a single-point fault metric (SPFM) rate above 90 % at system level to satisfy ASIL B.

SA364: The evaluation of the effectiveness of the architecture demonstrates a latent fault metric (LFM) rate above 60 % at system level to satisfy ASIL B.

SA365: The evaluation of the effectiveness of the architecture demonstrates a probabilistic metric for random hardware failures (PMHF) rate below 10^{-7} per hour of operation (100 FIT) at system level to satisfy ASIL B.

SA366: The safety metrics from system integration follow ISO 26262 according to defined ASIL for assumed safety goals.

4.8.2 HB2000 component architecture metrics

SA402: Permanent and transient faults are evaluated separately (SPFM LFM evaluated for permanent fault; SPFM evaluated for transient fault).

SA403: The based failure rate for permanent faults has been derived from recognized industry reliability data book like IEC/TR 62380.

SA404: The based failure rate for transient faults shall be derived either from JEDEC standards or measured data on product developed with equivalent technology.

- To meet ASIL B, the architecture shall demonstrate a single point fault metric (SPFM) rate above 90 % at the device level.
- To meet ASIL B, the architecture shall demonstrate a latent fault metric rate (LFM) above 60 % at the device level.
- To meet ASIL B, the architecture shall demonstrate a probabilistic metric for random hardware failures (PMHF) rate below 10^{-7} per hour of operation (100 FIT) at the device level.

5 HB2000 functional safety concept

5.1 Functional safety block diagram

Figure 5 shows the functional safety block diagram of the device.

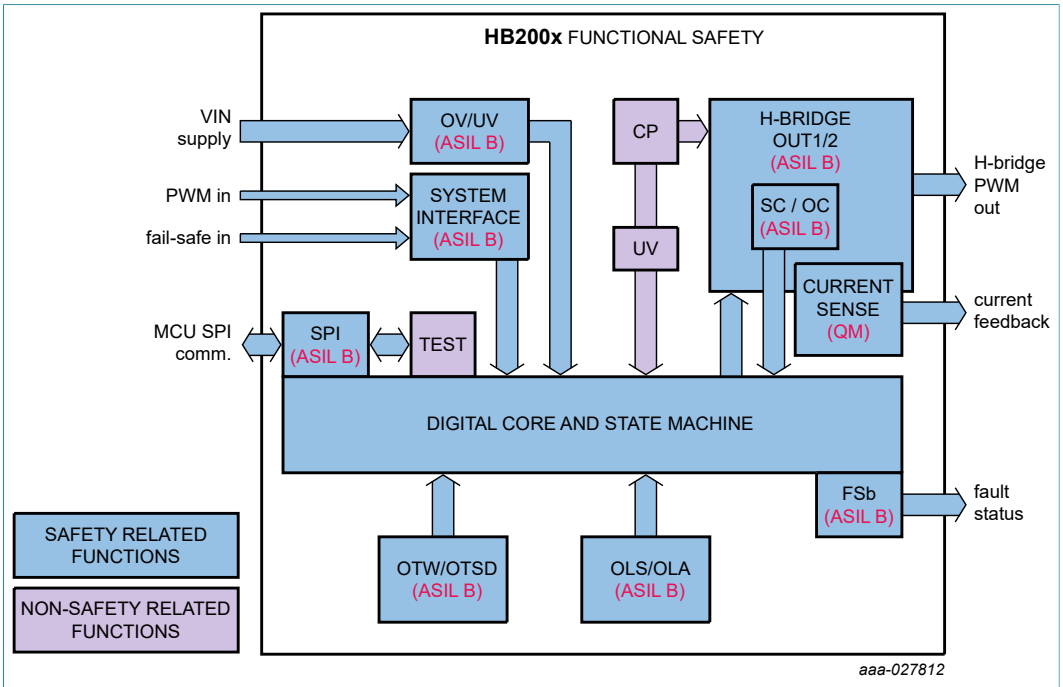

Figure 5. Device functional safety block diagram

5.2 Safety related functions

The functional safety block consists of I/Os, digital logic and monitoring circuits.

The safety block brings and keeps the application in determined safe state based on the criticality of the detected failures.

The safety block allows the application to recover from a safe state when there is no safety critical issue anymore.

The digital core and state machine, SPI, test and FSb blocks have all been included in the FIT calculations for the logic block to support ASIL B.

The status of the safety related features can be read via SPI by reading the associated registers. Such information can be used for diagnosis and servicing failures. This information is continuously available whenever the device is powered.

The HB2000 is defined in a context of safety and provides a set of features to achieve the safety goals on such context.

- VIN OV/UV – input voltage monitoring and protection
  - POR – Power-on reset
- System interface
  - PWM IN (IN1/IN2)
  - Fail-safe IN (ENBL/DIS)
- MCU communication
  - SPI communication with framing
  - SPI secure test mode access
  - Fault status (FSb)
- H-bridge Out1/2 (PWM OUT)
  - Short-circuit/overcurrent

– Current sense
– Open load (OLS/OLA)
– Overtemperature shutdown

5.2.1 Functional block classifications

The blocks in the HB2000 block diagram are classified in Table 4.

Table 4. Functional block classifications

#	Functional block description	Classification	ASIL
A	**Functional blocks**		
A1	**VIN OV/UV – Input voltage monitoring and protection**	**Safety related**	**B**
A1a	POR – Power-on reset	Safety related	B
A2	**System interface**	**Safety related**	**B**
A2.1	PWM IN (IN1/IN2)	Safety related	B
A2.2	Fail-safe IN (ENBL/DIS)	Safety related	B
A3	**MCU communication**	**Safety related**	**B**
A3.1	SPI communication with framing	Safety related	B
A3.2	SPI secure test mode access	Safety related	B
A3.3	Fault status (FSb)	Safety related	B
A4	**H-bridge Out1/2 (PWM OUT)**	**Safety related**	**B**
A4.1	Short-circuit/overcurrent	Safety related	B
A4.2	Current sense	Safety related	QM
A4.3	Open load (OLS/OLA)	Safety related	B
A4.4	Overtemperature shutdown	Safety related	B

5.2.2 Safety mechanisms

All safety mechanisms and their associated diagnostic coverage and fault indication times are listed in Table 5. See FMEDA for diagnostic coverage justification. The complete FMEDA is available for review upon request when covered by an NXP Semiconductors NDA. Please contact your local sales representative.

Table 5. Safety mechanisms

#	Safety mechanism	Functional block allocation	Device safety goal allocation	Fault indication time
SM001	Input voltage undervoltage	Supply voltage monitor/ output voltage monitor	SG03	< 1.0 ms
SM002	Input voltage overvoltage		SG03	< 1.0 ms
SM003	POR (Power-on reset) monitor		SG01, SG03	< 1.0 ms
SM004	Power-up sequence		SG01, SG03	< 1.0 ms
SM005	Detection of Enable (ENBL) and Disable (DIS)	Logic	SG01	< 1.0 ms
SM006	Detection of PWM inputs (IN1 and IN2)		SG01	< 1.0 ms
SM007	SPI communication with framing		SG01, SG03	< 1.0 ms
SM008	SPI secure test mode access		SG03	< 1.0 ms
SM009	Fault status output (FSb)		SG03	< 0.5 ms
SM010	Short-circuit protection	Current sense and limit	SG01, SG03	< 1.0 ms
SM011	Overcurrent protection		SG02, SG03	< 1.0 ms
SM012	Current sense		SG01, SG03	< 1.0 ms
SM013	Open load detection	Logic	SG03	< 0.5 ms
SM014	Thermal monitor interrupts and Shutdown	Overtemperature monitor	SG01, SG03	< 1.0 ms
SM015	Pin level redundancy	Pads	SG01, SG02, SG03	—
SM016	Signal integrity (EMI)	Common	SG01	—
SM017	Must be detected externally	External	SG01, SG02, SG03	—
SM018	MCU verification of communication	External	SG01, SG03	—

5.3 Technical safety requirements (TSR)

5.3.1 Input over/undervoltage protection block

5.3.1.1 Technical safety requirements for input over/undervoltage protection

Table 6 shows technical safety requirements with unique IDs and corresponding ASIL.

Table 6. Safety requirements for input over/undervoltage protection

Ref. #	Technical safety requirement
SAF545	The HB2000 will monitor input voltage out of range.
SAF546	The HB2000 will report input voltage under the operating range.
SAF547	The HB2000 will report input voltage over (exceeding) the operating range.

5.3.1.1.1 Rationale for safety

The HB2000 voltage range is defined to maintain normal control of the outputs. When the input voltage range is exceeded, there is a high risk of loss of control of the load. When the voltage is too high, the output drivers could break down resulting in an inadvertent energizing or loss of control of the output. When the voltage is too low, there is a risk of loss of control of the logic that controls the outputs. The undervoltage condition is

considered to be more likely and much more critical for normal operation, because it directly impacts logic control of the outputs.

5.3.1.1.2 Entering the safe state

The system safe state is reached through various safety measures:

- Detection of input undervoltage is implemented with an independent undervoltage comparator.
  - The undervoltage fault is reported by SPI register.
  - An undervoltage condition will bring the outputs to safe state (outputs turned off).
- Detection of input overvoltage is implemented with a single comparator function.
  - The overvoltage fault is reported by SPI register.
  - An overvoltage condition will bring outputs to the modified safe state (load is turned off, but high-side output FETs are on).

5.3.1.1.3 Exiting the safe state

The device will exit the safe state when a fault is no longer present with no MCU intervention.

The fault indication may be cleared by the MCU after the fault condition is no longer present.

When the HB2000 is programmed to shut down upon a VIN OVLO condition, VIN returning to the operational voltage range will allow the device to return to normal operation.

5.3.1.2 Technical safety requirements for POR (power-on reset) monitor

Table 7 shows technical safety requirements with unique IDs and corresponding ASIL.

Table 7. Safety requirements for POR monitor

Ref. #	Technical safety requirement
SAF563	The HB2000 will continuously monitor the internal analog and digital voltage regulators, independently of the regulator references.
SAF564	The HB2000 will prevent any logic or output operation when either regulator output voltage is less than the POR threshold.

5.3.1.2.1 Rationale for safety

This is an undervoltage monitoring mechanism independent of the UV monitor. In the event of a faulty OV/UV monitoring block, the device may lose the ability to detect an OV/UV fault condition during normal operation. The POR monitor prevents catastrophic loss of logic control when the regulator output reaches a state that cannot reliably maintain control. Placing a POR on both logic regulator and the analog regulator provides a safe redundancy for detection with completely independent circuits, which permits an ASIL B rating. The POR in conjunction with the UV monitor comprise an ASIL B under voltage protection because they operate independently from each other. The POR threshold will be reached at a lower input voltage than UV monitor threshold, but is still high enough to ensure that logical control of the outputs is not compromised.

5.3.1.2.2 Entering the safe state

In the event a POR condition is detected, the logic shall be placed in a reset condition, preventing the device from leaving the safe state.

5.3.1.2.3 Exiting the safe state

When the POR condition clears, the logic begins the normal power-on sequence from a reset condition. If the normal power-on sequence cannot be completed, the system will not be allowed to enter normal operation.

5.3.1.3 Technical safety requirements for power-up sequence

Table 8 shows technical safety requirements with unique IDs and corresponding ASIL.

Table 8. Safety requirements for power-up sequence

Ref. #	Technical safety requirement
SAF790	The HB2000 will perform a specific power on sequence prior to accepting input control signals on IN1 and IN2.

5.3.1.3.1 Rationale for safety

A power-on sequence ensures that latent faults will not compromise the device performance. Should the sequence not be completed, the outputs will remain disabled, preventing operation that does not meet specification.

5.3.1.3.2 Entering the safe state

The HB2000 does not enter the safe state, because it is already in the safe state.

5.3.1.3.3 Exiting the safe state

The HB2000 exits the safe state when the power-on sequence is properly completed.

5.3.2 System interface

5.3.2.1 Technical safety requirements for detection of Enable (ENBL) and Disable (DIS)

Table 9 shows technical safety requirements with unique IDs and corresponding ASIL.

Table 9. Safety requirements for detection of ENBL and DIS

Ref. #	Technical safety requirement
SAF574	The HB2000 has two logic level input pins to enable normal function, the logic input levels must be ENBL as logic high and DIS as logic low for the HB2000 outputs to function.

5.3.2.1.1 Rationale for safety

The ENBL pin in the HB2000 is assumed to be connected to an output from the MCU or a secondary safety processor independent of the processor connected to DIS. The DIS pin in the HB2000 is assumed to be connected to an output from the MCU or a secondary safety processor independent of the processor connected to ENBL. The ENBL pin is assumed to be held at logic high by the MCU or processor as long as its software continues to operate normally. The DIS pin is assumed to be held at logic low by the MCU or processor as long as its software continues to operate normally. The

MCU and a secondary safety processor are assumed to have checks and balances. The process indicates when control of the load is normal and when the control is not following the expected input controls, requiring an external shutdown. This external shutdown is accomplished via the ENBL and/or DIS pins in the HB2000.

5.3.2.1.2 Entering the safe state

Assume in the event of a software and/or hardware issue, the MCU or processor shall pull down the ENBL input in HB2000. When the ENBL is pulled low, a safe state is reached by bringing the outputs to a default known state. Assume in the event of a software and/or hardware issue, the MCU or processor shall pull up the DIS input in HB2000. When the DIS is pulled high, a safe state is reached by bringing the outputs to a default known state. The ENBL and DIS act independently of each other when asserted.

5.3.2.1.3 Exiting the safe state

The device gets out of the safe state when the MCU clears the condition and enables the device.

5.3.2.2 Technical safety requirements for detection of PWM inputs (IN1 and IN2)

Table 10 shows technical safety requirements with unique IDs and corresponding ASIL.

Table 10. Safety requirements for detection of PWM Inputs (IN1 and IN2)

Ref. #	Technical safety requirement
SAF591	The HB2000 will monitor PWM input pins (IN1 and IN2) logic level thresholds to control the outputs.

5.3.2.2.1 Rationale for safety

It is assumed, the MCU is responsible to maintain the IN1 and IN2 inputs in the normal logic level input range. It is assumed, the system model has an external return mechanism that drives the load to a safe state when de-energized. It is assumed the reverse direction on the load will aid returning the load to the system safe state. When the HB2000 input pin IN1 and IN2 random failure rate is at this low level, the outputs will be controlled reliably as commanded from the MCU.

5.3.2.2.2 Entering the safe state

The HB2000 only supports the system safe state control. The system enters the safe state as a result of the default reaction to the input controls in combination with the external system design. In case IN2 fails as an open circuit, the output will be unpowered in high-side recirculation mode. This is a safe state.

5.3.2.2.3 Exiting the safe state

The device gets out of the safe state based on MCU when normal input control is restored.

5.3.3 MCU communication

5.3.3.1 Technical safety requirements for SPI communication with framing

Table 11 shows technical safety requirements with unique IDs and corresponding ASIL.

Table 11. Safety requirements for SPI communication with framing

Ref. #	Technical safety requirement
SAF781	Communication of device configuration and fault detection status shall be a function of the SPI registers.
SAF604	In order to avoid erroneous information transmitted through the SPI bus, all data must match the bit length of the SPI interface.

5.3.3.1.1 Rationale for safety

Erroneous configuration of the registers can lead to unintended clearing of faults or changes in the device configuration. These changes can degrade system performance, or result in incorrect or hazardous system recovery conditions. Having readable SPI registers provides assurance that the SPI communication link is not faulted. This condition also ensures that the commanded settings were properly sent and received. The framing of the data is used to ensure the data transmitted is not corrupted by either dropped or inserted bits. Detailed fault information obtained from the SPI status register enables the MCU and system to respond properly to the fault condition. Clearing the SPI fault codes in the status register provides indication when fault modes have been removed and permits the MCU to recover from the fault condition.

5.3.3.1.2 Entering the safe state

When an erroneous SPI transaction is detected, discard the data received. A status bit shall be set to announce that there has been an erroneous SPI transaction. Follow the MCU for corrective actions.

5.3.3.1.3 Exiting the safe state

Follow the MCU commands. MCU clears the status bit.

5.3.3.2 Technical safety requirements for SPI secure test mode access

Table 12 shows technical safety requirements with unique IDs and corresponding ASIL.

Table 12. Safety requirements for SPI secure test mode access

Ref. #	Technical safety requirement
SAF617	To prevent unintended access to the HB2000 test registers, a secure write feature shall be provided for access to test mode registers.

5.3.3.2.1 Rationale for safety

A communication error may erroneously request entering a test mode, disabling one or more safety functions during the normal operation. To prevent this from happening, test mode registers require the MCU to confirm the validity of the command to enter test mode.

5.3.3.2.2 Entering the safe state

Ignore all incorrect attempts to access the test mode.

5.3.3.3 Technical safety requirements for fault status output (FSb)

Table 13 shows technical safety requirements with unique IDs and corresponding ASIL.

Table 13. Safety requirements for fault status output (FSb)

Ref. #	Technical safety requirement
SAF623	It is assumed the system requires a safety signal to disable or trigger a specific behavior during a safety fault.
SAF624	The HB2000 will provide indication via the fault status output (FSb) to the MCU when in the standby mode.
SAF625	The HB2000 will provide indication via the fault status output (FSb) to the MCU, which indicates a normal power up sequence.
SAF626	The fault status output (FSb) will be programmable by the MCU to assert when one or more specific fault conditions occurs.
SAF627	The HB2000 will provide information about the type of event that caused the FSb to be asserted.

5.3.3.3.1 Rationale for safety

The HB2000 does not have any safety related responsibility, it is only supporting MCU and system level safety functions. A hardware feedback status pin is useful to communicate to the MCU that a normal power-up sequence has been initiated and when the device is ready to begin normal operation. It is also useful to indicate the device is in the standby mode (DIS asserted), especially when a separate safety circuit is responsible for operating the DIS pin. The use of the Fault Status pin as a fault indicator permits critical faults to generate an interrupt for the MCU, which could reduce the fault response time. During power-up (when ENBL transitions to high), the FSb pin is asserted until all supplies are in normal operating range and DIS is deasserted.

5.3.4 H-bridge Out1/2 (PWM OUT) protection

The H-bridge output is the main function output for the device. There are no direct monitors to verify normal operation, but there are several support functions to verify proper operation of the load.

5.3.4.1 Technical safety requirements for short-circuit/overcurrent protection

Table 14 shows technical safety requirements with unique IDs and corresponding ASIL.

Table 14. Safety requirements for short-circuit/overcurrent protection

Ref. #	Technical safety requirement
SAF637	In the event the current exceeds an overcurrent threshold, the device will report an overcurrent condition.
SAF638	In the event the current exceeds a short-circuit threshold, the device will report a short-circuit condition and turn off the outputs.
SAF639	Short-circuit fault detection reports shall indicate if the fault is to GND or to VPWR.

5.3.4.1.1 Rationale for safety

The HB2000 monitors the forward current through each output FET. An overcurrent condition does not by itself indicate a safety violation. It needs to be reported to allow the MCU to make the system level decision for appropriate action. As current increases, the first threshold to be exceeded is the current limit threshold. This threshold level notifies the MCU through the status register that the threshold has been exceeded and attempts

to perform a PWM-based current regulation. The current sensing for the current limit function is part of the high-side MOSFETs of the H-bridge and is also used as the high-side short-circuit detector, however, the comparator and logic circuits are separate. The short-circuit threshold is set at a higher current than the current limit threshold, so the two step threshold provides redundant and graduated protection against high current levels. If the short-circuit threshold is exceeded, it is an immediate indication of a loss of control of the load. Because two MOSFETs are in series with the load with independent short circuit sensors on each MOSFET, there is a redundancy of protection that elevates the level of protection for shorted load to ASIL B. The additional diagnostic, which identifies if the short-circuit is to GND or to VPWR provides the MCU with information that may be helpful in fault mitigation. Since there is only one sensor for short to GND and one for short to VPWR per output, the direction diagnostic and short to VPWR/GND per output is ASIL A(D).

5.3.4.1.2 Entering the safe state

When an overcurrent threshold is exceeded, the device will notify the system and enter the current limit mode of protection unless disabled by the MCU, within FTTI. When a short-circuit condition is present, an interrupt is sent to the system and the device will automatically turn off the H-bridge within 100 µs.

5.3.4.1.3 Exiting the safe state

When the overcurrent condition is no longer present, the device continues to operate normally with no intervention. However, the MCU is responsible to clear the overcurrent status bit. When a short-circuit interrupt is sent, the MCU is in responsible to clear the interrupt and take action to prevent any system damage.

5.3.4.2 Technical safety requirements for current sense

Table 15 shows technical safety requirements with unique IDs and corresponding ASIL.

Table 15. Safety requirements for current sense

Ref. #	Technical safety requirement
SAF654	The HB2000 provides an output that is a scaled current proportional to the current through the H-bridge high side MOSFETs. The current sensing shall be independent of the current sensing for overcurrent and short-circuit.

5.3.4.2.1 Rationale for safety

The current sensed current output is used as a feedback signal to the MCU. This is an independent means of verifying and controlling the current through the load. With the intelligence in the MCU, this is a primary means of detecting the load response to the input control signals. Keeping this output sense mechanism separate from the overcurrent and short-circuit sense ensures a fault in one sense circuit and will not compromise the entire system. It is only required to meet hardware random failure rate to ASIL B because all response and diagnostic is provided by the MCU.

5.3.4.2.2 Entering the safe state

The device does not have any direct response to the current sense output. The MCU is responsible for making decisions and responding with safe state control as needed.

5.3.4.2.3 Exiting the safe state

The MCU is responsible for making decisions determining when safe state control is no longer needed.

5.3.4.3 Technical safety requirements for open load detection

Table 16 shows technical safety requirements with unique IDs and corresponding ASIL.

Table 16. Safety requirements for open load detection

Ref. #	Technical safety requirement
SAF663	The HB2000 provides detection of an open load on demand in the Standby mode to the MCU.
SAF664	The HB2000 provides detection of an open load during normal PWM activity in the normal mode to the MCU.
SAF665	The HB2000 Standby mode open load detection and normal mode open load detection function independently of each other.
SAF666	The HB2000 provides a single common status response to the MCU indicating the presence or absence of the load as detected shall meet the required random failure rate.

5.3.4.3.1 Rationale for safety

The information about the presence of the load provides an early indicator to the MCU of the ability to respond to system requirements. This improves the ability of the system to anticipate and react safely. The standby detection and active PWM Normal mode detection are independent of each other and so comprise a redundant detection. The detection is independent to prevent interference. The single status reporting is the logical OR of the output of the two detectors meeting the requirements for ASIL B. This performs a redundant detection of load to the MCU.

5.3.4.3.2 Entering the safe state

The device does not have any direct response to the open load output. The MCU is responsible for making decisions and responding with safe state control as needed.

5.3.4.3.3 Exiting the safe state

The MCU is responsible for making decisions determining when safe state control is no longer needed. Open load status, which is detected in the standby mode, is cleared by the MCU. Open load status, which is detected during normal operation, is cleared by normal operation with the load attached or by the MCU.

5.3.4.4 Technical safety requirements for thermal monitor interrupts and shutdown

Table 17 shows technical safety requirements with unique IDs and corresponding ASIL.

Table 17. Safety requirements for thermal monitor interrupts and shutdown

Ref. #	Technical safety requirement
SAF676	A temperature threshold is provided at 150 °C.
SAF677	As the temperature rises, the HB2000 provides a thermal status, announcing the event to the system.

Ref. #	Technical safety requirement
SAF678	A 12 °C hysteresis is provided on the temperature threshold during the falling temperature.
SAF679	A thermal shutdown threshold is provided at 175 °C.
SAF680	When the junction temperature reaches the thermal shutdown threshold, the device initiates a thermal shutdown.
SAF681	The thermal shutdown operates independent of the logic state machine.

5.3.4.4.1 Rationale for safety

The system is designed to operate within a maximum junction temperature range of −40 °C to 150 °C. Operating outside of this range may cause reliability issues on the internal blocks and the system itself. Separating the shutdown response from the state machine ensures that even in the event the state machine becomes unresponsive, the thermal shutdown will perform properly preserving system safety. By providing independent thermal warning and shutdown sensors in each output FET means that the thermal warning and thermal shutdown are redundant, satisfying a functional safety level ASIL B.

5.3.4.4.2 Entering the safe state

Thermal interrupts are provided to detect and report excessive temperature rise in the system, if this condition is not properly addressed by the system, the HB2000 takes action to prevent system damage.

5.3.4.4.3 Exiting the safe state

Clear the source creating the thermal condition. A thermal threshold crossed is cleared with a 12 °C hysteresis on the falling temperature. When a thermal shutdown is reached, the device shall not regain operation until a 12 °C hysteresis is reached on the falling temperature.

5.3.5 Common blocks and safety mechanisms

5.3.5.1 Technical safety requirements for pin level redundancy

Table 18 shows technical safety requirements with unique IDs and corresponding ASIL.

Table 18. Safety requirements for pin level redundancy

Ref. #	Technical Safety Requirement
SAF776	HB2000 has redundant power and ground pin connections.

5.3.5.1.1 Rationale for safety

The power and ground are required for the device to be able to perform all functions. Multiple connections to ground and power are required to ensure that a single open pin fault does not compromise all device functions. This enables the system level functional safety to be increased more easily.

5.3.5.1.2 Entering the safe state

There is no safe state associated with this mechanism, because it is entirely passive in nature.

5.3.5.2 Technical safety requirements for signal integrity (EMI)

Table 19 shows technical safety requirements with unique IDs and corresponding ASIL.

Table 19. Safety requirements for signal integrity (EMI)

Ref. #	Technical safety requirement
SAF784	To control systematic faults, the design possesses features that make the component tolerant against environmental stresses including electromagnetic disturbances.

5.3.5.2.1 Rationale for safety

The system is designed to operate in an environment that can interfere with proper operation of sensitive electronic circuits. By providing designs that can be operated within the standards established for this environment, continued accurate control of the load and reporting of the load behavior is ensured. Exceeding the EMI/EMC environment specified in the standards can result in behavior which is beyond the ability of this device to predict or protect against. This requirement includes the filtering necessary to eliminate sporadic false responses.

5.3.5.2.2 Entering the safe state

There is no safe state associated with this mechanism. This is because it is an environmental constraint on the design, which is not the responsibility of this device to detect.

5.3.5.3 PMHF requirement

Table 20 shows technical safety requirements with unique IDs and corresponding ASIL.

Table 20. PMHF requirement

Ref. #	Technical safety requirement
SAF526	All safety related functions and blocks are designed to preserve the PMHF calculations for all safety goals at less than 3.0 FIT.

5.3.5.3.1 Rationale for safety

The PMHF calculation must support the assumed system level goal of ASIL D. This defines the worst case contribution the HB2000 will make to the overall system FIT.

5.3.5.3.2 Entering the safe state

This is a general requirement for all safety mechanisms. Entering and leaving safe states is defined by each of the individual safety mechanisms.

5.3.5.4 Response times

Table 21 shows technical safety requirements with unique IDs and corresponding ASIL.

Table 21. Safety requirements for response times

Ref. #	Technical safety requirement
SAF804	All diagnostic safety mechanisms will diagnose and report in less than 0.5 ms.

5.3.5.4.1 Rationale for safety

Diagnostic detection and reporting at less than 0.5 ms keeps an internal margin of 0.5 ms for the response, which places the device into the designated safe state. This preserves the 1.0 ms total response time indicated in the device safety goals.

5.3.5.4.2 Entering the safe state

All safety mechanism responses shall enter designated safe states in less than 0.5 ms.

5.3.5.4.3 Exiting the safe state

There is no timing requirement for leaving safe state.

5.3.5.5 Technical safety requirements (TSR) mapping to safety mechanism and device safety goal mapping

Table 22 shows mapping of technical safety requirements to safety mechanisms and device level safety goals.

Table 22. Technical safety requirements mapping to safety mechanism and device safety goals

Safety mechanism ID	Safety mechanism	Mapping to TSR ID
SM001	Input voltage undervoltage	SAF545,SAF546
SM002	Input voltage overvoltage	SAF545,SAF547
SM003	POR (power-on reset) monitor	SAF563,SAF564
SM004	Power up sequence	SAF790
SM005	Detection of enable (ENBL) and disable (DIS)	SAF574
SM006	Detection of PWM inputs (IN1 and IN2)	SAF591
SM007	SPI communication with framing	SAF604,SAF781
SM008	SPI secure test mode access	SAF617
SM009	Fault status output (FSb)	SAF623,SAF624,SAF625,SAF626,SAF627
SM010	Short-circuit protection	SAF638
SM011	Overcurrent protection	SAF637
SM012	Current sense	SAF654
SM013	Openload detection	SAF663,SAF664,SAF665,SAF666
SM014	Thermal monitor interrupts and shutdown	SAF676,SAF677,SAF678,SAF679,SAF680 ,SAF681
SM015	Pin level redundancy	SAF776
SM016	Signal integrity (EMI)	SAF617
SM017	External sensors and analysis of indirect effects	
SM018	External MCU verification of communication	

5.3.5.6 Failure modes requiring external safety mechanisms

Safety mechanisms are allocated to the failure modes to prevent a failure from violating a safety goal. An independent failure of a block other than the block considered in the failure mode may cause violation of one or more safety goals. In some failure modes,

external safety mechanisms (outside the device) may be required to prevent such failures from being latent. The following table lists these failure modes with some hints regarding the type of external safety mechanism required to cover latent failures.

Table 23. Failure modes requiring external safety mechanisms

Failure Mode ID	Block	Failure mode	SG01 Violation	SG02 Violation	SG03 Violation
FM012	Current Sense & Limit	Current limit too low	Yes	No	Yes
FM013	Current Sense & Limit	Sense current too high	No	Yes	No
FM014	Current Sense & Limit	Sense current too low	No	Yes	No
FM016	Gate Drives	Gate driver stuck off (gate drive low)	Yes	No	No
FM024	Logic	Input control malfunction as IN1 high	Yes	No	No
FM025	Logic	Input control malfunction as IN1 low	Yes	No	No
FM026	Logic	Input control malfunction as IN2 high	Yes	No	No
FM027	Logic	Input control malfunction as IN2 low	Yes	No	No
FM034	Logic	SPI message corrupt interpretation no input control	No	No	Yes
FM035	Logic	SPI message corrupt interpretation of input control	Yes	No	Yes
FM072	Pads	CFB stuck high	No	Yes	No
FM073	Pads	CFB stuck low	No	Yes	No

6 Hardware safety analysis results

A comprehensive summary of the hardware safety analysis results (available under NDA via the link in Section 2.4 "Supporting documents") are given in the HB200x safety analysis report, overviewing the items below:

- Fault tree analysis (FTA)
- Design FMEA (DFMEA)
- Pin FMEA (PFMEA)
- Dependent failure analysis (DFA)
- Failure rate (FIT) evaluation
- FMEDA
- Fault injection testing

The product described by the component data sheet have been developed as a Safety Element Out of Context. Design and architecture of the products are based on the design and architecture of similar well-trusted designs. The developers are not able to predict the complete scope of the possible application(s) at the system level.

7 Safe integration requirements

7.1 Safe integration requirements

- Comply with HB2000's absolute maximum ratings specifications
- Protect HB2000 from radiated and conducted EMI
- Protect HB2000 from ESD (IEC, HBM, CDM, ESD gun, etc.) events beyond specifications

- Protect HB2000 from environmental stresses (thermal, moisture, etc.)
- Program HB2000 with SPI register values that permit appropriate protection and operating conditions for the motor
- Provide appropriate external capacitor to ensure proper operation of the HB2000 charge pump
- Provide appropriately stable supply for VDDQ, and MCU shall monitor the integrity of this supply
- Provide appropriate resistor for CFB pin, and MCU shall monitor the current feedback
- System MCU to monitor the FS_B pin and manage faults reported over SPI
- System MCU shall check incoming SPI messages for CRC and/or framing errors, and monitor the FS_B pin for outgoing SPI errors

7.2 Recommendations

Recommendation 1: It is recommended to use good programing practices incorporating writes to SPI registers, immediately verified by reads to the registers.

Rationale: This will ensure a reliable communication between MCU and HB2000. MCU is responsible for detecting any malfunction in the communication that may come up due to hardware or software failure. For example, MOSI shorted to power or VDD rail is detectable by reading the status of any SPI register. The read operation will take about 34 SPI clock cycles as shown in the diagram below. Considering a slow SPI clock of 10kHz (although the maximum clock is 10 MHz) the time elapsed is 3.4 ms, which is well within the system Fault Tolerant Time Interval (FTTI) of 10 ms.

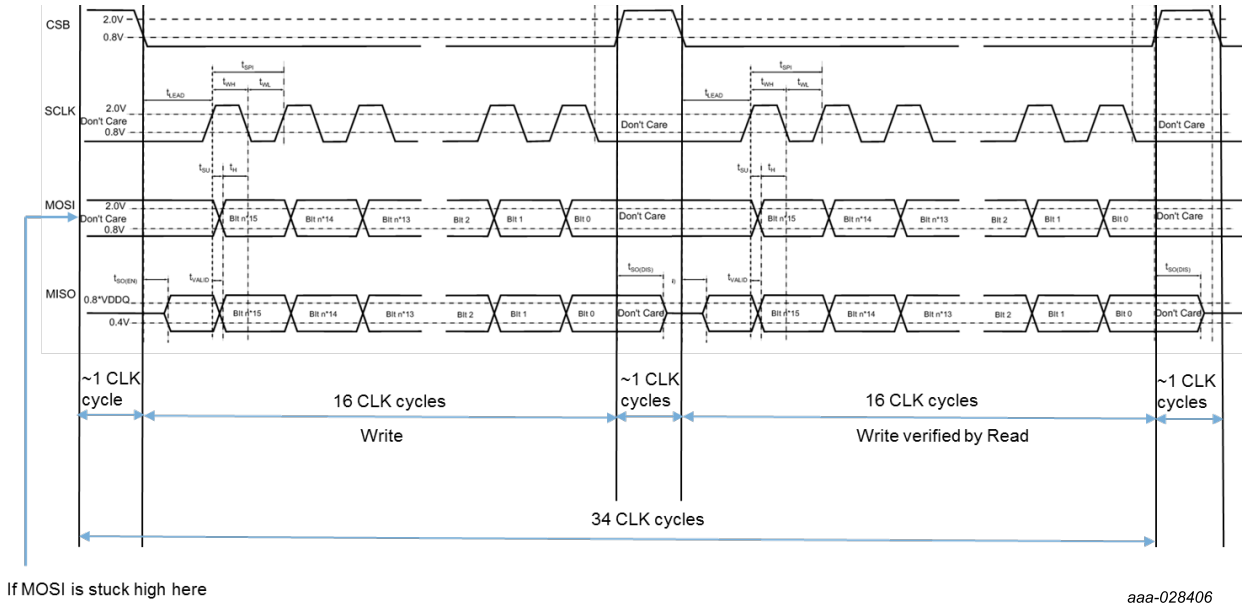

Figure 6. Diagram showing verification of a write operation by performing a read operation on the same register.

Recommendation 2: The HB2000 has a serial peripheral interface consisting of chip select (CS_B), serial clock (SCLK), master in slave out (MISO), and master out slave in (MOSI). This device is configured as a SPI slave and is daisy-chainable (single CS_B for multiple SPI slaves). The daisy-chain feature of the SPI may be used by the MCU to verify data is being transmitted and received back from the device by transmitting a long command chain which wraps through the device buffer and be transmitted back to the MCU. The last 16 bits of the command change would be retained by the device as

a command, and the first 16 bits received from the device would be the normal register feedback. This verifies normal input and output function of the SPI.

Recommendation 3: It is recommended to have forward direction on H-bridge with 100 % duty cycle is fail safe for the valve or actuator in the specific application.

Rationale: Identify fail safe position for the application and ensure that even with accidental turn on of the outputs due to MOSI shorted to power or VDD rail as explained in the rationale for 'Recommendation 1' as an example does not pose any risks at system level.

Recommendation 4: Utilize series resistors or Zener diodes between HB2000 output pins (FS_B, MISO, and CFB) going to the MCU inputs.

Rationale: In case of a short-to-battery or other pin fault to high potential on the HB2000 side, a series resistor will prevent any low-impedance short to high potential, causing excessive current or heating or on the MCU side. A Zener diode on the MCU side will have the effect of protecting the MCU pin from high voltage as well. These HB2000 pins will survive excursions up to 36 V.

8 Additional information

8.1 Acronyms and abbreviations

A short list of acronyms and abbreviations used in this document are summarized for completeness:

Table 24. Acronyms and abbreviations

Term	Definition
EMC	Electromagnetic compatibility
EMI	Electromagnetic interference
ETC	Electronic throttle control
FET	Field-oxide transistor
FMEDA	Failure modes, effects and diagnostic analysis
FTTI	Single-point fault tolerant time interval
L-FTTI	Latent-fault tolerant time interval
LF	Latent fault
LFM	Latent fault metric
MCU	Microcontroller Unit
MOSFET	Metal-oxide semiconductor field-effect transistor
MPF	Multiple-point fault
OV	Overvoltage
OLA	Open-load, active mode
OLS	Open-load, standby mode
PCB	Printed circuit board
PMHF	Probabilistic metric for random hardware failure
POR	Power-on reset
PWM	Pulse-width modulation
SPF	Single-point fault
SPI	Serial peripheral interface
UV	Undervoltage
VIN	Input voltage

9 Revision history

Revision history

Revision number	Date	Description
6.0	11/2018	• Changed document id from MC33HB200xSMUG to UM11163 • Updated as per CIN 201811002I • Rewrite to target HB2000 part number only • Added new recommendation #4 to accommodate possible high-voltage fault on certain pins • Added new safe integration requirements list • Hardware analysis information moved to safety analysis report • Various formatting and organizational changes
5.1	5/2018	• Modified Table 3
5.0	11/2017	• Corrected typo in Table 5
4.0	10/2017	• Modified Section 4.8.2, Requirement: HB200x will meet the random failure rate for ASIL D for system level as specified in SG04. • Modified Table 22 SM004, SM005, SM007, SM010, SM011, SM012, SM013, SM014, SM015, SM016, SM017, SM018
3.0	9/2017	• Complete rewrite
2.0	5/2016	• Complete rewrite. This revision applies to the silicon revision 2.1 for MC33HB2001 and 1.1 for MC33HB2000
1.0	6/2015	• Initial version of the document

10 Legal information

10.1 Definitions

Draft — The document is a draft version only. The content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

10.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, 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. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors. In no event shall 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, 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 NXP Semiconductors.

Right to make changes — 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 — 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 NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of 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. 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 NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the 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. 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 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). NXP does not accept any liability in this respect.

Suitability for use in automotive applications — This NXP Semiconductors product has been qualified for use in automotive applications. Unless otherwise agreed in writing, the product is 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 NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

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 competent authorities.

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

10.3 Trademarks

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

SafeAssure — is a trademark of NXP B.V.

SMARTMOS — is a trademark of NXP B.V.

Tables

Figures

Contents

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 12 November 2018
Document identifier: UM11163