Functional Safety in a Data Acquisition System

By **Chris Norris**

Share on

Introduction

Functional safety is part of an overall safety strategy within many industries that attempts to reduce, to a tolerable level, the probability of harm coming to humans or operating equipment. The requirement for systems to be functionally safe has grown significantly in recent years. From nuclear power plants to medical devices, an errorless system has become an ideal for some and a necessity for others. For example, in the sensing world, acquiring incorrect or corrupted data can be devastating and potentially lethal depending on the system and the level of risk involved.

Traditionally, the onus was on the system developer to incorporate diagnostic and failure prevention mechanisms onto their products to ensure integrity of the data coming from the sensing IC. This came at the cost of PCB area, bill of materials, processing overhead, and, ultimately, expense. Since then, through extensive engagement with system design engineers, a solution has been developed to address this problem for them. To that effect, functional safety features have begun to be designed in at the IC level.

This article explores the functional safety potential of ADCs in terms of ensuring the overall integrity of a data acquisition system.

A Legacy Functionally Safe Solution vs. a Better Way

In Figure 1, we see an example of a functionally safe system as it was in years gone by, and we compare it with a more modern solution. At the epicenter is the data acquisition ADC that converts the analog inputs and transmits the data to a microcontroller. To achieve this solution, however, requires many external components, repeated SPI transactions, and even a redundant ADC, which greatly increases the bill of materials, PCB area, processing overhead, and cost. It also places extra burden, such as development time and reliability, on system designers to develop this solution.

There is a single IC solution available, with minimal external components required, to operate the functional safety features.

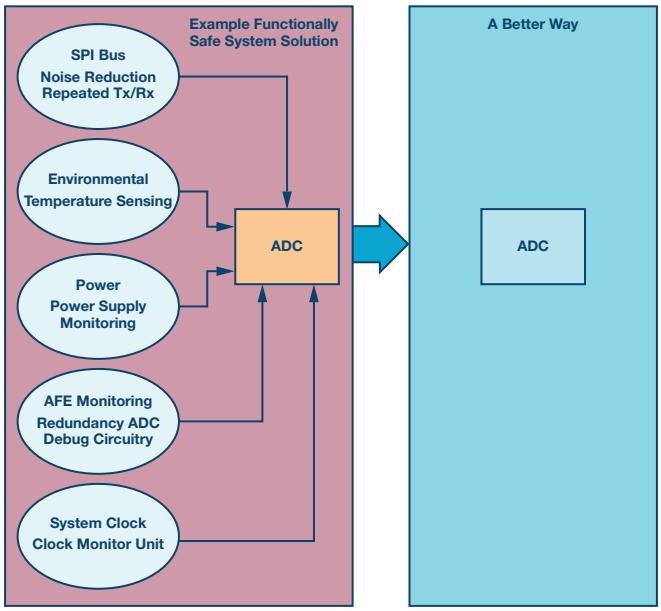

Figure 1. Integration from multicomponent functional safety system to single-chip ADI solution.

An Example System with Functional Safety Requirements

In data acquisition systems that contain an ADC, many faults can occur that may increase the risk to human or machine health depending on the application. System designers must distinguish between acceptable and nonacceptable risk.

As an example, in a system that measures and regulates the pressure in a gas chamber, using a sensor that has a tolerance of 5% may be seen as

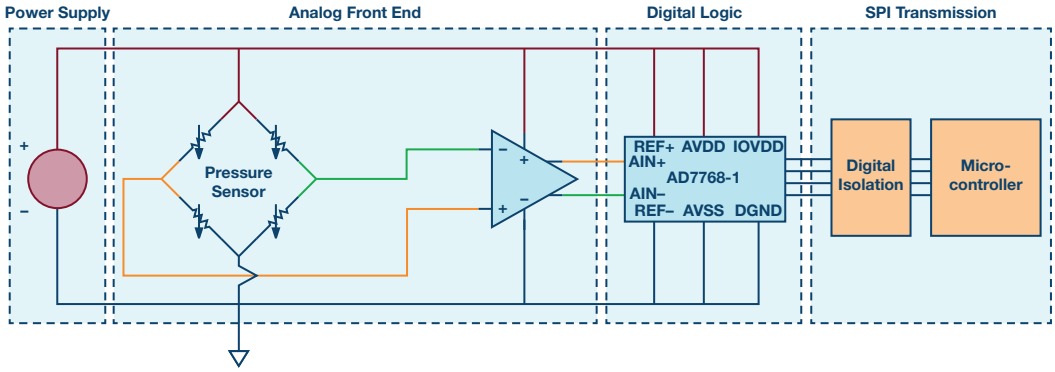

Figure 2. Identifying the potential sources of failure in a pressure sensor system.

an acceptable risk if the pressure inside the tank should not deviate greatly from the outside pressure. However, if the microcontroller receives incorrect ADC data, this could lead to a potentially fatal occurrence whereby the pressure in the chamber causes an implosion or explosion, both of which can injure or kill people nearby. This level of risk is unacceptable. Therefore, some functional safety measures should be put in place to ensure the integrity of the information being received by the controller.

Some sources of fault that could cause these type of errors are

- Power supply: low power supply voltage, low voltage output of the low dropout (LDO) regulators.
- Analog front end (AFE): damaged sensors or amplifier driving an incorrect voltage to the ADC.
- Digital logic: bit errors in the digital domain that can affect the converted result. For example, the factory gain or offset trim coefficient.
- SPI transmission: bit errors in the transmission of the converted data and receiving of commands due to a noisy environment of the transmission line.
- Environmental: out of the specified ambient temperature for the IC.

The AD7768-1, one of the Σ-Δ ADCs within ADI's functional safety portfolio, has a vast suite of diagnostic features intended to allow users the ability to detect and diagnose errors and more. Figure 2 highlights the sources of some of the possible faults in a typical pressure sensing system.

Using the ADC to Diagnose the System Errors

Within the functional safety portfolio of ADI ADC products comes the ability to use an ADC to help diagnose and/or reduce the system errors. This ability to measure system errors is important in maintaining accurate measurements, and in a system that has functional safety requirements, this accuracy is even more crucial.

Positive and negative full-scale voltages, taken from the reference inputs, are used to measure the gain error of the system. A zero-scale internal short is used to measure the offset error. Users can then trim the offset and gain error performance of their system using the gain and offset trimming registers of the ADC.

A temperature sensor identifies changes in the temperature locally of the IC, including out of bounds temperatures. In a system sensitive to offset and gain error drift over temperature, this can be an attractive function. If a sizable temperature change has occurred, users may decide to trim out the gain and offset errors at this new temperature. Figure 3 illustrates how an analog diagnostic mux is connected to the ADC internally in the AD7768-1.

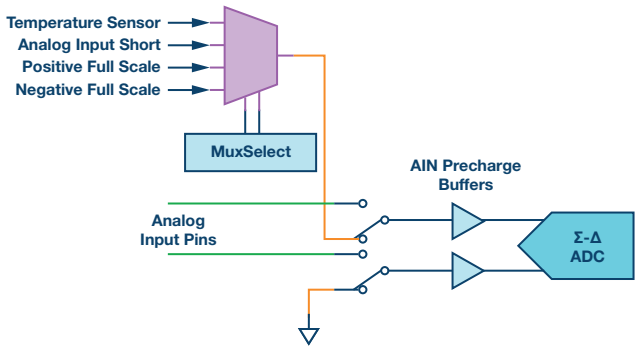

Figure 3. Switching to convert the analog diagnostic mux.

Diagnostic Error Flags: The Register Map Diagnostic Status Indicators

Several diagnostic features may be enabled and their status can be flagged to the user, typically via the register map. If a fault occurs, an error flag is set in a register. Users can investigate further once they are alerted to the fault.

Let's speculate on some real life faults that can occur and that can be diagnosed using the portfolio of ADI functional safety ADCs. Let us first presume that our pressure sensor system is based in an industrial plant, with fluctuating temperatures, several shutdowns in power due to essential maintenance, and electromagnetic interference (EMI) from the surrounding industrial setting that can be conducted onto the system PCB.

ADC Supply Error

Let's assume that, due to the high temperatures present in the environment and inrushes of current caused by the power cycling of the system, the LDO capacitors tasked with holding charge close to the ADC's LDO supply outputs have become worn and damaged. Maintaining these outputs at a known voltage requires an external capacitor and is essential for correct operation. If the capacitors are damaged due to this fault, users can notice that the converted ADC data or performance of other functions are unexpected. By enabling LDO monitors, once the voltage level drops below a certain trip point, an error flag will be set to alert users of issues at the LDO outputs.

Analog Front-End Error

Let's presume this is a system where the inputs to the ADC should not exceed the full-scale range of the ADC. If users accidentally program an incorrect value to the gain register that increases the voltage seen by the

ADC to be greater than the full-scale range, then this will greatly affect the gain error performance of the system and should be seen as a serious risk. However, the **Filter Saturated** error checker monitors ADC output and will alert users to an out-of-range analog input.

Digital Logic Random Bit Errors

Random bit errors occur occasionally within digital logic and memory blocks. In our example pressure system, let us say that a bit error has occurred loading the default factory offset setting during power-up. This is an intolerable fault as it disturbs the default offset error of the system, affecting the converted result. Within the ADI portfolio of functional safety ADCs there are functions available that run cyclic redundancy checks (CRCs) on the various memory blocks at regular intervals and flag faults to the user whenever a bit error occurs. A reset of the system will solve all of these faults.

SPI Transmission Errors

Every system that transmits data along a medium will incur some bit errors along the way.

The rate at which this occurs can be estimated for every system, called a bit error rate (BER).

In our example pressure system, a BER of less than 10^{-7} can be assumed if transmitting to a microcontroller on the same PCB over a distance of 10 cm through digital isolation.

Let us presume that some electromagnetic interference is conducted onto the SPI lines and this results in a bit error in the transmission of converted ADC data from the AD7768-1 to the microcontroller. A bit error in the ADC data could be potentially devastating if it masks any building pressure in the gas chamber. By appending a CRC to the end of the transmitted data, users can identify if a bit error has occurred during transmission and can recheck the ADC conversion result.

External Master Clock Error

If users are concerned about rejecting the frequencies of the main power supply (50 Hz/60 Hz) in a pressure sensor application, then an accurate low jitter external master clock source is important to align the notch of the digital filter to the correct frequency. If a source becomes disconnected, worn, or damaged, this is a huge concern as some frequency components of the main supply may become visible in the converted ADC data.

The external clock qualifier can flag an error to the users if the external clock source has not been connected successfully or if it has been removed. Users can then perform emergency conversions with the internal RC oscillator while essential maintenance is carried out on the external master clock source.

POR Flag

Once a system is powered-up or successfully reset, the POR flag within the ADC will be set.

However, if an unexpected reset occurs, users may see unexpected results in the ADC data. They can identify this unexpected reset by checking the POR flag.

Figure 4 shows how many of these internal diagnostic features within the AD7768-1 hook up to the functions they will be monitoring.

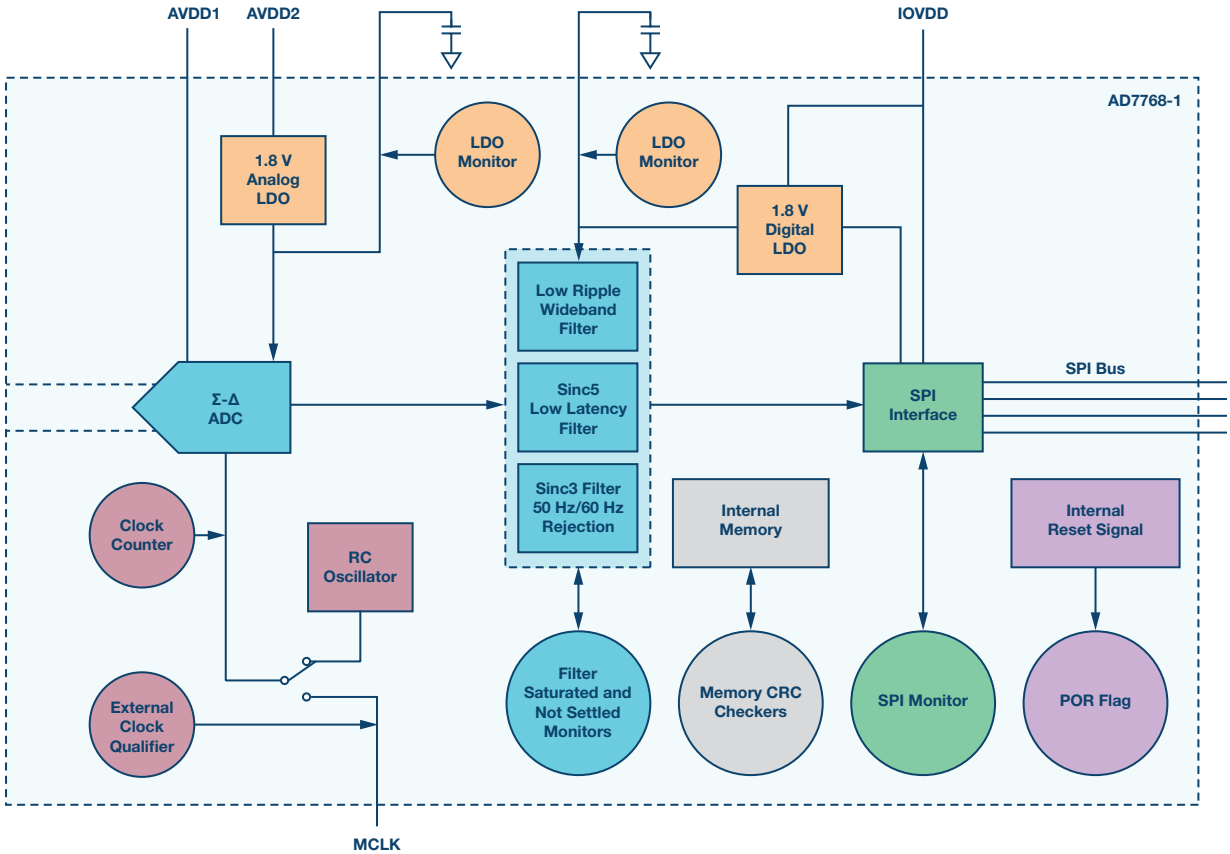

Figure 4. Internal diagnostic monitors of the AD7768-1.

The Ultimate Functional Safety Solution Using the AD7768-1

Using the functional safety features provided by the AD7768-1, the following data acquisition system is possible. Users can power up the part and enable the following functional safety features:

- SPI integrity monitors
- LDO regulator output level monitoring
- A filter saturation monitor
- An external clock qualifier
- Internal logic and memory CRC monitors

System calibrations can be validated with the internal analog diagnostic mux. LDO regulator outputs can also be verified this way.

Next, users can enable the functions to append the 8-bit status byte to the end of the 24-bit data stream and the 8-bit SPI CRC word. The 8-bit CRC is calculated based on the 8-bit command word, the 24-bit data stream, and the 8-bit status word. If users are concerned about the amount of processing overhead, they can enable **Continuous Read-Back** mode, which removes the need to provide the 8-bit command. Instead, users may clock out the data register contents upon providing serial clocks to the part, as shown in Figure 6.

The result of this procedure is a data acquisition system whose gain and offset error have been verified and that is providing diagnostic information to the user every time they read back data the ADC data.

The LDO regulator outputs, analog front-end inputs, internal digital logic, and memory are continuously monitored. The users can be certain of the integrity of the SPI communications and that the temperature of the IC is known.

Conclusions

As the requirements for functional safety within many industries grow, so too must the technology that supports these requirements. Analog Devices is continuing to develop the technology within our portfolio of products to support system designers in their quest for functionally safe operation.

The AD7768-1 takes much of the burden off the shoulders of the customer and has provided a solution that is more compact, less complex, and reducing processing overhead and the bill of materials required to produce the required solution. This single component approach can also ease the burden on system designers who wish to earn a Safety Integrity Level (SIL) certification for their designs.

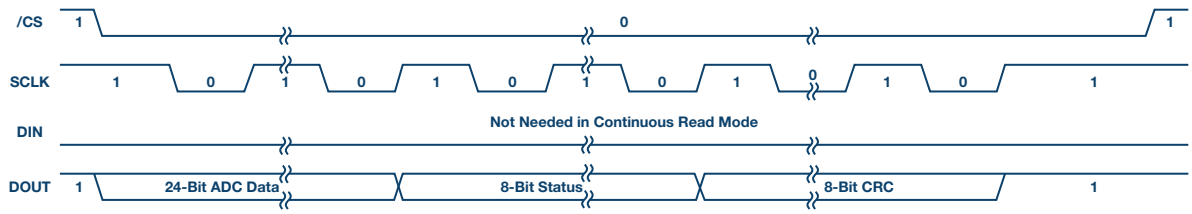

*Figure 5. Reading back the data register with appended status byte and CRC byte of the AD7768-1 in **Continuous Read-Back** mode.*

Chris Norris [christopher.norris@analog.com] is an ADC design evaluation engineer with Analog Devices in Limerick, Ireland. He received his Bachelor of Science in electronic engineering from Waterford Institute of Technology in 2012 and joined ADI as a graduate the same year.

Chris Norris