Safety Manual for DRV3201 Three-Phase Motor Bridge Driver

1. Introduction

A system and equipment manufacturer or designer (as user of this document) is responsible to ensure that their systems (and any TI hardware or software components incorporated in their systems) meet all applicable safety, regulatory and system-level performance requirements. TI provides all application and safety-related information in this document (including application descriptions, suggested safety measures, suggested TI products, and other materials) for reference only. Users understand and agree that their use of TI components in safety critical applications is entirely at their risk, and that user (as buyer) agrees to defend, indemnify, and hold harmless TI from any and all damages, claims, suits, or expense resulting from such use.

This document is a safety manual for the Texas Instruments DRV3201 device, three-phase motor bridge driver for safety-critical applications. Devices use a common safety architecture, implemented in multiple application focused products.

This safety manual provides information needed by system developers to assist in the creation of a safety-critical system using a supported DRV3201 three-phase motor bridge driver. This document contains:

- An overview of the superset product architecture
- An overview of the development process utilized to reduce systematic failures
- An overview of the safety architecture for management of random failures
- The details of architecture partitions, implemented safety mechanisms, and recommended usage

The Safety Analysis Report documents the following information, which is not covered in this document:

- Failure rates estimation
- Qualitative failure analysis (Design FMEA and FTA)
- Quantitative failure analysis (quantitative FMEDA)
- Safety metrics calculated per targeted standards per system example implementation

The safety case documents the following information, which is not covered in this document:

- Evidence of compliance to targeted standards
- Results of assessments of compliance to targeted standards

It is expected that the user of this document shall havs a general familiarity with DRV3201 device. This document is intended to be used in conjunction with the pertinent datasheets and other documentation for the products under development. This partition of technical content is intended to simplify development, reduce duplication of content, and avoid confusion as compared to the definition of safety manual as seen in IEC 61508:2010.

2. Product Overview

The DRV3201 is a three-phase motor bridge driver designed to control three-phase brushless dc motors in safety-critical applications. The device provides six dedicated drivers for normal level N-channel MOSFET transistors. The device can switch three high-side and three low-side gate drivers individually with low propagation delay.

The driver capability by design handles gate charges of 250 nC, and the driver source and sink currents are programmable for easy output-slope adjustment. The digital-core logic prevents simultaneous activation of high- and low-side driver of the same channel. One can be access a configuration and status register through SPI communication interface.

The device incorporates sophisticated diagnosis, protection and monitoring features through SPI communication interface. The internal logic, including the SPI communication interface, operates even if battery voltage drops down to 3 V when coming from full functional battery voltage range (that is, between 4.7 V and 30 V).

The boost converter supplies both the high-side and the low-side gate drivers. The boost converter with integrated FET provides the overdrive voltage, allowing full control on the power stages even for battery voltages down to 4.75 V. It has a separate enable/disable B_EN pin that can be controlled by external MCU.

VCC5 is an internal supply for the current-sense amplifiers and other internal analog circuitry. VCC5 has an internal current limit to avoid any internal damage due to an external short to ground on the VCC5 pin. VCC3 is an internal supply for the internal logic. Because the VCC5 regulator supplies VCC3, the VCC5 current limit limits the VCC3 output current. This configuration prevents internal damage in case of an external short to ground on the VCC3 pin.

The DRV3201 interfaces with either 3.3-V or 5-V MCUs. Connecting the I/O voltage of the MCU to the VDD_IO pin of the DRV3201, and connecting the ADC reference voltage of the MCU to the ADREF pin of the DRV3201, achieves this dual-voltage interface. All digital outputs are relative to VDDIO, and all analog outputs are relative (clamped) to ADREF. All digital inputs are relative to internal supply VCC3, except the EN pin.

All digital input pins (except the EN pin) have a threshold voltage relative to the internal VCC3 supply Therefore, the state of digital input pins is independent of the VDDIO level being out of limits. These digital input pins have a fail-safe ESD structure with only a reverse diode path to ground, and no reverse diode path to any supply voltage. Depending on the function, these input pins have an internal passive pulldown or pullup.

All digital output pins (marked LVO_D) have a push-pull stage between VDDIO and ground. Therefore, the logic high-levels are relative to VDDIO.

The DRV3201 supports two operating modes, SLEEP mode and ACTIVE mode. The EN (enable) input pin allows putting the device into SLEEP mode and the gate drivers actively pull the gates of the external power FETs low. Afterwards, the internal supplies VCC5, VCC3, the Boost Converter and the Current Sense Amplifiers are switched off, and a semi-active pull-down resistor pulls the gates of the external power FETs low. During SLEEP mode, the internal logic is put in reset state, all internal registers are cleared and no diagnostic information is available.

A rising edge on the EN pin puts the device in ACTIVE mode after power-up time. In ACTIVE mode, the supplies VCC5 and VCC3 are present and the input on the B_EN pin can enable or disable the boost converter. Because SLEEP mode clears all internal registers, the MCU must program the DRV3201 to the desired settings after each wake-up from SLEEP mode to ACTIVE mode.

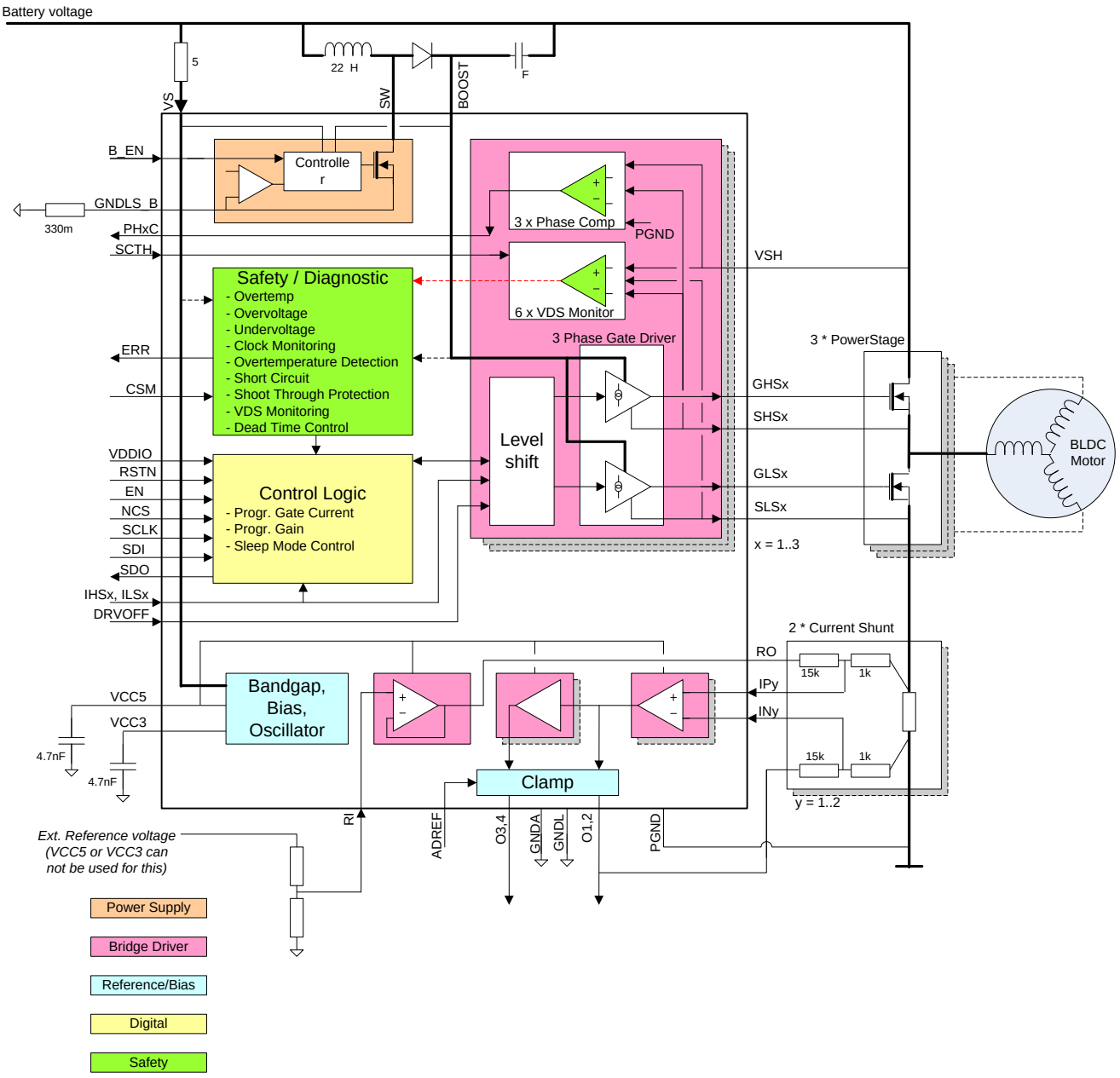


Figure 1: DRV3201 Device Architecture Overview

2.1. Target Applications

The DRV3201 device targetes general-purpose safety-critical applications. Analysis of multiple safety critical applications during the concept phase enabled support of Safety Element out of Context (SEooC) development according to ISO 26262-10:2011. Example target applications include:

- Electronic power steering (EPS) systems and electrical vehicle (EV) power train
- Electrical brake and break assist
- Oil Pump
- Transmission
- Industrial safety critical motor driver applications

In the case of overlapping requirements between target systems, TI MSA has attempted to design the device respecting the most stringent requirement. For example, the fault-tolerant response time intervals in an EPS application is in the order of 10 ms, while for other motor driver applications the interval could be greater than 100 ms. In such a case, TI has performed timer subsystem analysis respecting a fault tolerant time interval less than 10 ms.

While TI MSA has considered certain applications while developing this device, this should not restrict a customer who wishes to implement other systems. With all safety-critical components, the system integrator must rationalize the component safety concept to the system safety concept.

2.2. Product Safety Constraints

For safety components developed according to many safety standards, it is expected that the component safety manual provide a list of product safety constraints. For a simple component, or more complex components developed for a single application, this is a reasonable response. However, DRV3201 device is both a complex design, development of which did not target a single, specific application. Therefore a single set of product safety constraints cannot govern all viable uses of the product. The safety analysis report provides an example implementation of the DRV3201 product in a common system, with relevant product-safety constraints.

3. DRV3201 Development Process for Management of Systematic Faults

For a safety critical development it is necessary to manage both systematic and random faults. Texas Instruments MSA has created a unique development process for safety-critical semiconductors which greatly reduces probability of systematic failures. This process builds on a standard quality-managed development process as the foundation for safety-critical development. A second layer of development activities, which are specific to safety critical developments targeting IEC 61508 and ISO 26262, then augments this process.

TI MSA first saw the need to augment our standard new-product development process in order to develop products according to IEC 61508. During 2007 a new product development process has been updated according to IEC 61508.

By mid-2009, it became clear that the emerging IEC 61508 2nd edition and ISO 26262 functional safety standards would require enhanced process-flow capabilities. Due to the lack of maturity of these draft standards, it was not possible to implement a development process which ensured compliance before final drafts were available. TI joined the ISO 26262 working group in mid-2009 as a way to better understand and influence the standard with respect to microcontroller hardware component development. As part of the US Technical Advisory Group (TAG) and international working group for ISO 26262, TI has notable contributions to:

- ISO 26262:5-2011, Annex D - informative section describing failure modes and recommended diagnostics for hardware components, enhanced by TI's detailed knowledge of silicon failure modes and effectiveness of diagnostic methods
- ISO 26262:10-2011, Clause 9 - informative section describing development of safety elements out of context, a technique which legitimizes and enables the use of Commercial Off The Shelf (COTS) safety critical components
- ISO 26262:10-2011, Annex A - informative section describing how to apply ISO 26262 to microcontrollers, influenced by TI's lessons learned in application of IEC 61508 to microcontroller development

In early 2011, TI MSA started development of a process flow compliant to IEC 61508 second edition and ISO 26262 draft baseline 18. The process applied to the first DRV3201 silicon covered by this document incorporates all changes through ISO 26262 draft baseline 21 (July 2011).

3.1. TI MSA New Product Development Process

Texas Instruments MSA has been developing mixed-signal automotive ASICs for safety-critical and non-safety-critical automotive applications for over 15 years. Automotive markets have strong requirements on quality management and high reliability of product. Though not explicitly developed for compliance to a functional safety standard, the TI MSA new-product development process already featured many elements necessary to manage systematic faults.

The TI MSA new product development process is certified compliant to ISO TS 16949 as assessed by Det Norske Veritas Certification, Inc.

The standard development process breaks development into phases:

- Business Planning
- Validate
- Create
- Evaluate
- Process to Production

Figure 3 illustrates the standard process.

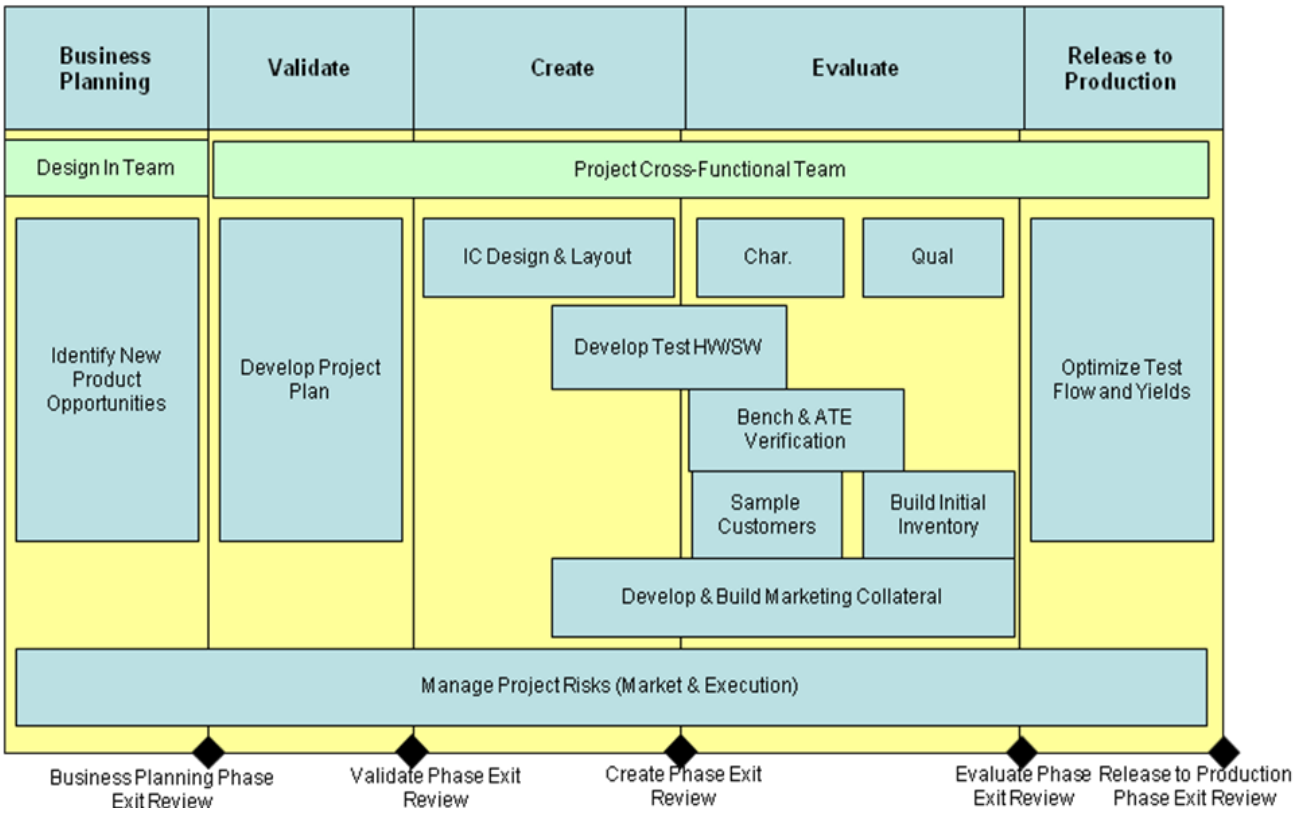


Figure 2: TI MSA New Product Development Process

3.2. *TI MSA Safety Development Flow*

The TI MSA safety-development flow derives from ISO 26262 as a set of requirements and methodologies for application to mixed-signal circuit-safety development flow. This flow is an integrated part of TI MSA new-product development process. The goal of the safety development flow is to reduce systematic faults.

The safety-development flow is targeted for compliance to IEC 61508 second edition and ISO 26262 baseline 21, and is under a process of continuous improvement to incorporate new features of future ISO 26262 working-group drafts. It aligns with TI MCU enhanced-safety development process.

While not directly targeted at other functional safety standards, TI expects that other functional safety systems can readily use product developed to industry state-of-the-art.

Key elements of the MSA safety-development flow are:

- Assumptions on system-level design, safety concept, and requirements based on TI's expertise in safety-critical systems development
- Combined qualitative and quantitative or similar safety-analysis techniques comprehending the sum of silicon failure modes and diagnostic techniques
- Fault estimation based on multiple industry standards as well as TI manufacturing data
- Integration of lessons learned through multiple safety critical developments to IEC 61508 and participation in the ISO 26262 international working group

The following figure illustrates these activities overlaid atop the standard QM development flow.

Phase 0 Bussiness Planning	Phase 1 Program Planning	Phase 2 Create	Phase 3 Evaluate	Phase 4 Ready for Production	Phase 5 Sustaining
Is Safety Process required?	Generate Safety Plan	Device Design Specification	Validation of Safety Elements in Silicon	Plans for Support of operation and production	Ongoing production support
Nominate Safety Manager	Initiation of the Safety Case	Qualitative Analysis of Design Specification	Characterization of Safety Elements	Release of final safety case	End of Life Production
Execution of Development Interface Agreement	Identify System and component safety requirements	Validation of Safety Design implementation at transitor/schematicand RTL level	Qualification of safety related design features	Confirmation review	Decommissioning of products in the field
	Confirmation Review	Quantitative analysis of design	Release of safety manual		Periodic confirmation reviews
		Re-validation of Safety Design with back-annotated circuit parasitics	Release of safety analysis report		
		Confirmation Review	Confirmation Review		

Figure 4: TI MSA New Product Development Process

3.3. *Development Interface Agreement*

The intent of a development interface agreement (DIA) is to capture an agreement between a customer and supplier towards the management of shared responsibilities in developing a functional safety system. In custom developments, the DIA is a key document executed between customer and supplier early in the development process. As DRV3201 device is a commercial, off-the-shelf (COTS) product, TI has prepared a standard DIA which describes the support which TI can provide for customer developments. Refer requests for custom DIAs to your local TI sales office for disposition.

The following sections highlight key points of the standard DIA.

3.3.1. *Requirements Transfer*

DRV3201 product is developed as a safety element out of context (SEooC) with ASIL-D process capability. Detailed safety requirements were not available from lead customers during development. Due to this, TI analysis of target safety applications was basis for the safety requirements used.

TI is willing to discuss acceptance of new-customer safety requirements for future designs; please contact your local TI sales office for further information.

3.3.2. *Availability of Safety Documentation*

Table 1: Safety Documentation

Deliverable Name	Contents	Availability	Delivery
Safety Product Preview	Overview of safety considerations in product development and product architecture. Delivered ahead of public product announcement.	NDA material	October 2011
Safety Manual	User guide for the safety features of the product, including system level assumptions of use.	Public	February 2012
ISO 26262 Safety Analysis Report	Results of FTA, FMEA, and FMEDA safety analysis execution and resulting metrics per the ISO 26262 standard. For use in conjunction with the safety manual.	NDA material	March 2012
Safety Case Report	Detailed summary of the conformance of the product to the ISO 26262 and IEC 61508 standards.	NDA material	4Q2012

3.3.3. *External Product Audits*

TI has no current plans to perform an external audit of DRV3201 device to IEC 61508 or ISO 26262 standards. Detailed documentation can be made available after product qualification to support system audit and certification for the customer.

Forward any request for an independent audit of TI product by an external assessor to your local TI sales office for disposition.

4. *DRV3201 Device Architecture for Management of Random Faults*

For a safety-critical development, it is necessary to manage both systematic and random faults. The DRV3201 product architecture includes many safety mechanisms which can detect and respond to random faults when used correctly.

The device has a core set of modules allocated for continuously operating hardware safety mechanisms:

- PRCM (power, reset, clock management) Controller
- Device state controller
- External power-stage short-circuit protection with VDS monitoring and adjustable detection levels
- External power-stage shoot-through protection with programmable dead time
- Three real-time phase comparators monitoring state of external power stages
- Two independent high-accuracy current sense amplifiers with two programmable gain stages
- Over- and under-voltage monitoring and protection
- Overtemperature warning and shut down
- SPI Communication monitor

4.1. *Device Operating States*

The DRV3201 device has two operating states, SLEEP and ACTIVE. The system developer should monitor these operating stages in their software and system-level design concepts. The following paragraphs describe the device operating-states.

SLEEP STATE

- Default state at power-up with EN pin held low
- Device transitions from ACTIVE to SLEEP state on the EN input falling edge
  - The gate drivers actively pull the gates of the external power FETs low
  - Afterwards (min 20μs, max 35μs later) the internal supplies VCC5, VCC3, the Boost Converter, and the Current Sense Amplifiers switch off.
  - A semi-active pulldown resistor pulls the gates of the external power FETs low
- The device puts internal logic in the reset state and clears all internal registers.
- No diagnostic information is available

ACTIVE STATE

- Entered from SLEEP state on EN input rising edge after power-up time.
- VCC5 and VCC3 are present.
- Controlling B_EN input pin allows enabling or disabling the boost converter.
- The MCU must configure the DRV3201 for desired settings.
- All safety related monitoring, diagnostics, and protection functions are active.

4.2. *RESET Input*

The MCU can reset the DRV3201 by driving RSTN input low. When RSTN input is low:

- The device clears all status bits and register settings.
- The boost converter and the current sense amplifiers are off.
- Actively pulling the gate-driver outputs low (with the maximum setting for the sink current) turns off the external power FETs.
- Internal supplies VCC3 and VCC5 remain active.

The input high and low thresholds of RSTN are relative to VCC3 and independent of VDDIO; hence, the VDDIO level being out of limits does not impact the state of the RSTN input.

4.3. *GATE Drivers*

The DRV3201 has three High Side and three Low Side Gate-Drivers.

- Each high side and low side gate driver contains a programmable sourcing current to charge the gate of the external power FETs.
- Each high side and low side gate driver contains a programmable sinking current to discharge the gate of the external power FETs.
- The direct mode (6-input operation) is a default operation mode after each wake-up from the SLEEP state. The digital input pins IHSx and ILSx control all gate drivers individually.
- PWM Mode (3-input operation) allows controlling all six gate drivers with only three PWM signals. The valid controls in PWM Mode are the IHSx inputs. The device derives the low side controls from the corresponding IHSx signals.
- With the DRVOFF pin high, the programmed setting for the sink current actively puls the gate driver outputs low to turn off the external power FETs.

The boost converter, the current cense amplifiers, and the internal VCC3 and VCC5 supplies are still active with DRVOFF forced low. The input high and low thresholds of DRVOFF are relative to VCC3 and independent of VDDIO; hence, the VDDIO level being out of limits does not impact the state of the DRVOFF pin.

Having the external power FETs turned off while the DRV3201 is in the active state causes the gate drivers to provide a low-resistance active pulldown. When gate-source voltage of the power FETs has dropped below 2 V, the programmed current-sink behavior changes into an R_{DSON} behavior to increase the pull-down strength.

The digital logic prevents simultaneous activation of high- and low-side gate drivers of one power stage. If the MCU commands simultaneous activation, the command is flagged as a failure in the status register.

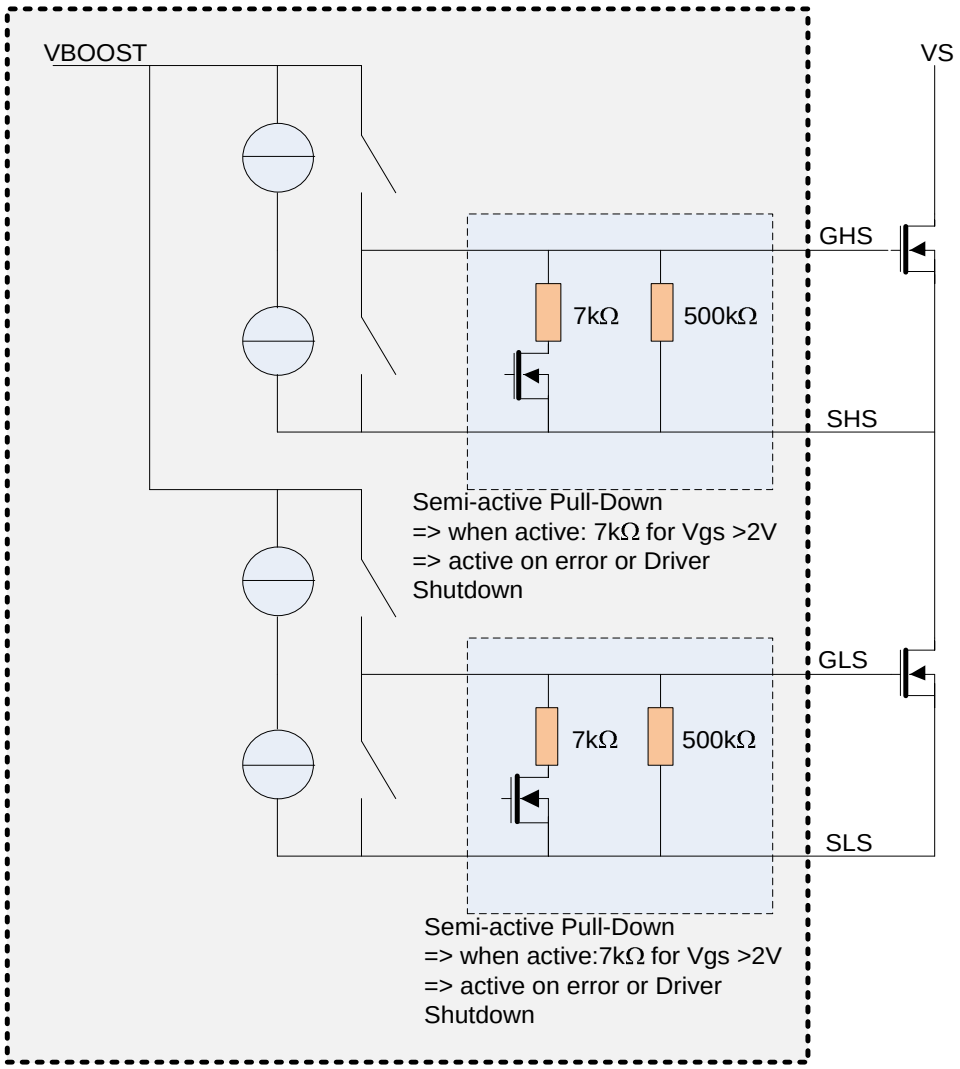


Figure 3: Gate Drivers Concept

5. *DRV3201 Architecture Safety Mechanisms and Assumptions of Use*

System and equipment manufacturer or designers (as users of this document) are responsible to ensure that their systems (and any TI hardware or software components incorporated in their systems) meet all applicable safety, regulatory and system-level performance requirements. TI provides all application and safety related information in this document (including application descriptions, suggested safety measures, suggested TI products, and other materials) for reference only. Users understand and agree that their use of TI components in safety-critical applications is entirely at their risk, and that user (as buyer) agrees to defend, indemnify and hold harmless TI from any and all damages, claims, suits, or expense resulting from such use.

This section summarizes the safety mechanisms for each major functional block of DRV3201 architecture and provides general assumptions of use. Use this information to determine the strategy for using safety mechanisms. The product specification and FMEDA document contain the details of each safety mechanism. The safety analysis report notes the effectiveness of these safety mechanisms.

TI classifies technical recommendations for the use of safety mechanisms in this section into a number of categories. Do not consider the TI recommendations infallible. There are many diverse ways to implement safe systems, and alternate safety mechanisms may be possible which can provide support to achieve desired safety metrics. The categories of recommendation are as follows:

- Mandatory - A mandatory notation indicates a safety mechanism which is always operable during normal functional operation and cannot be disabled by user action.
- Highly Recommended - A highly recommended notation indicates a safety mechanism which TI believes to provide a high value of diagnostics which are difficult to implement by other means. The users retain the choice whether or not to use the safety mechanism in their design, as there is a need for user action either to enable or disable the safety mechanism.
- Recommended - A recommended notation indicates a safety mechanism which TI believes to provide a valuable diagnostic for which there may also be other means of implementation. The users retain the choice whether or not to use the safety mechanism in their design, as there is a need for user action either to enable or disable the safety mechanism.
- Optional - An optional notation indicates a safety mechanism which TI believe to provide a lower value diagnostic for which there may also be other means of implementation. The users retain the choice whether or not to use the safety mechanism in their design, as there is a need for user action user action either to enable or disable the safety mechanism.

5.1. Operating Voltage Range

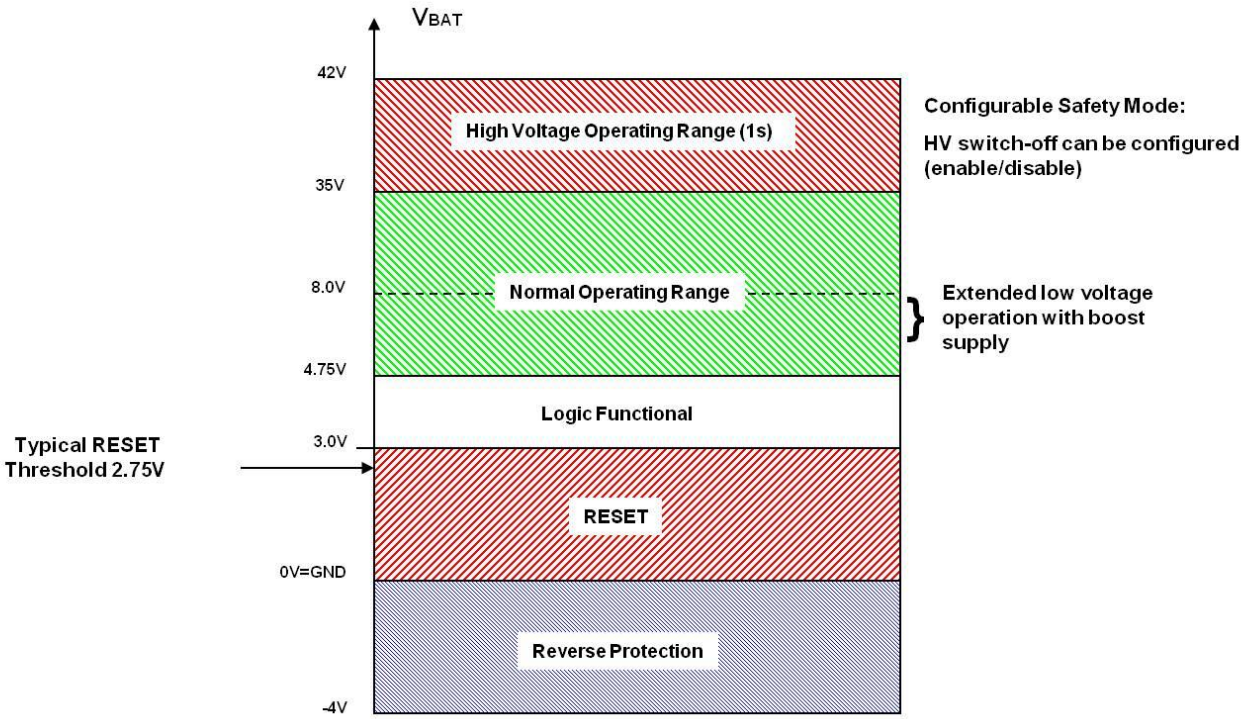


Figure 4: DRV3201 Operating Voltage Range

5.2. Gate-Driver Shoot-Through Detection and Programmable Dead Time

The DRV3201 provides a mechanism that prevents both external power FETs of each power stage from switching ON at the same time, and thus connecting VS directly to GND. If the digital control inputs try to force the device to switch-on high-side gate-drivers and low-side gate-drivers of one power stage, this condition sets an error in the status register and switches the bridges according to Figure 5.

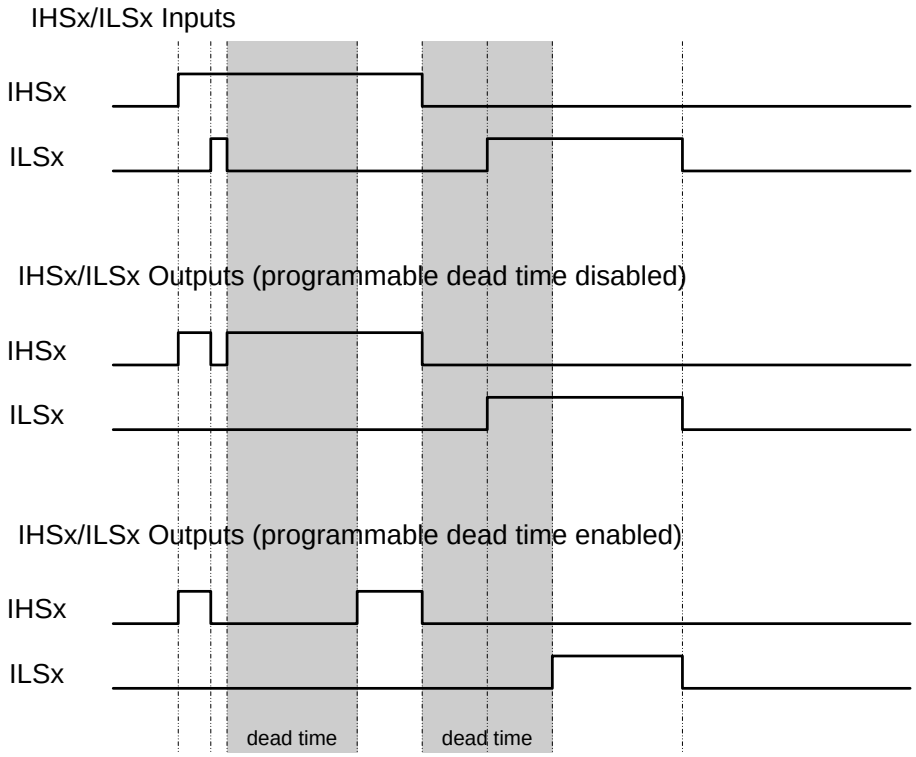


Figure 5: Driver output during control input failure

The dead time is programmable in eight steps between 200 ns and 3000 ns in configuration register 0, bits 2:0. The programmed dead time is valid for all three power stages. An internal 10-MHz oscillator is the time reference for creating the dead-time steps.

The configurable safety mode allows disabling the dead time (see Section *Configurable Safety Mode*) when operating in direct mode. PWM Mode does not support disabling the programmable dead time.

5.3. Gate Drivers – Shutoff Paths

Table 2 summarizes the possible states of the EN, RSTN and DRVOFF pins and the effect on the Gate-Drivers.

Table 2: Gate-Driver Shutoff

EN	RSTN	DRV OFF	Any non-masked error	Gate-Driver shutoff	Logic
Unpowered device (1)				Semi-active pull-down and passive pull-down	-
0	X	X	X	Semi-active pull-down and passive pull-down	Reset
1	0	X	X	Active pull-down	Reset
	1	1	X	Active pull-down	Enabled
		0	1 (1)	Active pull-down	Enabled
		0	0	Active, controlled by inputs	Enabled
1 ->0	X	X	X	Active pull-down, afterwards device enters sleep-mode -> semi-active pull-down + passive pull-down	Enabled during active pull-down, afterwards Reset in sleep-mode

(1) For 3V < VS < 4.75V, the VS undervoltage detection actively pulls down the gates of the external FETs. For VS<3V, these gates have semi-active pulldown.

5.4. External Power FET Drain-Source Voltage Monitoring

The DRV3201 provides a drain-source voltage monitoring feature for each external power MOSFET. After driving input pin IHSx/ILSx high to turn on the external power FET, the DRV3201 monitors the FET drain-source voltage. If this voltage stays higher than the Vds threshold for filter-time t_{vds}, then the device flags the error and sets the status flag for this power FET.

An external analog input voltage applied to SCTH pin sets the internal Vds threshold for the VDS monitoring which scales by a factor between 0 and 1 in eight steps through SPI in configuration register 0 (CFG0), bits [5:3].

For each gate driver, the VDS Comparator configuration is as illustrated in Figure 6. As can be seen from Figure 6, use of the VSH as a sense input voltage for the high-side VDS comparators. Connect this VHS pin externally to the star-point of the positive supply of the power stages.

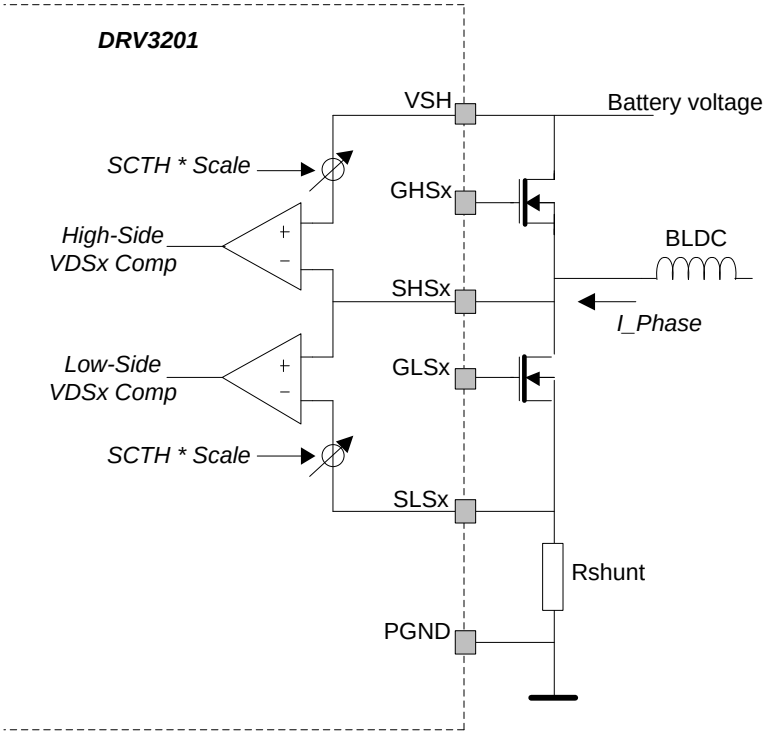


Figure 6: VDS Comparator configuration for each driver stage stage

To perform VDS comparator diagnostics during normal operation, either lower the scale factor through SPI or lower the SCTH voltage externally. The scale factor sets lower VDS threshold (depending mostly on the random comparator offset <+/-100mV), which causes the comparators to toggle at relative low current through the external power FETs (during normal operation without overcurrent).

Figure 7 illustrates the process. During this verification, one can disable the VDS error handling as described in Table 4 (Configuration Register 1 (CFG1), bits [3:4]), to flag VDS errors in SPI status register 0 (STAT0) and at the ERR pin only)

The SCTH pin is a high-impedance input to a MOS gate with internal ESD protection to ground. There is no reverse pullup path present to any supply (fail-safe ESD structure).

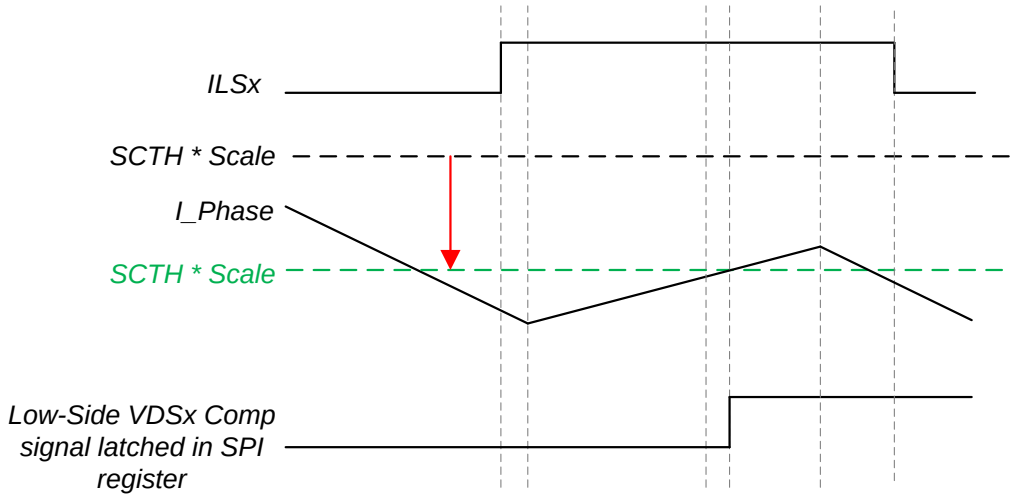


Figure 7: Comparator diagnostics during normal operation

5.5. External FET Gate-Source Voltage Monitor

The DRV3201 provides a gate-source voltage monitoring feature for the external MOSFETs. For each external MOSFET, a comparator with 1 V as the lower threshold and 9 V as the upper threshold monitors Vgs.

For each external MOSFET, there is a status flag in SPI status register 2 (STAT2), bits 0:5. The respective Vgs rising above 9 V sets its status bit to 1, and the respective Vgs dropping below 21 V sets its status bit to 0. Use of this feature is for diagnostics after startup, to turn the external MOSFETs on and off and check the respective status bits.

5.6. Phase Comparators

The device contains three real-time phase comparators usable for sensorless commutation and diagnostics. Each comparator switches typically at 75% and 25% of the supply voltage and has an individual digital output going to the MCU. The phase comparators are always active as long as EN is high.

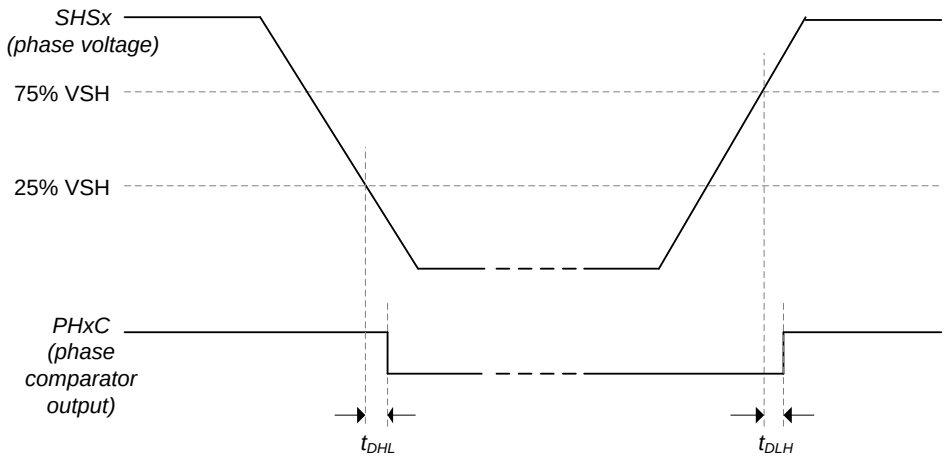


Figure 8: Phase comparator rise and fall thresholds

Use the phase comparators to check the operation of the bridge during normal functional mode:

- Real-time observation of the phase switching on node SHSx.
- Measure the time between the Input HIS or ILSx and the phase comparator output PHxC
- Verify time drift of previous measurements and/or other driver-stages

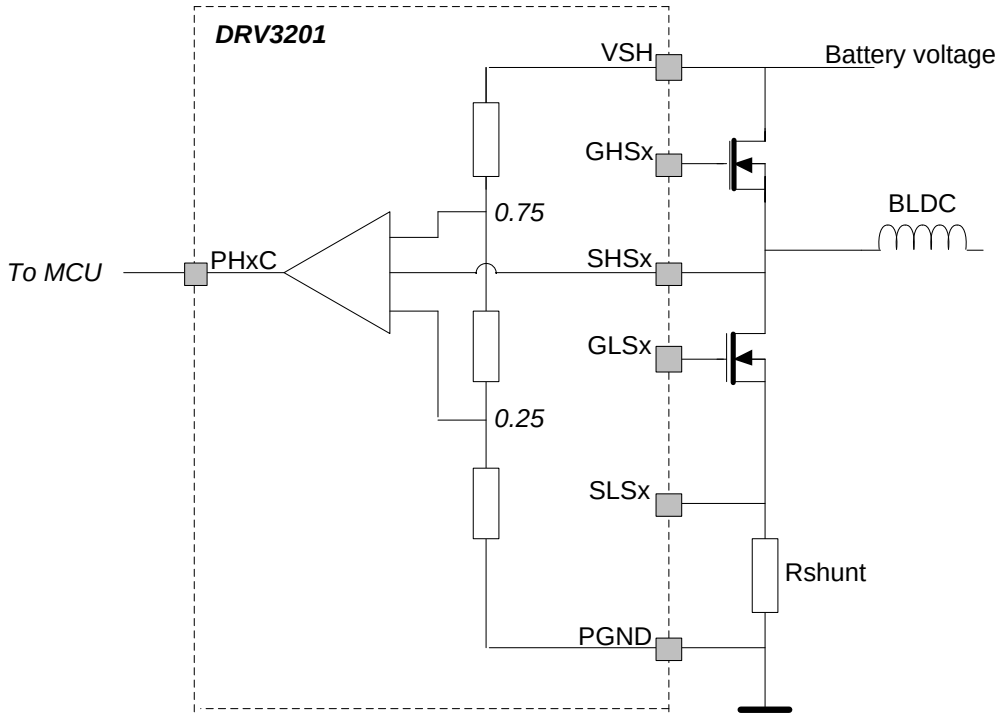


Figure 9: Phase comparator application diagram

As Figure 9 shows, the VSH and PGND pins are sense inputs used to create the high-side and low-side threshold levels for the phase comparators. Externally, the VSH pin is to be connected to the star-point of the positive supply of the power stages. Connect the PGND pin to the power-ground star-point of the power stages. The total resistance of the internal voltage divider is typical 248kΩ.

5.7. Voltage Monitoring

5.7.1. Boost Undervoltage Error

If the boost converter output voltage is below the undervoltage threshold level $V_{VBOOST,UV}$ (11V…11.9V) for t_{BCSD} time (5µs…6µs), the device sets the boost undervoltage SPI status flag bit in SPI status register 1 (STAT1). Depending on the configured cafety mode (see section *Configurable Safety Mode*), the device pulls all gate-driver outputs and the ERR pin low.

5.7.2. VS Undervoltage Shutdown

The VS voltage dropping below the undervoltage threshold level $V_{VS,UV}$ (4.5V…4.75V) for $t_{VS,SHD}$ time (5µs…6µs) sets the VS under-voltage SPI status flag bit is set in SPI Status Register 1 (STAT1) and pulls the gate-driver outputs and the ERR pin low. This occurs regardless of the configured safety mode (see section *Configurable Safety Mode*). The SPI interface works down to 3V. Below 3V on VS, internal reset occurs.

5.7.3. VS Overvoltage Error

The VS voltage exceeding the overvoltage threshold level $V_{VS,OV}$ (30V…30.5V) for $t_{VS,SHD\ time}$ (5µs…6µs) sets the VS overvoltage SPI status flag bit in SPI Status Register 1 (STAT1). Depending on the configured safety mode (see section *Configurable Safety Mode*), the device pulls all gate-driver outputs and the ERR pin low.

5.7.4. VS Comparator Check

Check the VS under- and overvoltage comparators by using the *LOC test/ VS comparator* bit in the Configuration Register 0 (CFG0). As long as this bit is set, the comparators toggle and flag the undervoltage and the overvoltage at the same time.

Also the error handling is active, which shuts down and pulls the ERR pin low. To reset the flags, reset the *LOC test /VS comparator* bit first and then read the flags via SPI. After this, the ERR pin goes up again as well. This self-check is combined with the loss-of-clock self-test (see section *Loss-of-Clock Monitor*).

5.8. Overtemperature Warning and Shutdown

The device stores the thermal overload detection and protection on five temperature sensors and two thresholds, T_{msd1} (thermal warning) and T_{msd2} (thermal global reset):

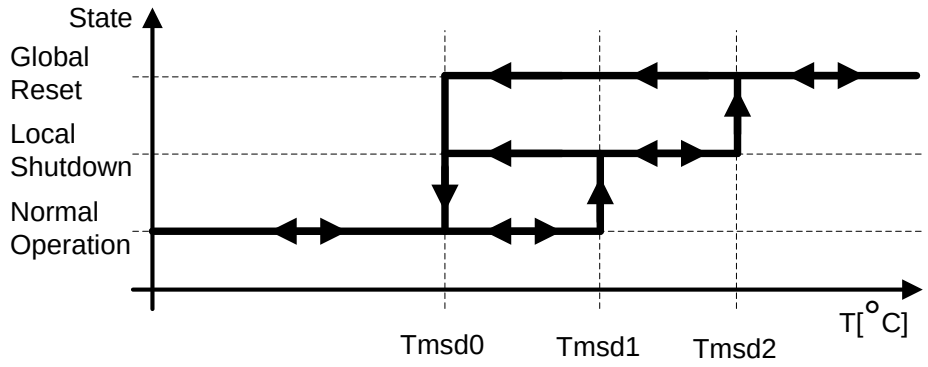


Figure 10: Thermal Protection

Normal Operation

- Gate-Drivers and boost converter are fully operational.

Thermal Warning - Over temperature Warning flag is set to 1

- The device stores the thermal warning as the overtemperature warning bit in status Register 0 (STAT0). Reading out the MCU register resets this bit.

Global Reset - Device in shutdown:

- The device generates an internal reset.
- The boost converter stops.
- The temperature monitor block monitors the temperature and does not release the reset until the temperature drops below T_{msd0}.
- Thermal hysteresis prevents any oscillation between shutdown and restart.
- t_{SHDOWN} filters the overtemperature shutdown (to prevent unwanted shutdown by noise).

5.9. SPI Communication Monitor

The DRV3201 monitors SPI communication with external MCU:

- If an invalid write or read access command is received, the SPI OK bit in Status Register 1 (STAT1) is set to 0. This bit will be set to 1 after read out of this register by the MCU.
- The device ignores any SPI frame with an invalid number of SPI clock cycles.

5.10. Analog Trim EEPROM CRC Check

After each transition to ACTIVE state, the DRV3201 performs an EEPROM CRC check. If the calculated CRC8 checksum does not match the expected CRC8 checksum stored in the EERPOM, the device sets the EEPROM Data CRC Failed flag in Status Register 1 (STAT1).

5.11. Configuration Data CRC Check

The DRV3201 offers a security feature to ensure device configuration integrity permanently by employing a CRC8 checksum mechanism. The MCU can start a CRC8 checksum calculation within the DRV3201 over all configuration registers by setting bit 0 in CRC Control Register (CRCCTL) to 1. This bit will stay set until CRC calculation is finished.

There may not be any write access while the CRC engine is running; writing could corrupt the CRC8 checksum. After calculating the CRC8 checksum value, the DRV3201 stores it in the CRC calculated checksum register (CRCCALC).

The MCU itself can also calculate the expected CRC8 checksum value, based on the following vector, and store this expected value in the CRC expected checksum register (CRCEXP). Do this before the MCU initiates the CRC8 checksum calculation within the DRV3201. After completion of the CRC calculation by the DRV3201, failure of the expected CRC stored in CRCEXP register to match the calculated CRC in CRCCALC register results in setting the configuration data CRC failed flag bit in status register 1 (STAT1).

The MCU may then read back all configuration registers to search for the bit error and perform corrective actions. The CRC8 calculation mechanism is a generic one with following presets:

- The polynomial used is: (0 1 2 8)
- Initial value is: 11111111

5.12. Loss of Clock Monitor

If the internal system clock is stuck the loss of clock monitor pulls the ERR pin low. During test of this block, ERR is also low. The device combines this self-check with the VS comparator self-test.

5.13. IHSx/ILSx Control-Input Readback and Edge Counter

To verify the signal path to the DRV3201, the device allows reading back the logic level of all IHSx and ILSx inputs from the RB0 address. These values directly reflect the state of the pin without latching. Ensure that the state of the IHSx and ILSx pins do not change while reading back their levels via SPI.

IHSx and ILSx input readback remains operational even if choosing PWM mode. In this case, one may use the ILSx readback to read any logic-level signal.

The edge counter allows a more-robust and less-time critical verification of the ILSx and IHSx signal chain and may be more convenient to use during normal operation. One may use this counter to count the number of edges on one or more IHSx and ILSx inputs. The MCU may select the inputs for observation and arm the counter by writing to SPI register RB1. Immedietly after removing the start bit, the counter stops counting edges. One can read the obtained counter value from SPI register RB2 and reset the counter by setting the CLEAR bit in SPI register RB1.

As soon as the counter has reached its maximum value of 255, it stops counting and remains in this state. IHSx and ILSx edge counter remains operational even in PWM mode. In this case, one may use the edge counter to count edges at any connected input.

5.14. Device Safety Mode Configuration

The DRV3201 can work in two different safety modes controlled by the external pin CSM, as described in Table 3. The user can read back the pin state via SPI register RB0.

Table 3: Safety Modes

CSM	Description
LOW	Full Safety Mode: Activates all internal protection features.
HIGH	Configurable Safety Mode: Enables the protective actions selected in configuration register CFG_REG_1 and sets diagnostic flags; de-selected ones only set diagnostic flags without protective action. With this mode, users can operate the device outside the normal operating range but below absolute maximum ratings at their own responsibility.

Table 4 defines the Protective Actions taken on certain Error Conditions. When the device is in Full Safety mode, all internal protection features are activated, hence all Protective Actions as listed below are taken if the respective Error Condition is detected.

When the device is in Configurable Safety Mode (CSM), the Error Conditions for which CSM is available, and the Protective Action and ERR pin indication (see next paragraph) can be configured with the corresponding bit in CFG1. The diagnostic flags will always be set if the respective Error Condition is present, regardless of the CSM setting.

Table 4: Error Conditions and Protective Actions

Error Condition	Protective Action	Recovery	Selectable through CFG_REG_1 in CSM	Error Indication ERR pin
VS undervoltage	Switch all gate-driver outputs to low (active pulldown).	Flags will be cleared with MCU reading Status Register or through RESET. If the failure remains after read out of the register, flags are immediately set again.	No	Always
VS overvoltage			Yes	Selectable by CFG_REG_1
Boost converter undervoltage			Yes	
HS VDS-Error			Yes	
LS VDS-Error			Yes	
Programmable dead-time window failure	Enforce programmable dead time.		Yes	
Shoot-through protection violated	Switch HS and LS gate-driver outputs of affected power stage to low (active pulldown). If enabled, enforce dead-time to high side and low side.		No	Always
SPI error	SPI command is ignored.		No	None
Configuration data CRC Error	Reported via SPI		No	None
EEPROM-data CRC error			No	None
Overtemperature first threshold			No	Always
Over temperature second threshold	Shutdown of device	After thermal recovery, device performs power on reset	No	Always
LOC error	ERR pin low		No	Always

The ERR pin is an indicator for a detected error condition. It may act as interrupt to the external MCU, after which the MCU reads all status registers to identify the detected error condition.

After entering active mode, this pin remains high until the detection of an error; in case of a detected error condition, the ERR pin goes low. Error reporting occurs according to Table 5.

Table 5: Error reporting in the Safety Modes

CSM	ERR pin configuration (CFG1)	Description
LOW	Don't care	All Error Conditions are flagged on ERR pin
HIGH	1	ERR pin will only show errors for Protective Actions being enabled in CSM
	0	All Error Conditions are flagged on ERR pin

The ERR pin will go up again after read-out of the respective error flag in the status register once the respective violation condition has disappeared. In case the MCU reads out the respective error flag in the status register while the respective Error Condition is still present, the ERR pin will show a short positive pulse (pulse width typ. 100ns).

This behavior helps, for instance to distinguish between a loss-of-clock error and a VS undervoltage or overvoltage error flag during self-tests of these safety features. After activation of these self-tests (configuration register 0 (CFG0) bit 6), the ERR pin will go down.

After MCU read-out of the VS undervoltage and overvoltage flags (Status Register 1 (STAT1) bits 1:0), the ERR pin should stay low if the loss-of-clock self-test is working properly. If the ERR pin shows a positive pulse (pulse width typ. 100ns), then this is an indication of a failure in the loss-of-clock self-test.

5.15. Redundant Current Sensing and Measurement

Performance of the two-channel current measurement consists of measuring the voltage drop across two external shunt resistors. It contains one shift buffer, two first, and two second stages.

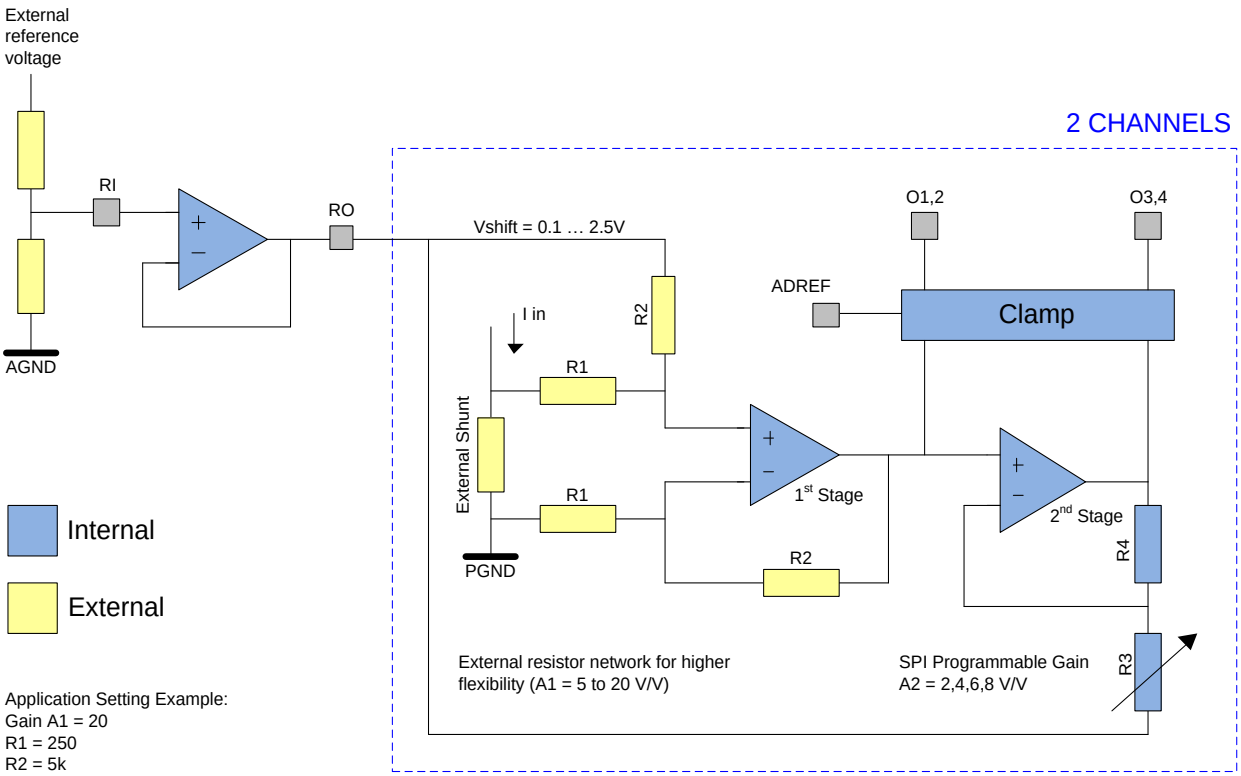


Figure 11: Current Sense application circuit

5.15.1. Shift Buffer

The DRV3201 offers a unity-gain amplifier that normally supports a shift voltage with lower output impedance. This allows each current-sense path to handle negative common-mode voltages across the external shunt resistor. Apply the shift-voltage externally on the RI pin; the actual shift-voltage buffering on the RO pin.

The RI input pin is a high-impedance input to a MOS gate with internal ESD protection to ground. No reverse-pullup path is present to any supply (fail-safe ESD structure).

5.15.2. The First-Stage Amplifier

A first stage operational amplifier operates with an external resistor network for higher flexibility to adjust the current measurement to the application requirements.

In a recommended application, adding a shift voltage can move the transfer curve. The basis for this shift voltage can be an external reference, for example, an external voltage regulator. Each channel of the first amplifier has its own output going, for example, to the input of the MCU ADC.

The input of the first stage is high-voltage compatible, enabling use of the device to measure the voltage drop across the LS MOSFET for low-requirement applications. The ADREF voltage is the clamp level for the maximum output voltage of the O1 and O2 pins.

The input INx and IPx pins are high-impedance inputs to a MOS gate with internal ESD protection to ground. There is no reverse-pullup path present to any supply (fail-safe ESD structure).

5.15.3. The Second Stage Amplifier

The second stage amplifiers with separately programmable gain enable higher-resolution measurement at low current. They can have direct connection to inputs of the MCU ADC.

Programming of the gain of the second stage amplifiers is in steps 2, 4, 6 or 8 by SPI using the CFG2 register.

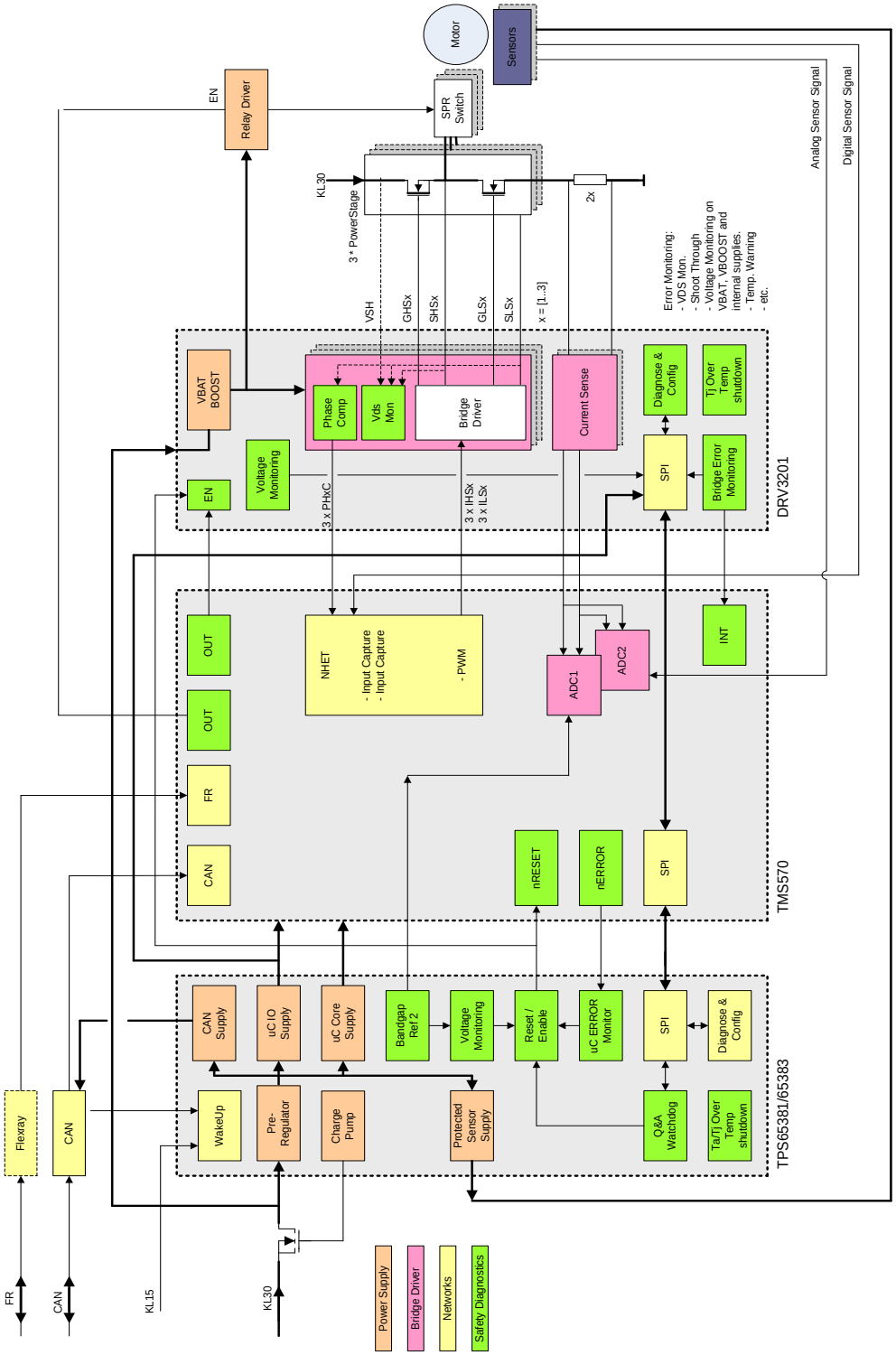
The ADREF voltage is the clamp level for the maximum output voltage of the O3 and O4 pins.

5.15.4. ADREF Voltage Clamp

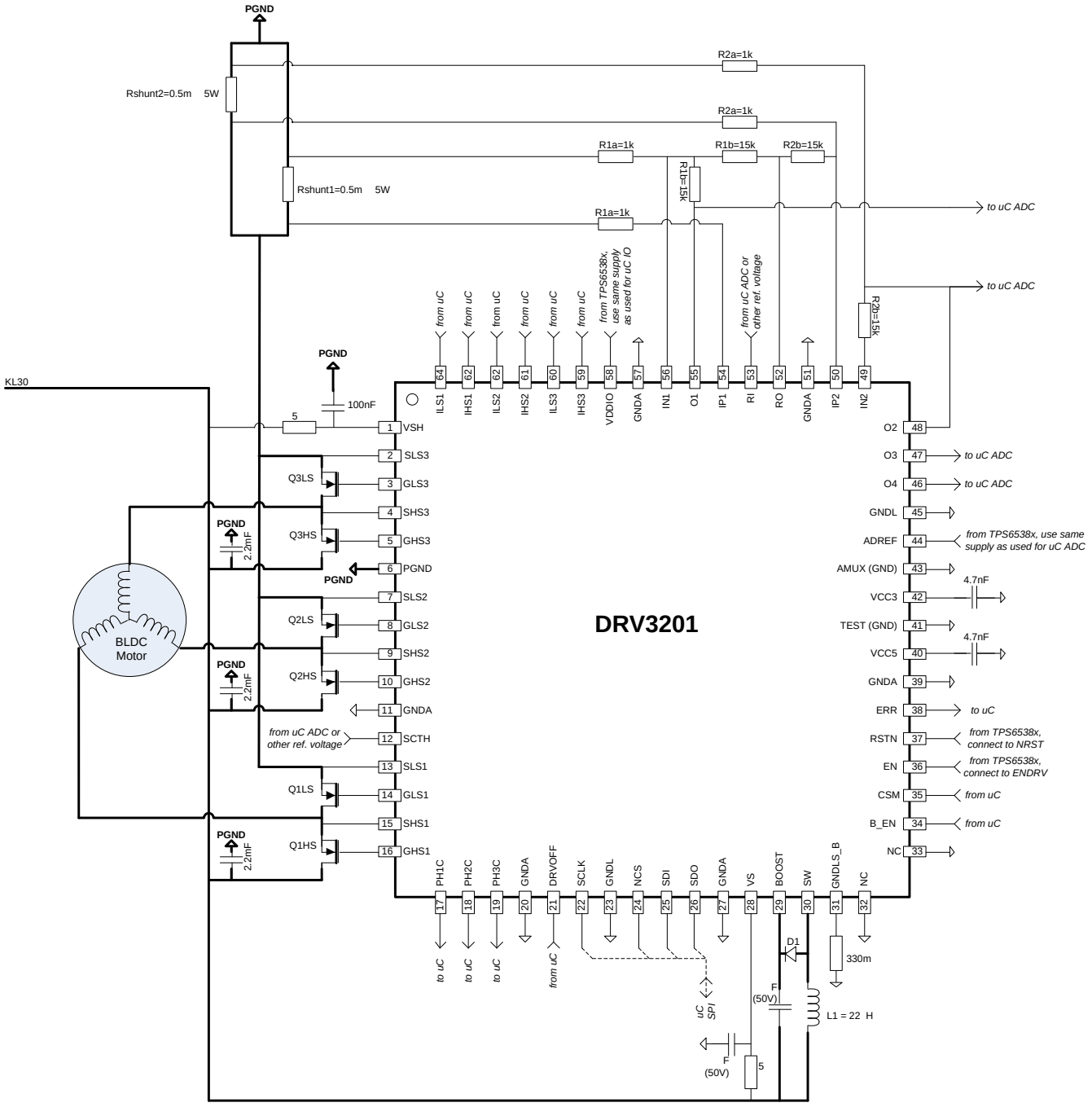
An active clamp clamps the maximum output voltage of pins O1-O4 to the voltage applied to ADREF. The ADREF voltage is the reference supply voltage for the ADC in the MCU. In this way, the outputs O1-O4 have maximum signal range related to the input range of the ADC in the MCU. The active clamp consumes maximum of 100μA from the ADREF pin.

6. Application Diagrams

6.1. EPS Example

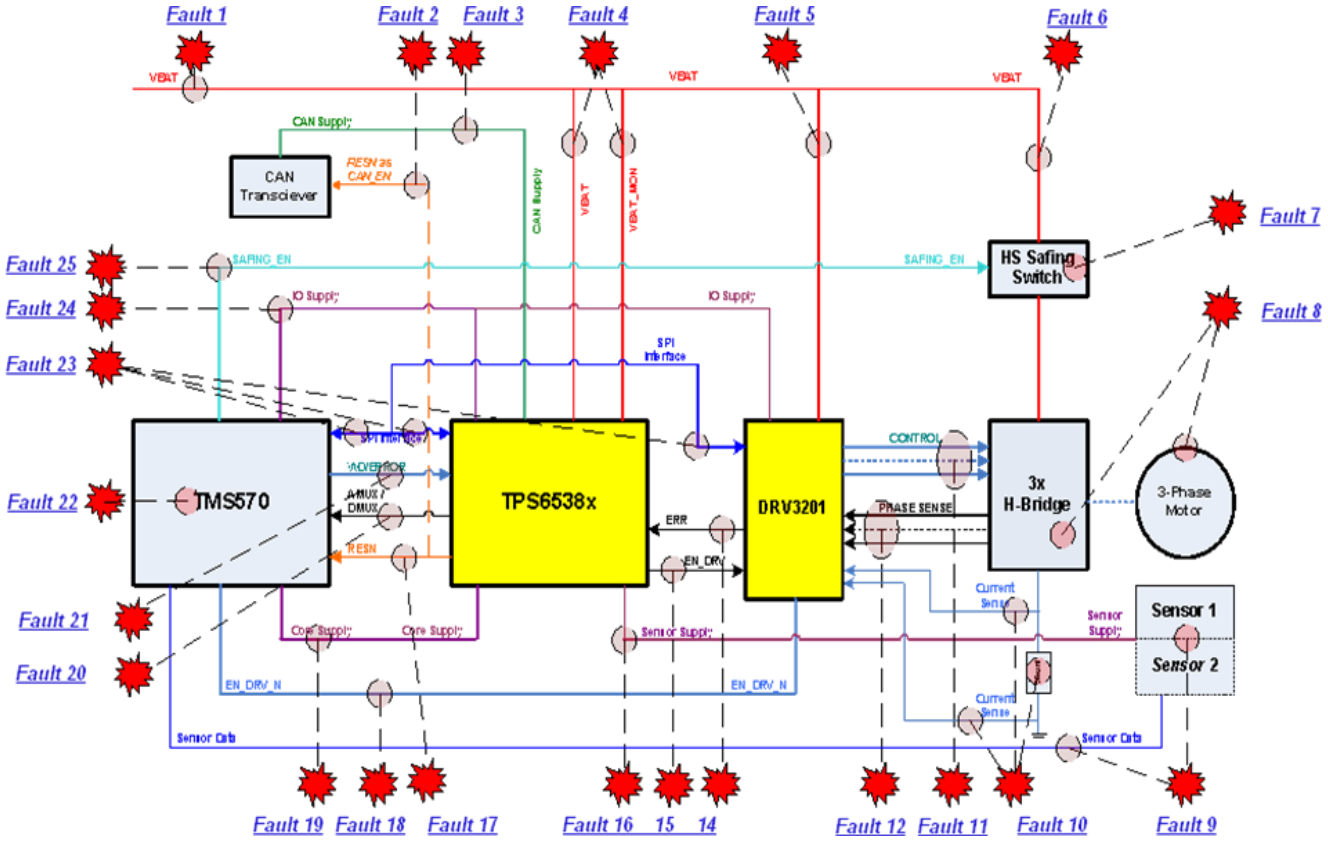


6.3. *DRV3201 Application Circuit*



L1=B82442A1223K000	INDUCTOR,SMT,22uH,10%,480mA)
D1=SS28	(DIODE,SMT,SCHOTTKY,80V,2A)
QxHS, QxLS = IRFS3004PBF	(HEXFET,N-CHANNEL,POWER MOSFET,D2PACK)
Rshunt1,2 = BVR-Z-R0005	(RES,SMT,4026,PRECISION POWER,0.0005 OHMS,1%,5W)

6.4. DRV3201 - Safety Element out of Context (SEooC) Analysis



- **Fault 1 – VBAT Supply Short / Open**
  - **Impact:**
    - It is a common-cause failure that affects complete EPS ECU
  - **Detection and Protection**
    - UBAT Under-Voltage detected by TPS65381 and system brought to SAFE state

- **Fault 2 – CAN Enable Short / Open**
  - **Impact:**
    - Disabled CAN PHY with no back-plane communication to domain controller
  - **Detection & Protection:**
    - MCU Safing function detects it with a dedicated GPIO to sense CAN PHY Enable signal
    - *NOTE: CAN PHY Enable signal can be the same as MCU power-on reset driven by TPS65381*

- **Fault 3 – CAN Supply Short / Open**
  - **Impact:**
    - CAN PHY is not functional and there is no back-plane communication to domain controller
  - **Detection & Protection**
    - In case of CAN supply short-to-GND fault, TPS65381 detects UV condition and resets the system
    - In case of CAN Supply Open fault, MCU detects no communication to domain controller

- **Fault 4.1 – TPS65381 VBAT Supply Short**
  - **Impact:**
    - No regulated power supplies
    - MCU in reset state
    - Bridge driver in reset state
  - **Detection and Protection**
    - TPS65381 UBAT UV monitor detects UV condition and brings system to SAFE state (reset)
    - System powers down

- **Fault 4.2 – TPS65381 VBAT Supply Open**
  - **Impact:**
    - No regulated power supplies
    - MCU in reset state
    - Bridge driver in reset state
  - **Detection & Protection:**
    - System powers down and remains in SAFE state

- **Fault 4.3 – TPS65381 VBAT_MON Supply Short**
  - **Impact:**
    - No system supply monitoring functions are available
    - MCU remains in reset state
    - Bridge driver remains in reset state
  - **Detection & Protection**
    - Internal voltage monitor indicates undervoltage event keeping MCU supply OFF

- **Fault 4.4 – VBAT_MON Supply Open**
  - **Impact:**
    - No system supply monitoring functions are available
    - MCU remains in reset state
    - Bridge driver remains in reset state
  - **Detection and Protection**
    - Internal voltage monitor indicates undervoltage event keeping MCU supply OFF

- **Fault 5 – DRV3201 VBAT open**
  - **Impact:**
    - DRV3201 powered down
  - **Detection & Protection**
    - MCU monitoring and diagnostics

- **Fault 6 – Bridge VBAT Open**
  - **Impact:**
    - No running motor
  - **Detection & Protection**
    - DRV3201 monitoring and diagnostics
    - MCU monitoring and diagnostics

- **Fault 7 – HS Safing Switch Fault**
  - **Impact:**
    - Bridge could be permanently powered (in case of short to UBAT), or
    - Bridge could be permanently powered-down (in case of short to GND)
  - **Detection & Protection**
    - System requires redundant and independent HS safing-switch enable for most-reliable protection.

- **Fault 9 – Sensor Data Short or Open**
  - **Impact:**
    - MCU disables bridge pre-driver (DRV3201), thus disabling system.
  - **Detection & Protection**
    - Part of MCU safing function that process sensor data

- **Fault 10 – Current Shunt Short or Open**
  - **Impact:**
    - Bridge pre-driver disabled
  - **Detection & Protection**
    - No current measurement detected and bridge disabled by MCU

- **Fault 11 – Bridge Driver Controls Short or Open**
  - **Impact:**
    - MCU disables bridge pre-driver (DRV3201), or
    - DRV3201 protection disables bridge
  - **Detection & Protection**
    - VDS monitoring failure leads to disabling bridge driver, or
    - MCU detects mismatch between its control outputs and phase comparator inputs, and disables DRV3201

- **Fault 12 – Phase Sense Short or Open**
  - **Impact:**
    - MCU disables bridge pre-driver (DRV3201)
  - **Detection & Protection**
    - Phase comparator outputs to MCU do not follow MCU bridge driver controls
    - MCU disables DRV3201

- **Fault 13 – Current Sense Short or Open**
  - **Impact:**
    - Bridge pre-driver is disabled
  - **Detection & Protection**
    - No current measurement detected and bridge disabled by MCU

- **Fault 14 – TPS65381 ERROR pin Short or Open**
  - **Impact:**
    - MCU error pin failure detected
    - MCU reset asserted and system disabled
  - **Detection & Protection**
    - MCU ERROR pin diagnostics fail after power-up event
    - MCU ERROR pin monitor detects an ERROR pin failure in the active state

- **Fault 15 – TPS65381 EN_DRV Short or Open**
  - **Impact:**
    - External power-stage enable (or safing-path enable) is not controllable
  - **Detection and Protection**
    - EN_DRV diagnostics can detect the failure by using SPI readback function to confirm the state of EN_DRV
    - The second system-safing path enable should provide needed redundancy in case of EN_DRV short to VBAT.

- **Fault 16 – TPS65381 Sensor Supply Short or Open**
  - **Impact:**
    - No functioning sensor in the system
    - Potential sensor damage if short to VBAT occurred
  - **Detection & Protection:**
    - Sensor supply monitor detects both UV or OV events and disables sensor supply and external power stages.
    - Sensor supply monitor covered by internal diagnostics and its status reported to MCU via SPI.

- **Fault 17 – TPS65381 RESn pin Short or Open**
  - **Impact:**
    - MCU reset function not correct
      - In case of short to GND, MCU remains in permanent reset with system disabled.
      - In case of short to VBAT, MCU never reinitializes.
      - In case of open, MCU remains in permanent reset due to internal pulldown on MCU RESn input pin, and system remains disabled
  - **Detection & Protection**
    - Diagnostics and monitoring detects RESn external faults
      - Watchdog function
      - Error-pin Function
      - Interconnect diagnostics

- **Fault 19.1 – TPS65381 VDD3/VDD1 Short or Open (MCU Core Supply Fault)**
  - **Impact:**
    - In case of short to GND
      - MCU is powered down and system is disabled
      - VDD3 disabled
  - **Detection & Protection**
    - Diagnostics and monitoring detects VDD3 short to GND
      - VDD3 current limit kicks in
      - VDD3 UV detected and power-stages disabled (EN_DRV driven low)
      - With VDD3 current limit, eventually overtemperature condition occurs and disables VDD3

- **Fault 19.2 – TPS65381 VDD3/VDD1 Short or Open (MCU Core Supply Fault)**
  - **Impact:**
    - In case of open
      - MCU powered-down and system disabled
  - **Detection & Protection**
    - Diagnostics and monitoring detects VDD3 open fault
      - MCU is not responsive and WD/ERROR pin failure detected

- **Fault 20 – TPS65381 AMUX/DMUX Short or Open**
  - **Impact:**
    - MCU disabled the system due to failed TPS65381 diagnostics
  - **Detection & Protection**
    - All MCU-TPS65381 interconnect diagnostics fail and MCU application can disable the system

- **Fault 21 – TPS65381 WD/ERROR Short or Open**
  - **Impact:**
    - System disabled
  - **Detection & Protection**
    - WD/ERROR failure detected and system disabled

- **Fault 22 – MCU Locks**
  - **Impact:**
    - MCU powered-down and system disabled
  - **Detection & Protection**
    - WD/ERROR failures detected
    - When error count reaches programmed threshold, TPS65381 powers down MCU

- **Fault 23 – TPS65381 SPI Interface Short / Open**
  - **Impact:**
    - MCU powered down and system disabled
  - **Detection & Protection**
    - WD/ERROR failures detected
    - When error count reaches programmed threshold, TPS65381 powers-down MCU

- **Fault 24 – IO Supply Short / Open**
  - NOTE: same as Fault 19

Functional Safety Disclaimer for Safety Critical Solutions

TI's safety critical solutions, including integrated circuits, software and tools help TI's customers create end products that may be used in appropriately designed safety-critical applications to comply with functional safety standards or requirements.

Buyers represent and agree that they have all the necessary expertise to design, manage and assure effective system-level safeguards to anticipate, monitor and control system failures in safety-critical applications. Buyers agree and accept sole responsibility to meet and comply with all applicable regulatory standards and safety-related requirements concerning their systems and end-products which use TI's safety-critical applications. Buyers will fully indemnify TI and its representatives against any damages arising out of the use of TI products in safety-critical applications.

TI integrated circuits are not authorized for use in FDA Class III (or similar life-critical medical equipment) unless authorized officers of the parties have executed a special agreement specifically governing such use.

IMPORTANT NOTICE

Texas Instruments Incorporated and its subsidiaries (TI) reserve the right to make corrections, enhancements, improvements and other changes to its semiconductor products and services per JESD46, latest issue, and to discontinue any product or service per JESD48, latest issue. Buyers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. All semiconductor products (also referred to herein as “components”) are sold subject to TI’s terms and conditions of sale supplied at the time of order acknowledgment.

TI warrants performance of its components to the specifications applicable at the time of sale, in accordance with the warranty in TI’s terms and conditions of sale of semiconductor products. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by applicable law, testing of all parameters of each component is not necessarily performed.

TI assumes no liability for applications assistance or the design of Buyers’ products. Buyers are responsible for their products and applications using TI components. To minimize the risks associated with Buyers’ products and applications, Buyers should provide adequate design and operating safeguards.

TI does not warrant or represent that any license, either express or implied, is granted under any patent right, copyright, mask work right, or other intellectual property right relating to any combination, machine, or process in which TI components or services are used. Information published by TI regarding third-party products or services does not constitute a license to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

Reproduction of significant portions of TI information in TI data books or data sheets is permissible only if reproduction is without alteration and is accompanied by all associated warranties, conditions, limitations, and notices. TI is not responsible or liable for such altered documentation. Information of third parties may be subject to additional restrictions.

Resale of TI components or services with statements different from or beyond the parameters stated by TI for that component or service voids all express and any implied warranties for the associated TI component or service and is an unfair and deceptive business practice. TI is not responsible or liable for any such statements.

Buyer acknowledges and agrees that it is solely responsible for compliance with all legal, regulatory and safety-related requirements concerning its products, and any use of TI components in its applications, notwithstanding any applications-related information or support that may be provided by TI. Buyer represents and agrees that it has all the necessary expertise to create and implement safeguards which anticipate dangerous consequences of failures, monitor failures and their consequences, lessen the likelihood of failures that might cause harm and take appropriate remedial actions. Buyer will fully indemnify TI and its representatives against any damages arising out of the use of any TI components in safety-critical applications.

In some cases, TI components may be promoted specifically to facilitate safety-related applications. With such components, TI’s goal is to help enable customers to design and create their own end-product solutions that meet applicable functional safety standards and requirements. Nonetheless, such components are subject to these terms.

No TI components are authorized for use in FDA Class III (or similar life-critical medical equipment) unless authorized officers of the parties have executed a special agreement specifically governing such use.

Only those TI components which TI has specifically designated as military grade or “enhanced plastic” are designed and intended for use in military/aerospace applications or environments. Buyer acknowledges and agrees that any military or aerospace use of TI components which have ***not*** been so designated is solely at the Buyer's risk, and that Buyer is solely responsible for compliance with all legal and regulatory requirements in connection with such use.

TI has specifically designated certain components which meet ISO/TS16949 requirements, mainly for automotive use. Components which have not been so designated are neither designed nor intended for automotive use; and TI will not be responsible for any failure of such components to meet such requirements.

Products		**Applications**	
Audio	www.ti.com/audio	Automotive and Transportation	www.ti.com/automotive
Amplifiers	amplifier.ti.com	Communications and Telecom	www.ti.com/communications
Data Converters	dataconverter.ti.com	Computers and Peripherals	www.ti.com/computers
DLP® Products	www.dlp.com	Consumer Electronics	www.ti.com/consumer-apps
DSP	dsp.ti.com	Energy and Lighting	www.ti.com/energy
Clocks and Timers	www.ti.com/clocks	Industrial	www.ti.com/industrial
Interface	interface.ti.com	Medical	www.ti.com/medical
Logic	logic.ti.com	Security	www.ti.com/security
Power Mgmt	power.ti.com	Space, Avionics and Defense	www.ti.com/space-avionics-defense
Microcontrollers	microcontroller.ti.com	Video and Imaging	www.ti.com/video
RFID	www.ti-rfid.com		
OMAP Applications Processors	www.ti.com/omap	**TI E2E Community**	e2e.ti.com
Wireless Connectivity	www.ti.com/wirelessconnectivity		

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265