Network Centric Core Avionics

Sergio Montenegro (sergio.montenegro@dlr.de)
Gunter Schoof (schoof@ihp-microelectronics.com)
Ebrahim Haririan (ebrahim.haririan@dlr.de)

Current space craft data handling systems are primary computer-oriented building computer-centric systems. In this model the central computer has to provide high computing power, large memory, high dependability, fault tolerance management, and too many input/output connections. This makes the central computer development, very difficult.

In our approach we aim to build a network centric system, where the central element is not a computer but a powerful space craft area network (SCAN). The network is built using dependable intelligent switches. These switches will be designed and manufactured as ASICs using the IHP technology.

1 The First step toward dependable computing

Our first step designing dependability for space computers was first used in the (DLR-) BIRD satellite [2]. In this architecture there are two or four redundant control computers, each of the nodes is able to execute all control tasks. One node (the worker) is controlling the satellite while a second node (supervisor) is supervising the correct operation of the worker node. If an anomaly of the worker node is detected by the supervisor node, the supervisor takes over the control of the satellite and becomes the new worker node. The old worker node is enforced to execute a recovery function and if there is no permanent error detected, it becomes the supervisor node.

2 Integrated software and hardware structures

The next step to improve this structure was a software-only step. While the hardware structure stayed the same, the software structure was improved by adding a middleware (for communication). Instead of having many different interfaces, for example among applications or between application and I/O-drivers, there is only one interface for all communications in the system. The middleware provides a message-interface which can be used to interchange data among all entities in the system. Therefore there is no extra I/O- driver interface. I/O-devices are controlled by applications which are called I/O-managers.

Another improvement is the inter-node communication. The functionality of the system is implemented as a network of applications which can be distributed among many computers in the system (Figure 1).

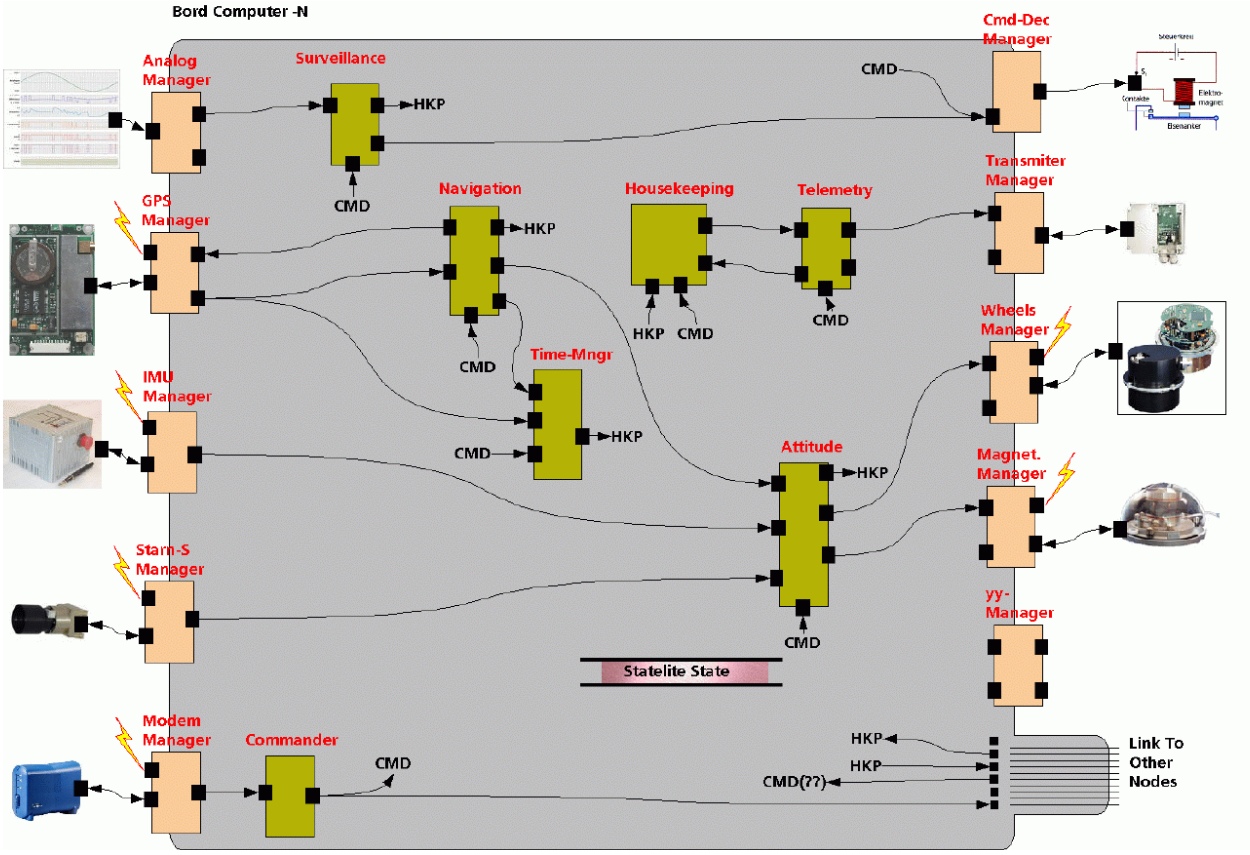

Figure 1: communicating applications

3 The Middleware Switch

3.1 Middleware architecture

The next step is to unify software and hardware in an integrated architecture. Figure 2 shows a typical data/control flow to access I/O-devices.

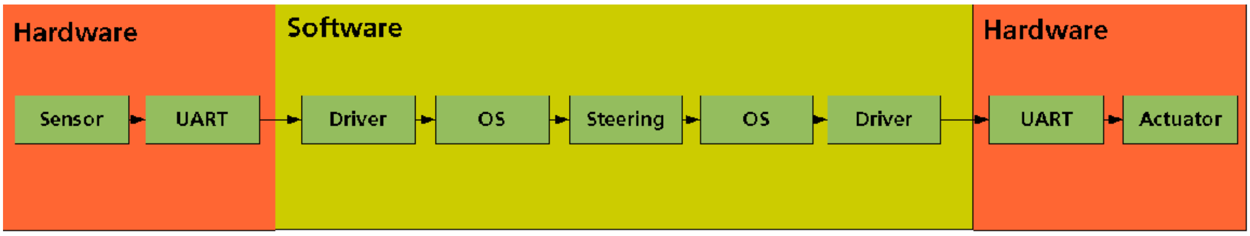

Figure 2: typical data/control flow from devices to applications

The capabilities of the FPGA (programmable hardware) emerging technology allows us to implement middleware functionality directly in the hardware I/O-interface to reach a structure like in figure 3. Our intension is to implement our middleware in form of an Application Specific Integrated Circuit (ASIC).

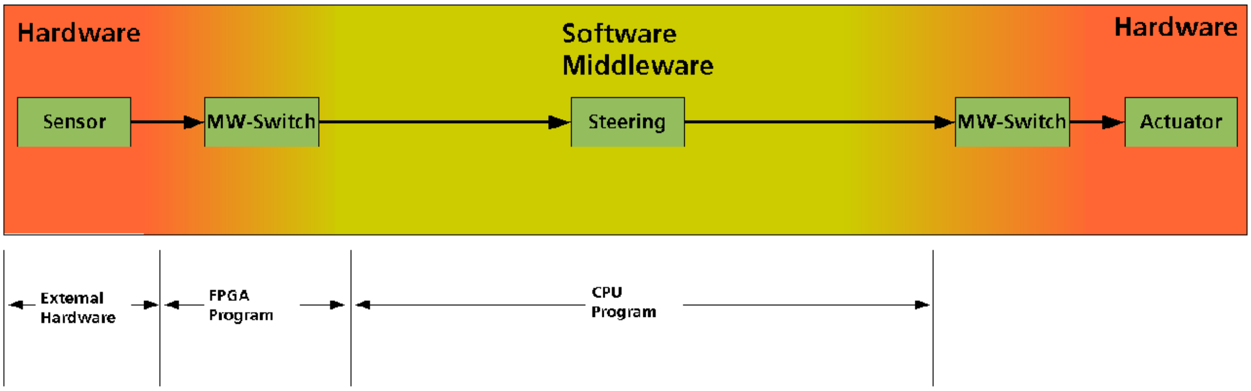

Figure 3: merging software and hardware in the Middleware

The I/O interface (traditionally an UART) will then have on one side the required device interface and on the other side it will be directly integrated to the middleware protocol. The structure from figure 2 can then be extended to the structure in figure 4.

An embedded controller in the middleware switch recognizes communication requests from the I/O ports and connects/disconnects the ports accordingly. For cost-sensitive applications we will also investigate how it could be done to manage I/O links automatically by hardware without need of software controlled embedded processing resources.

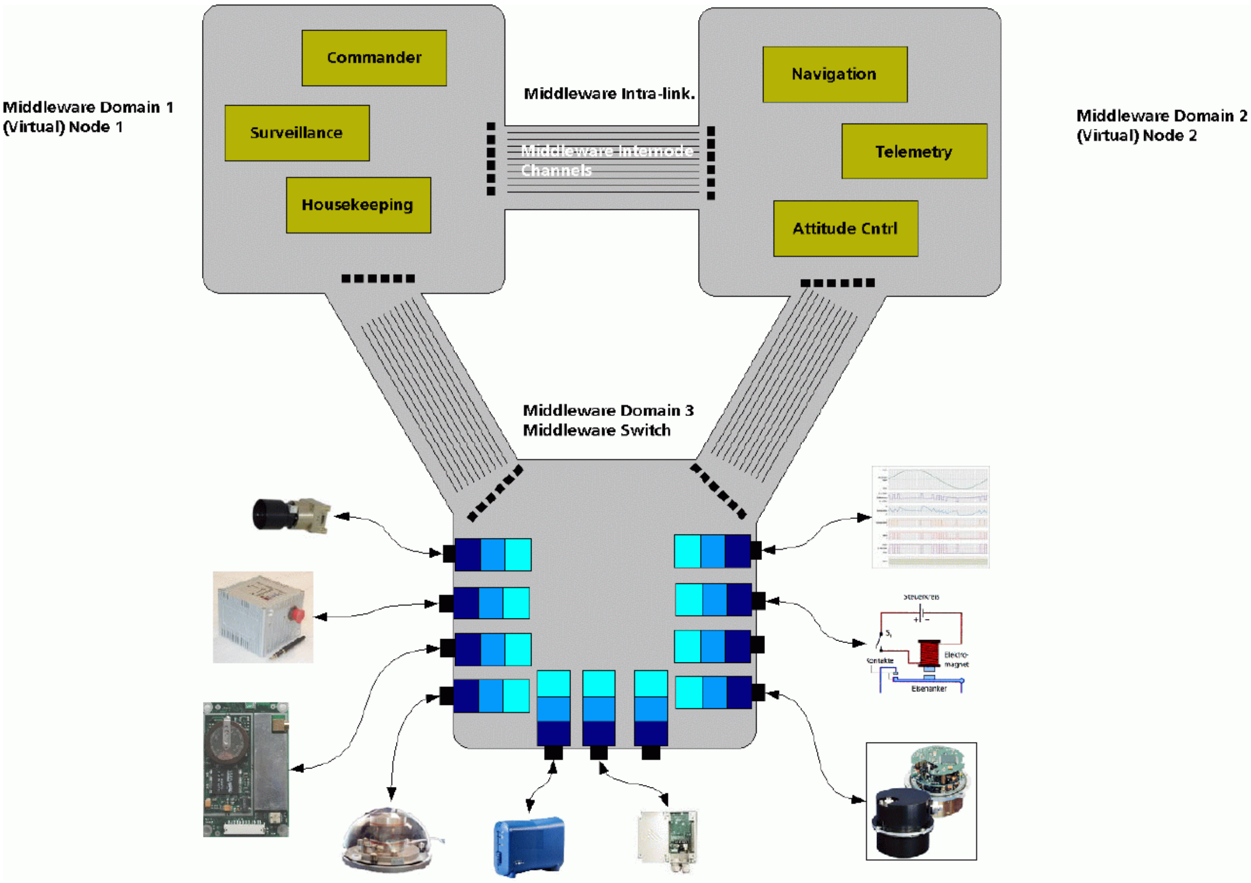

Figure 4: I/O-interfaces integrated in the Middleware

3.2 ASIC design

The middleware switch is planned with many configurable I/O ports. Each port translates (converts) a dedicated I/O protocol to a generic middleware protocol. So any data stream from one port can easily be switched to any other port, supporting unidirectional, bidirectional or multicast connections. The configurability of I/O ports within an ASIC is useful to support many different system architectures with varying types and number of communication interfaces. In general such configuration is made only once for a given system architecture which allows radiation-hard one-time-programmable (OTP) configuration techniques. The ASIC implementation of the middleware switch will be managed using IHP Technology described in section 4.

4 Advanced technology for radiation-hard ASIC designs

4.1 IHP technology

The IHP radiation immune technology SGB25VD is based on 0.25 um BiCMOS structures. Radiation tests were organized e.g. from our industrial partner Kayser-Threde, Germany and made at GSF Eldorado, Munich and RADEF, Finland. Main results of the radiation tests on standard structures in 2007 are as follows:

- No degradation of NPN-bipolar and MOS transistors up to 200 krad detected
- No latch-up detected during all tests
- SEUs on unprotected circuits detected but can be mitigated easily with well-known design techniques (e.g. TMR – triple modular redundancy)
- Result: Radiation tests successfully completed

Several other radiation test chips are prepared and tested. An ESA and DLR funded project aims to develop an integrated wideband frequency synthesizer for HDTV satellite communications and internet-via-satellite services such as DVB-RCS.

4.2 IHP design techniques

Together with Gaisler Research (now Aeroflex Gaisler) a full SEU protected Leon3-ft processor was designed and tested with 100% SEUs corrected. The tests were made at ESTEC using 35 MeV Cf-252 with 1300 particles per second and mm². SEU protection was achieved with TMR-protected flip-flops and BCH-code protected memories and register files.

The next step to increase radiation hardness even more was made with providing a new ASIC design library optimized for high radiation immunity by improved cell layouts.

To meet very high dependability requirements further activities are ongoing to make ASICs both SEU and SEL tolerant by new effective design techniques and simultaneously avoiding huge area penalties. To support such design developments with standard design tools a new automatically design flow is under development.

Radiation protection by design techniques is generally useful if the existing protection by technology and layout means is not sufficient e.g. for high dependable space missions. The improved design will accept local SEU or even SEL effects, correct them and synchronize the affected circuit part automatically. All these activities will happen without affecting the real-time behavior of the overall system [1].

5 System dependability

The middleware switch is a core component of the whole system architecture and therefore must be high dependable and reliable. Big effort is planned and necessary to achieve internal radiation hardness of the ASIC.

Unlike FPGAs, in which the configuration of logic and the data path are stored in SRAM cells, in ASIC technologies, the data path and logic are not susceptible to SEUs. Therefore, we only need to protect flip-flops against upsets. For this purpose, we have applied Triple Module Redundancy (TMR) scheme in our design to combat SEUs [3]. All flip-flops are replicated and voted with majority voters to yield a corrected output in case of any failure. The achieved higher reliability, compensates the extra power consumption and area overhead of TMR. Furthermore, advances in ASIC design and methodologies, reduce amount of redundancy compared to that of FPGAs.

Moreover, it is intended to use additional external redundancy to backup the middleware switch in case of failure.

The big advantage of such strategy is that external components (i.e. sensors, memories, processors, etc.) are not required to be highly dependable. Higher system dependability is easily achieved by adding redundant components to the middleware switch which can replace other defective or occasionally not correctly working components. This replacement can be fully or partly, statically or temporarily dependant on the device status.

In this way it is even possible to negotiate smoothly between higher system performance on one side and higher system dependability on the other side. Also multiple links between switch and components are possible. This can increase both dependability and performance at the same time.

6 References

[1] Fault-Tolerant Design for Applications Exposed to Radiation
G. Schoof, R. Kraemer, U. Jagdhold, C. Wolf
Data Systems in Aerospace (DASIA) 2007, Napoli, May 29 - June 02, 2007, Italy

[2] BIRD-Spacecraft bus controller
Montenegro, S.; Bärwald, W.
Small Satellites for Earth Observation,
Digest of the 3rd International Symposium of the International
Academy of Astronautics, Berlin, April 2-6, 2001

[3] A Comparison of TMR With Alternative Fault-Tolerant Design techniques for FPGAs
IEEE Transactions on Nuclear Science, Vol. 54, No 6, December 2007