QMR with 2oo4D - the Architecture of Third-Generation Safety Systems

Four years ago Honeywell introduced the Quadruple Modular Redundant (QMR™) architecture with 2oo4D voting. Since then, the award winning QMR technology and 2oo4D architecture have become a new standard in the world of Safety Instrumented Systems.

Within a very short time, the unique QMR technology, based on a high level of self-testing and diagnostics, has proven itself in a number of ways. It has proven that QMR is the best available future technology for Safety Instrumented Systems (SIS). It has proven that it has an optimal safety integrity level (SIL 3) for the process industries, with a safety availability of more than 99.99%. And it has proven that it has 20% higher availability than most other safety systems.

It did not take long before experts agreed that QMR, with its Multi-Fault-Tolerant capabilities, is the future towards which Safety Systems should be heading. QMR offered a basic SIL 3 architecture, irrespective of the chosen configuration. Unrestricted runtime was no longer an issue, neither in dual nor single channel operation.

Besides industrial experts, the general marketplace also recognized that QMR is the base for the future. During the last four years, and with more than 1900 QMR systems installed and operating, Honeywell has become the market leader for diagnostic-based safety systems.

The importance of diagnostics has gained full recognition; not just by end-users but also by official approval bodies all over the world. Whereas other vendors are still trying to take their first steps in this area, Honeywell has applied self-testing and diagnostics technology for more than 15 years already!

Online self-testing and diagnostics have the advantage that the proof test interval, as required by IEC-61508, can be extended to more than 10 years, depending on the required SIL level. The extended proof test interval will give you far more process uptime, leading to more profit and lower operational and maintenance costs.

QMR:
- IEC 61508 Compliant
- Integrated with all DCS systems, including Experion PKS
- Highly scalable system
- One platform for all safety applications (ESD, F&G, BMS)
- High safety integrity
- High process availability
- Choice of today's experts
- SIL 3 single configuration
- Unrestricted runtime
- More than 5,000 (DMR and QMR) diagnostic based safety systems installed worldwide
- Lower maintenance costs
Design

The QMR technology is available in two formats – the Quad Processor Pack* (QPP) and the Quad Processor Module* (QPM). Each of these 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 Quad module, establishing true quadruple modular redundancy. This has the advantage that it does not result in a ‘heavy’ hardware system, which results in a smaller footprint and lowers the costs for installation.

QMR perfectly serves the two most important purposes of a Safety Instrumented System (SIS):
- Safety integrity of the system
- Process availability.

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 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 in a single configuration!

Process Availability

The Safety System should be highly reliable in that it should not cause an undesired process shutdown as well. For this, the Quad 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 Quad modules be configured with redundancy, the I/O section and I/O buses are able to be similarly configured. The figure below lists these possibilities:

<table>
<thead>
<tr>
<th>Configuration type</th>
<th>QPP or QPM*</th>
<th>I/O</th>
<th>I/O bus</th>
<th>Safety Integrity</th>
<th>Process Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMR</td>
<td>Single</td>
<td>Single</td>
<td>Single</td>
<td>SIL3</td>
<td>Basic</td>
</tr>
<tr>
<td>QMR</td>
<td>Redundant</td>
<td>Single</td>
<td>Single</td>
<td>SIL3</td>
<td>Increased</td>
</tr>
<tr>
<td>QMR</td>
<td>Redundant</td>
<td>Redundant</td>
<td>Redundant</td>
<td>SIL3</td>
<td>Optimal</td>
</tr>
<tr>
<td>QMR</td>
<td>Redundant</td>
<td>Redundant and Single</td>
<td>Redundant and Single</td>
<td>SIL3</td>
<td>Optimal</td>
</tr>
</tbody>
</table>

* QPP is available for Safety Manager PKS while QPM is applied for FSC system
Online Self-Testing and Diagnostics

Proven in use
The QMR Safety System has evolved from the DMR-1002D system. This system has been using a high level of self-testing and diagnostics over the last 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 other 2003 or 2004 systems.

Lower costs of operation
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!

2004D: Two-Fault Tolerant

Multiple Fault 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 more than one fault without losing any safety function. Diagnostics combined with the 2004D technology makes the system capable of discovering and isolating even more faults before a nuisance trip will occur.

Safety Integrity: Two Faults
The QMR Safety System is the first system, and currently the only one, that uses a truly two-fault-tolerant architecture. It is the only system that 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.

It is no wonder that 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 time limitation.

Process Availability
With regard to system availability, the 2004D 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.

Moreover, a full download can be done 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.
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 200 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 areTÜV 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. The complete development, engineering and manufacturing also complies with the IEC 61508 standard. Honeywell in Den Bosch was the first safety organization in the world to be IEC 61508 certified as an organization. The QMR Safety System therefore is a truly IEC 61508 SIL 3 compliant system!