Technical Article

How Voltage References and Supervisors Help Achieve ASIL Functional Safety Goals

Many safety related automotive systems are required to meet Automotive Safety Integrity Level (ASIL) as defined by International Organization for Standardization (ISO) 26262.

It is a common misconception that integrated circuits (ICs) not developed following the ISO 26262 standards cannot be used to achieve functional safety goals. Many automotive OEMs have been able to use the features and reliability of non-ASIL compliant semiconductor devices to develop systems that target ASIL requirements. In this post, it will be demonstrated how both voltage references and supervisors can help you achieve ASIL compliance for your automotive systems.

Voltage References and Supervisors

Devices such as voltage references and supervisors (reset ICs) are common semiconductor devices that can help automotive system integrators develop functionally safe systems. When used in automotive applications, these devices provide diagnostic coverage or redundant monitoring capability.

Figure 1 is taken from ISO26262-10:2018, 9.2.3.4 and is an example of how safety elements out of context (SEooC) can implement voltage supervisors and watchdogs as safety mechanisms.

9.2.3.4 Step 1b — Assumptions on system level design

Some examples of system level design assumptions, external to the SEooC:

a) The system will implement a safety mechanism on the power supply to the MCU to detect over voltage and under voltage failure modes.

b) The system will implement a windowed watchdog safety mechanism external to the MCU to detect either clocking or program sequence failures of the MCU.

Figure 1. System-level Design Assumptions for SEooC Based on ISO 26262

Features and Mechanisms of Voltage Reference and Supervisors

A voltage supervisor can help achieve system-level functional safety targets by providing power supply fault detection. A voltage supervisor implements a safety mechanism to the microcontroller (MCU) when an overvoltage or undervoltage failure mode is detected on the power supply. Some voltage supervisors can also provide digital diagnostics with watchdog timers that can detect clocking failures of an MCU. Clocking failures include late pulses or early pulses sent from the MCU. The window watchdog timer can monitor these pulses and alert the system that a fault has occurred. Another method of under and overvoltage monitoring is to use an analog-to-digital converter (ADC) with a precision voltage reference to monitor multiple voltage rails. Figure 2 shows how a window watchdog timer operates. In some cases, systems with very high diagnostic coverage goals may require redundant safety mechanisms in order to achieve system-level functional safety goals. This means that in addition to an ADC and voltage reference to monitor potential voltage supply failures, a supervisor is also required to monitor the same voltage rails to ensure safety and diagnostic coverage.

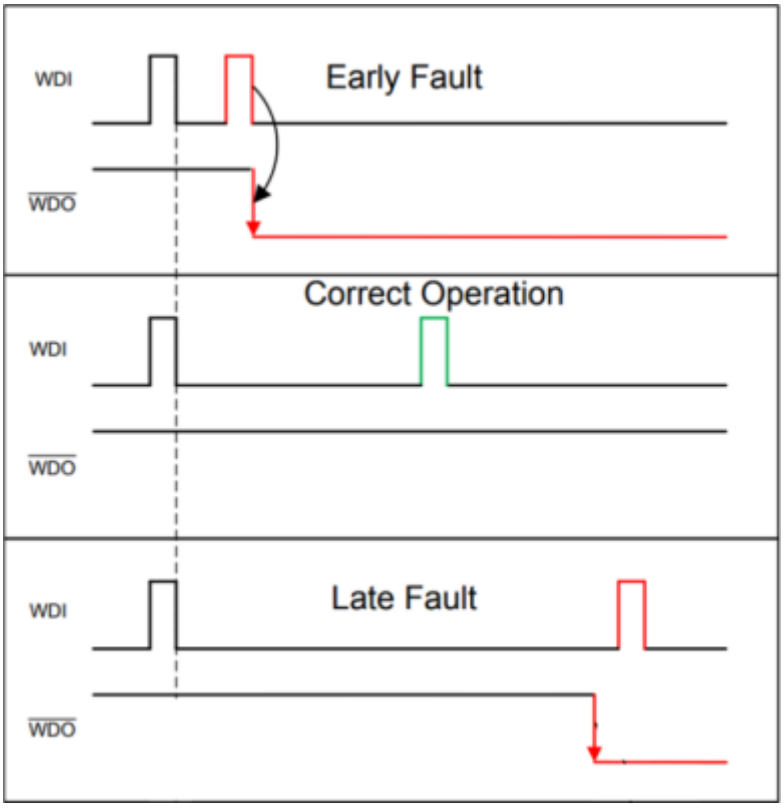

Figure 2. Window Watchdog Timing Diagram

Device Functional Safety Collateral

Risk assessments of automotive systems show that faults can occur due to IC failures; therefore evaluations at the device level are required in some functionally safe systems. TI can provide device information needed for evaluating the IC versus the requirements of the functional safety system concept. TI can provide device collateral such as qualification reports, failure in time (FS-FIT), failure mode distributions (FMD), and design failure mode and effect analysis (DFMEA) for voltage references and supervisors.

Automotive Reference Designs with Functional Safety Considerations

The "ADAS power reference design with improved voltage supervision" shows how voltage references and supervisors can help in implementing functionally safe systems. The voltage reference and supervisors used in this reference design can help enable the designers achieve the system-level functional safety goals when combing the devices' functionality, features and device collateral.

The reference design provides an automotive power solution with additional voltage supervision and a window watchdog for safety MCUs in advanced driver assistance systems (ADAS). The design helps achieve accurate voltage monitoring with precision supervision of 1% maximum across temperature and includes features such as flexible reset delay and manual reset. The TPS3703-Q1 provides overvoltage and undervoltage monitoring in a small footprint, with minimal needs for external components to help solve space constrained problems.

Figure 3 describes how the TPS3703-Q1 detects overvoltage and undervoltage. For potential clocking failures, the TPS3850-Q1 doubles as an overvoltage/under-voltage monitor and window watchdog timer which is illustrated in Figure 2 and Figure 3. It also has the flexibility of changing the watchdog timeout and window ratio and disabling the watchdog timer. In cases where only undervoltage monitoring is necessary, the TPS3890-Q1 can provide accurate voltage monitoring at a very low quiescent current to save system power consumption. Last but not least, the LM4132-Q1 provides precision voltage to reference the ADC for voltage monitoring. With 0.05% initial accuracy and low temperature drifts of 10 ppm/°C, the LM4132-Q1 solves accurate voltage monitoring at a low supply current cost of 60 µA.

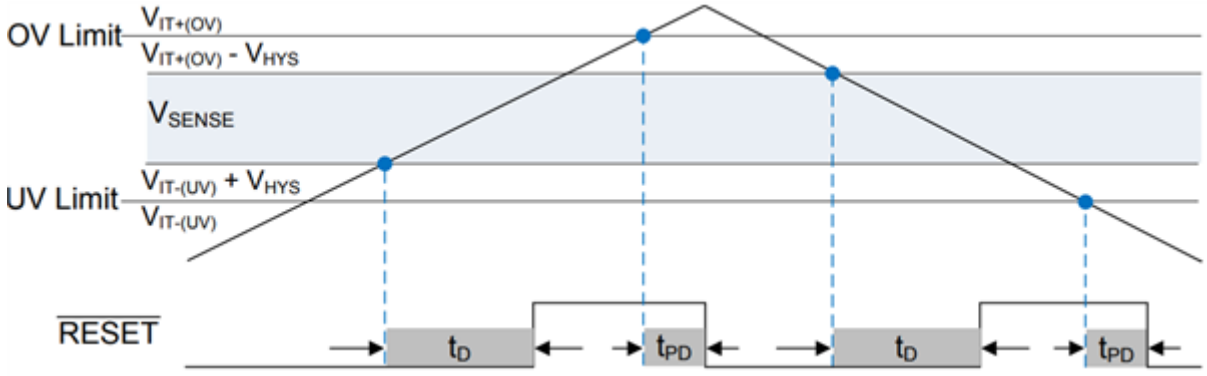

Figure 3. Under-voltage and Over-voltage Window Detector Timing Diagram

Accommodating the ISO 26262 Standard in the ADAS Power Reference Design

The reference design takes ISO 26262 and its guidance on power-supply voltage monitoring and watchdog diagnostics into consideration. Figure 4 explain the need for detecting failures in the power supply and failures in a defective program sequence. Figure 4 is taken from ISO26262-5:2018, Annex D. This annex is intended to evaluate diagnostic coverage and is used as a guideline to choose appropriate safety mechanisms to detect possible system failures. The reference design can help in implementing system-level safety mechanisms shown in Figure 4.

D.2.6 Power supply

Global objective: To detect failures caused by a defect in the power supply.

D.2.6.1 Voltage or current control (input)

NOTE This technique/measure is referenced in Table D.7.

Aim: To detect as soon as possible wrong behaviour of input current or voltage values.

Description: Monitoring of input voltage or current.

D.2.6.2 Voltage or current control (output)

NOTE This technique/measure is referenced in Table D.7.

Aim: To detect as soon as possible wrong behaviour of output current or voltage values.

Description: Monitoring of output voltage or current.

D.2.7 Temporal and logical programme sequence monitoring

NOTE This group of techniques and measures is referenced in Table D.8.

Global objective: To detect a defective programme sequence. A defective programme sequence exists if the individual elements of a programme (for example, software modules, subprograms, or commands) are processed in the wrong sequence or period of time, or if the clock of the processor is faulty.

D.2.7.1 Watchdog with separate time base without time-window

NOTE This technique/measure is referenced in Table D.8.

Aim: To monitor the behaviour and the plausibility of the programme sequence.

Description: External timing elements with a separate time base (for example, watchdog timers) are periodically triggered to monitor the processor's behaviour and the plausibility of the programme sequence. It is important that the triggering points are correctly placed in the programme. The watchdog is not triggered at a fixed period, but a maximum interval is specified.

Figure 4. Safety Mechanism Examples for Power-supply and Watchdog Failures Based on ISO 26262

The voltage supervisors and references used in this reference design can provide an additional layer of safety by providing extra diagnostic coverage, safety mechanisms or redundant safety monitoring. The product's performance and functionality of detecting faults can help achieve functional safety goals in automotive systems. Additionally, TI can provide collateral to improve time-to-market for system integrators.

Additional Resources

- For more information on why watchdog timers are important, read the blog post, “What is a watchdog timer and why is it important?”

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

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