# Lockstep microcontrollers advance aerospace electronics safety

Anthony Vaughan, Texas Instruments, www.ti.com

 Aerospace electronics must achieve some of the highest levels of functional safety found in any industry. A failure or anomalous behavior in the electronics of an aerospace system could lead to catastrophic aircraft failure resulting in multiple serious or fatal injuries.  Design assurance guidelines like DO-254 have led designers to create highly complex safety systems; many employing elaborate checking and voting architectures using multiple dissimilar embedded controllers to mitigate failures. Electronic hardware designers for aerospace systems must take several safety requirements into account and perform an extensive functional failure path analysis of the system. Some of the safety attributes that must be addressed include circuit monitoring, random and latent failure handling, and management of single event upsets. Recent advances in commercial off-the-shelf (COTS) embedded processor design could enable new system architectures capable of achieving all safety and availability goals required in aerospace electronics. Mechanisms like lockstep CPUs, Error Correction Code (ECC) logic for embedded memories, and automated Built-In Self Test (BIST) engines integrated into embedded controllers may greatly simplify and reduce the development time needed to design and certify safety critical electronic systems for the aerospace industry.

To understand why numerous safety aspects are dictated for aerospace electronics, it helps to understand the types of faults to which embedded controllers are susceptible.  In general, faults can be classified into two main categories: systematic and random.  Systematic faults can include hardware defects, software errors and problems resulting during the manufacturing process.  Random faults can include single event upsets (SEU) caused by cosmic rays containing alpha or neutron particles. The CPU, peripherals, configuration registers, flash memory, SRAM and interconnects in embedded controllers are all susceptible to both systematic and random faults. Systematic failures can usually be mitigated via continuous process improvement and design/software verification; however, the rate of random failures cannot generally be reduced, but risk mitigation measures can be taken to detect and respond to these assaults appropriately when they do

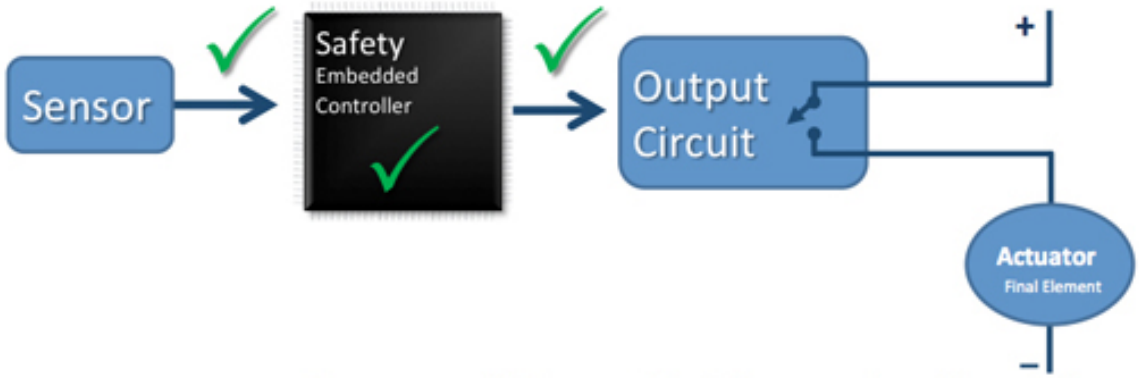
occur.

For years, embedded aerospace electronic systems have been designed to withstand both systematic and random failures via unique architectures. One of the most common architectures employed in systems needing to meet the most stringent design assurance levels is a Two out of Three System (2oo3). The 2oo3 System is usually comprised of three, sometimes dissimilar embedded controllers, and a complex output voting circuit. When there is a fault in one out of the three controllers the output of the other two are used to control the system. This fail operational architecture has proven to be very effective in flight critical applications in which fault tolerance is required to allow the system to continue functioning despite a failure.

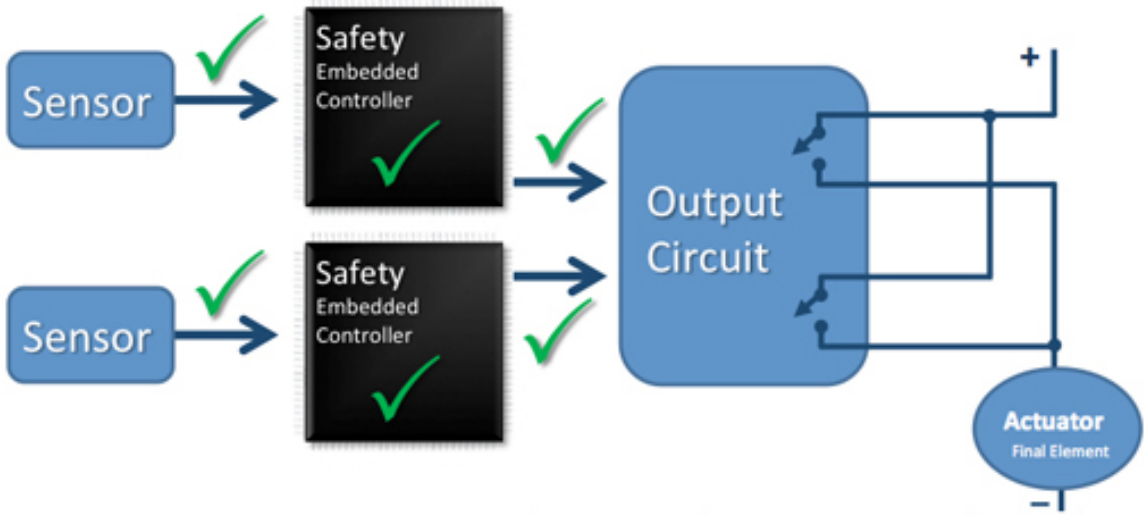
The aforementioned safety architecture has traditionally required a tremendous amount of hardware and software development time and effort due to the inherent complexity. At the heart of this complexity lies the duplication of the entire embedded controller and the need to implement sophisticated software safety algorithms to provide a safety net to mitigate potential faults in the embedded controller. Not only does this add software and hardware development burdens, this architecture actually increases the system's overall susceptibility to random failure events. The amount of logic that is susceptible to alpha and neutron particle strikes significantly increases as the number of embedded controllers in a system increases.

Enhancements to embedded controllers have emerged in order to combat the shortcomings of traditional safety systems. Some embedded controllers, like the lockstep RM4 and TMS570 families that are part of the SafeTI design packages available from Texas Instruments Incorporated (TI), are now available with integrated embedded hardware diagnostics to address a multitude of functional safety concerns. These embedded controllers apply continuously operating hardware-based safety mechanisms on components like the CPU, flash memory, SRAM, power and clocks in order to ensure accurate software execution. The CPU is extremely complex thus making it a prime candidate for using a dual core lockstep safety mechanism. A compare module confirms that the outputs of the two cores are identical on a cycle-by-cycle basis. To address embedded flash memory and SRAM integrity, many controllers incorporate error-correcting code (ECC) technology that encodes data in a way that enables detection of corruption and allows correction of single-bit errors so system operation can continue uninterrupted. Built-in self test (BIST) engines have also been incorporated into embedded controllers to provide robust diagnostic testing on the CPU and memories even when the system is not running code. Multi-bit configuration register keys are also employed to mitigate the risk of SEU inadvertently changing a critical configuration register setting.

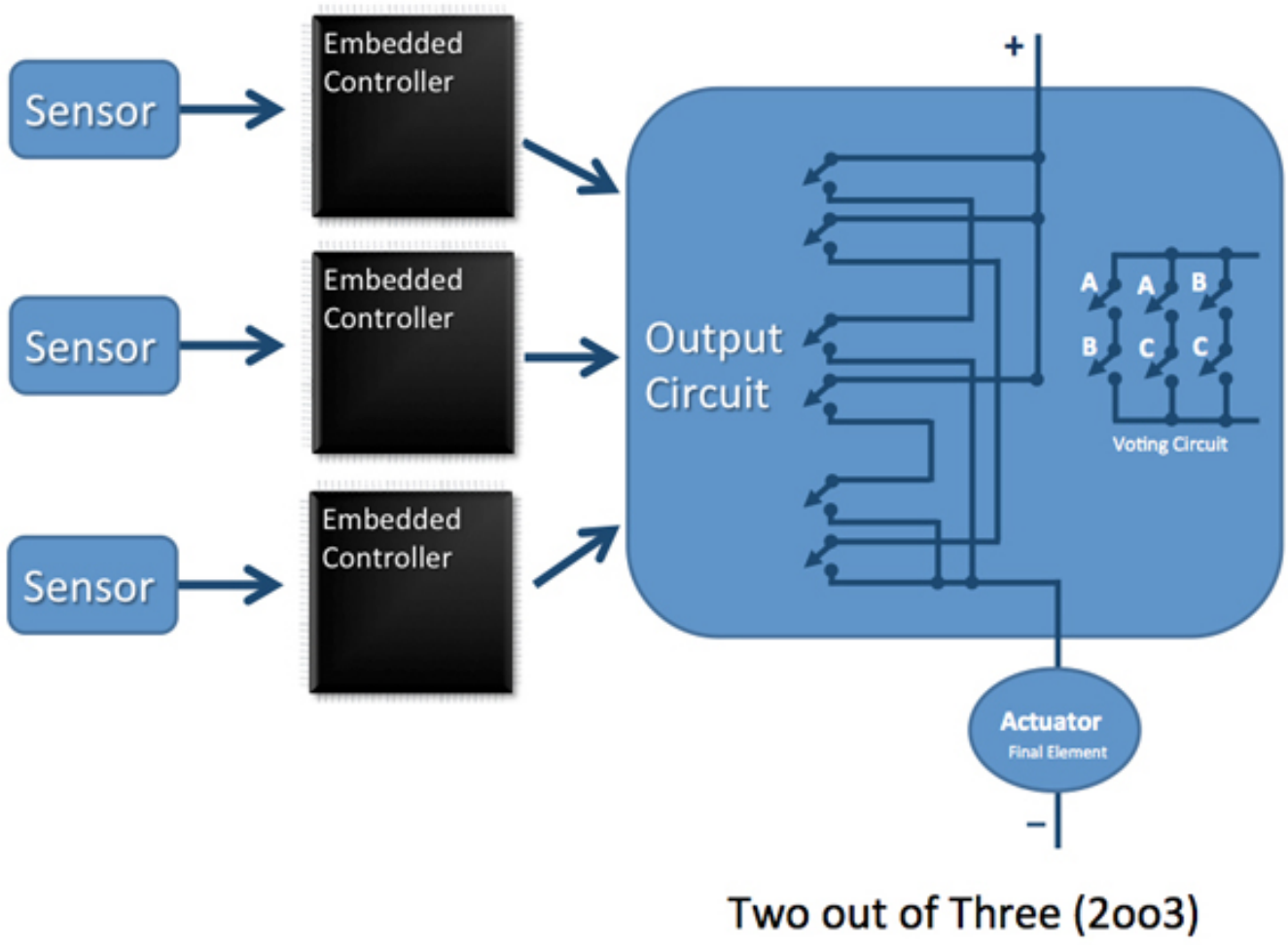
**Figures 1 and 2. The combination of integrated safety features into a single IC has enabled new, streamlined safety system architectures to emerge.**




One out of One with Diagnostics (1oo1D)




Two out of Two with Diagnostics (2oo2)




Two out of Three (2oo3)

Combining integrated safety features into a single integrated circuit has enabled new, streamlined safety system architectures to emerge including the One out of One with Diagnostics (1oo1D) system. This type of safety architecture has been deployed in a wide variety of fail safe systems where an extremely low failure rate is required. While this architecture is not suitable for fail operational aerospace systems, lockstep based safety microcontrollers do provide a path for new architectures to emerge for use in fail operational systems. Instead of utilizing a complex 2oo3 System, designers could potentially utilize a simpler and more cost efficient Two out of Two with Diagnostics (2oo2D) architecture to create fail operational systems. This system architecture could provide low failure rates and high availability. The diagnostic channel of each embedded controller could be leveraged as part of the system safety net concept as a mechanism to detect faults and signal when output control should be relinquished to the other controller. This type of system could also be less susceptible to SEU than comparable 2oo3 systems since fewer embedded controllers are implemented in this architecture.

The aerospace industry understandably has some of the most rigorous functional safety requirements in the world. While the complexity of aircraft is increasing at an unprecedented rate, the advent of safety embedded controllers could help decrease the cost, complexity and development time of safety critical electronics systems. Designers of aerospace electronics now have the option to utilize COTS microcontrollers with integrated hardware safety features to significantly reduce safety software development time and the total number of components needed in the system while still providing a high level of functional safety and reliability. These embedded controllers also open up exciting new possibilities for aircraft safety net design and safety system architectures.

*Anthony Vaughan is the North America manager, Hercules safety microcontroller group, at Texas Instruments. He joined TI as a product engineer in the imaging and audio group. Vaughan then became an applications engineer with TI's automotive and safety microcontroller group. He holds a B.S. in electrical engineering from Texas A&M University.*