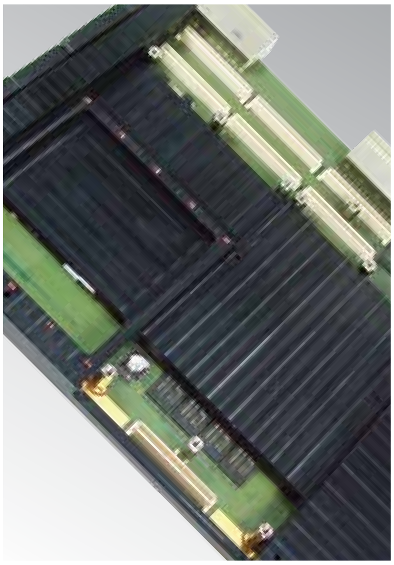
Safe Computers for Demanding Applications

COTS assemblies with onboard redundancy certified to SIL 4 or DAL-A



Safe Computers

One of the key design elements of a safety-critical system is redundancy. The complex architecture of such systems usually requires equally complex software, resulting in a very time-consuming and expensive development process.

With CompactPCI® and VMEbus based CPU cards MEN has taken redundancy to the board level. Aside from incorporating doubled or tripled processors, the CPU cards feature redundant main memory, local voltage supply, FPGA technology, event logging, conduction cooling options and other safety relevant functions.

They have been developed according to DO-254 and EN 50129, are compliant with DO-160 and EN 50155 and are certifiable up to DAL-A and SIL 4.

MH50C – MEN Train Control System

- SIL 4 certified safe CPU board with 3x Intel Atom CPU, 1.6 GHz
- QNX SIL 4 safe operating system available
- SIL 4 certified safe I/O boards
- SIL 4 certification packages available
- Extensible by distributed safe I/O boxes connected via real-time Ethernet
- Optional MVB interface, RS232, RS422, RS485, CAN, GPS
- System supervision (temperature, fan and power supply)

The MH50C is the central controller of the MEN Train Control System and is a modular system platform usable for safety-critical train applications like train control, automatic train operation (ATO) and automatic train protection (ATP).

The MH50C system is application-ready, but not yet fixed to the final application. Instead, it can be configured to control anything in the train under SIL 4 requirements, by adding the application based on the basic operating system and driver software.

Based on CompactPCI, the system is always configured with a safe system CPU, a real-time Ethernet card, a power supply and a shelf controller. Other cards can be added as a BTO (build-to-order) option or by the user. The safe I/O cards support the common I/O requirements requested in trains.

F75P – 3U CompactPCI® PlusIO Intel® Atom™ Safe Computer

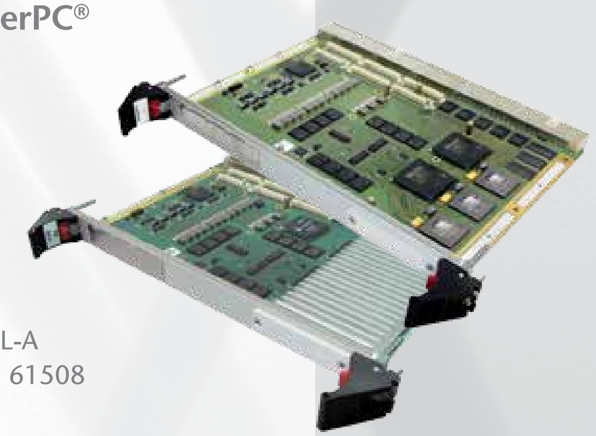
- 2x Intel® Atom™ E6xx, 512 MB DDR2 RAM (each) for onboard dual redundancy
- 1x Intel® Atom™ E6xx, 1 GB DDR2 for I/O
- Independent supervisors for each block
- Fail-safe and fail-silent board architecture
- Clustering of two F75P to raise availability
- Event logging
- Certifiable up to SIL 4 (with report from TÜV SÜD)
- Developed according to EN 50129, EN 50128 and IEC 61508
- Full EN 50155 compliance
- -40°C to +85°C with qualified components
- Conformal Coating

The CompactPCI PlusIO SBC unites three CPUs on one 3U CompactPCI® PlusIO card. It makes Intel® Atom™ E6xx ("E600") performance with dual redundancy extremely compact and can replace multiprocessing systems by a flexible small-footprint, low-power solution.

While two independent Control Processors with independent DDR2 RAM and Flash and a supervision structure provide safety, a third processor controls the I/O interfaces and is built up like a classic CompactPCI® CPU board, including DDR2 RAM, front and rear I/O.

F75P is designed to SIL 4 according to EN 50129, which is certified by TÜV SÜD.

D602/A602 – 6U CompactPCI® or VME64 PowerPC® Safe Computer



- 3x PowerPC® 750 (lockstep mode), 3x 512 MB DDR RAM
- Fail-operational, fault-tolerant behavior
- Fail-safe and fail-silent board architecture
- Clustering of two boards to raise availability
- Board management, BITE
- SEU (radiation) tolerant
- Certifiable up to SIL 4 (with report from TÜV SÜD) and DAL-A
- Developed according to RTCA DO-254, EN 50129 and IEC 61508
- EN 50155 compliance
- Up to -40°C to +70°C with qualified components
- Convection or conduction cooling

The 6U CompactPCI® D602 or 64-bit VME A602 COTS computer with onboard functional safety realizes triple redundancy on a single board. Its three processors run in lockstep mode with 2-out-of-3 (2oo3) voting implemented in a complex FPGA-based design. This helps dramatically lower software development costs as it automatically manages the system's triple-redundant processors and memory.

The D602/A602 have been developed according to DO-254, are compliant to DO-160 and certifiable up to DAL-A in avionics applications. Additionally, the products meet the requirements of EN 50128/EN 50129 and can be deployed in signalling and rolling stock applications up to SIL 4.

The Special Challenges of Safety-Critical Electronics

Failures of safety-critical electronic systems can result in loss of life, substantial financial damage or can severely harm the environment. Such systems are used for example in medical equipment, in airplanes, in trains, or in nuclear power stations. In applications like these, no margin of error is tolerable. There is no opportunity to „tweak“ improvements on the fly or to allow for unanticipated problems.

Different Safety Requirements in Different Markets

Computer architectures with safety-critical requirements are very complex. Considerations about such systems include safety-critical characteristics, reliability questions, error behavior modes, Safety Integrity Levels (up to SIL 3 or SIL 4) and the major IEC and EN standards, e.g., EN 50129 for railways or DO-254 for avionics (up to DAL-A or DAL-B).

For all its COTS safe computers, MEN offers a certification package that documents the board's suitability up to SIL 4 requirements. The A602 and D602 also meet avionics demands up to DAL-A.

A safety-critical system is affected by safe hardware boards and systems, a safe operating system and application software, even the tools that are used must be safe. And last but not least there is a dedicated development and validation, production and qualification process.

While the architecture concepts for different markets are rather similar, the way of thinking and developing a computer system for a safety-critical application is rather diverse between railways, avionics, medical engineering or car manufacturing – to name just a few.

Tools and Methods to Achieve Safety

The measures to achieve safe hardware include powerful planning tools with version management, the V-Model as one of the most popular development models, safety-management tools like risk management, requirement tracing, obsolescence management, product qualification, HASS and HALT.

Risk analysis methods describe how safety can be evaluated. The tools that can be used to calculate safety range from the well-known MTBF and MTBR values to Lambda, FMEA and BITE identification.

Consequently, a safe system architecture, both in hardware and in software, can have different structures of redundant sub-units, enhanced by diversity, and considering the relation between safety and availability.

Learn more about
safe computers!
www.men.de/000506

ISO 9001:2008
ISO 14001:2005
EN 9100:2009

www.men.de
www.men-france.fr
www.menmicro.com