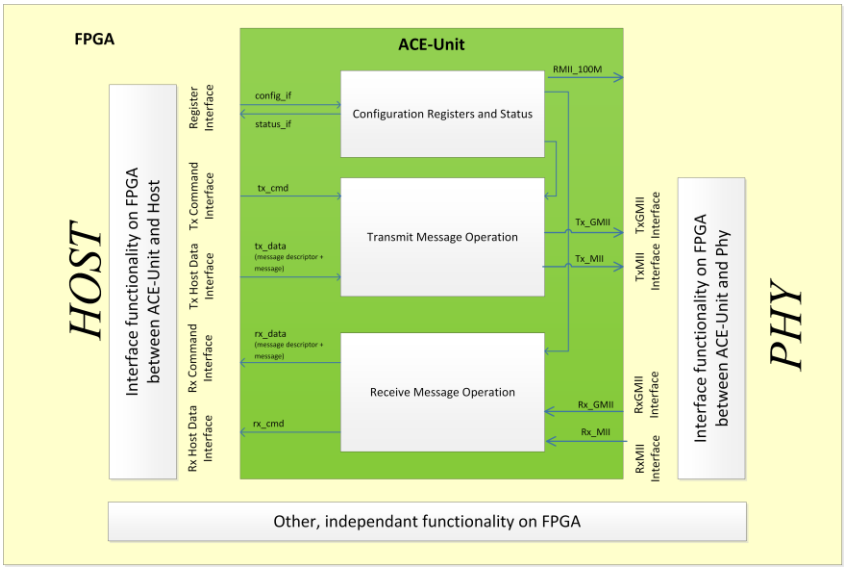
Functional Safety for Avionics in an Ethernet MAC

If electronics must function reliably under all circumstances, then the project must be set up and carried out correctly from the beginning. How to do this was the main topic of the project "ACE Avionics Certifiable Ethernet".

Technically it was about the development of a "Media Access Control" block (MAC) to be used in FPGAs. Although such blocks are available on the Internet for free download, but they do not meet the requirements of functional safety. For this reason, this block should be newly developed according to the special requirements of the industry partner and the process requirements of the aviation authorities.

Partner
Mercury Mission Systems International SA (MMSI) in Lancy (Switzerland) is part of the Mercury Systems company. It develops computer systems for use on the ground and in aircrafts according to the requirements of DO-254, the quality standard for electronic hardware in avionics applications. The Institute of Sensors and Electronics developed the functional block and worked out the general processes for the development according to the requirements of functional safety.

Function
An Ethernet MAC forms the interface between the driver to the data cable ("PHY") and a processor ("Host"). The MAC receives Ethernet packets, analyzes them and passes them on to the host with the extracted header data; conversely, it assembles transmission jobs with header and payload received from the host and sends them to the line in the correct format. To do this, it must also correctly intercept all errors in the interest of functional safety.
Especially in avionics there is another requirement: At flight altitudes of 10 kilometers and more, there is a significantly increased risk of bit errors within the FPGA: Ionizing particles can strike the chip and change the state of a flip-flop, a so-called Single Event Upset (SEU). These SEUs must be detected and handled without interrupting the function if possible. Under no circumstances should the MAC pass on false information as correct.
The function is implemented in a library element called "ACE unit", which can be integrated into a larger FPGA design by the customer.



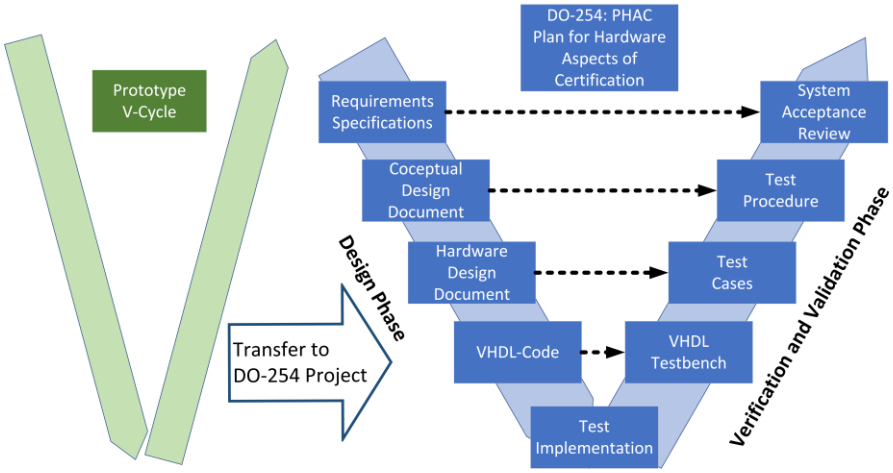
Architecture of the ACE unit as an interface between a host (left) and a PHY (physical interface chip, right) The ACE unit is designed for bidirectional data communication at 1 Gb/s and 100 Mb/s. It must be operated in an FPGA with a system clock frequency of 125 MHz.

Functional safety

Functional safety means that systematic errors are avoided during the development of a system, that random errors are detected during operation, and that in the event of an error the system is always brought to a state defined as safe.

Since there is no such thing as 100% freedom from defects, the required reliability must be defined for each application. For a system such as the ACE unit, which is used in aircrafts where an error can lead to their crash, an error may occur at most once per one billion hours of operation.

This reliability is achieved in two ways: random errors such as the SEUs mentioned above can be prevented by error detection and correction or by redundancy. In the event of a one-bit error, it is automatically corrected. Or, in the case of an uncorrectable multiple error, the system is reset.



V-model for the development of complex and reliable systems: First a prototypical pre-development, then transfer into the project according to DO-254 with the design path from the system specification via the detailed design to the prototype, then on the verification/validation path back to the system level.

The only way to prevent systematic errors is to strictly follow processes and rules during development. This starts with the V model with separate design and verification paths, leads to a pedantic change management and to reviews at all major milestones.

The system specification is translated into both a design and a test specification. With the VHDL testbench, the VHDL design is then tested via black-box tests, thus achieving nearly 100% coverage. For the remaining functions and especially the functions against SEU, simulations on white box level are required. In the case of the ACE unit, these simulations took almost 100 hours for each run. And finally, there are single code blocks as well as the general design rules which can only be checked by a code review.

Results and experiences

After about four years of intensive work, the project result was handed over to MMSI. This period also included two fundamental extensions of the requirements by the client, which had to be handled correctly and cleanly in the process as well as in the design.

The experience gained is now being incorporated into the training of the Bachelor and Master students, especially in the field of microelectronics, and thus helps to ensure that not only the staff of the ISE but also the graduates in the ISE environment are ready for the future of functional safety.

Contact

Prof. Michael Pichler
T +41 56 202 75 26, michael.pichler@fhnw.ch

University of Applied Sciences and Arts Northwestern Switzerland FHNW
School of Engineering
Institute for Sensors and Electronics
Klosterzelgstrasse 2
CH-5210 Windisch
T +41 56 202 80 22
www.fhnw.ch/ise