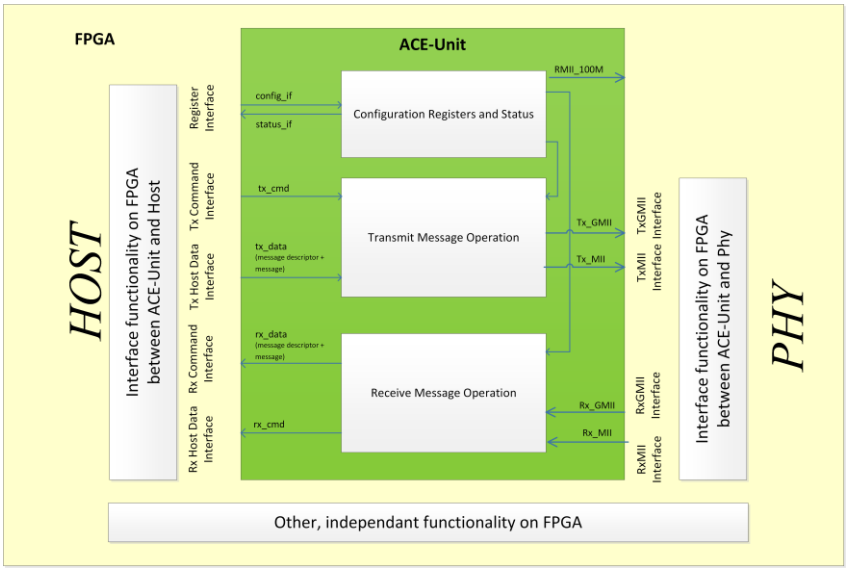
Funktionale Sicherheit für Avionik bei einem Ethernet MAC

Wenn Elektronik unter allen Umständen zuverlässig funktionieren muss, dann muss das Projekt von Anfang richtig aufgesetzt und durchgeführt werden. Wie man das macht, war das Hauptthema beim Projekt "ACE Avionics Certifiable Ethernet".

Technisch ging es um die Entwicklung eines "Media Access Control" Blocks (MAC), der in FPGAs eingesetzt werden soll. Solche Blöcke gibt es im Internet sogar gratis zum Herunterladen, allerdings entsprechen diese nicht den Anforderungen an Funktionale Sicherheit. Aus diesem Grund sollte dieser Block neu entwickelt werden, nach den speziellen Anforderungen des Industriepartners sowie nach den Prozessanforderungen der Luftfahrtbehörden.

Partner
MMSI Mercury Mission Systems International SA in Lancy ist Teil der Firma Mercury Systems. Sie entwickelt Rechner-Systeme für den Einsatz am Boden und im Flugzeug nach den Anforderungen DO-254, der Norm für Qualität bei Elektronik-Hardware für Luftfahrt-Anwendungen. Das Institut für Sensorik und Elektronik entwickelte den Funktionsblock und erarbeitete dabei für das Institut die generellen Prozesse für die Entwicklung nach den Anforderungen der Funktionalen Sicherheit.

Funktion
Ein Ethernet MAC bildet die Schnittstelle zwischen Treiber zum Datenkabel ("PHY") und einem Prozessor ("Host"). Der MAC empfängt Ethernet-Pakete, analysiert sie und gibt sie mit den extrahierten Header-Daten an den Host weiter; umgekehrt setzt er vom Host erhaltene Sendeaufträge aus Header und Payload zusammen und schickt sie im richtigen Format auf die Leitung. Dazu muss er im Sinne der Funktionalen Sicherheit auch alle Fehler korrekt abfangen.
Speziell in der Avionik kommt eine weitere Anforderung dazu: Bei Flughöhen von 10'000 Metern und mehr besteht ein deutlich erhöhtes Risiko von Bitfehlern innerhalb des FPGAs: Ionisierende Partikel können in den Chip einschlagen und ein Flip-Flop kippen, einen sogenannten Single Event Upset (SEU). Diese SEU müssen erkannt und möglichst ohne Unterbrechung der Funktion behandelt werden. In keinem Fall darf der MAC falsche Informationen als korrekt weiterverbreiten.
Die Funktion ist in einem Bibliotheks-Element mit Namen "ACE-Unit" realisiert, das vom Kunden in einen grösseren FPGA-Design eingebunden werden kann.



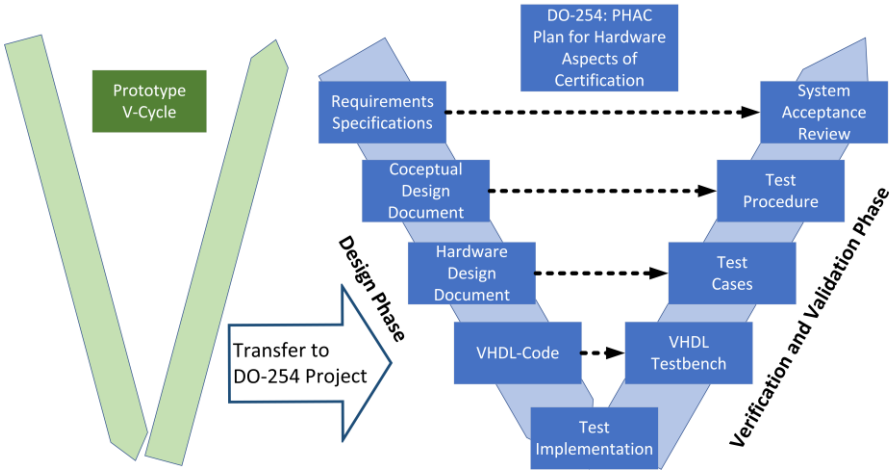
Architektur der ACE-Unit als Schnittstelle zwischen einem Host (links) und einem PHY (Physical Interface-Chip, rechts)
Die ACE-Unit ist für die bidirektionale Datenkommunikation mit 1 Gb/s und 100 Mb/s ausgelegt. Sie muss in einem FPGA mit einer System-Clock-Frequenz von 125 MHz betrieben werden.

Funktionale Sicherheit

Funktionale Sicherheit bedeutet, dass bei der Entwicklung eines Systems systematische Fehler vermieden werden, im laufenden Betrieb zufällige Fehler erkannt werden und das System bei einem Fehler stets in einen als sicher definierten Zustand geführt wird.

Da es keine 100% Fehlerfreiheit gibt, muss je nach Anwendung die verlangte Zuverlässigkeit definiert werden. Bei einem System wie der ACE-Unit, das in Flugzeugen eingesetzt wird, wo ein Fehler zum deren Absturz führen kann, darf ein Fehler nur höchstens einmal pro eine Milliarde Betriebsstunden auftreten.

Diese Zuverlässigkeit wird auf zwei Wegen erreicht: Gegen zufällige Fehler wie z.B. die oben erwähnten SEU hilft Fehlererkennung und -behebung oder Redundanz. Im Fehlerfall wird ein Ein-Bit-Fehler selbständig korrigiert oder bei einem unkorrigierbaren Mehrfach-Fehler das System resettet.



V-Modell für die Entwicklung komplexer und zuverlässiger Systeme:
Zuerst eine Prototypische Vorentwicklung, dann Transfer ins Projekt nach DO-254 mit dem Design-Pfad von der System-Spezifikation über den Detaildesign bis zum Prototypen, dann auf dem Verifikations-/Validationspfad wieder zurück bis zur Systemebene.

Gegen systematische Fehler hilft nur die strikte und aufwändige Befolgung von Prozessen und Regeln bei der Entwicklung. Das beginnt beim V-Modell mit personell getrennten Design- und Verifikations-Pfaden, führt über ein pedantisch geführtes Änderungsmanagement bis zu Reviews bei allen wesentlichen Meilensteinen.

Die System-Spezifikation wird in eine Design- und eine Testspezifikation übersetzt. Mit der VHDL-Testbench wird dann der VHDL-Design über Black-Box-Tests geprüft, damit soll eine fast 100% Abdeckung erreicht werden. Für die übriggebliebenen Funktionen und besonders die Funktionen gegen SEU sind Simulationen auf White-Box-Ebene nötig. Diese Simulationen dauerten im Fall der ACE-Unit für jeden Run nahezu 100 Stunden. Und schliesslich gibt es die generellen Design-Regeln sowie einzelne Code-Blöcke, die nur über eine Code-Review überprüft werden können.

Ergebnis und Erfahrungen

Nach gut vier Jahren intensiver Arbeit konnte das Projektergebnis an MMSI übergeben werden. In dieser Zeit enthalten waren auch zwei grundlegende Erweiterungen der Anforderungen durch den Auftraggeber, die im Prozess sowie auch im Design korrekt und sauber abgewickelt werden mussten. Die Erfahrungen fliessen nun in die Ausbildung der Bachelor- und Master-Studierenden v.a. im Bereich Mikroelektronik ein und helfen damit, dass nicht nur das ISE sondern auch die Absolventinnen und Absolventen im Umfeld des ISE bereit für die Zukunft der funktionalen Sicherheit sind.

Kontakt

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

Fachhochschule Nordwestschweiz FHNW
Hochschule für Technik
Institut für Sensorik und Elektronik
Klosterzelgstrasse 2
CH-5210 Windisch
T +41 56 202 80 22
www.fhnw.ch/ise