The New Quad Architecture: Explanation and Evaluation

By: Dr. Lawrence V. Beckman
HIMA-Americas, Inc.

ABSTRACT

The new HIMA Quad (QMR) Architecture now available for Safety and Critical Control Applications is a major breakthrough in safety performance. The architecture provides four (4) processors, and remedies problems associated with dual processor architecture, as regards the dangerous undetected failure of one of the two (dual) processors.

This major technological enhancement allows the safety system to operate at the SIL 3 level (RC6) on either one or both channels for an unrestricted period of time, without the need for external devices of any kind. As such, it achieves a significant increase in both safety and availability which exceeds that provided by TMR architectures by a factor of three. In addition, it has significantly less susceptibility to common cause failure because of the absolute separation, isolation and operation of the redundant channels.

Given the safety performance and availability improvements, the most attractive advantage of this new architecture is a lower overall life cycle cost, which will enable it to be used effectively on both small and large safety projects.

Background

The New Quad Architecture now available for safety and critical control applications is a significant development in the evolution of Safety Instrumented Systems (SIS). This evolution has progressed from dual architecture to triplicated, and now to quad redundancy.

The typical dual system can be implemented in either a safe configuration (2-0) or an available configuration (2-1-0). In the safe configuration, the system is not fault tolerant and a failure in either operating channel will cause a spurious trip. As such, it is extremely safe, but has low availability. In fact, it is three times safer than the triplicated (TMR) architecture, but considerably less available.

The 2-1-0 configuration provides high availability, but very poor safety performance. Indeed it is three times more available than the triplicated (TMR) architecture, but only half as safe as a simplex (single channel) configuration. This is because both channels must fail for the system to experience a spurious trip, and both must operate for the system to achieve the safe state, and herein lies the problem.

In an attempt to provide both safety and availability, dual architectures are now being implemented in a 1oo2D configuration. This architecture is fault tolerant, being that it normally operates in the 2-1-0 mode; but reverts to the 2-0 mode if a fault occurs which cannot be resolved. As such, its safety performance is heavily dependent upon the effectiveness of the system's internal diagnostics, and its operational availability on the system's ability to resolve faults and disable the failed channel, while continuing to operate safely on the remaining good channel.

Not all 1oo2D implementations are alike, and some experience significant availability problems resulting from the implementation of the required comparison diagnostics. However, all have one problem in common; that being a severe restriction on the operating time in single channel mode. Some suppliers attempt to circumvent this restriction by using a mathematical model to predict the process demand rate, and thereby extend the time allowed for single channel operation. This approach is certainly not recommended for safety, as the data used in such models is at best an estimate, and the results obtained are inappropriate for use in making critical safety decisions.

Triplicated (TMR) systems are well known and continue to be the generic architecture of choice for the under informed. They are often used in many situations without being technically or economically justified. While this architecture is both safe and available, it must operate 3-2-0 for safety applications. A TMR system implements diagnostics by voting or comparison (after the loss of one channel). As such, it is not allowed to operate on a single channel, because it lacks comprehensive internal diagnostics, and cannot be considered to be safe. In fact, time limitations are imposed for two-channel operations, and steps must be taken to insure the system will shut down after the loss of a second channel. Another problem which affects TMR architecture is higher (3 times) susceptibility to common cause faults due to both the third level of redundancy, and the fact that multiple channels share a common hardware platform; i.e., a common I/O or

Processor Module, etc. In addition, both the initial cost and the life cycle cost (including maintenance) of the system are high.

Quad Architecture

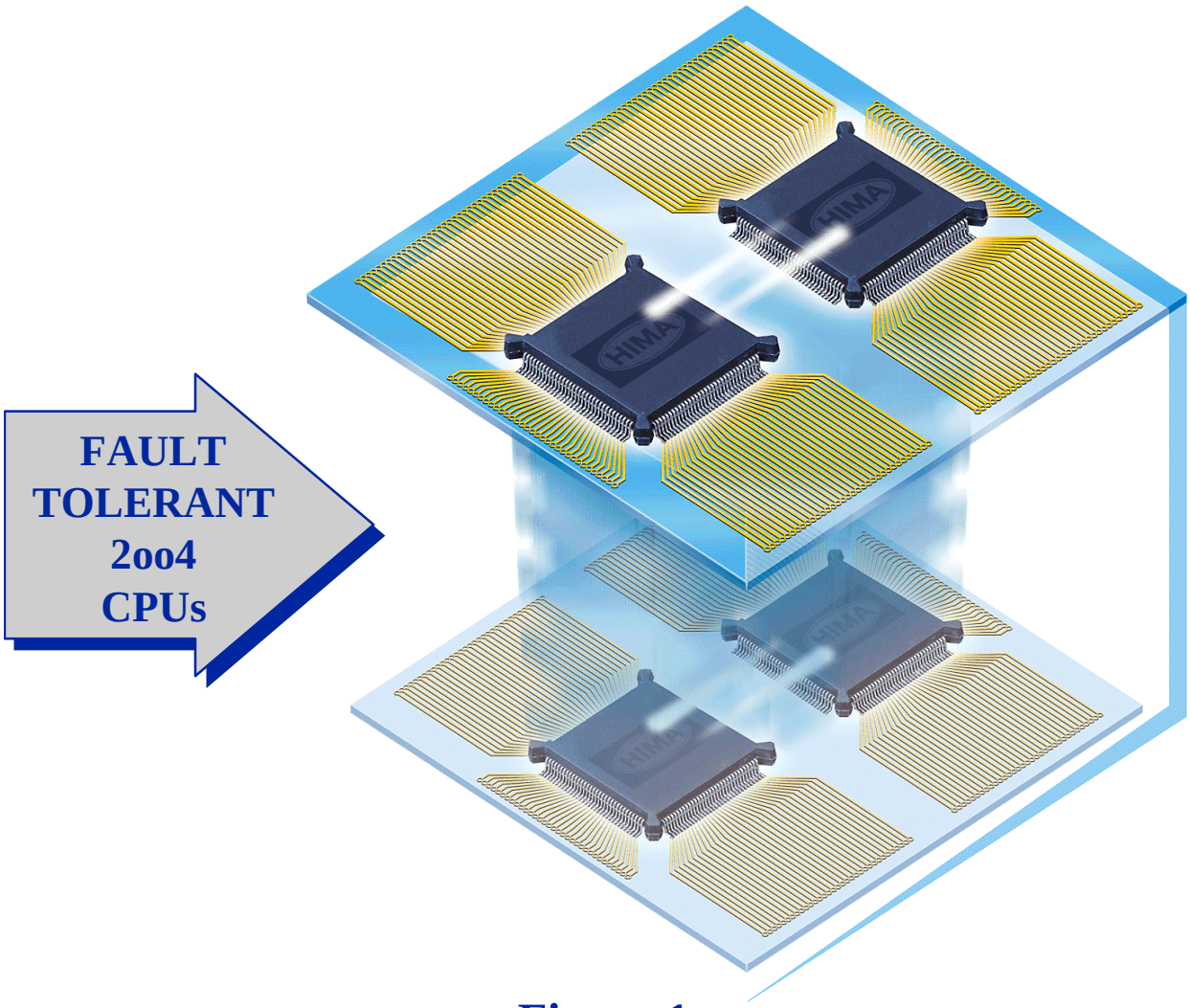

Figure 1

The new Quad (QMR) Architecture is a major breakthrough in safety performance. This architecture provides four (4) processor - two per channel, and remedies problems associated with dual processor architectures, as regards the dangerous undetected failure of one of the two (dual) processors. Please refer to Figure 1 for additional information. Both pairs of active processors operate synchronously with the same user program. A hardware comparator and a separate fail-safe watchdog monitors the operation of each pair of processors to diagnose and resolve anomalies. As such, this architecture can operate at the SIL3 (RC6) level on either one or both channels, for an unrestricted period of time. It achieves a significant increase in both safety and availability which exceeds that provided by TMR architectures by a factor of three. In addition, it

has significantly less susceptibility to common cause failure because of the absolute separation, isolation and operation of the redundant channels. Please see Figure 2 for more details on the HI Quad Architecture.

Given the safety performance and availability improvements, the most attractive advantage of this new architecture is a lower overall life cycle cost, which will enable it to be used effectively on both small and large safety projects.

HIQuad Architecture

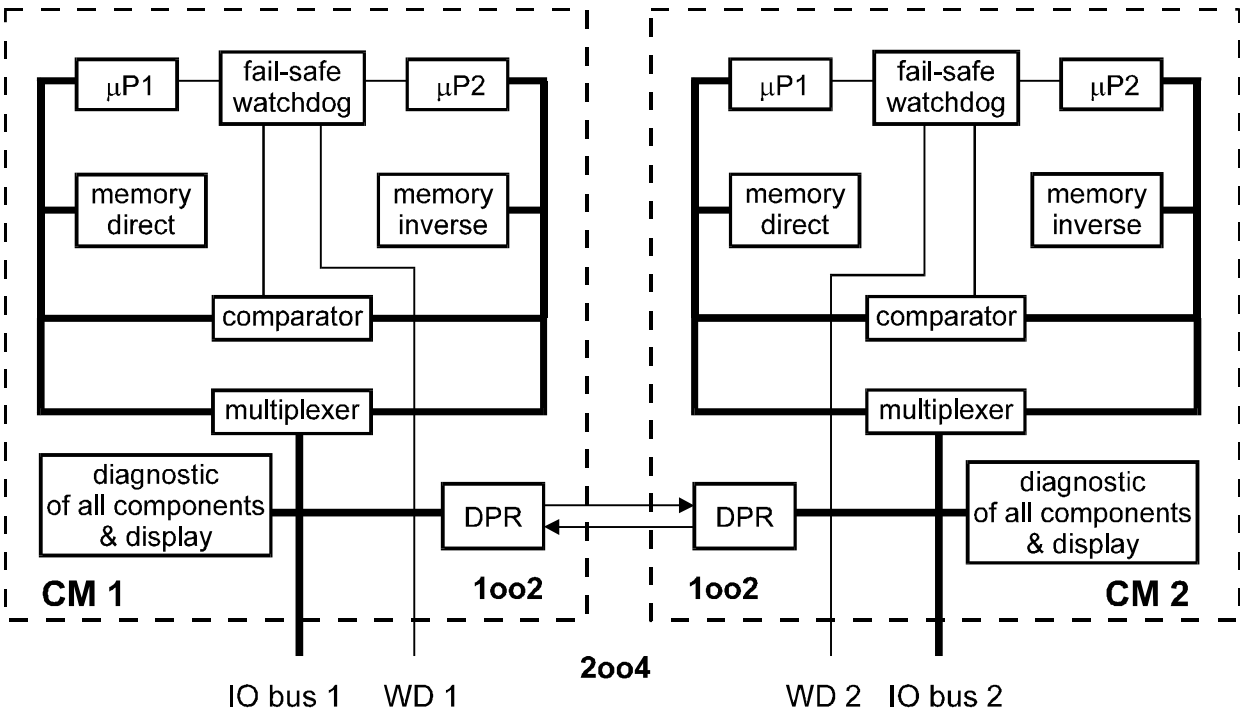

Figure 2

Operation Under Fault Conditions

For safety applications, single channel systems (1-0) are not fault tolerant and must fail safe. Dual architectures can either operate fail safe (2-0) or degrade to single channel operation (2-1-0) under specific fault conditions, and with severe time limitations as defined in their safety certification report. Obtaining a copy of this report for any PES under consideration is highly recommended.

Both the TMR (3-2-0) and Quad (4-2-0) architectures degrade to a 2-0 mode of operation after the first fault. However, the Quad (QMR) architecture retains its comprehensive internal diagnostics, has no time restrictions while operating in this mode, and provides full SIL3 (RC6) protection as well. Please refer to Figure 3 for a table of operating scenarios after the First Fault.

Degraded operation at the SIL3 (RC6) level requires that the PES provide a secondary means of de-energizing outputs. This can be either external, or integrated into the output modules, but it must be implemented in order to be safety compliant. Restrictions likewise apply to the operation of the PES after a second fault. For the TMR architecture, the second fault can be either CPU or I/O related. Either occurrence will require the system to be shut down. For the QMR architecture, only a CPU fault on the second channel mandates system shutdown, as I/O faults can be managed independently, due to its more comprehensive internal diagnostics. As such, the QMR architecture provides additional fault tolerance, and a higher level of operational availability.

Safe Operation After First Fault

Simplex:	**1 - 0**	→	**Fail-Safe (RC4 only)**
Dual:	**1oo2D**	→	**1oo1D (Severe Time Restriction)**
TMR:	**2oo3**	→	**1oo2 (Time Restriction)**
QMR:	**2oo4**	→	**1oo2D (No Time Restriction)**

Figure 3

Safety Performance

It is imperative that PES architectures provide both safety and availability. Frequent spurious trips of the process are both dangerous and economically undesirable. Given that a dual architecture is inherently more available than a triplicated architecture, the objective is how to make the dual architecture equal to or better than TMR in safety performance.

Heretofore, the crux of the problem has been the dangerous undetected failure of one of the two (dual) processors. A single processor cannot diagnose itself sufficiently to be considered completely safe, and the possibility exists that such a failure could cause both channels to fail in a dangerous state, and render the PES incapable of providing its intended safety function. This is of course why severe time restrictions are imposed at the SIL3 (RC6) level for dual architectures operating under fault conditions.

The Quad (QMR) architecture provides a pair of dual processors operating in the safety (2-0) mode for each channel. The resulting significant increase in diagnosability of the operation of these processors has in fact completely remedied safety concerns related to dangerous undetected failure of the processors, and consequently the removal of all time restrictions on single channel operation of the system.

A comparison of safety performance (Probability of Failure on Demand - PFD) of the various safety architectures can be enlightening. Referring to ISA TR84.02, Part 2, 1998, one can quickly determine that the Quad (2oo4) architecture is comparable to the ultra safe 1oo3 architecture, as both have cubic terms in their equations for PFD. By comparison, TMR (2oo3) is comparable to the 1oo2D architecture in that both have squared (second order) terms in their equations. This comparison concludes that the QMR (2oo4) architecture provides an order of magnitude better safety performance than either TMR (2oo3) or 1oo2D architecture, and is a major technological enhancement in safety system performance. Please refer to Figure 4 for a comparison of these architectures.

Comparison of The Best PFD avg.

1oo2: $PFD_{avg.} = (\lambda^{DU})^2 \times \frac{TI^2}{3} + \ldots$

1oo3: $PFD_{avg.} = (\lambda^{DU})^3 \times \frac{TI^3}{4} + \ldots$

2oo3: $PFD_{avg} = (\lambda^{DU})^2 \times TI^2 + \ldots$

2oo4: $PFD_{avg} = (\lambda^{DU})^3 \times TI^3 + \ldots$

Source: dTR84.02, Part 2-1998

Figure 4

Another important consideration in the performance of safety systems is the ability of the PES to detect an internal fault and correct it quickly. In fact, the PES must be able to respond within the specified safety time of the process it is protecting.

The Process Safety Time (PST) of a given process is in essence the fault-tolerant time of that process, prior to becoming a dangerous condition. Thus, if a dangerous condition exists for longer than the PST, the process enters a dangerous state. Given this requirement, the PES must maintain a safe state by detecting dangerous internal faults and correcting them within the PST, or consequently be considered unsuitable for safety applications on that process.

A typical example would be a Burner Management System (BMS) where the PST is defined by the TÜV (DIN VDE 0116) as one (1) second. Given that two (2) scan cycles of the PES are required to detect and correct an internal fault, the Fault Detection-Correction Time (FDCT) of the PES cannot exceed five-hundred (500) milliseconds. If the safety PES cannot meet this requirement, it cannot be utilized for safety in the BMS application per the standard.

Life Cycle Cost Considerations

Safety standards in existence today and in the near future require that SIS be implemented to mitigate the risk associated with the operation of hazardous processes. Ignoring these requirements is no longer an option, and it behooves those concerned to comply fully, and as cost effectively as possible. As such, both the initial cost and life cycle cost of the SIS must be considered.

It is a fact that some architectures because of their inherent complexity are both more expensive to acquire and to operate. In particular, this is true for smaller projects, or projects requiring either SIL1 or SIL2 protection. For such projects, using a triplicated (TMR) architecture might prove to be prohibitively expensive; considering both the initial and life cycle cost.

In addition, if a process can be classified as requiring SIL1 or SIL2 in lieu of SIL3, significant savings can be achieved in other areas such as sensors and final elements, which may no longer need to be dual or triple redundant as required for SIL3 applications.

The New Quad Architecture can be configured to address the performance requirements of all three SILs. It can operate as a single channel or redundant system; with single, dual or triplicated field devices as required for each safety loop. In either the simplex, selectively redundant, or fully redundant configuration, it provides SIL3 safety performance. As redundancy is added, availability increases dramatically and safety performance is maintained.

Adding redundancy is not prohibitively expensive, as the price of processor and I/O modules is significantly less expensive than alternative architectures. In addition, because these modules are less complex than comparable TMR modules, their MTBF is significantly longer as well, and the system maintenance expense is substantially reduced.

Because this new architecture is extremely cost effective, it provides the additional benefit of dedicating the PES to the process unit it is protecting. This single unit per PES concept has been incorporated in several recent safety standards. As such, combining multiple process units into a single PES, in an effort to be cost effective, is no longer necessary. As a result, safety system implementation, testing and maintenance are less complex, and less prone to human error.

In addition to enhanced safety, the dedicated PES is substantially easier to maintain and modify. The possibility of inadvertent shutdown of other process units is completely eliminated, and testing procedures are more easily implemented. The overall advantages of this one-on-one approach are significant indeed, and should be given careful consideration.

Conclusions

The New Quad (QMR) Architecture is a major technological enhancement in safety system performance. It provides both higher levels of safety and availability than either TMR (2oo3) or 1oo2D. It has significantly less susceptibility to common cause failure than TMR because of the absolute separation, isolation and operation of the redundant channels.

Because each channel has a pair of dual processors operating in the safety (2-0) mode, a dangerous undetected failure of the processors has been eliminated; and the system provides unrestricted SIL3 operation in either a simplex, selectively redundant, or fully redundant configuration.

This new architecture is highly configurable and can be used for SIL1, SIL2, and SIL3 applications. However, the most attractive advantage is a lower life cycle cost, which will enable it to be utilized effectively on both small and large safety projects. Consequently, combining multiple process units into a single PES, in order to be cost effective, is no longer a necessity.

Glossary

2-0 Mode of operation where the dual system shuts down after the first diagnosed fault.

2-1-0 Mode of operation where the dual system shuts down after the second diagnosed fault.

3-2-0 Mode of operation where the triplicated system shuts down after the second diagnosed fault.

4-2-0 Mode of operation where the quadruplicated system shuts down after the second diagnosed fault.

QMR Quad Modular Redundancy (2oo4).

PES Programmable Electronic System (not a PLC-Programmable Logic Controller).

RC6 Requirement Class 6 per DIN 19250.

SIL Safety Integrity Level (1, 2 or 3).

TI Proof Test Interval.

λ_{DU} Dangerous Undetected Failure Rate.