Enabling precision delta-sigma ADCs in functional safety applications

By Lars Lotzenburger
System Engineer

Introduction

This article discusses analog-to-digital converter (ADC) failure modes and introduces options to address them in functionally-safe systems. Additionally, the trade-offs between single-channel and redundant-channel functional safety architectures are discussed. This article assumes that the reader is familiar with functional safety basics and nomenclature. Please refer to IEC61508-4: "Definitions and Abbreviations" for more information.

A standard ADC in the functional safety context

According to IEC 61508, a software-programmable ADC is rated a complex device (type B). "For complex components, where a detailed analysis of each failure mode is not possible, a division for failures into 50% safe, 50% dangerous is generally accepted" [IEC61508-6 Annex C]. The resulting safe failure fraction (SFF) of 50% does not even satisfy the requirements of a system with a safety integrity level (SIL) of one and a hardware fault tolerance (HFT) of zero, but turning dangerous (undetected) faults into detectable faults through additional monitoring and diagnostics increases the diagnostic coverage (DC) and SFF.

The following are commonly assumed failure modes for a multi-channel ADC:

- *ADC offset out of specification*—caused by an imbalance of the two analog inputs (AIN+, AIN–). The real ADC transfer function has a positive or negative offset to the ideal transfer function. The offset error is composed of the initial error (at 25°C) and the offset drift over temperature.

- *ADC gain out of specification*—mainly caused by accuracy and drift of the integrated or externally connected voltage reference, but also from the ADC. The real ADC transfer function has a different slope compared to the ideal transfer function. The gain error is composed of the initial gain error (at 25°C) and the gain drift over temperature.

- *ADC clock frequency out of specification*—a variation of the ADC system clock over temperature and time. The clock accuracy is particularly important in delta-sigma ADC architectures with a digital filter. The filter curve of a built-in SINC-type filter, often used for 50-/60-Hz mains frequency rejection, is directly dependent on the clock accuracy.

- *ADC output-code bit error*—one or more sample code bits cannot change its value (stuck-low or stuck-high). This stuck-at fault may lead to the wrong output codes.

- *Communication error*—a one- or multi-bit error in the bidirectional communication between the ADC and the host (microcontroller or microprocessor). A possible reason for a bit flip may be electromagnetic interference (EMI).

- *Soft error*—a random bit flip in a volatile register caused by high-energy particles. A random bit flip can cause unpredictable ADC behavior. A reset/power cycle can remove this transient fault.

- *Incorrect channel selected*—in a multichannel ADC topology, the converter samples a different channel than intentionally selected. Even cross-channel conversions are possible if the differential ADC input voltage comprises signals from two channels.

- *Channel-to-channel short*—a short circuit between two analog input channels in a multichannel ADC topology, caused by board manufacturing issues or bond-wire displacements.

- *Short circuit of any two pins*—the impact of a short of any two pins of the ADC is assessed with the pin failure mode analysis (FMA) provided by the ADC vendor.

At a system level, additional failure modes may be present:

- *Supply voltage out of specification*—any supply voltage to the ADC must be in a valid range. An under-voltage condition may lead to unpredictable behavior of the ADC. An overvoltage condition may damage the ADC.

- *Ambient temperature out of specification*—exposing the ADC to temperatures outside its specified limits may result in the wrong conversion results. The accelerated aging caused by an over-temperature condition may affect device reliability over its lifetime.

Single-channel ADC architecture

This section discusses options to handle the previously defined failure modes. Figure 1 shows a possible block diagram of single-channel architecture with the ADS1259 and two analog input channels.

ADC *offset error* can be determined by converting a 0-V input signal (short). The result provides the offset, which is deducted from successive real measurements.

Gain errors, mostly introduced by the voltage reference, can be detected by applying an externally generated voltage at/near full scale. This differential voltage is generated by two precision resistor ladders independent of the reference voltage of the ADC and is temporarily connected to the analog input pins. The resistor ladders have multiple taps to generate test voltages with different polarities, spans and common modes.

The ADC *system clock accuracy* may be monitored by the host using time relation of communication signals between an ADC and host. As the conversion time (in ADC clock cycles) is deterministic, it is possible to measure the duration of a conversion. The ADS1259 used in the example features a dedicated START signal to start a conversion and data ready (#DRDY) signal to indicate an end-of-conversion event to the host. Both signals may be captured by a host capture unit available in most of the microcontrollers in the market today. Replacing the START signal with a software start command may save a communication signal.

The ADC *output code bit error* is detectable by forcing predefined output codes. Applying two voltage inputs resulting in bit-complementary output codes verifies the vitality of ADC output code bits. The corresponding voltages may be generated as part of the precision resistor ladder described earlier. Alternatively, a dedicated digital to analog converter (DAC) can be used, which generates voltages that only one output code bit is set for a given conversion (walking bit test).

A *communication error* between the ADC and the host can cause the ADC to behave unexpectedly, e.g. by writing a control register with incorrect data. If no further communication diagnostics, such as cyclic redundant check (CRC), are in place, then an inbound data transfer (e.g. register write) may be verified by an immediate read of the same register. An outbound data transfer (e.g. data read) may be performed multiple times and compared to ensure data integrity. Recently-released ADCs from TI, including the ADS1260, verify digital communication integrity with a CRC in both directions. The serial interface (SPI) should reset between transfers either by timeout or the chip select (CS#), which clears unintended pulses caused by EMI, for instance.

A *soft error* may be detected by frequent readouts of the ADC register map. The SPI clock is in the tens-of-megahertz range, with optimized read commands in place, such as bulk register read, to perform this task as fast and effectively as possible within the diagnostics test interval. Hardware-only configurable ADCs like the ADS1225 have a functional safety advantage as no registered soft errors can occur at the cost of flexibility and feature set. However, an ADC may use one-time programmable (OTP) fuses for the internal configuration of the device.

Figure 1. Single-channel ADC architecture with the ADS1259
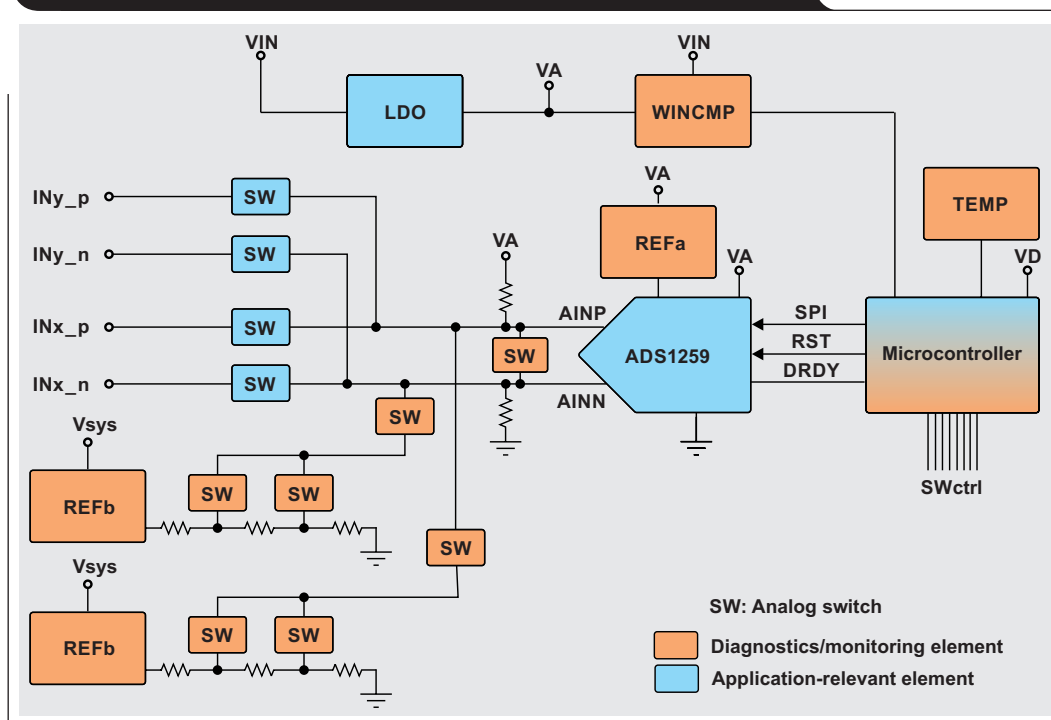
The *incorrect channel selected and channel-to-channel short* failure modes cannot occur at the chip level as the example in Figure 1 features a single-channel ADC. If multiple analog input channels are required, an external multiplexer may be easier to diagnose than an integrated multiplexer due to the use of discrete (simple type A) components and accessibility of control signals.

The *supply voltages* at the system level are permanently monitored by window comparators. Actions in case of a voltage out-of-range may vary from temporary disconnection of the supply voltage up to passivation of the entire application—depending on the application requirements.

The *temperature* is permanently monitored by an analog output temperature sensor to ensure the components work in the specified ambient temperature range.

Generally, the sanity check of successive sample series can help to detect failures in the signal chain. For instance, if a low-pass in the analog front-end is in place, a maximum allowed delta of successive samples can be determined.

Fault-tolerant (redundant) architecture

Working with redundant channel architectures may increase the fault-tolerance of the system. The additional functional safety challenge, which comes with it, is the common-cause fault. These faults impact all system channels equally and therefore cannot be detected by comparison of the channel outputs. For example, if both channels of a 1oo2 architecture drift the same way due to temperature or EMI, they may appear to be intact. However, such faults can still be detected by per channel diagnostics.

Still, the channel output comparison is an effective means to detect faults which are not related to common-cause source. If the outputs differ beyond an accepted delta the safe state may be entered. Figure 2 shows a redundant analog signal chain block diagram.

Temperature-dependent faults like *offset drift, gain drift* and *clock drift* errors can occur on both ADCs, as they are (also) temperature dependent. Therefore, protective measures implemented in the single-channel architecture remain.

Figure 2. A redundant analog signal chain
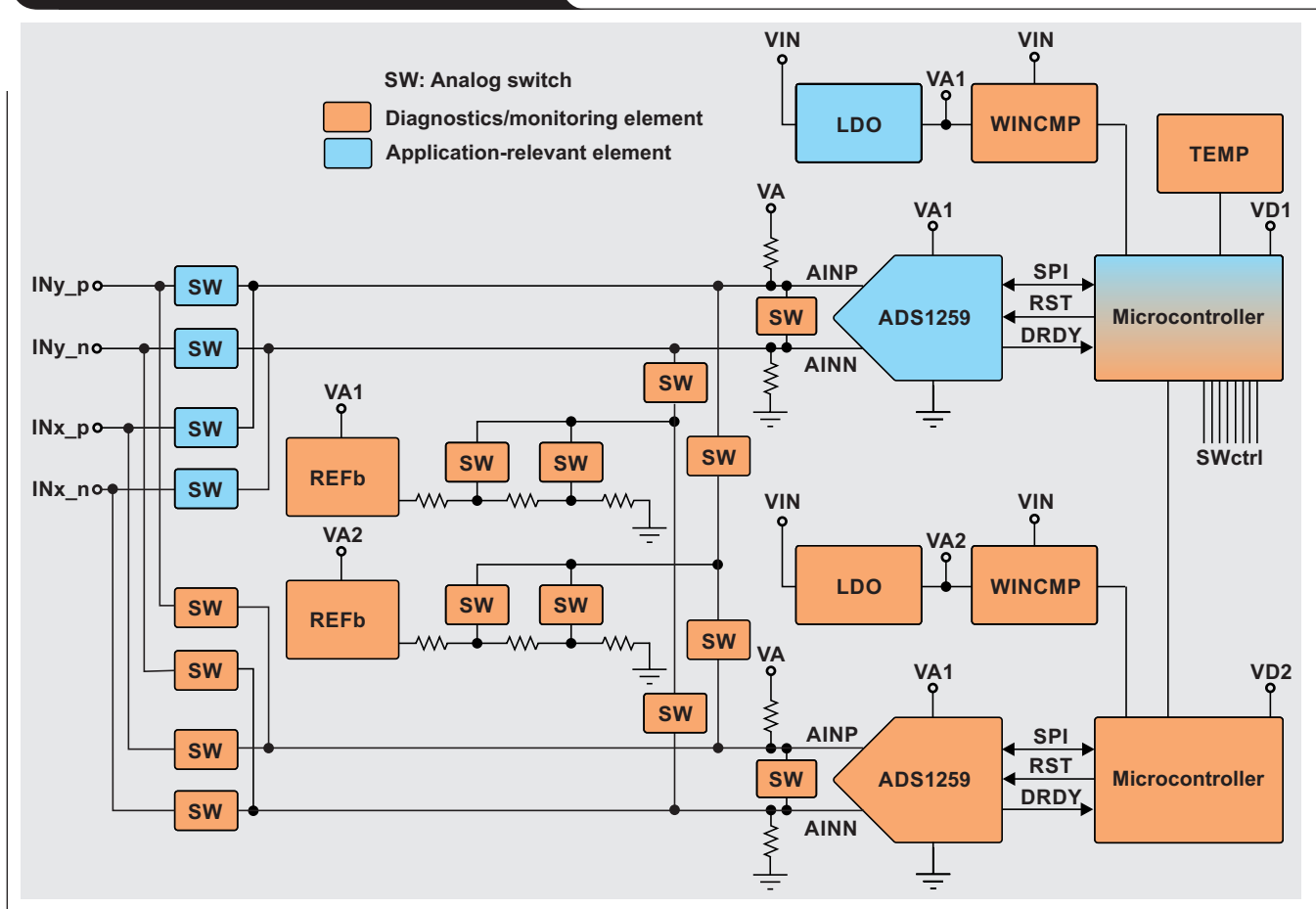
Comparing channel results reveals *ADC output code bit errors* and *communication errors* during data sample reads. More immunity against radiation can be achieved by setting a small time delay for the communication to the ADCs to minimize the risk that both data frames are identically affected.

A relevant *soft error*—for example, a register bit flip—is also detectable by comparison, as the likelihood that this happens to both ADCs at the same time to the same register is nearly zero. Still, the frequent read out of the register map of each ADC is useful to determine which channel is faulty.

Each channel should have its own power tree. It is common that an invalid power supply voltage may affect both channels the same way.

Related Web sites

General information:

IEC 61508: Overview (Wikipedia)

ISO 13849: Overview (Wikipedia)

Product information:

Functional safety landing page, Texas Instruments
ADS1225
ADS1259
ADS1260

TI Worldwide Technical Support

TI Support

Thank you for your business. Find the answer to your support need or get in touch with our support center at

www.ti.com/support

China: http://www.ti.com.cn/guidedsupport/cn/docs/supporthome.tsp

Japan: http://www.tij.co.jp/guidedsupport/jp/docs/supporthome.tsp

Technical support forums

Search through millions of technical questions and answers at TI's E2E™ Community (engineer-to-engineer) at

e2e.ti.com

China: http://www.deyisupport.com/

Japan: http://e2e.ti.com/group/jp/

TI Training

From technology fundamentals to advanced implementation, we offer on-demand and live training to help bring your next-generation designs to life. Get started now at

training.ti.com

China: http://www.ti.com.cn/general/cn/docs/gencontent.tsp?contentId=71968

Japan: https://training.ti.com/jp

![Texas Instruments logo]

SLYT792

IMPORTANT NOTICE AND DISCLAIMER