Erfolgsfaktoren bei der Entwicklung der OBCE-WW

Dr. Thomas Buchberger

SIS PSE CVD CCC 3
Siemens AG Österreich
Erdbergerlände 26
A-1030 Wien
thomas.buchberger@siemens.com

Abstract: "GSM on Board" ist eine Lösung, welche die Benutzung von Handys in Flugzeugen ermöglicht. Die Erfahrungen, die wir bei der Entwicklung einer Teilkomponente - der OBCE-WW - gemacht haben, sind jedoch nicht spezifisch für den Bereich Aerospace (DO-178B), sondern typisch für alle Entwicklungen sicherheitskritischer Systeme.

1 Einführung

SIS PSE CVD CCC 3 ist eine Siemens Organisationseinheit, welche ihre Tätigkeit auf die Entwicklung von "Safety Devices" in den Bereichen Aerospace, Automotive und Transport konzentriert.

Unser wichtigstes Projekt in den vergangenen 2 Jahren war bzw. ist die Entwicklung einer Kontrolleinheit für die Generierung und Überwachung von HF-Signalen im System "GSM on Board", welches die Benutzung von Handys in Flugzeugen ermöglicht. Dieses aus Hardware und Software bestehende Gerät (OBCE-WW) wird im Auftrag von Airbus Deutschland für weltweiten Einsatz entwickelt. Die geltende internationale Richtlinie für Software-Entwicklung im Bereich Avionics ist der RTCA Standard DO-178B, der dem Produkt zugeordnete Software Level ist "C" bzw. "D".

Rückblickend haben folgende Konzepte beziehungsweise Tätigkeiten entscheidend zum Erfolg des Projektes beigetragen:

1. Tool-unterstütztes Requirements-Management
2. HW und SW Partitioning als Grundlage des Designs
3. Eigenentwicklung eines einfachen Tools für die Ermittlung der Statement Coverage
4. Testkonzept, Testautomatisierung

Auf diese 4 ausgewählten Schwerpunkte wird im Folgenden eingegangen.

2 Requirements-Management

System Requirements wurden vertikal in Teilbereiche aufgebrochen (HW, Level „C“ SW, Level „D“ SW, Prozess), in horizontalen Hierarchien verfeinert (High-Level bzw. Low-Level Requirements) und bis zu Test-Spezifikation und Test-Ergebnissen bidirektional verlinkt. Als Tool wurde Telelogic DOORS verwendet. Folgende Vorteile wurden von uns sehr geschätzt:

- Hersteller und Kunde „sehen“ dieselbe Version
- Einheitlicher Aufbau und einheitliches Format fördern Übersichtlichkeit und gemeinsames Verständnis
- Unterstützung des Requirement Linking und Tracing (Traceability Matrix, uncovered Requirements, suspect links)

3 Partitioning

Der Kundenwunsch nach einem hochsicheren Betriebs-Mode (Level „C“) und einem etwas weniger kritischem Maintenance-Mode (Level „D“) wurde mit HW und SW Partitioning implementiert

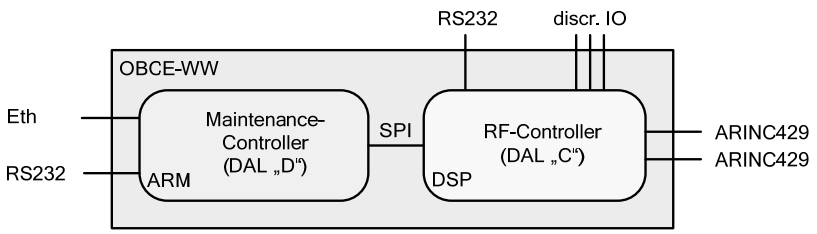

Abbildung 1: HW Partitioning (2 Prozessor Lösung)

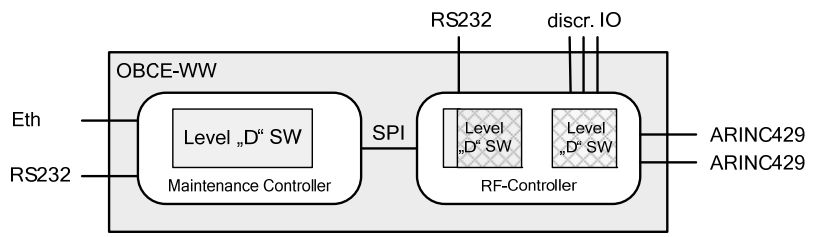

Abbildung 2: SW Partitioning

Im RF-Controller wird je nach Betriebsmode eine unterschiedliche Load verwendet. Die Maintenance-Load benutzt die Module der Betriebs-Load und stellt zusätzliche Funktionalität zu Verfügung.

4 Nachweis der Statement Coverage im Test

Der Einsatz kommerzieller Tools zur Ermittlung der Statement Coverage ist in kleinen Projekten nicht immer möglich, da die in sicherheitskritischen Umfeldern verwendeten Tools qualifiziert werden müssen bzw. auf speziellen Targets auch nicht sofort einsetzbar sind. Beides kann enorme Kosten und Aufwand verursachen.

Für das Projekt OBCE-WW wurde ein einfaches und „billiges“ Umfeld zur Ermittlung der Statement Coverage geschaffen. Instrumentierung des Source Codes und Visualisierung der Coverage erfolgen tool-unterstützt, der Einfluss auf das Laufzeitverhalten ist akzeptabel (<50%) und der Speicherbedarf minimal. Für die SW wurde eine Statement Coverage >99% erreicht.

5 Testkonzept, Testautomatisierung

Die Anforderung an die Verifikation, mittels eines weitgehend automatisch ablaufenden Test Frames ein abgeschlossenes embedded System als „Black-Box“ zu testen und dabei eine Statement Coverage von 100% zu erreichen scheint widersprüchlich, zumal aus den erwähnten Gründen kommerzielle Tools weitgehend ausscheiden, vollständige Transparenz gefordert wird und ein nur zum Testen verwendeter Code als „dead code“ gilt und somit nicht zulässig ist.

Als praktikable Methode die Testziele zu erreichen hat sich eine Auftrennung in einen Grey-Box und einen Black-Box Teil erwiesen. Im Grey-Box Test wird eine Test-Applikation zur Target SW dazugebunden, die einerseits das Interface erweitert und andererseits Zugang zu internen Daten und Funktionen ermöglicht.

Bei der OBCE-WW erfüllt der Maintenance-Mode exakt die Anforderungen an diese Test-Applikation, er kann also beinahe unverändert dazu herangezogen werden. Damit und mit der laufend erweiterten Automation konnte der Systemtest unseres durchaus komplexen Targets soweit verbessert werden, dass jetzt mehr als 80% der Testfälle automatisch ablaufen, wobei 90% aller SW Requirements abgedeckt und 85% aller Source Code Statements durchlaufen werden.

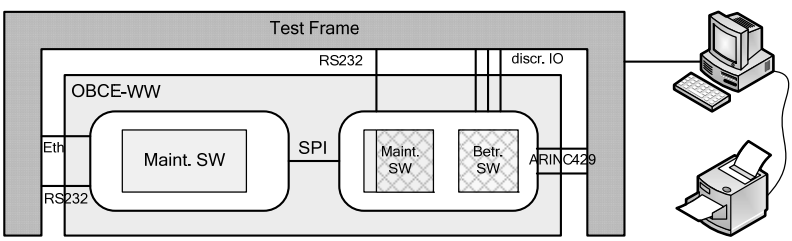

Abbildung 3: Test Setup