

Ready for SIL 4: Modular Computers for Safety-Critical Mobile Applications

Susanne Bornschlegl, MEN Mikro Elektronik

June 2012

Safety-critical applications are a huge challenge, especially where electronics are used. And today electronics are omnipresent, particularly in trains and aircraft. How can you build up a computer in such a way that it is certifiable, which obstacles are there and can you find a way to make a computer like this modular and available "off the shelf"?

The Challenge: Safe, Robust and Competitive	2
An Approach: How a Computer Becomes "Safe"	3
Redundancy Structure	3
Radiation-Resistant FPGA, Safe Memory	5
Deterministic Behavior	6
Diverse Redundancy and Clustering	7
The Framework: Not Only the Computer Must Be "Safe"	8
Standardized Safety	8
Qualification of the Manufacturer	9
Certification	10
Conclusion: Putting All Your Eggs in One Basket can be Safe, too	11
Product Information	11
About MEN Mikro Elektronik	12

MEN Mikro Elektronik GmbH

Neuwieder Straße 3-7
90411 Nürnberg
Deutschland

Tel. +49-911-99 33 5-0
Fax +49-911-99 33 5-901

E-Mail info@men.de
www.men.de

The Challenge: Safe, Robust and Competitive

Electronics are safety-critical wherever errors or failures potentially result in loss of life or cause major damage to the environment but also to property. Systems like these are subject to strict standards that prescribe the safety criteria for each market. You can find typical applications in trains, buses, ships and aircraft. Both hardware and software need to work reliably here. There is no margin for error.

Through their use inside vehicles, further requirements are added for electronics. They not only have to be safe but extremely robust, too. These two aspects increase the cost of such systems compared to commercial electronics. Yet, costs must not get out of hand, as they would have to be passed on to customers. The vehicles and consequently the provider, especially in mass transit, would no longer be competitive.

In the embedded area, modularity can reduce costs. 19-inch bus systems like CompactPCI and VMEbus are classic examples. Both have been tried and tested for many years, even in mobile applications up to airplanes. A large number of manufacturers offers standard cards for these systems, and many of them are already equipped for severe environmental conditions.

Still the aspect of functional safety remains a challenge of itself, in particular if you think about the central processing unit of a system. Can you design a computer in such a way that it compensates calculable risks by its very design? This includes accidental failures that occur through component failure, EMC influence or cosmic radiation, and possible design errors that can be avoided as early as in the development phase by using corresponding processes.

MEN Mikro Elektronik has addressed this problem. The resulting design is now available in the shape of two standard boards – for CompactPCI and VMEbus – in double Eurocard format (6U). The following gives greater detail of what you need to consider when you want to make a computer "safe", and how MEN has tackled this question.



MEN Mikro Elektronik GmbH

Neuwieder Straße 3-7
90411 Nürnberg
Deutschland

Tel. +49-911-99 33 5-0
Fax +49-911-99 33 5-901

E-Mail info@men.de
www.men.de

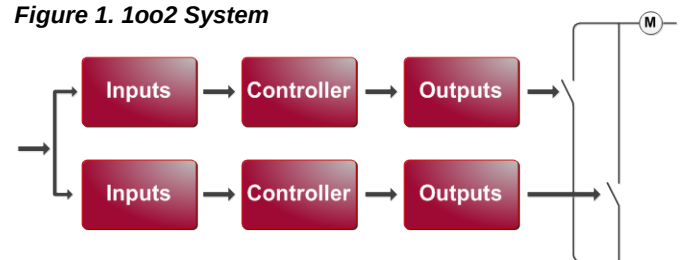
An Approach: How a Computer Becomes "Safe"

Redundancy Structure

The most important strategy to make a system less vulnerable to risk is to multiply significant components. A component that by failing brings the entire system to a halt is called a "Single Point of Failure" (SPOF). If critical components, such as the CPU, are redundant, the availability and/or reliability of the functions increase. Depending on what you want to achieve, you can use different redundancy configurations. To do this, you name the number of functions that must be in working order in case of a failure (M) compared to the total number of redundant functions (N). This results in "M out of N", abbreviated as MooN.

A 1oo2 constellation increases availability of the system and, by consequence, the Mean Time Between Failures (MTBF). If one of two processors fails, a 1oo2 system can still go on operating. This is called "fail-operational". The MTBF rises by a factor of 1.5.

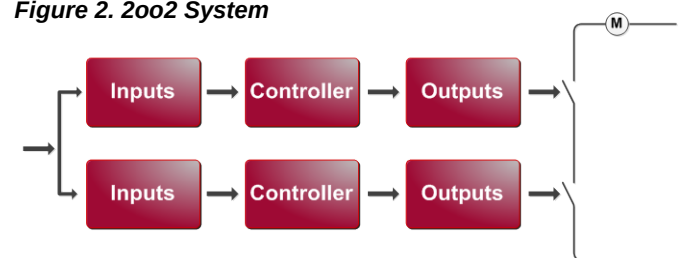
Figure 1. 1oo2 System



With safe redundant functions, all components must also deliver the same computing results, to allow for the detection of errors, in the simplest case in a 2oo2 system. This scheme requires both systems to operate identically at any time. In turn this reduces availability (MTBF) by a factor of 0.5.¹

When you think of rolling stock, e.g., a train is supposed to come to a complete stop in the case of an error. It then goes to a safe state, i.e. the system is "fail-safe".

Figure 2. 2oo2 System

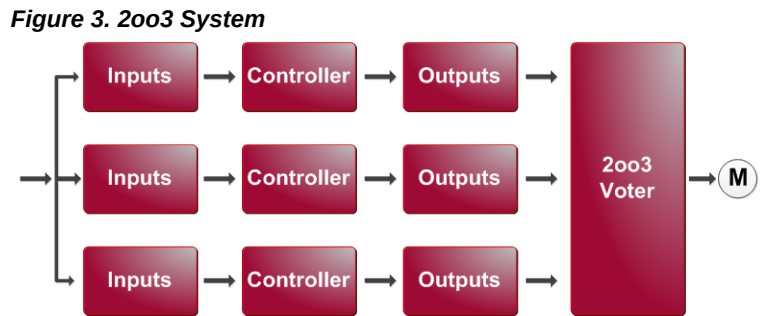


For the right type of redundancy, however, the question is not if you need more safety or availability. You can't just switch off a mission-critical function on board an aircraft. It has to be available continuously and safely. If you need a high degree of redundancy, you will accordingly build up a 2oo3 or 2oo4 system.

¹ This White Paper refers to the following definition: In a MooN system, M out of N channels must operate for the system function to work. In our example the system function would be the switching on of a motor. In the first example (Figure 1) it is sufficient if one channel is operable; it can switch on the actor by itself. In the second example, both channels must be operable for the actor to be switched on.

With such a level of complexity, a voting mechanism, or voter, is an inherent part of the system. It permanently compares and analyzes computing results. In the case of a deviation the voter recognizes the erroneous CPU, but the system can go on operating using the other two components.

The 2oo3 set-up is used frequently, because it increases both safety and availability to such a measure that is statistically sufficient and reasonable, and because the involved overhead remains acceptable. The MTBF rises by a factor of approx. 1.2. The set-up may be acceptable but it is still complex: three subsystems must be synchronized and must communicate – especially for software this is not an easy task. What's more, the performance might go down.



Modular systems based on standard plug-in cards allow a relatively easy set-up for a redundancy like this: you simply triple all cards. This has drawbacks: three parallel systems need space, they also triple power dissipation, and the implementation of the software and a voter for the three computers can be complicated.

This is why MEN has taken redundancy to the board level. Apart from the tripled PowerPC 750 processor, the CPU card also features redundant main memory, local voltage supply, clock generators and Flash memory. The voter is implemented as an IP core inside an FPGA (Field Programmable Gate Array).

If one CPU fails, the voter isolates it and keeps it in reset state. It also notifies the software and keeps comparing the remaining CPUs in continued operation. The system is still fully functional, as long as none of the remaining processors fails.

This solution requires considerably less power and space than three individual boards. The fact that software issues are greatly simplified is at least as important, if not more so. The three PowerPCs operate in an architecture called "lockstep". The processors are completely synchronized. For the software, they are one unit. Redundancy becomes invisible to it.

In practice this means that the software itself does not have to be redundant. The overhead for its integration dramatically reduces, and with it the total development costs. The code necessary to keep three processors synchronous is rather simple. Even existing systems basing on a single CPU can be retrofitted at low expense.

MEN Mikro Elektronik GmbH

Neuwieder Straße 3-7
90411 Nürnberg
Deutschland

Tel. +49-911-99 33 5-0
Fax +49-911-99 33 5-901

E-Mail info@men.de
www.men.de

Radiation-Resistant FPGA, Safe Memory

As mentioned above, every important component can be a "Single Point of Failure". Especially in airborne applications memory errors caused by cosmic radiation are a problem. These include effects like SEUs – Single Event Upsets – or MBUs – Multi-Bit Upsets –, where one or more bits are "flipped" in flip flops or RAM cells, i.e. accidentally change from 0 to 1 or vice versa.

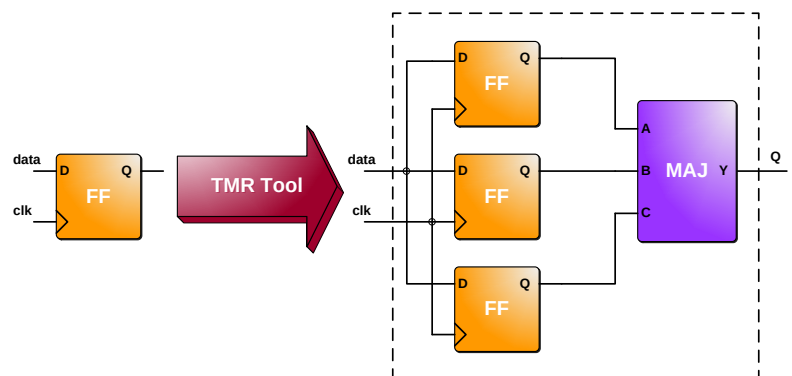
This is the case especially for memory components and the FPGA, which plays a prominent role in the MEN design. It not only contains the voter for the CPU but also controls the RAM banks. In order to automatically detect and correct bit errors you can also put three banks in redundancy – again Triple Modular Redundancy (TMR) is employed.

All read and write accesses are done in parallel in all banks at once. The voter analyzes the data read from the memory cells according to the majority principle. Independently, the entire memory is periodically read out in the background – one word with every refresh cycle. The determined majority value is written back. This mechanism is called "scrubbing". It prevents an accumulation of flipped bits.

In a similar fashion, the IC designers have also "hardened" the flip flops in the FPGA's registers. Randomly toggled flip flops can lead to several different error effects at the FPGA's interfaces, from skewed output data up to completely erratic behavior. The synthesis tool of the component allows to turn one flip flop into a block of three flip flops, and to place a two-out-of-three voter (2oo3) downstream. The failure rate of a TMR block is approx. 0.000001 FIT (Failure In Time)², so that flip flops become virtually meaningless when you consider possible errors in the system.

The IP cores inside the FPGA were designed according to the DO-254 avionics standard. With these prerequisites you can use a standard FPGA component even in a safe computer. It is just as resistant to radiation but at the same time much more inexpensive and flexible than a component specially developed for aerospace, for instance.

Figure 4. Tripled flip flops as a TMR block in the FPGA



² The unit "FIT" gives the number of failures that occur within 10^9 hours: 1 FIT corresponds to 1 failure in 10^9 hours, or 1 failure in 114 000 years.

Since long-term availability is also an important factor in safety-critical applications, using an FPGA also protects the design from component obsolescence. Especially with extremely complex functions this can reduce development costs in the long run. One example would be an AFDX interface.

The **Avionics Full Duplex Switched Ethernet** handles communication between an aircraft's systems. It builds on Ethernet and additionally prescribes characteristics such as high data integrity, redundancy and deterministic behavior. Implementing an AFDX function potentially involves a lot of development work, which can pay off in the application only after a longer period of time. Designing this interface into an FPGA is an extremely sustainable economical approach.

Deterministic Behavior

"Deterministic" as an AFDX feature is applicable to the entire system, too. Next to failure safety, mission-critical environments also demand calculable execution times. The system must react to an external event within a defined time, even under worst case conditions.

Typical computer architectures use interrupts and DMA structures. These may have an effect on reaction times, however. The demanded deterministic, i.e. predictable behavior would then be hard to achieve. This is why you just avoid common mechanisms like the ones mentioned above.

Instead, engineers need to consider possible behavior and its consequences in detail at an early stage, in preparation for their actual design. A definition of the different scenarios and error situations that is exact and as comprehensive as possible, paired with the then determined behavior of the computer, results in a high level of predictability. The primary goal is to detect errors before they can harm the entire system.

In terms of hardware and firmware, BITE components are used here – Built-In Test Equipment. Errors handling techniques such as ECC (Error Correcting Code) or the monitoring of internal voltages play an important role, here, too.

When it comes to software, the most essential choice is which operating system to use. System integrators in need of deterministic behavior select a real-time system like VxWorks or PikeOS. These have optimized, for example, their memory and task management for minimum latency, so that the system remains predictable.

Wherever there can be interruptions in power supply, short start-up times are vital, too. For this reason MEN's designers have optimized their boards for fast booting. With an 8-MB boot image, you can attain a start-up time of 500 ms. This is practically immediately after power-up.

Diverse Redundancy and Clustering

To make systems even safer, you not only use redundancy but additionally use the principle of diversity. Identical subsystems (homogeneous redundancy) can fail simultaneously by a common cause. You can counter this by building in differences that reduce vulnerability to Common Mode Failures (CMF, failures with a uniform behavior) and Common Cause Failures (CCF, failures that occur by one common cause).

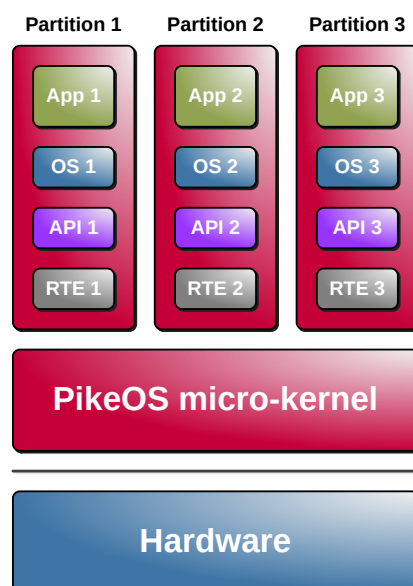
For instance, you can run different, independently designed software applications on the subsystems. On the hardware side you could use different I/O interfaces. Identical functions are implemented in varying ways. In the end the two dissimilar set-ups must lead to the same result, so that the system can act in a defined way.

Diversity is even possible on one single board: memory management of the PowerPC processors in the MEN design allows to partition the resources, which is in turn supported by real-time operating systems like PikeOS. The partitions are assigned specific memory areas. The applications and tasks being executed within the partitions can be completely different.

It is also possible to combine two assemblies to form a highly available computer cluster. In a set-up like this, every channel – being redundant itself – works independently, but only one channel is active. If the active channel fails, the system automatically switches to the second channel.

The boards can be connected using dedicated serial interfaces: UARTs (DEX) make for communication between the two channels. A direct connection between the Board Management Controllers (BMCX) controls the switch-over from the active to the inactive channel.

Figure 5. Diversity by partitioning in PikeOS



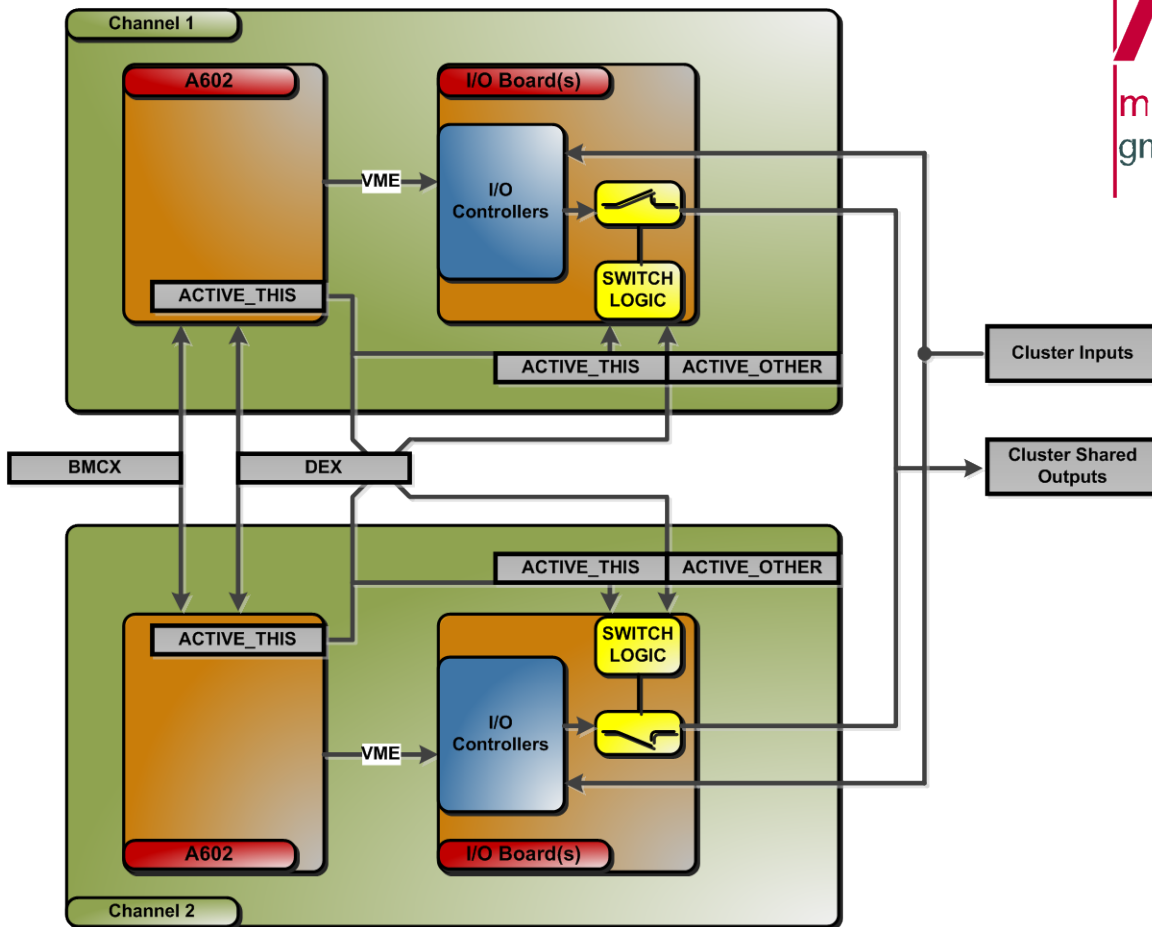
MEN Mikro Elektronik GmbH

Neuwieder Straße 3-7
90411 Nürnberg
Deutschland

Tel. +49-911-99 33 5-0
Fax +49-911-99 33 5-901

E-Mail info@men.de
www.men.de

Figure 6. Two A602 VMEbus CPUs as a cluster with one active and one inactive channel



The Framework: Not Only the Computer Must Be "Safe"

Standardized Safety

A general standard, IEC 61508 by the International Electrotechnical Commission, covers functional safety in electronic systems. It defines the Safety Integrity Levels SIL 1 up to SIL 4. Manufacturers are obliged to find out the necessary SIL for safety-relevant systems or functions by carrying out a hazard and risk analysis. It gives the measure for the effectiveness of a safety function and is expressed by the probability of failure of this function. Different scenarios match a defined scale of numerical values.

Several bodies have added specific standards for the varying industries and applications. For railways, the European Committee for Electrotechnical Standardization (CENELEC) has issued relevant documents. These include EN 50126 (Reliability, Availability, Maintainability and Safety (RAMS) in rail systems), EN 50128 (Software for railway control and protection systems) and EN 50129 (Safety related electronic systems for signaling).

MEN Mikro Elektronik GmbH

Neuwieder Straße 3-7
90411 Nürnberg
Deutschland

Tel. +49-911-99 33 5-0
Fax +49-911-99 33 5-901

E-Mail info@men.de
www.men.de

EN 50129 also contains the exact definition of SIL levels specially for railway applications. It derives the matching SIL from the Tolerable Hazard Rate (THR) per hour and per function. SIL 4 allows a range of 10^{-9} to 10^{-8} , down to SIL 1 with 10^{-6} to 10^{-5} .

In the aviation industry, the RTCA DO-254 and RTCA DO-178B (EUROCAE ED-12B) standards define five safety levels called Design Assurance Levels (DAL) for airborne hardware and software. Levels DAL-A (highest) down to DAL-E basically correspond to SIL 4 to SIL 0 (not safety-relevant) and also derive from possible damage in the case of malfunction.

The two examples of railway and aviation very well represent further safety-relevant areas. They are among the most demanding markets. In any case designers must take into account all applicable standards in the development of electronics. This requires experience and expertise of the manufacturer.

Qualification of the Manufacturer

The ISO 9001 quality management standard has conquered the rank and file, including even small to medium-size companies. To qualify manufacturers for demanding industries, there are standards that build upon ISO 9001 but at the same time go far beyond. The EN/AS 9100 standard takes this role for avionics, while IRIS (International Railway Industry Standard) covers the rail market. Both involve periodical, intensive audits.

In order to fulfill the high requirements of the mentioned quality standards, a manufacturer should ideally have years of experience with relevant development projects, and should have the necessary infrastructure already in place. This includes traceability of all steps in the entire value chain. Supplier assessment or component obsolescence management in purchasing, traceability of components in production up to risk management in general are only some examples. Inspection departments regularly use test methods such as HALT (Highly Accelerated Life Test) and HASS (Highly Accelerated Stress Screening).

However, development is one of the biggest chunks. Functional safety needs the highest level in quality for design processes, which allow to recognize and eliminate design errors at an early stage. Design teams must have completely taken in the safety aspect, because it is impossible to make a design safe in retrospect.

A method called V-model supports this by going through defined steps according to a fixed scheme, from the requirement to the architecture specification on the system and component level, and through the design itself on to integration and validation of all components and of the system. This also includes traceability, for example of the fulfillment of all the requirement items.

MEN has been certified both to EN 9100 and to IRIS for several years, and in the design of the boards described here has observed both the guidelines of avionics (DO-254) and railways (EN 50129). The cards comply with environmental standards DO-160 and EN 50155. With this background, both assemblies are certifiable according to the most severe safety levels – SIL 4 for railways or DAL-A for avionics.

Certification

Certification for safety-critical applications is a procedure that involves many details, includes all components of a system and is therefore the task of the system integrator. If on the board level all applicable standards were observed and requirements fulfilled, and if this was accordingly documented, the manufacturer can make the system integrator's life easier by providing this documentation. For the integrator this translates into lower cost and faster time-to-market on a high level of quality.

MEN is currently certifying its design according to SIL 4 in cooperation with the German TÜV SÜD organization. In railways this is possible even for a single board. The governing standards for this are EN 50128 (FPGA) and EN 50129 (hardware). Customers who integrate the card into a complete system are able to make use of a package that includes all the necessary documents for this component, such as the required Safety Case. Together with the safety-related application conditions, the customer receives the documentation required by the standard, and is then able to integrate the component into his application at the required safety level.

This kind of certification on board level is not possible in avionics, where it always relates to the entire system. However, MEN's design derived from a custom avionics project that was already DAL certified. This makes for a firm basis that is planned to be further solidified.

The CPU boards from MEN support Sysgo's PikeOS and Wind River's VxWorks – two certifiable real-time systems specially directed towards safety-critical applications. For VxWorks, Wind River offers platforms certifiable up to DAL-A or SIL 4.

MEN Mikro Elektronik GmbH

Neuwieder Straße 3-7
90411 Nürnberg
Deutschland

Tel. +49-911-99 33 5-0
Fax +49-911-99 33 5-901

E-Mail info@men.de
www.men.de

Conclusion: Putting All Your Eggs in One Basket can be Safe, too

The approach of accommodating a fault-tolerant computer with triple redundancy on a single board that is usable in existing standard 6U systems is unique in the industry. MEN has managed to both meet the high requirements of its target markets railways and avionics and to fulfill the demand for modularity.

The boards have all the features of a "safe" computer. By implementing the typical safety mechanisms on one card, considerably less software overhead is necessary, for example to port applications that were written for a single CPU, or by the integrated voter.

Another fault-tolerant computer is being developed at MEN, this time even more compact and based on 3U CompactPCI with three Intel Atom processors.

Paired with the know-how and comprehensive quality management of MEN and an optimum support in certification, these products help to lower costs in building up systems in safety-critical applications. Their clear-sighted design and extensive documentation make the two cards ready for use on board aircraft, trains or in other areas.

Product Information

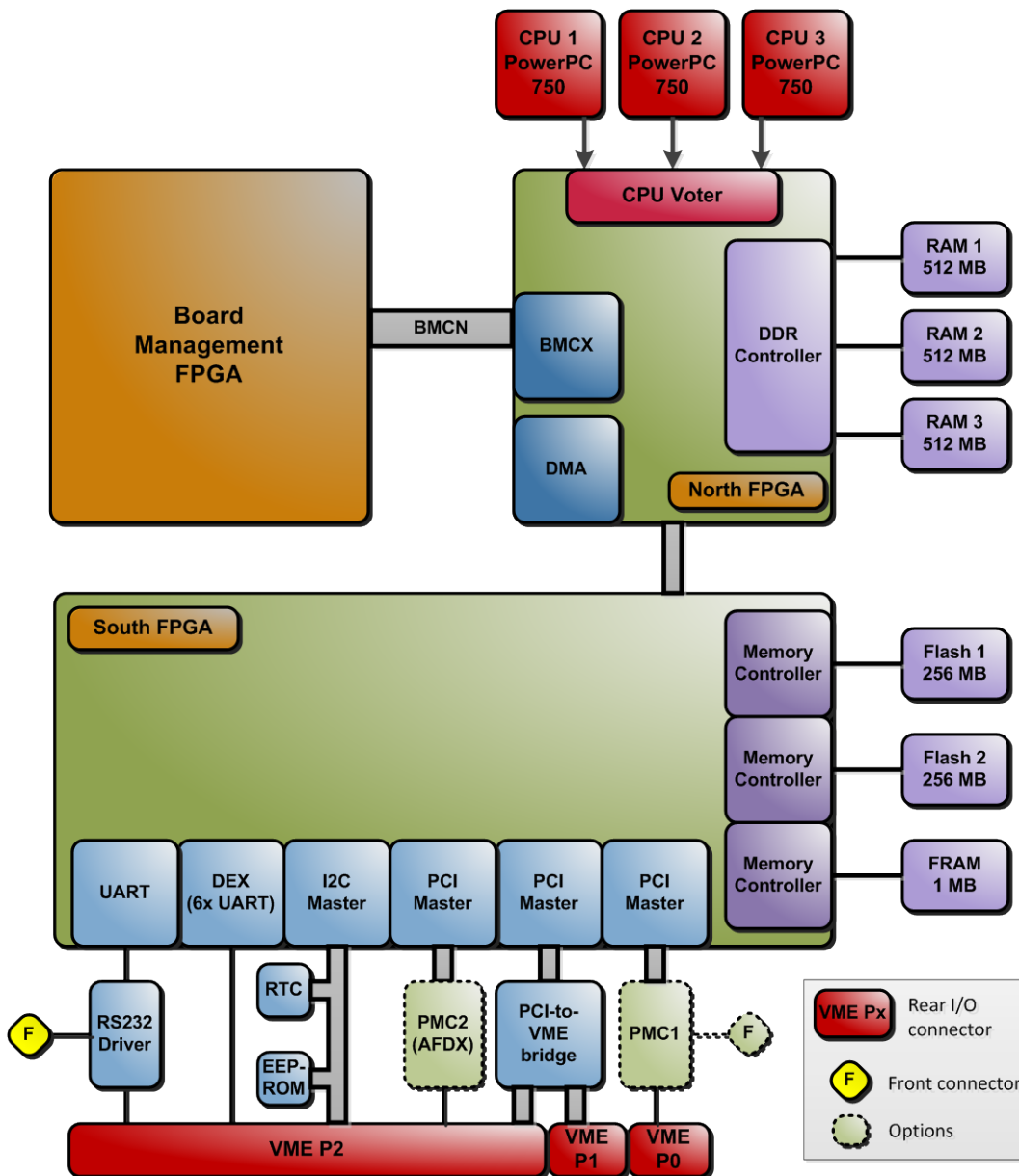
The A602 VMEbus CPU is a 64-bit VME master, the D602 is a system-slot CPU for CompactPCI. Both are double Eurocards with a 1-slot front panel.

- Triple redundancy (2oo3) on a single board
- 3x PowerPC 750 CPU,
1 GHz, lockstep architecture
- 3x DDR RAM, 512 MB
- 2x ECC Flash, 256 MB
- 1x ECC FRAM, 1 MB
- Redundant local power supply
- FPGA hardened against cosmic radiation
- 2 PMC slots (PMC1 with rear I/O)
- Further rear I/O
- Certifiable up to SIL 4 / DAL-A
- -40 to +50°C with qualified components
- Suited for conduction cooling up to +70°C

Data Sheets

- A602, VMEbus: www.men.de/01A602-.html
- D602, CompactPCI: www.men.de/02D602-.html

Figure 7. Block diagram A602 (VMEbus, 6U)



About MEN Mikro Elektronik

Since its foundation in 1982 our company designs and manufactures failure-safe computer boards and systems for extreme environmental conditions in industrial and safety-critical embedded applications.

You can find more information about MEN under www.men.de/corporate/about.html.

MEN Mikro Elektronik GmbH

Neuwieder Straße 3-7
90411 Nürnberg
Deutschland

Tel. +49-911-99 33 5-0
Fax +49-911-99 33 5-901

E-Mail info@men.de
www.men.de