

A New Approach to Input and Output Monitoring for Microcontrollers Supporting Functional Safety

Simon P. Brewerton
Infineon Technologies UK Ltd

ABSTRACT

It is very common that a microcontroller is used in a safety relevant system to acquire data from sensors, process the data and then control actuators. With the shrink of technology every few years it becomes ever more common to use digital serial interfaces and high speed PWM links for both inputs and outputs. The microcontroller vendors have responded to the need for functional safety in the CPU cores by lock-stepping them and adding ECC to buses and memories. They are also implementing highly flexible and complex timer peripherals to be able to automate much of the real-time processing of the digital signals. However these timers are becoming significantly large, and many have their own embedded sequence engines or microkernels, which although powerful, often lack the rigorous diagnostic mechanisms required to reach ASILD. Currently the only solution is to use an application level measure to detect timer failures, but the large quantity of signals can lead to a substantial CPU load just for the monitoring tasks. This paper describes how a new I/O Monitoring peripheral can be used to 'lockstep' digital input and output signals, using two redundant or diverse timer peripherals. It will outline the problems, the current state of the art, and the proposed new solution, together with some typical use-cases of braking, electrical power steering and airbag.

CITATION: Brewerton, S., "A New Approach to Input and Output Monitoring for Microcontrollers Supporting Functional Safety," *SAE Int. J. Passeng. Cars – Electron. Electr. Syst.* 6(1):2013, doi:10.4271/2013-01-0185.

INPUT & OUTPUT SUPERVISION USECASES

Digital signals are gradually superseding analog signals in automotive applications due to the greater noise immunity, higher bandwidth and ability to multiplex multiple sets of information in one physical connection. This is becoming especially important in safety relevant automotive applications where signal integrity needs to be continually monitored, with techniques such as redundancy and diversity of data values, time-stamping of packets, and error detection / correction strategies (such as CRC).

There is also a growing trend for electrification of mechanically driven systems such as Electrical Power Steering, Automatic Transmissions, and Suspension Systems. There are also the standard fit systems such as ABS/VSC Braking, and Airbags. These systems typically use either rotational torque directly from synchronous motors (to allow high torque in small package volumes) or hydraulic valves to supply force via pistons (with synchronous motors driving a hydraulic pump to supply the high pressure fluid). There are also distributed systems where the control is performed

centrally but the sensors and/or actuators are remotely connected.

Although at first sight these systems may seem disparate, there is a great deal of commonality with respect to the microcontroller connections and peripherals required to drive the power circuits. These fall into 3 main categories:

- Pulse Width Modulation (period, duty, dead-time, phase)
- Serial Bus (SPI, LIN, CAN, PSI5)
- Arbitrary waveforms (special cases)

The normal requirement for error detection capabilities when generating or capturing these different types of signals is that 2 independent methods are employed. These methods require encoding schemes for the data (for single channel) with data or signatures sent in a predetermined pattern or timeslot, or the use of 2 port pins and peripherals (in the case of PWM generation) to ensure that disturbance of the timers, ports, external connections (bond wires, lead frame, solder pads, PCB traces and other ASIC connections) can be adequately detected.

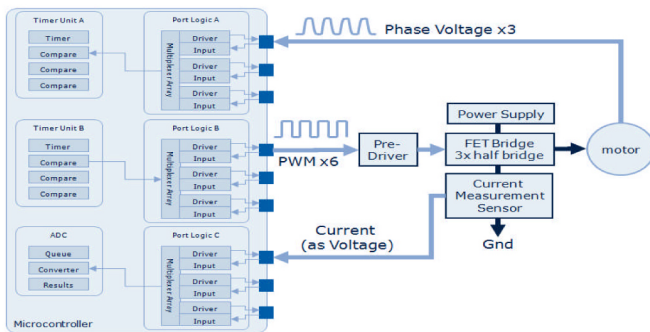


Fig 1. Simplified PMSM to microcontroller Connections

In the case of high current drives (Figure 1) the actual current of the power stage is also normally measured (via ADC sampling of a voltage from a resistive shunt or Hall Effect sensor). The measured voltage has an equivalency to the motor current, which in turn has an equivalency to torque. Torque management is normally one of the safety goals for such a system, but the correct torque measurement absolutely relies on the correct time triggering of the ADC system, which in turn is driven by a pulsed trigger from a timer, so again the monitoring of the timer triggers becomes critical.

The use of the ever increasing power drive capability of modern FET and IGBTs used in the main power bridges also creates another potential safety goal violation, as the high side and low side transistors must never be turned on at the same time. This is normally achieved by adding a specific 'dead-time' between the signals driving the high and low side bridge drivers, to prevent 'shoot through currents' that destroy the power devices and can cause thermal runaway and possible fires. The generation of the 'dead-time' is normally from the PWM generation peripheral and the monitoring of the 'dead-time' is normally performed via the bridge driver ASIC, however the addition of 'dead-time' causes resonances in the motor windings that can be audibly heard, so for large motors (such as traction motors) or motors inside the vehicle cabin (such as column mounted EPS motors) the noise and vibrations can be disturbing and not fitting the refinement targets for the vehicle brand. Therefore, it is desirable to minimize the used 'dead-time' to the absolute minimum. This includes different 'dead-time' for turning ON the transistors as opposed to turning them OFF, and estimating the effective gate capacitance of the main power FETs or IGBTs to drive only exactly the charge required to prevent shoot-through currents. All these techniques improve the refinement; however they potentially make the 'dead-time' insertion and monitoring safety relevant, which is undesirable as it becomes more difficult to monitor for plausibility and is therefore processor intensive. It also requires a low latency periodic task to be performed to be able to react in a short enough time to prevent heating and consequent destruction of the power stage transistors.

STATE OF THE ART SUPERVISION OF INPUT AND OUTPUTS

The basic principle for monitoring serial and PWM signals is to feedback a second version of the signal to another instance of the same (or diverse) digital capture peripheral and then run some interrupt software to make a decision on the plausibility of the captured waveform. The benefit of this is that any aspect of the measured signal can be qualified (as software has full flexibility), however the significant downside is that even simple monitoring leads to a high number of real-time interrupts to service.

As shown in Figure 2, a timer can be written using one single line of software and will then continuously generate a PWM. But the monitoring of this generated signal requires many interrupts.

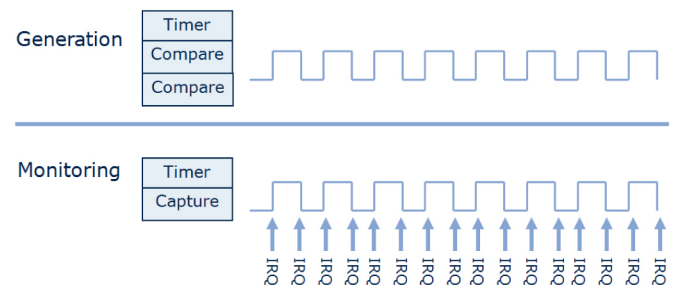


Figure 2. Typical interrupt loading produced when monitoring a PWM signal

For example, a typical PMSM bridge might use a 20KHz modulation frequency. If it is required to monitor the 'dead-time' then all 6 generated pre-driver signals need capturing, and if diagnostics of the FET or estimates of the FET gate capacitance are required then a further 3 signals are needed for the phase feedback monitoring. So in this example it requires 9 feedback signals to be captured at a 20KHz frequency, which is 180KHz or an average of one interrupt every 5.5us. It is precisely this issue that is addressed by the new hardware accelerator to provide measurement and plausibility of serial and PWM signals.

KEY PROPERTIES OF MONITORED SIGNALS

The qualification of any digital signal relies on the basic assumption that the captured signal has some attributes within it that can be used to determine its correctness.

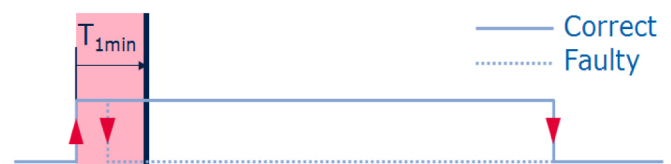


Figure 3. Pulse too short (rising to falling edges)



Figure 4. Pulse too long (rising to falling edge)

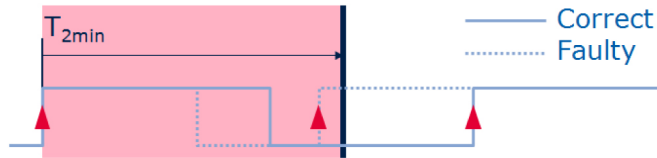


Figure 5. Period too short (rising to rising edge)



Figure 6. Period too long (rising to rising edges)

For one signal the relevant deviancies of the properties are shown in [Figure 3](#), [4](#), [5](#) and [6](#). The red areas indicate the boundary limits of the signal properties that must be respected for the signal to meet the plausibility criteria. The signals must not transition within these red areas. So it follows that these single instance signals can be described purely in terms of edge transitions (rising or falling or both) with respect to time.

The relevant signals vs. time properties are:

- Duty cycle too long
- Duty cycle too short
- Period too long
- Period too short

For multichannel signals the individual signal properties remain important, however it is also the relative times between edges on different signals that are also critical. These are shown in [Figures 7](#) and [Figure 8](#).

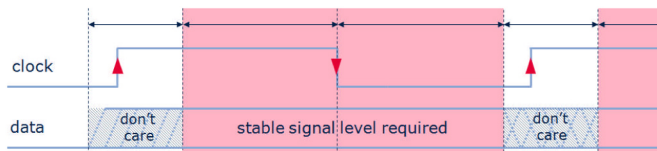


Figure 7. Setup and Hold times. The signal must not transition within the critical periods highlighted in red.

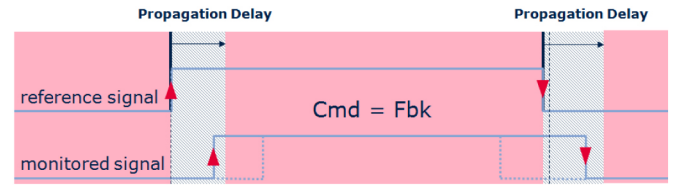


Figure 8. Command and Feedback. The monitored signal must transition within a certain maximum propagation delay. Signals that are too early or too late are classified as erroneous (shown highlighted in red)

The relevant signals vs. signals properties for these use cases are:

- Setup time violation (signal transitions when required to be stable)
- Hold time violation (signal transitions when required to be stable)
- Command and feedback (propagation delay violations, which can also be unique values for rising and for falling edges)

Examples of these cases are setup and hold time for SPI bus and the command and feedback as needed in motor and solenoid valve control applications and previously illustrated and discussed ([Figure 1](#)) in that context.

AUTOMATED INPUT & OUTPUT MONITORING ARCHITECTURE

Signal Preprocessing

The digital signals that are captured in the feedback monitor often originate in a high power (high current and/or high voltage) domain. As such, they are often very noisy and have many extra digital edges even after they have been cleaned up by a Schmitt trigger input circuit. Building a peripheral to make sense of such signals is very challenging, so the architecture is defined to include some blocks for digital input filtering. The digital filter blocks can remove extra edges in 3 basic modes:

- Low pass
- Band pass
- High pass

These different modes also have the ability to be programmed to record any detected glitches so that software can periodically read the glitch history and determine a 'Quality of Service' indicator for the raw incoming signal. An example of one of these digital filter modes is illustrated in [Figures 9](#).