White Paper

Railway Computer 3.0: An Innovative Board Design Could Revolutionize The Market

Susanne Bornschlegl, MEN Mikro Elektronik
October 2012

When you have designed and built up redundant computer systems for the safety-critical railway market for many years, you both appreciate the upsides and know about the downsides of an established bus system. It's good if you have some new ideas then. A new board design in 3U CompactPCI shapes a possible answer to the question "What if...?"

Safe, Robust, Compact, Modular – And Competitive?

A computer that you want to build into a vehicle must work reliably, both in terms of hardware and software. It has to be safe and at the same time extremely robust. This makes the price of such systems rise. Yet, costs must not get out of hand, as they would be passed on to customers. The vehicles and consequently the provider, especially in mass transit, must stay competitive, however.

Still, functional safety plays the leading role in system design, because errors or failures potentially result in loss of life or cause major damage to the environment but also to property. Strict standards demand the safety criteria for each market, from railways to buses and ships up to airplanes.

In order to build up robust systems, you can use matured industry standards and commercial-off-the-shelf (COTS) CPU boards, which help keep the costs within reason. This is why you can find 19-inch CompactPCI technology in many places in railway transportation.

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

Classic: 19-Inch Systems

3U CompactPCI is doubtless a perfect way to build up a modular computer system including redundancy. The benefits are obvious: exchangeable COTS boards are relatively inexpensive and easy to maintain. The format is compact enough, e.g., for the switching cabinet on board a train. A typical, functionally safe system consists of two or three processor plug-in cards, which are connected using network cables. To do this, you normally use robust M12 connectors at the front side, which are tightly screwed and do not work loose by the vibrations prevalent in rolling stock.

Very generally you can say that two or three individual boards always result in a multiple in volume, weight and costs. The power dissipation multiplies, too. By itself this does not have to be a major disadvantage, as long as all the factors are in a reasonable relation to the use, and as long as the system fulfills all the requirements. When having a closer look at this constellation backed up by experience, however, you will encounter drawbacks that come up especially in demanding applications.

Figure 1. Typical 3U CompactPCI systems from railway applications with redundant architecture but simple RJ45 connectors at the front

- *2 diverse control computers per card cage*
- *1 I/O computer*
- *Each computer with its own power supply*
- *Communication between CPUs via front-panel Ethernet*

- *2 control computers*
- *1 I/O computer*
- *1 power supply unit per housing*
- *Communication between CPUs via LVDS*
- *Communication between several card cages via front-panel Ethernet*

Connecting redundant computers in a network involves cabling efforts. And cables are expensive. On the one hand, it's the material itself, and on the other, it takes more time to build up the system. This may still be manageable with two boards, but with three boards you already get a rat's nest of cables in the system.

Even if the connection itself is absolutely reliable owing to M12 connectors, the network connections are prone to errors, making the entire system more susceptible to faults and increasing maintenance efforts. After all, the individual

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

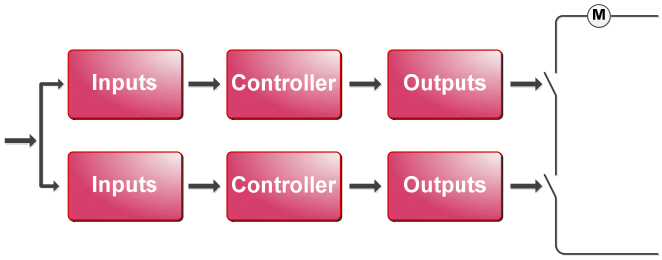
components of a redundant set-up that is supposed to make for functional safety must be interconnected in an uncompromisingly reliable way. A failure in inter-communication leads the whole idea of redundancy ad absurdum.

Redundant: Better Safe Than Sorry

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 describe them, you give the number of functions that can trigger a safe state (M) compared to the total number of redundant functions (N). This results in “M out of N”, abbreviated as MooN.[1]

With safe redundant functions, all components must deliver the same computing results, to allow for the detection of errors, in the simplest case in a 1oo2 system. This scheme requires both instances to operate identically at any time. In our example in figure 2, the system function would be the activation of a motor. In case of an error, one channel can already deactivate the motor safely.

Figure 2. 1oo2 system: one channel can already deactivate the motor safely



Fail-Safe: Full Stop?

When you think of rolling stock, for example, 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”. This sounds simple and logical. But how does the computer enter this safe state? The most reliable method is to power off the CPU boards. With a CompactPCI example system using dual redundancy, this goes for both boards. This in turn sounds trivial but in fact involves additional effort.

Common CPU cards lack important characteristics to react in a controlled way to make the system “fail-safe”. For a computer to deliver correct results, it must be operated within its specification. This includes the operating temperature as well as the different voltages on the board, up to the clock frequency of diverse functions. Every card has a number of supervisory mechanisms of its own, which are standard features of industrial computers. The technology is mature, and is sufficient for operation in a less critical environment. This is why

[1] This definition is valid for IEC 61508. You can view the MooN principle from different sides, so that differing interpretations are possible.

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

diagnose functions like these usually supervise only a portion of the parameters.

In many cases even the CPU itself takes over diagnosing tasks. If it is running outside its specification, then it possibly cannot reliably supervise itself any longer. Can you still rely on the CPU, and – having become an element of uncertainty itself – can it still effect a change into a safe state, together with a "twin assembly" in the system?

Behavior that is not predictable is undesired in a safety-critical environment. Apart from its vital functions, a computer must also provide calculable execution times, i.e. deterministic behavior. The system must react to an external event within a defined time, even under worst case conditions.

State-of-the-art COTS CPU cards use interrupts and DMA structures; they can dynamically change their clock and are designed for high-performance multicore operation. All of this may have an effect on reaction times, however. The demanded predictable behavior is hard to achieve. It is rather uncertain whether response times can be observed at all times.

Back-up: Change Of Shift!

Let's assume the CPU cards in our redundant system are accordingly equipped, their behavior is deterministic and they synchronize continuously. A fatal error occurs, the system powers off. The example of a train that stops is only a highly prominent one. If the train stops inside a tunnel, of course, the passengers are not supposed to be able to open the doors simply by pressing a button. On the other hand, the lighting inside the train should continue working. There are numerous subsystems with special functions, which in case of an error need to react in different ways.

To assure safe operation, you can multiply the existing system and make it available as a back-up unit. One system is always active, while the other runs in "stand-by mode". This again sounds good but once again involves additional effort: In order to implement the changeover to a back-up system, you need logics that define and correctly manage the roles of the two systems.

And if that were not enough: Errors happen, and it's easy to be wise after the event – if you know the exact cause of the error. Searching for a cause is difficult if you do not have an event log. If there is a service incident and you want to look up an event protocol, you must have had implemented one in the first place. A centralized system error logging can only be implemented using supplementary hardware. In the end, the function should also be available if the software crashes.

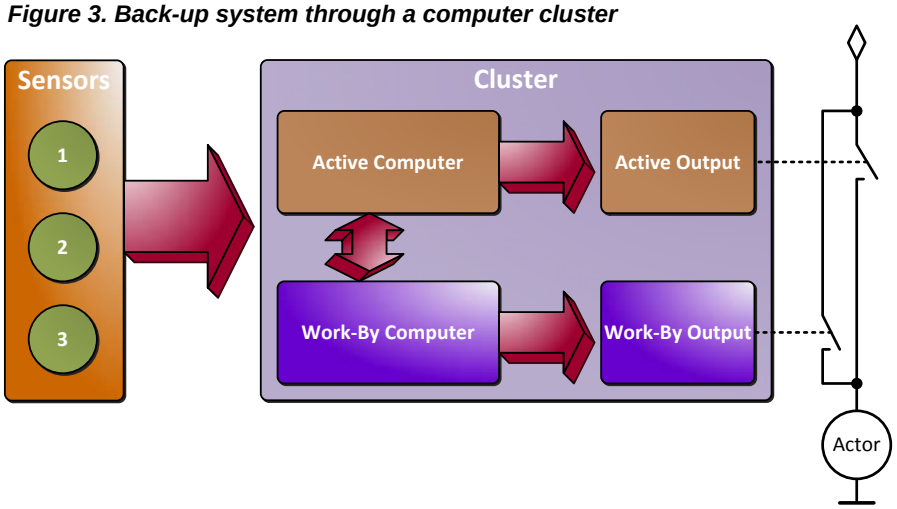
MEN Mikro Elektronik GmbH

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 3. Back-up system through a computer cluster



Standards: Strictly Uniformed

The requirements concerning functionality and ease of maintenance are one thing. In railway applications the applicable standards add further demands. EN 50129 defines the safety requirements for the Safety Integrity Levels SIL 1 to SIL 4 regarding the functional safety of electronic systems in railway applications. 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.

If the system integrator wants to certify a computer system to SIL 3, for instance, he needs to check if its individual components fulfill specific criteria. The Tolerable Hazard Rate (THR) is an important measure here. It gives the probability of a dangerous failure per hour and per function. The demanded value depends on the SIL level to be met. The higher the SIL level, the lower the value has to be, i.e. the smaller may be the probability of a dangerous failure. The THR must be between 1E-7/h and 1E-8/h for SIL 3, while SIL 4 requires 1E-8/h to 1E-9/h.

The problem is that these values are usually not available for COTS boards. The system integrator has to find out the failure rates from the design data – provided he has access to this data at all.

Experience: Driving Innovation

In any case, the system integrator makes a good decision if he selects a manufacturer with experience and know-how, who already knows the applicable standards, and takes these into consideration as early as during electronics development. Quality management according to IRIS (International Railway Industry Standard) is a solid base for products in the railway industry. This standard exceeds the popular ISO 9001 and, among others, requires more intensive auditing.

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

MEN Mikro Elektronik has a background of activities in the railway area and has grown with its challenges, too. From supplier assessment or component obsolescence management in purchasing, traceability of components in production up to risk management in general the company has consistently improved its processes and continues to do so due to its IRIS qualification.

Functional safety needs the highest level in quality for design processes, which allow recognizing and eliminating design errors at an early stage. Design teams must have completely taken in the safety aspect, because it is virtually 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 includes traceability, for example of the fulfillment of all the requirement items.

Many years of experience with CompactPCI systems has brought and keeps bringing MEN's product management new impetus. If you want to build forward-looking computers, you have to break new ground and must never tire of questioning the status quo.

Food For Thought: What if…?

If you could design everything to be even more compact, if the computer was not built up from single boards and had to be wired, and if you placed several processors on one card? Is the space sufficient for all of this? Can you still handle thermal characteristics? There are many questions to answer, many partial solutions to find, if you dare to take this design challenge. The F75P CompactPCI plug-in board in compact 3U format proves that it is possible after all.

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

First-Class Ticket For The Customer

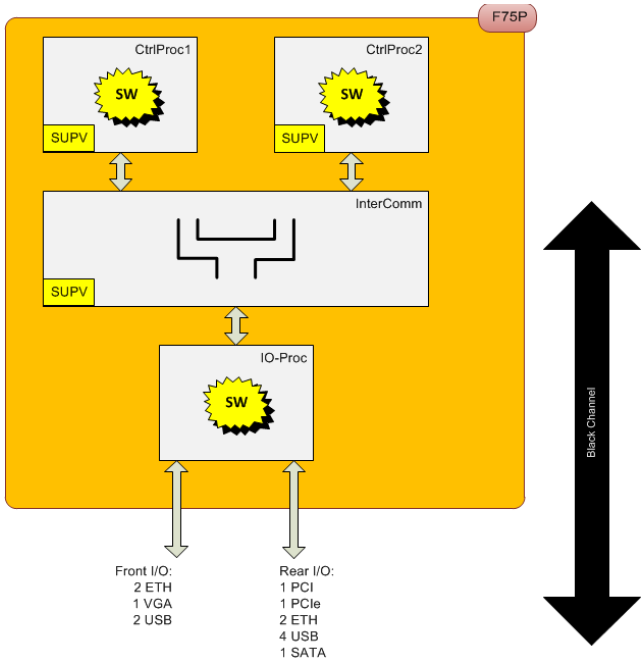
Every new design is ideally driven by the wishes and needs of the customers, also and especially if it is not an explicit custom design. As more and more functions are computerized in railways, what is sought after are robust electronics that are inexpensive and can easily be integrated into systems. Apart from price pressure, there are also high demands concerning functional safety. Bad compromises would be out of place here. A commercial-off-the-shelf solution where everything is just right can bring along enormous reliefs.

After having designed standard 6U assemblies with triple redundancy on one board, MEN Mikro Elektronik takes another step and wants to make safe systems more compact even in 3U format with a new computer. Of three assembled processors, only two are redundant this time, and take over the essential function of a central control (Control Processors, CP). The third CPU is independent and is responsible for I/O functions (I/O Processor, IOP).

The three processors use an internal Ethernet connection directly on the board to communicate with each other, which completely eliminates elaborate wiring. Their redundant architecture allows the two Control Processors to recognize single errors in one of them and to react accordingly.

In addition the computer supports the CompactPCI PlusIO standard: fast serial interfaces are routed to the J2 backplane connector, building a bridge to the serial standard of the future, CompactPCI Serial.

Figure 4. General architecture of 3U computer F75P



Versatile Control Center

A typical application would be a cross comparison to detect discrepancies: The same application logic is identically executed on each of the processors. Both CPUs calculate their outputs and compare their results with the other channel.

The board is not restricted to any special compare strategy. The user can integrate it in many kinds of ways, because he has complete freedom in implementation. It is true that this means more work for the system integrator, for example when setting up a voter mechanism. On the other hand he can realize different functions using the same, known assembly, while saving costs. Where a lower SIL level is sufficient or the function is less complex, less effort is needed compared to an extremely critical SIL 4 application.

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

If you want to use an existing software architecture that was originally implemented on individual boards, this is also possible without any problems. You can execute identical or diverse software on the Control Processors. They support VxWorks and PikeOS, which are real-time operating systems common in critical environments, but they also support Linux.

An interesting and not so obvious aspect is that dissimilarity of the operating system can in fact lower system costs. While you would need an operating system like VxWorks/Cert to achieve SIL 2 with a single CPU, this SIL level can also be achieved using two CPUs and dissimilarity. A combination of Linux and the “plain” VxWorks would be sufficient. The licensing costs of VxWorks/Cert have such magnitude that diversity becomes competitive despite the higher development effort.

The I/O processor is where control elements like sensors on board the train are actually connected to. In addition to its core function, it can take over other, non-safety-critical tasks, such as control of a fieldbus or graphical output of operation data. As the tasks can vary, this CPU also supports different operating systems. Linux or Windows would be typical choices for a comfortable user environment and the usual graphics capabilities.

Attention, Please, We Have To Stop Shortly…

In case of a serious error the board behaves to be "fail-safe" and "fail-silent", i.e. the computers are powered off. The card can no longer generate output; it has entered a safe state. This state is kept until a power cycle is performed. The behavior can also be configured in such a way that the computers automatically restart, if this is required. In both cases the configuration is determined by hardware, and is always unambiguous.

To reliably coordinate and monitor the processors on the board, it has two independent supervisor components (SUPV) designed to SIL 4. These make sure that both Control Processors are operated within their specification. Each supervisor can put the board into the safe state. The software of each Control Processor can also switch the board into the safe state, independently of the other processor.

This dedicated monitoring has the benefit of being separated from the CPU. It checks the usual parameters like voltage, temperature and frequencies but also registers internal errors of each processor. The FPGA component that controls communication with I/O has a supervisor of its own for error recognition.

During operation, events like a voltage drop, excess temperature or reset can occur and lead to malfunction. If you log these events, searching for errors in case of an incident is much easier, and chances are higher to avoid the error

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

cause in the future by taking precautions. To do this, MEN's F75P has an event logger that saves a history of the last 256 events in a non-volatile FRAM. These entries are basically predefined hardware events, but the application software can generate events, too, making the protocol more specific and more detailed.

…And We Can Continue

Where design engineers want to equip supervisory circuits with all the mechanisms necessary especially in safety-critical applications, they 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.

As far as software is concerned, the MEN board uses real-time systems like VxWorks or PikeOS to assure deterministic behavior. These have optimized, for example, their memory and task management for minimum latency, so that the system remains predictable. You would usually pair this set-up with a PowerPC processor.

The F75P is different: To support existing X86 applications, a decision was made in favor of the Intel Atom E6xx series, which brings together a solid base and higher performance. For the demanded behavior to remain guaranteed, you have to take a close look at the processor and cross out a couple of its features.

Hyper Threading, for example, is deactivated, because it would allow the hardware to handle several processes in parallel. The card also does without SpeedStep technology. Otherwise the processor could change its clock rate, i.e. its performance. Behavior would no longer be calculable. BIOS interrupts are off limits, too.

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

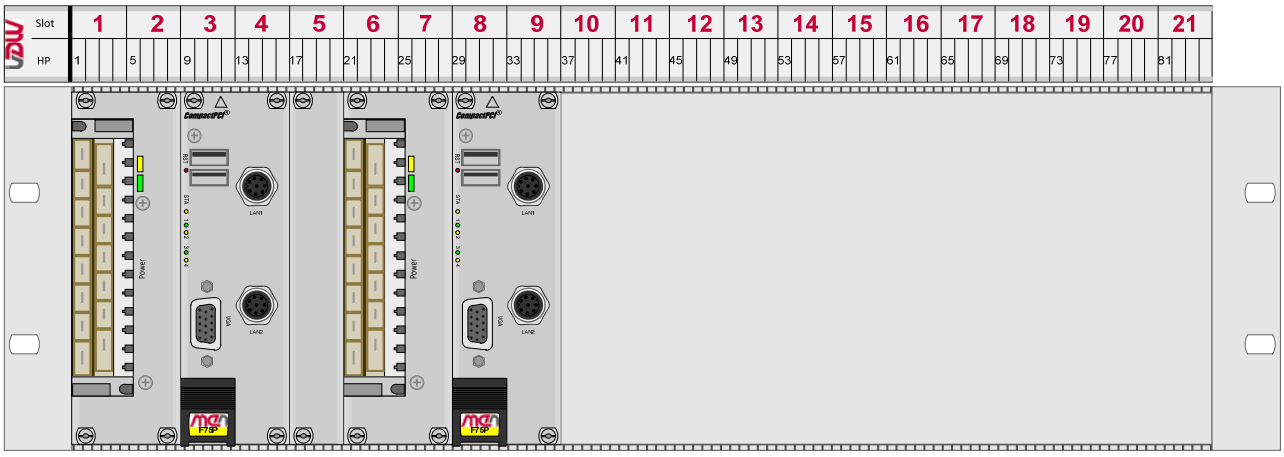
E-Mail info@men.de
www.men.de

Marathon Operation: Just Keep Running

For critical functions, a computer system should rather switch itself off than output wrong data. Where such functions must stay available, the obvious solution lies in a computer cluster, which links up two boards. In a set-up like this, every channel – being safe 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: A direct UART connection between the Board Management Controllers (BMC) provides communication between the two channels and controls the switch-over from the active to the inactive channel. The F75P's UART is an RS422 interface led to the CompactPCI backplane. By consequence, there are no cabling efforts involved.

Figure 5. Compact cluster system using two F75P cards, each with its own power supply (cf. Figure 3)



Tickets, Please!

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.

Several bodies have added specific standards for the varying industries and applications, mostly basing on IEC 61508. For railways, these include the 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) standards.

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

MEN has observed the guidelines of EN 50129 and EN 50128 for the development of the F75P computer. The assembly completely fulfills rail electronics standard EN 50155, too. MEN is currently certifying its design according to SIL 4 in cooperation with the German TÜV SÜD organization. In railways this is possible for a single board. EN 50129 is particularly important in this respect, as it contains the exact requirements for the SIL levels specially for railway applications.

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. These include a certificate from TÜV and the required Safety Case according to SIL.

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 greatly facilitates the certification of a complete system.

The CPU board from MEN supports Sysgo's PikeOS and Wind River's VxWorks – two certifiable real-time systems specially directed towards safety-critical applications. In 2012, PikeOS has been officially certified to SIL 4 by TÜV SÜD (according to EN 50128).

The Course Is Set

The pioneering new design of the F75P computer in 3U CompactPCI takes MEN one step further towards its goal of both meeting the high requirements of the railway industry and of fulfilling the demand for modularity. MEN has already proved this through its existing 6U CPU cards with onboard triple redundancy.

However, the current computer is neither a competitor of the 6U products nor their successor. It simply has an entirely different architecture, focusing on different aspects. Its flexibility makes it an interesting component for existing 19-inch CompactPCI systems that are past their prime, but also for new vehicles that can benefit from technology innovations right from the start.

The design is just as interesting for other markets where electronics are safety-critical or increasingly become so, as is the case in automation or medical engineering. This is due to the compact set-up of the computer, but especially to the free implementation of its redundant control CPUs.

Paired with the know-how and comprehensive quality management of MEN and optimum support in certification, these products help lower costs in building up systems in safety-critical applications. Its clear-sighted design and extensive documentation makes the innovative computer ready for use on board rolling stock or in other areas where functional safety is more and more becoming an issue.

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

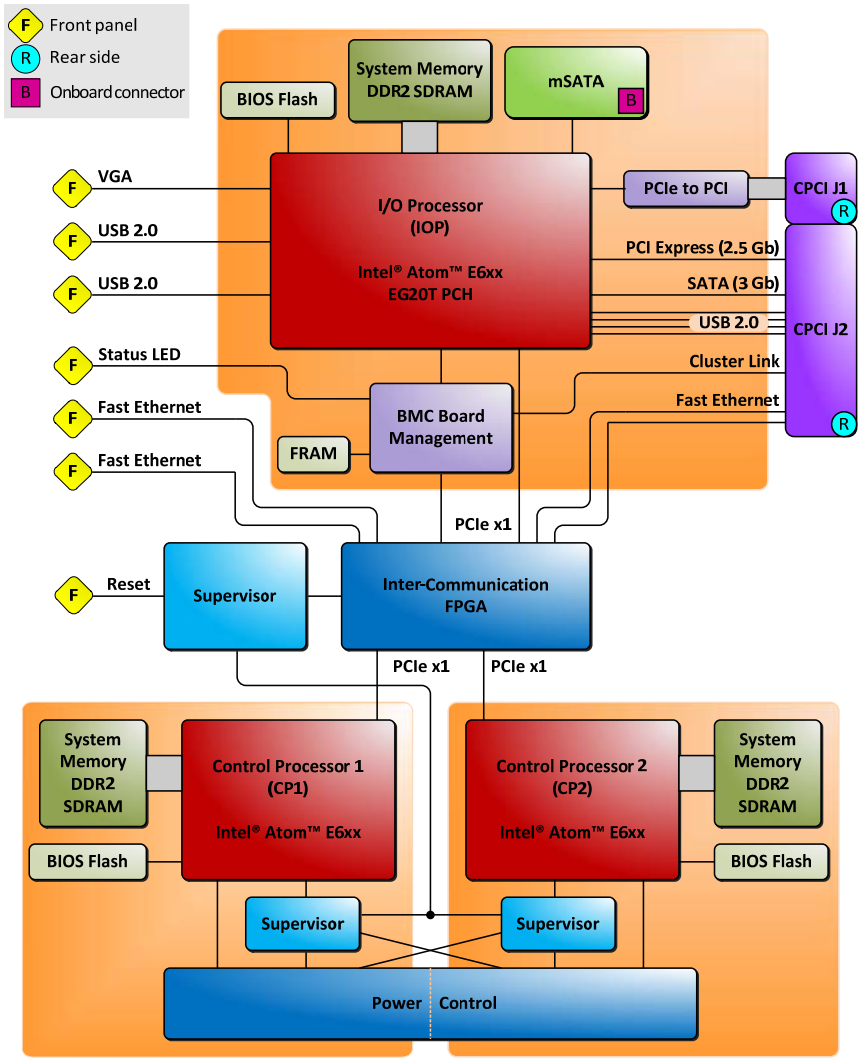
Product Information

The F75P is a system-slot computer for CompactPCI and CompactPCI PlusIO systems in 3U format. It integrates three independent Intel Atom processors on one card.

- Two redundant control CPUs: Intel Atom E6xx, 512 MB DDR2 RAM each
- Dedicated CPU for I/O: Intel Atom E6xx, 1 GB DDR2 RAM
- Independent supervisory circuits for all three blocks
- Fail-safe and fail-silent architecture
- Clustering of two F75P to raise availability
- Event logging
- Certifiable up to SIL 4 (with report from TÜV SÜD)
- Developed according to EN 50129, EN 50128 and IEC 61508
- Tolerable Hazard Rate (THR): ≤ 1E-9 / h
- Full EN 50155 compliance
- -40 to +85°C with qualified components and tailored heat sink (8 HP)
- Conformal coating by standard

Data sheet: www.men.de/02F075P.html

Figure 6. Block diagram of F75P



About MEN Mikro Elektronik

Since its foundation in 1982 our company has designed and manufactured 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