SAFETY CONCEPT OVERVIEW OF HIGH-VOLTAGE (HV) TRACTION INVERTER

ANTOINE DUBOIS, ERIK SANTIAGO, SANDEEP KUMAR

This document is an overview of a system safety concept for a high-voltage traction inverter for electric vehicles. To help NXP customers design a functionally safe electric vehicle, we propose a safety concept example based on NXP components for a traction inverter.

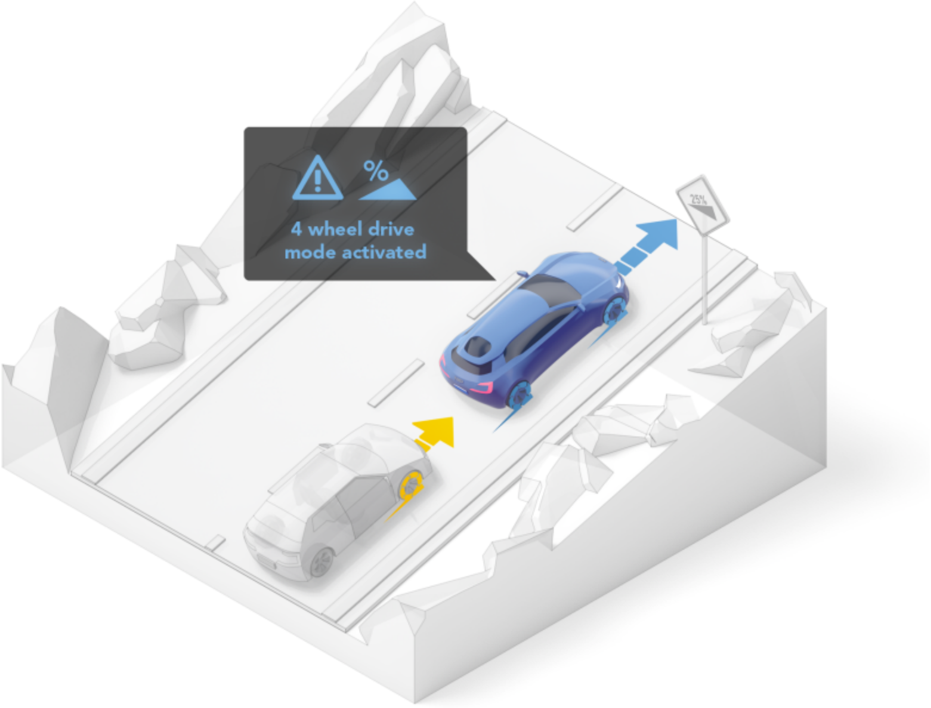

TABLE OF CONTENTS

SAFETY CONTEXT OF THE TRACTION INVERTER

A traction inverter is the main traction system of an electric vehicle. It accelerates the main traction motor and provides regenerative braking according to the torque request from a vehicle control unit (VCU) (Figure 1). For a battery-powered electric vehicle, the motor is generally attached directly to the wheel with a simple gearbox with a 8:1 to 10:1 ratio. The main safety hazards for this type of system are usually unintended traction, unintended braking and high-voltage electrocution. These concerns are addressed differently by car manufacturers and their ASIL ratings vary from ASIL B to ASIL D. In this analysis, the safety goals we considered were:

- **SG1:** Avoid overaccelerating torque beyond 50 Nm or +5% of the requested torque (ASIL D, FTTI=200 ms)
- **SG2ß:** Avoid overbraking torque beyond 50 Nm or +5% of the requested torque

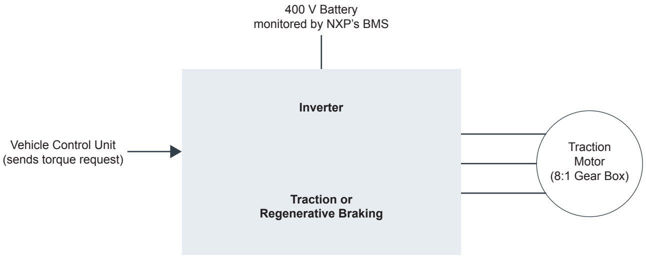

Figure 1: Traction inverter definition

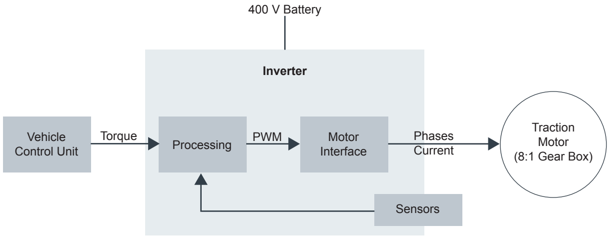

Figure 2: Traction inverter simplified architecture

Typically, the control flow for this type of system is:

- – A torque command is sent from a VCU to the inverter over CAN
- – This torque command is received by the processing unit
- – The processing unit computes the next PWM duty cycle depending on the command and the state of the system
- – The motor interface turns the motor phases on or off depending on the PWM received
- – The processor measures the state of the system: current, position, speed, voltage to close the loop and correct the error

This simplified architecture can be used to explain the safety concept of NXP's traction solution. This document is a summary of a more detailed ISO 26262 methodology that covers the safety goals and the functional, technical, hardware and software requirements.

DOER-CHECKER PROCESSING ARCHITECTURE

In the processing domain, the main failure mechanism that could violate our safety goals, SG1 and SG2, could be summarized as a failure of communication or a failure of computation. This document does not cover the communication failure: the safety mechanism for a system of this type is usually a standard integrity checker in the CAN command to guarantee the integrity of the received command and the availability of the sender and receiver.

The doer-checker architecture (Figure 3) is used to prevent computation failures in this system. This architecture implements the main functional requirements with complex algorithms such as field-oriented control, advanced control techniques and maths functionality. The checker detects unsafe situations and brings the system into a safe state. This allocation reduces the complexity of the safety development as all the safety requirements will be allocated to the checker, while the doer will focus on the performances of the system. In ISO 26262 vocabulary this means that all the requirements allocated to the doer are QM (quality managed), while the safety requirements allocated to the checker are ASIL D. In this study, we regrouped the checker functions and requirements into a system module called safety manager.

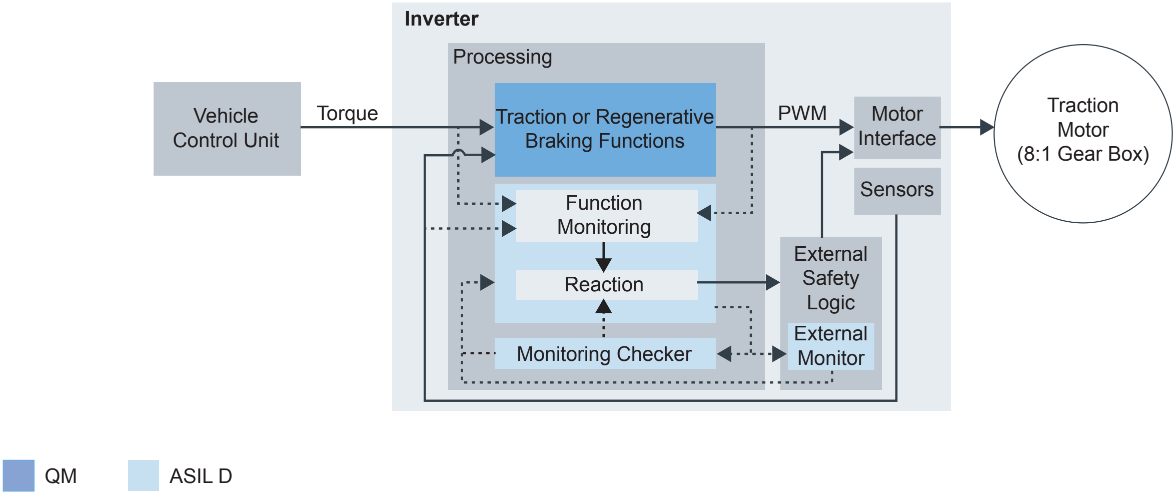

Figure 3: Safety processing allocation

The combination of NXP's MPC5775E microcontroller + FS65 functional safety SBC is suitable for implementing this type of architecture (Figure 4). While the doer is implemented into Core 0 (Non-Lockstep) of the MPC5775E MCU, the safety manager (checker) is implemented into the lockstep Core 1. The common cause of failure between the two cores is detected with a combination of safety mechanisms inside the MPC5775E MCU itself, or inside the external FS65 functional safety SBC. These mechanisms can include the fault collection and control unit (FCCU), the clock monitoring unit, the power management unit, the MPU, and the clock, power, memory and software execution within the FSSBC. Safety manager failures are detected by external monitoring of the FS65 SBC, which brings the system into safe state by directly controlling the motor interface.

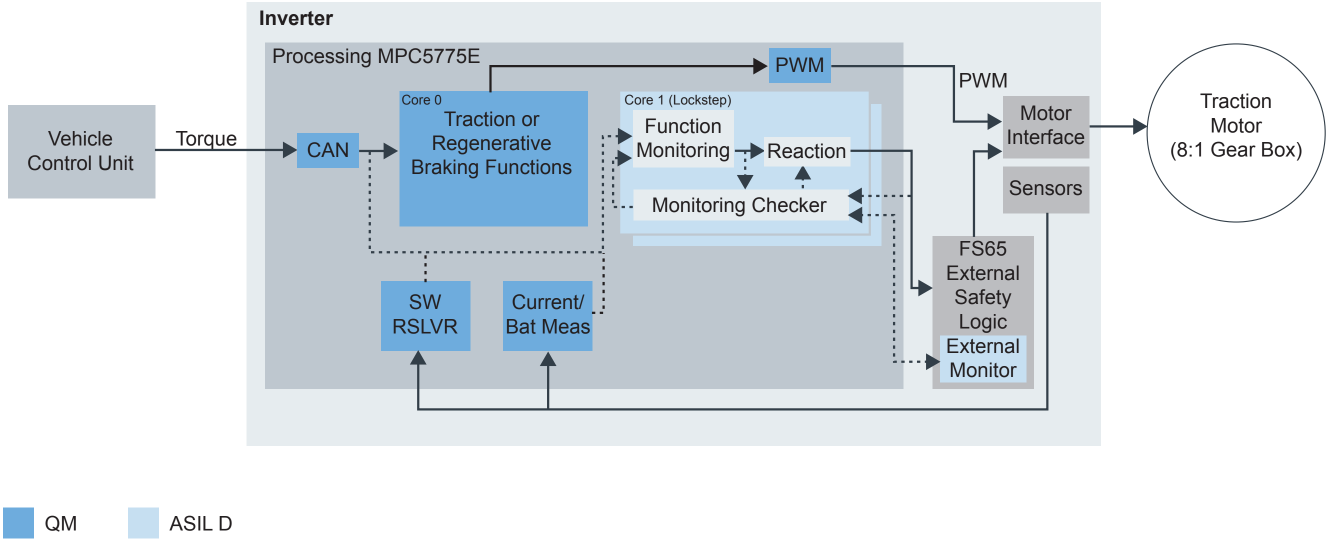

Figure 4: Traction inverter definition

The safety runtime framework for the power inverter is a flexible and modular library of functions to implement the safety manager requirements in accordance with NXP's safety concept.

MOTOR INTERFACE SAFETY CONCEPT FOR A PERMANENT MAGNET MOTOR

One constraint of the new generation of electric vehicles is the high-back EMF generated by the permanent magnet synchronous motor. At high speed, if the PMSM's phases are left open (Figure 5), the generated BEMF voltage can be higher than the battery voltage. This causes a regenerative current and an unintended braking torque for the vehicle. To prevent this hazard, the system must react by shorting the high-sides (3-phase high-side short [3PSHS]) (Figure 6) or the low sides (3-phase low-side short 3PSLS) (Figure 7) of the half bridges to bring the system to a safe state.

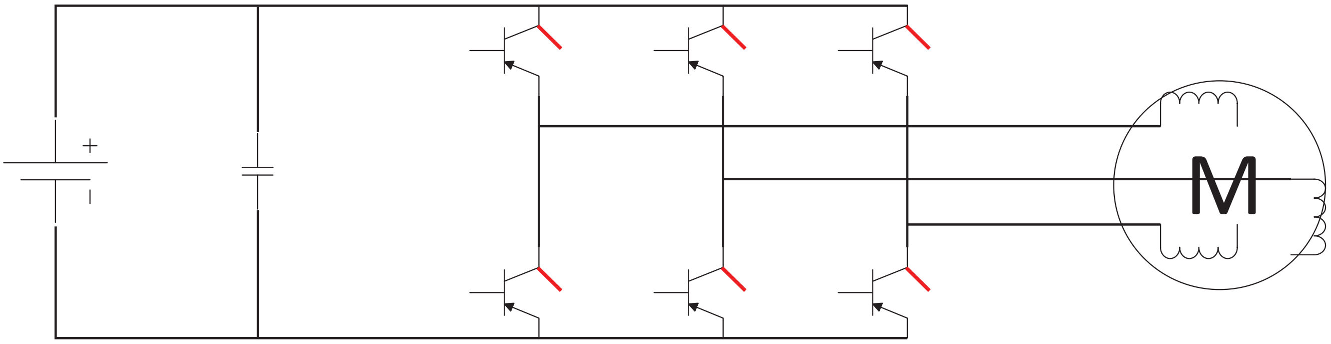

Figure 5: Three-phased open, unsafe at high speed

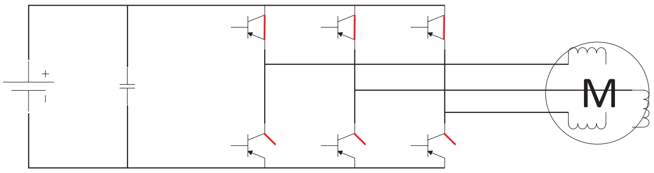

Figure 6: Three-phased short high side

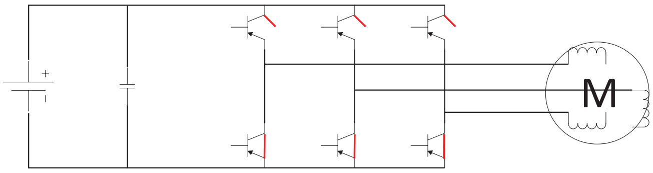

Figure 7: Three-phased short low side

These application specific requirements translate into the following architecture:

- **An independent architecture for the control of the high and low side of the driver bridge:** if a single point failure makes both the high side and the low side unavailable, the system will not be able to react appropriately.
- **Quick short circuit protection (Figure 8a):** A short circuit could permanently damage the complete bridge and place it in an unsafe state. This type of failure occurs too quickly to be handled by the microcontroller, so the GD3100 gate driver must detect and prevent the short circuit independently.
- **High level of diagnostics for appropriate reaction (Figure 8b):** Failure of the motor interface may have different causes: motor phases, IGBT, gate driver, discrete components, cooling; and different reactions to bring it into a safe state. A high-side short failure requires the three phases shorted to the battery (3PSHS) while a high-side open failure requires the three phases shorted to ground (3PSLS) at high speed. The GD3100 gate driver was developed following an ASIL D process. Therefore, it has a high level of diagnostics and can detect 99% of its own faults, in addition to other system failures, including motor and IGBT. It reports them to the MCU safety manager through a redundant interface.
- **Reaction channel (Figure 8c):** Once the fault is reported, the MCU-safety manager can decide which safe state is the most appropriate. The safety state can be controlled through a dedicated pin via a redundant channel of the GD3100. The decision and reaction must be taken within the FTTI ~100 µs.

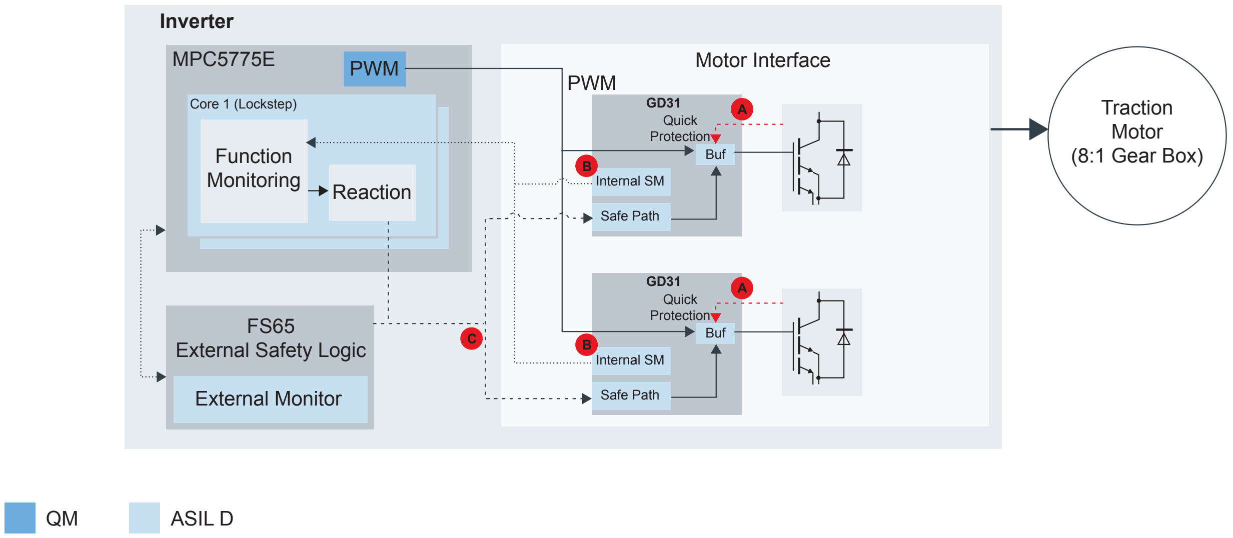

Figure 8: Motor interface simplified safety architecture

NXP's GD3100 gate driver is a key part of this architecture. Key differentiators are:

- Direct control of the IGBT/SiC without booster, which allows a reduction of the overall failure rate and a direct control of the safety path through the gate driver.
- Quick short circuit protection, <2 µs for IGBT, faster for SiC, with turn-off wave-shaping management to avoid destructive overshoot (SSD 2LTO).
- High diagnostic coverage: The GD3100 gate driver was designed from scratch for an automotive ISO 26262 process and has a high diagnostic coverage for internal fault, BIST, watchdog and CRC.

SAFETY CONCEPT OF COMMUNICATION AND SENSORS

To close the loop, the motor control algorithm uses the current, the motor angle position, and battery voltage phases. A wrong sensor acquisition will have a direct impact on the command applied to the motor. The safety requirement regarding sensors is to be able to diagnose any failure of the acquisition chain—the sensors, amplification, analog to digital conversion, and sensor data pre-processing. In the scope of this document we will only focus on the motor position as an example; the methodology is similar for the current and battery voltage.

The system uses a mechanical resolver mounted on the shaft of the motor, an amplification chain and a software resolver (eTPU). The eTPU is a combination of a processor and timer channels, to process complex timing events. The advantage of this architecture is to avoid any computing cycle consumption on the core 0.

The flow chain is represented in blue in Figure 9 (below):

- The eTPU creates an excitation signal to excite the primary of coil
- Two coils shifted 90 degrees measure the sin and cos of this signal. The received excitation varies depending on the shaft angle.
- Sigma delta ADCs measure the two signals, synchronously of the excitation signal. The results are put in the eTPU RAM for processing.
- The signal is demodulated and the angle and speed are calculated using a tracking observer model. Then, to improve the accuracy, the angle is extrapolated to correct the error due to the delay between the acquisition time to the end of processing time.
- The angle is consumed by the motor control algorithm.

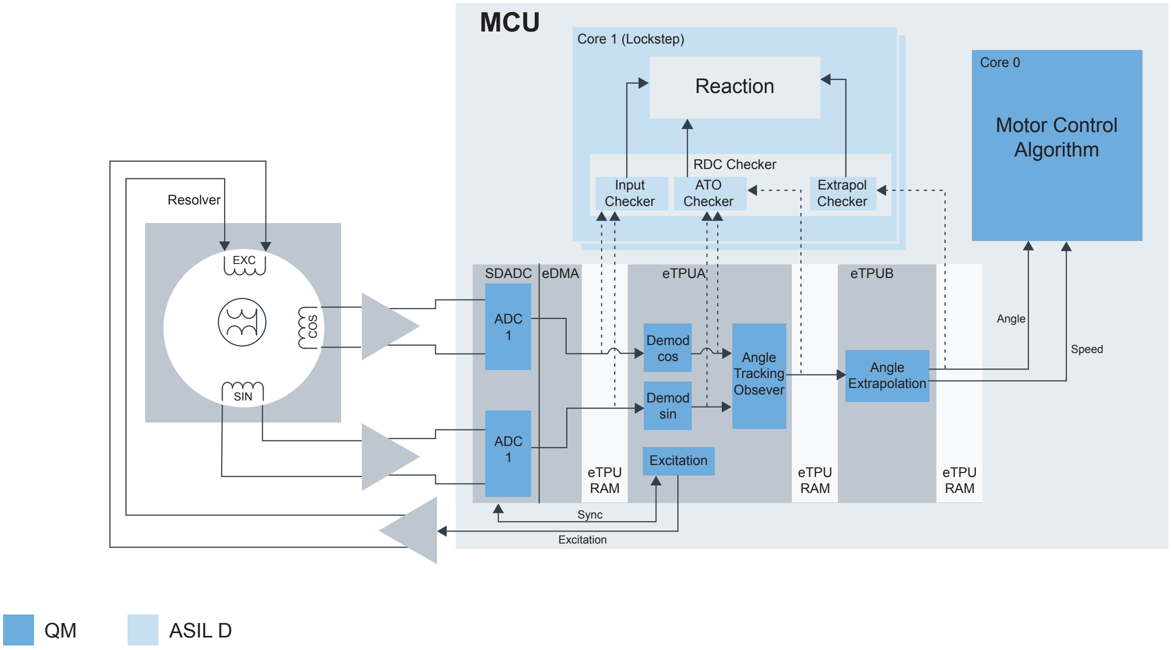

Figure 9: Motor position safety concept

The RDC checker library runs into the safety core and performs diagnostic into the flow chains to diagnose all possible faults. The input checker looks at the raw values to calculate the synchronization of the excitation signal with zero crossing, the maximum and minimum amplitude and the unit vector. With this checker, 99% of hardware failures concerning amplification, coils, excitation chains and SD-ADC are detected.

The ATO checker computes the angles differently to the eTPU tracking model and runs some plausibility checks. It detects failure of the ETPU computation. Similarly, the extrapolation checker implements safety mechanisms to detect failure of the angle extrapolation functions.

The RDC checker, motorinterface and MCU LL safety are part of NXP's safety library for the inverter.

This library is delivered with the hardware solution. It is a flexible and modular library for customers to adapt NXP assumptions to their own safety case.

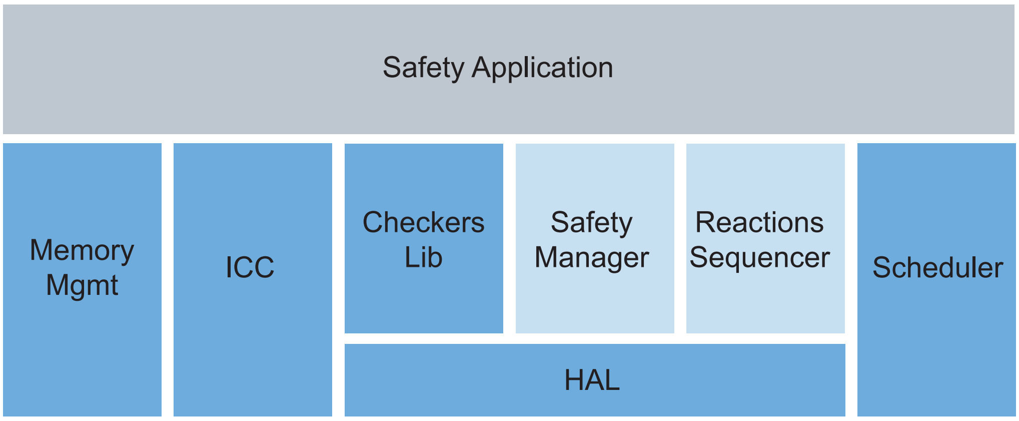

Figure 10: Simplified architecture of NXP safety inverter library

SAFETY ENABLEMENT DELIVERABLES

The processing, the motor interface and the motor position safety concepts are three simplified examples of NXP's safety architecture for EV tractions systems. A more detailed description that includes traceable requirements, ASIL allocation and decomposition, state machines and failure analysis is available in the functional safety concept and technical safety concept applications notes delivered under NDA to customers. These concepts are made to be flexible and adapted by customers to their own applications. They were implemented in hardware and software as part of NXP's EV power inverter reference platform: **https://www.nxp.com/design/designs/ev-power-inverter-control-reference-platform:RDPWRINVERTER.**

In addition, to simplify the usage of the complex hardware, software and system safety mechanism, NXP also offers an application-specific library to accelerate our customer safety development. Please contact the NXP Sales representatives for more information.

CONTRIBUTOR

Antoine Dubois, Erik Santiago,
and Sandeep Kumar

HOW TO REACH US

Home Page: www.nxp.com
Web Support: www.nxp.com/support

USA/Europe or Locations Not Listed:
NXP Semiconductors USA, Inc.
Technical Information Center, EL516
2100 East Elliot Road
Tempe, Arizona 85284
+1-800-521-6274 or +1-480-768-2130
www.nxp.com/support

Europe, Middle East, and Africa:
NXP Halbleiter Deutschland GmbH
Technical Information Center
Schatzbogen 7
81829 Muenchen, Germany
+44 1296 380 456 (English)
+46 8 52200080 (English)
+49 89 92103 559 (German)
+33 1 69 35 48 48 (French)
www.nxp.com/support

Japan:
NXP Japan Ltd.
Yebisu Garden Place Tower 24F,
4-20-3, Ebisu, Shibuya-ku,
Tokyo 150-6024, Japan
0120 950 032 (Domestic Toll Free)
www.nxp.com/jp/support/

Asia/Pacific:
NXP Semiconductors Hong Kong Ltd.
Technical Information Center
2 Dai King Street
Tai Po Industrial Estate
Tai Po, N.T., Hong Kong
+800 2666 8080
support.asia@nxp.com

nxp.com/safeassure

Document Number: INVERTERSAFWPA4 REV 1