Implementierung der Systemkonfiguration und Systemsteuerung gemäß ASAAC

Extended Abstract

Michael Förster
EADS München
michael.foerster@m.eads.net

Einführung

Basierend auf dem Prinzip der Integrierten Modularen Avionik (IMA) ist im vergangen Jahr die tri-nationale Technologiestudie „ASAAC“ (Allied Standard Avionics Architecture Council) nach sechsjähriger Laufzeit erfolgreich abgeschlossen worden. Sie wurde von den Verteidigungsministerien der Länder Frankreich, Großbritannien und Deutschland beauftragt.

Im Verlauf der Studie wurden Vorschläge für Standards und Architekturrichtlinien für die folgenden Themen erarbeitet, die auf realen Systemen implementiert und getestet wurden:

- Standards für Software Interfaces:
  - Application Interface: APOS (Application to Operating System)
  - Standards für die Verwaltung der Hardware im Betriebssystem: MOS (Module to Operating System)
  - Interface System Managements zur Systemkonfiguration: SMBP (System Management to Blueprints)
  - Interface des System Managements zum Betriebssystem: SMOS (System Management to Operating System)
- Standards für den Aufbau von Prozessorplatinen (Common Functional Modules (CFM))
- Standards für den Aufbau von Netzwerken
- Standards für des Packaging von CFM
- Richtlinien für die Architektur von IMA Systemen betreffend:
  - System Management
  - Fault Management
  - Initialisieren und Abschalten von Modulen und Systemen
  - den Aufbau und das Verändern von Konfigurationen
  - die Verteilung der Zeit in ASAAC Systemen
  - Security und Safety

Nach Beendigung des Programms stand der EADS als produktfähige Software die Module zur Prozessor lokalen (Resource Element (RE)) Kommunikation zur Verfügung, die mittlerweile in verschiedenen Systemen eingesetzt sind. Die Entwicklung restlichen Elemente der Systemsteuerung, Stichwort Generic System Management (GSM), ist Thema dieses Vortrags.

Architektur des System Managements nach ASAAC

Die Architektur des System Managements ist hierarchisch in drei unterschiedlichen Level Arten: RE, IA (Integration Area) und AC (Aircraft) mit je vier unterschiedlichen Aufgaben:

- Configuration Management (CM)
- Health Monitoring (HM)
- Fault Management (FM)
- Security Management (SM)

Die Basis bildet der RE GSM

Er ist auf jedem RE genau einmal verfügbar und ist verantwortlich für die lokale Konfiguration:

Er initiiert, startet und kontrolliert die lokalen Applikationen, darunter auch die GSM der höheren Level, die auf dem RE gemäß den Blueprints verfügbar sind, und die lokalen Anteile der Kommunikation.

Er überwacht die Funktionsfähigkeit des RE. Zum Konfigurieren bedient er sich der Blueprints, die er über das SMBP Interface einliest.

Die auszuführenden Aufgaben kommandiert er über das SMOS Interface. Beim Auftreten von Fehlern entscheidet er gemäß der Aktionslisten aus den Blueprints, ob er lokal auf dem RE den Fehler beheben kann oder auf Anweisungen der nächst höheren Instanz warten muss. Die nächst höhere Instanz ist der GSM des nächsten IA Level oder, wenn kein IA Level existiert, der AC GSM.

Der IA GSM bindet eine Anzahl von RE zu einer Verwaltungseinheit zusammen.

Bei größeren Systemen kann es mehrere IA GSM geben. die dann wiederum durch ein oder mehrere IA GSM kontrolliert werden. Innerhalb des IA Bereiches kann es mehrere Level geben. Er kann bei kleinen Systemen aber auch vollständig fehlen.

Die höchste Instanz ist der AC GSM.

Im Gegensatz zu der vorhergehenden kann er redundant vorhanden sein, im Allgemeinen abhängig von der Größe des Systems.

Die GSM der IA Level und des AC Levels bedienen sich zu ihrer Konfiguration ebenfalls der Blueprints, benötigen aber, im Gegensatz zum RE GSM, keinen Zugang zu den System Resourcen, nutzen also nicht das SMOS Interface.

Design der Elemente

Dem Design liegen die folgenden Requirements zugrunde:

- Implementation gemäß ASAAC Richtlinien unter Ausschluss des SM
- Flexibilität und Wartbarkeit
- Reuse von existierenden Komponenten aus anderen Programmen für HM, FM und CM
- Verfügbarkeit für verschiedene Betriebssysteme
  - für Application Development
  - und Application Runtime

Auf Grund dessen wurden folgende Designentscheidungen getroffen:

- Das Design wird objektorientiert für ADA mittels UML erstellt (Flexibilität und Wartbarkeit).
- Die Implementierung des SMOS Interfaces wird in eigene Prozesse ausgelagert, die mit dem Aufrufer über Betriebssystem inhärente Möglichkeiten kommunizieren, um die Betriebssystem spezifischen Anteile vom GSM fernzuhalten (Verfügbarkeit für verschiedene Betriebssysteme).
- Die Implementierung des SMBP Interfaces wird in eigene Prozesse ausgelagert, die mit dem Aufrufer über Betriebssystem inhärente Möglichkeiten kommunizieren, um flexibel Blueprinterweiterungen einbauen zu können (Verfügbarkeit für verschiedene Betriebssysteme).
- Die Aufgaben des GSM werden in drei unabhängigen Prozessen im Unix Sinne (eigener Datenraum) implementiert: HM, FM, CM. Betriebssysteme, die abgegrenzte Datenräume nicht unterstützen, werden z.Z. nicht berücksichtigt (Flexibilität und Wartbarkeit, Reuse).
- Die GSM der unterschiedlichen Level unterhalten sich über ASAAC konforme Kommunikation (Virtual Channel (VC)). Dieses Prinzip wurde auch auf die Kommunikation der Komponenten des gleichen Levels angewandt (Implementation gemäß ASAAC).
- Zur Reduktion der lokalen Kommunikation über VC - jede Message benötigt eigentlich einen eigenen VC - und zum Anbindung von fremden ASAAC konformen GSM wird die RE lokale Kommunikation über einen "Broker" gelenkt, der, entsprechend seiner Konfiguration durch Blueprints, die Verteilung der Nachrichten an die entsprechenden RE lokalen oder externen Komponenten übernimmt (Reuse, Flexibilität und Wartbarkeit, Implementation gemäß ASAAC).
- Die einzelnen GSM Komponenten HM, FM und CM erhalten ein Paket, das mit dem Broker kommuniziert (Reuse, Flexibilität und Wartbarkeit, Implementation gemäß ASAAC).
- Um bestehende Komponenten einzubauen, erhalten HM, FM und CM keinen direkten Zugang zu den ASAAC Interfaces. Der Zugang wird über einen Konverter abgewickelt, der entweder prozedural - bei dieser Implementierung - oder optional über Betriebssystem spezifische Inter Prozess Kommunikation aufgerufen wird, entsprechend der Implementierung des SMOS/SMBP (Flexibilität und Wartbarkeit, Reuse, Verfügbarkeit für verschiedene Betriebssysteme).

Zuverlässigkeit des Systems

Die Zuverlässigkeit beruht auf zwei Komponenten:

- Die Korrektheit der der Konfiguration zu Grunde liegenden Blueprints. Die Erzeugung und die Qualifizierung werden unabhängig vom GSM durchgeführt und wird hier als gegeben vorausgesetzt.
- Die Qualität des GSM
  - Durch die Designentscheidungen ist der GSM hochgradig modular in Einzelkomponenten aufgebaut.
  - Die Verwendung von UML und einer fast vollständigen Codeerzeugung aus den UML Diagrammen vermeidet den Bruch zwischen Design und ADA Sourcecode.
  - Durch schrittweises Implementieren und Testen wird die Korrektheit der Module nachgewiesen.
  - Beschränkung im Design auf möglichst statische Objektgenerierung vermeidet unkontrollierten Speicherbedarf.
  - Vermeidung von blockierenden Synchronisationspunkten in ADA erlaubt eine einfache Laufzeitanalyse.

Eine formale Qualifizierung wird im Rahmen dieses Projektes nicht durchgeführt. Sie ist wie die Implementierung des SM Aufgabe von Folgeprojekten.