Product Information Note

Honeywell

Quadruple Modular Redundant Technology for Safety Systems

Honeywell's Quadruple Modular Redundant (QMR) technology with award winning 2oo4D architecture sets the standard for how Safety Instrumented Systems should be designed.

This unique QMR technology, based on a high level of self-testing and diagnostics, has proven that QMR is the best available technology for Safety Instrumented Systems (SIS). It has an optimal safety integrity level (SIL 3) for the process industries with a safety availability of more than 99.99%. It also offers 20% higher availability than what is offered for most other safety systems.

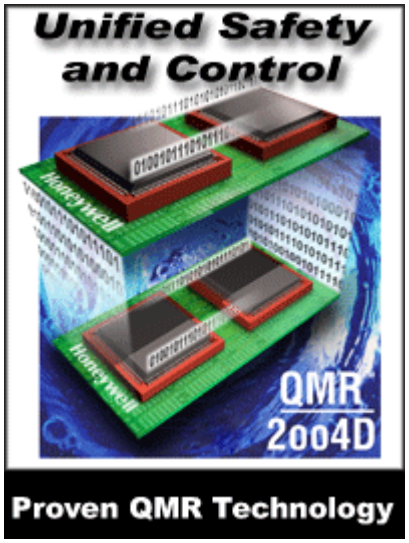
Experts agree that QMR, with its multi-fault-tolerant capabilities, is the future towards which safety systems should be heading. QMR offers a basic SIL 3 architecture, irrespective of the chosen configuration. Unrestricted runtime is no longer an issue, whether in dual or single channel operation.

The importance of diagnostics has gained full recognition; not just by end-users but also by official global approval bodies. Whereas other vendors are still trying to take their first steps in this area, Honeywell has been applying self-testing and diagnostics technology for over 20 years.

Online self-testing and diagnostics have the advantage that the proof test interval, as required by IEC-61508 and IEC61511, can be extended to more than 15 years, depending on the required SIL level. The extended proof test interval will provide far more process uptime, leading to more profit and lower operational and maintenance costs.

Honeywell's QMR technology features:

- IEC 61508 / IEC61511 compliant
- Fully Integrated with Experion PKS and the C300 controller
- Highly scalable system
- One platform for all safety applications
- High safety integrity
- High process availability
- Choice of today's experts SIL 3 single configuration
- Unrestricted runtime
- Lower maintenance costs



Design

The QMR technology has two processors running in parallel verifying each other. The processors are completely verified and tested for correct functioning, thus redundancy is established on one module. The results are also communicated with the second QPP module, establishing true quadruple modular redundancy. This has the advantage that it does not result in a 'heavy' and complex hardware system, which reduces the footprint and lowers the installed costs.

QMR perfectly serves the two most important purposes of a Safety Instrumented System (SIS): the **safety integrity** and the **availability** of the process.

Safety Integrity

Safety integrity is a measure of the reliability of the safety system. The higher the safety integrity, the higher the probability that the safety PLC will function properly. The quad modules are designed for optimal safety integrity relevant to the process industries served and are suitable for applications up to SIL 3, even when applied in a single configuration.

Process Availability

The safety system should be highly reliable in that it should not cause an undesired process shutdown. The QMR modules can be configured with redundancy, allowing multiple faults without any interruption of the process.

Scalable System

The safety system with QMR technology is highly scalable. Not only can the QPP module be configured with redundancy, the I/O section and I/O buses are able to be similarly configured.

Online Self-Testing and Diagnostics

Proven in use

The QMR Safety System has evolved from the DMR-1oo2D system. This system has been using a high level of self-testing and diagnostics over 15 years. During this period, it has proven its reliability and ability to boost availability.

Software Checks Hardware

Contrary to hardware, software will never degrade. Therefore, when the hardware is tested via software, faults can be discovered before a spurious trip will ever take place.

Reliability

The QMR safety system uses software for self testing and has a high level of diagnostics, all the way from the field up to the processors. This makes the QMR Safety System far more reliable than any other system not using extensive self-testing and diagnostics, including 2oo3 or 2oo4 systems.

Lower Operational Costs

Besides being capable of performing internal system self-testing, the QMR system is also capable of testing and diagnosing field loops. For both inputs and outputs, loop monitoring can be used. As soon as a short circuit or an open loop is discovered, an alarm will be generated. This automatic approach of testing and diagnosis reduces overall costs for maintenance and proof testing.

2oo4D: Two-Fault Tolerant

Multiple Faults Tolerant

The QMR system with diagnostics is capable of dealing with multiple faults, due to its ability to find and isolate faults anywhere in the system. As long as faults are not in the same section of the system, it is possible to have several faults without losing the safety function. Diagnostics combined with the 2oo4D technology makes the system capable of discovering and isolating even more faults before a nuisance trip will occur.

Safety Integrity: Two Faults

The QMR-based safety system is the first system that uses a truly two fault- tolerant architecture. It is capable of having two processor faults while retaining its ability to perform its safety function up to SIL3.

The following minimum failure scenarios are required before a safety function will be lost:

- A dangerous undetected failure of at least three microprocessors
- A detected failure on one module (which results in isolation of the module), in combination with a dangerous undetected failure on both microprocessors of the remaining board.

With these extremely remote and practically non-conceivable failure probabilities, the QMR system can operate as a single channel safety system at SIL 3 integrity with no limitation.

Process Availability

With regard to system availability, the 2oo4D concept is entirely one-fault tolerant. The following minimum failure scenarios are required before a spurious process trip will be initiated:

- A safe undetected failure on one module (one microprocessor) in combination with a detected failure on the other module
- A safe undetected failure of at least two microprocessors
- A detected failure on both modules.

Common Cause Failure

Because the QMR system consists of two processor packs, each containing two microprocessors, which operate completely independently from each other, a nuisance trip due to common cause is almost negligible.

Online Swap-Over and Repair

With the QMR Safety System, replacing faulty modules is easy and can be done online without the need for hot standby or intermediate modules, and without interrupting the safeguarded process. Because the two channels are running independently, it is possible to work on one channel without reducing the safety functionality of the system at all. The self learning principles in Safety Manager guarantee that application and system software is automatically synchronized without the need of a manual download to the system.

Moreover, a full download can be completed online without interrupting the process and reducing the safety integrity of the system. Before changing to the new application a check will be performed and values will be copied to ensure safe and correct continuous operation.

Performance

With the new QPP-0002, another major improvement with respect to cycle time and I/O size has been established: the average cycle time has been decreased with another 30% -40% allowing fast processing with average cycle times well below the 100 milliseconds. This fast processing is accomplished without additional configuration and without affecting the SIL. Applications with high I/O volumes (such as fire and gas) can also be handled with Safety Manager while keeping the cycle time far below limits defined by the application.

The new QPP-0002 can be used along with the existing QPP-0001.

Comprehensive Safety Services

At Honeywell, our services go beyond just supplying hardware and software. Honeywell has established a unique safety knowledge community located in expertise centers around the world. More than 250 safety engineers employed in these centers offer a wide range of Consulting, Project, and Lifecycle Support Services. With more than 30 years of safety management experience solving complex design safety issues and offering unparalleled safety solutions, Honeywell is indeed your ideal process safety partner.

Key engineers around the world are TÜV Certified Functional Safety Experts (CFSE), demonstrating the extensive knowledge and expertise that is available for your QMR projects and applications. With this knowledge, Honeywell can assist you with consultancy services, preparation of software requirement specifications, system requirement specifications, SIL validation, and much more.

It is not just the QMR Safety System that complies with IEC 61508 and IEC61511. The complete development, engineering and manufacturing also complies with the IEC 61508 and IEC61511 standard. Honeywell was the first safety organization in the world to be IEC 61508 certified as an organization. The Safety Manager was the first SIS to receive the IEC61511 certification. The Safety Manager System therefore is a truly integrated SIL 3 compliant system.

With more than 5000 QMR-based systems installed and operating, Honeywell has become the market leader for diagnostic-based safety systems.

More Information

For more information on Honeywell's Safety Manager, visit our website www.honeywell.com/ps, or contact your Honeywell account manager.

Automation & Control Solutions
Process Solutions
Honeywell
2500 W. Union Hills Dr.
Phoenix, AZ 85027
Tel: +1-602-313-6665 or 877-466-3993
www.honeywell.com/ps

PN-08-21-ENG
May 2008

Honeywell