Einsatz von Simulationen bei der Softwareentwicklung in Raumfahrtprojekten

Olaf Maibaum
Deutsches Zentrum für Luft- und Raumfahrt e.V.,
OE “Simulations- und Softwaretechnik”, Braunschweig

E-Mail: Olaf.Maibaum@dlr.de

1 Einleitung

An Systeme in der Raumfahrt werden hohe Anforderung hinsichtlich der funktionalen Korrektheit und der Einhaltung von Sicherheitsrichtlinien gestellt. Um diese Anforderungen zu gewährleisten ist der Entwicklungsprozess durch die ECSS-Norm vorgeschrieben, der alle europäischen Unternehmen und Institution in der Raumfahrt verpflichtet sind. Dieser Entwicklungsprozess und der Software Lebenszyklus ist im Abschnitt 2 beschrieben.

In allen Phasen des Entwicklungsprozesses nach ECSS-Norm kommen Simulationen zum Einsatz. Einen kurzer Überblick über den Einsatzzweck und die verwendeten Simulationspackete gibt Abschnitt 3.

Im Abschnitt 4 wird abschließend ein kurzer Überblick über die künftigen Aktivitäten im Bereich des Simulationseinsatzes in der Raumfahrt gegeben. Dies ist zum einen die Schaffung des „virtual Spacecraft“ zur durchgängigen Nutzung von Simulationsmodellen über den gesamten Entwicklungsprozess hinweg, zum Anderen die Nutzung neuester Softwaretechnologien zur Verbesserung der Kopplung und Wiederverwendbarkeit von Simulationmodellen.

2 Entwicklungsprozess nach ECSS-Norm

2.1 Allgemeiner Entwicklungsprozess

Der Aufbau von Raumfahtprojekten unterliegt dem durch die ECSS-Norm festgeschriebenen Phasen [1]. Dies sind im einzelnen

Phase 0: Missionsanalyse/Ermittlung von Erfordernissen (Mission Analysis/Needs Identification)

Es wird der Bedarf und die Anforderungen an eine Mission analysiert. Die Ergebnisse dieser Phase sind

- Merkmale und Beschreibung einer beabsichtigten Mission.
- Aussagen über die Ziele hinsichtlich Bedarf, der erwarteten Funktionalität, die Verfügbarkeit und die Gefahren.
- Beurteilung der operativen Randbedingungen, insbesondere die physikalische und die betriebliche Umgebung
- Identifikation eines möglichen Systemkonzepts mit dem Schwerpunkt auf den Innovationsgrad und der Kritikalität. Feedback von laufenden Programmen sollte hierin einbezogen werden.
- Vorläufige Beurteilung der Projektmanagementdaten (Organisation, Kosten, Zeitpläne)

Phase A: Machbarkeit (Feasibility)

Die Machbarkeitsphase dient der abschließenden Formulierung der in Phase 0 gefundenen Erfordernisse und der Formulierung von Lösungen zum Erreichen der wahrgenommenen Bedürfnisse.

- Quantifizieren und benennen der kritischen Elemente (technisch und ökonomisch)
- Aufstellen des Funktionsbaums
- Erarbeitung von einigen unterschiedlichen Systemkonzepten, um die Möglichkeiten, Eigenschaften und Kritikalität von bestimmten Elementen zu modellieren.
- Vergleich dieser Konzepte mit den Bedürfnissen um den Unsicherheits- und Risikograd zu bestimmen
- Feststellen der technischen und ökonomischen Machbarkeit
- Identifikation von Einschränkungen für jedes Konzept in Hinblick auf Kosten, Ablauf, Organisation, Nutzung (Betrieb, Implementation und Instandhaltung), Herstellung und Bereitstellung sowohl als auch den geschätzten Spielraum zur Erreichung der Ziele.

Phase B: Vorbereitende Definition (Projekt und Produkt) (Preliminary Definition)

Diese Phase beinhaltet die Projektvorbereitung. Dies umfasst

- Auswahl der technischen Lösung für das in Phase A ausgewählte Systemkonzept
- Erarbeiten einer genauen und präzisen Definition (Leistungen, Kosten, Ablauf) für jede Ebene und die Vorbereitung von Entscheidungsvorlagen für das Vorgehen in den folgenden Projektphasen durch die Festlegung von Vereinbarungen über die technische Durchführung des Projekts.
- Durchführung eines Review der Systemanforderungen auf System Level
- Auswahl von „*Make or Buy*"-Alternativen nach der Durchführung des Systemanforderungs-Review während die Auftraggeber die Arbeitspacketaufteilung aufstellen und die Produktspezifikation niederschreiben.
- Bestätigung der Machbarkeit der vorgeschlagenen Vorgehensweise als auch die Festlegung der operativen Auflagen (technisch und ökonomisch)

Phase C: Detailierte Beschreibung (Produkt) (Detailed Definition)

Diese Phase

- erlaubt eine ausführliche Studie über die ausgewählte technische Lösung in der vorherigen Projektphase als auch das Erstellen von maßgeblichen Elementen der Lösung, was zu einer detailierten Beschreibung des Systems und seiner Komponenten führt.
- erlaubt eine endgültige „Make or Buy"-Entscheidung für Produkte, sofern notwendig.
- Bewilligt die Bestätigung des Aufbaus, der Test- und Qualifikationsauflagen und initiiert die Methoden und Mittel für die Herstellung und Überprüfung.
- Start von Technologieeinschätzungen oder der Qualifikation (oder Fortsetzung dieser Tätigkeiten sofern sie bereits in Phase B begonnen wurden) sowie den Beginn von Beschaffungsmaßnahmen.
- ermöglicht die Aktualisierung des Production Master Plan für die standardmäßige Erstellung der ersten Systemmodelle.

- führt die Schnittstellen innerhalb des Entwicklungsprozesses ein und stellt die entsprechenden Schnittstellendokumente unter ein Konfigurationsmanagement.
- beinhaltet die Vorbereitung von „Phase E"-Aktivitäten.

Die Phase wird mit einem Critical Design Review abgeschlossen.

Phase D: Herstellung/Boden-Qualifikations Test (Production/Ground Qualification Testing)

Die Phase D stellt das Ende der Systementwicklung dar.

Der Production Master Plan und die Nutzerhandbücher werden in dieser Phase freigegeben.

Die Phase

- genehmigt eine geeignete Ausarbeitung der Produkte, Komponenten und des Systems an sich durch den Abschluß der Bodenqualifizierung und im einzelnen durch die Bereitstellung von experimentellen Ergebnissen zur Ergänzung der theoretischen Ergebnisse, welche in dieser und den vorhergehenden Phasen gewonnen wurden.
- beinhaltet die Erarbeitung von Materialen, Software und anderer Komponenten um die experimentellen Ergebnisse zu erhalten (Qualifikationsmuster und verbundende Mittel)
- erlaubt die Bestätigung und Qualifizierung von Methoden, Prozeduren und die Herstellungs- und Verifikationsmethoden zur Fertigung, Montage, Integration und Überprüfung und die Durchführung von Qualitätssicherungsmaßnahmen.

Die Phase endet mit einer Abnahme-Review aller oben beschriebenen Maßnahmen.

Die Phasen C und D lassen sich im allgemeinen durch die verwobene Natur der einzelnen Aktivitäten nicht voneinander trennen.

Phase E: Nutzung (Utilisation)

Diese Phase beinhaltet die Startvorbereitungen, den Start und die Flugakzeptanz von Raumsegementen als auch den eigentlichen Betrieb und die Wartung des System. Die Phase teilt sich in zwei Phasen auf.

Die erste von beiden ist die Inbetriebsnahme-Phase des Systems, welche durch ein Review abgeschlossen wird. Sie beinhaltet alle Aktivitäten zum Start, der „In-Flight"-Qualifikation und dem Akzeptanz-Test des Systems. Sie erlaubt die Bewertung und Messung der Leistungenstufen als auch dem Grad der bereitgestellten Dienste.

Die zweite Phase ist die eigentliche Nutzung des Systems.

Phase F: Ausserbetriebnahme (Disposal)

Die abschließende Phase ist die Ausserbetriebnahme, welche alle Maßnahmen umfasst um das System zu entsorgen, wie beispielsweise das kontrollierte Verglühen eines Raumfahrzeugs in der Erdatmosphäre.

Die kompletten Projektergebnisse werden abschließend betrachtet um ihre Eignung für zukünftige Projekte zu untersuchen.

2.2 Software-Lebenszyklus

Der Software-Lebenszyklus innerhalb von Projekten in der europäischen Raumfahrt besteht aus mehreren Phasen, welche sich nicht komplett mit den Phasen eines Raumfahrtprojektes decken. Der Software-Lebenszyklus besteht aus

- Software-Anforderungs-Definition
- Software-Design-Definition
- Verifikation und Validierung
- Softwarebetrieb
- Softwarewartung

Die Software-Anforderungs-Definition besteht aus der Anforderungsanalyse, dem Architekturdesign und der Aufstellung des Plans für die Verifikation und Validierung der Software. Diese Phase im Softwarelebenszyklus ist Teil der Phase B eines Raumfahrtprojekts.

Der nächste Punkt beinhaltet das Design der einzelnen Softwarekomponenten, deren Codierung und Test, als auch die Integration der Softwarekomponenten in das Gesamtsystem. Die Software-Design-Definition ist den Phasen C und D eines Raumfahrtprojekts zugeordnet.

Die Verifikation und Validierung im Software-Lebenszyklus schließt sich eigentlich dem Softwaredesign an. Es wird aber empfohlen mit der Verifikation bereits mit der Software-Anforderungs-Definition zu beginnen und die Validierung auch nach dem Vorliegen erster Softwarekomponenten zu beginnen, um frühzeitig mögliche Fehler in der Software aufzudecken um die Kosten für die Behehebung eines Fehlers möglich gering zu halten.

Der Softwarebetrieb im Software-Lebenszyklus deckt sich nicht mit der Phase E, da bereits in Phase D für die Durchführung der Boden-Qualifikations-Test und der Implementierung von Bedienprozessen die Softwareentwicklung abgeschlossen sein muß.

Die letzte Punkt im Software-Lebenszyklus, die Softwarewartung, beinhaltet die Analyse und Überprüfung von auftretenden Problemen mit der Software in den Phasen D und E von europäischen Raumfahrtprojekten. Falls Änderungen oder Verbesserung der Software im Betrieb notwendig werden, so sind diese Tätigkeiten der Softwarewartung zuzuordnen.

3 Simulationen im Entwicklungsprozess

3.1 Einsatzgebiete in den Phasen

Die einzelnen Phasen des Entwicklungsprozesses für die Raumfahrt werden durch den Einsatz von Simulationstechnik unterstützt. Die hierbei verwendeten Simulationspakete lassen sich dabei den unterschiedlichen technischen Disziplinen zuordnen, welche für die Durchführung eines Raumfahrtprojektes notwendig sind. In der folgenden Tabelle sind einige technische Disziplinen aufgeführt wie sie bei der ESA/ESTEC typischerweise verwendet werden.

System	Stromversorgung
Instrumente	Kommando- und Datenhandling
Missionsanalyse	Kommunikationssystem
Antriebstechnik	Bodensysteme und Betrieb
Lage- und Orbitsteuerung	Simulation
Struktur/Konfiguration	Kostenanalyse
Mechanik/Pyrotechnik	Risikoabschätzung
Thermalsystem	Programmatik

Um die Zusammenarbeit zwischen den einzelnen technischen Disziplinen zu fördern, kommen speziell ausgestattete Räumlichkeiten zum Einsatz, wie z.B. das bei der ESA/ESTEC eingerichtete Concurrent Design Falicity (CDF) [3]. Das CDF ist ausgestattet mit mehreren Projektionsflächen, einem Videokonferenzsystem und einen Rechnerarbeitsplatz für jeden Spezialisten einer technischen Disziplin. Die Projektionsflächen sind von jedem Rechnerarbeitsplatz aus einzusehen. Ausgestattet sind die Rechnerarbeitsplätze mit den Standardanwendungen und die für die jeweilige technische Disziplin nötigen Anwendungen und Simulationen.

In den Phasen 0/A werden bei ESA/ESTEC Spezialisten aus den benötigten Fachdisziplinen in das CDF eingeladen um mögliche Szenarien für ein geplantes Raumfahrtprojekt und den Ablauf der Mission in groben Zügen durch Planspiele erarbeiten und die Machbarkeit der Mission einzuschätzen. In den Planspielen werden gedachte Missionsszenarien anhand von Simulationen für die einzelnen technischen Fachgebiete durchgespielt und die Ergebnisse untereinander ausgetauscht und diskutiert. Bei auftretenden Schwierigkeiten oder abzusehenden hohen Risiken werden die Missionsszenarien modifiziert und der simulationsgestützte Planungsprozeß iterativ fortgesetzt bis ein Missionszenario gefunden wurde, welches die gewünschten Zielen des Raumfahrtprojekts erreicht [4].

Bei EADS Astrium kommt für diesen Planungsprozeß eine ähnliche Einrichtung zum Einsatz, welche als Satellite Design Office bezeichnet wird [5].

In den Phasen B/C werden Simulationen für die Spezifikation und Verifikation der operationalen und funktionalen Anforderung eingesetzt. So sind für die Regelungssysteme Grenzwerte hinsichtlich der Regelgenauigkeit und Nebenbedingungen zu formulieren. Beispielsweise darf die Lageregelung bei der Verwendung von Sternenkameras zur Lagebestimmung vorgegebene Beschleunigungswerte nicht übersteigen, oder für bestimmte Betriebsmodi des Satelliten müssen die Radiatoren zur Einhaltung der thermischen Faktoren in den freien Raum gerichtet werden. Diese Grenzwerte und Nebenbedingungen müssen durch Simulation der einzelnen Betriebsmodi gefunden und überprüft werden. Ebenso werden die in Phase C entwickelten Regelalgorithmen mit Hilfe von Simulation dahingegen überprüft, daß sie in ihrem Ablauf zur Erreichung des Regelungsziels geeignet sind.

In der Phase D werden Simulationen zur Validierung und Verifikation der entwickelten Software eingesetzt. Im Modultest werden die Ausgaben der Module gegen Daten getestet, welche mit den in Phase C entwickelten Algorithmensimulationen erzeugt

wurden. Die Qualifizierung einer Software im Integrationstest wird durch Software- und/oder Hardware-in-the-Loop-Tests (HiLT) durchgeführt. Der Software-in-the-Loop-Test kann für nicht zeitkritische Abläufe verwendet werden, in dem die zu testende Software mit einer Umweltsimulation verlinkt wird.

Zeitkritische und hardwareabhängige Tests werden mit Hilfe von HiLT durchgeführt. Dabei sind zwei Arten von HiLT zu unterscheiden. Mit simulierten Sensoren und Aktuatoren oder mit einem Labormuster zur Überprüfung einer bestimmten Funktionalität. So kommen beispielsweise für die Qualifizierung von Lageregelungsalgorithmen Luftlagertische zum Einsatz, welche im Versuchsaufbau die für die Lageregelung wichtigsten Sensoren und Aktuatoren in der korrekten Einbaulage enthalten.

Für die Phase E/F werden Simulatoren für das Verhalten des Raumfahrzeugs benötigt, um die Bedienmannschaften für den regulären Betrieb und Notfallbetrieb zu trainieren. Die für diesen Zweck eingesetzten Simulatoren müssen einen Housekeeping-Datenstrom erzeugen, welche das reale Verhalten des Raumfahrzeugs widerspiegelt und in die Konsolen der Bedienmannschaft eingespielt wird. Häufig wird für diesen Zweck ein Entwicklungsmuster des Raumfahrzeugs verwendet, welches in einer HiL-Simulation eingebunden ist, welche bereits in Phase D zur Qualifizierung des Raumfahrzeugs eingesetzt wurde.

3.2 Eingesetzte Simulationspakete

Die zum Einsatz kommenden Simulation sind meist historisch in ihren Fachgebieten gewachsen, insbesondere die in den Phasen 0/A zum Einsatz kommenden Simulationen. Eine Kopplung der unterschiedlichen Simulationspakete stellt daher aufgrund der unterschiedlichen verwendeten Sprachen (Fortran, C, C++, Matlab/Simulink in Verbindung mit Real-Time-Workshop und MOSAIC, u.a.) und der unterschiedlichen Schnittstellen eine Herausforderung dar. Zur Kopplung der Simulation stehen einige Frameworks zur Verfügung.

Das Athena Framework [6] wird gebildet aus drei Blöcken. Im ersten Block stehen CORBA Objekte zur Verfügung welche die Simulationspackete kapseln. Der zweite Block stellt die Mittel zur Ausführung einer verteilten Simulation auf mehreren CORBA-Servern bereit. Der dritte Block beinhaltet die Visualisierung der Simulation. Dies ist zunächst eine graphische Benutzeroberfläche zum Aufbau und der Parametrisierung der Simulation als auch 2D- und 3D-Visualisierungen der Simulation. Die durch die graphische Benutzeroberfläche erstellte Simulation wird als XML-Datei gespeichert.

CORBA zur verteilten Ausführung der Simulation verwendet ebenfalls die durch EADS Astrium verwendete SiMWARE [7]. SiMWARE besteht aus SIMIX, SIMGO/OC, SIMWORK, SIMVAL und generischen Simulationsmodelle. SIMIX ist ein Echtzeit-Kernel zur zyklischen oder asynchronen Ausführung von Modellen. SIMGO/OC ist ein Betriebsüberwachungs- und Steuersystem. Eine graphische Benutzeroberfläche zur Modellentwicklung und automatischen Codeerzeugung bietet SIMWORK. SIMVAL ist ein Modell-Testwerkzeug zur Überprüfung von Modellen mit Telekommandos basierend auf SIMIX.

Große Anwendung in der europäischen Raumfahrt findet auch EuroSim [8]. EuroSim ist ebenfalls ein Framework welches unter einer graphischen Benutzeroberfläche Mittel zur Modellbildung, der Modell-Parametrisierung, dem Simulationsablauf und der Auswertung zur Verfügung stellt.

Allen diesen Tools gemeinsam ist, daß sie im wesentlichen nur für die Projektphasen 0, A, B, C, E und F eingesetzt werden. Für die Überprüfung von Software können sie nur eingeschränkt verwendet werden. EADS Astrium hat für diesen Zweck das MDVE (Model based Development & Verification Environment) entwickelt [5]. Das MDVE erlaubt den Test von Onboard Software in einem simulierten Raumfahrzeug.

Für den Test kann eine Onboard-Computer-Simulation basierend auf einem Prozessor Emulator oder eine Hardware-in-the-Loop Simulation mit simulierten Sensoren und Akuatoren verwendet werden. Der Prozessor-Emulator ist ein künstliches Abbild des real eingesetzten Onboard-Computers wie ihn zum Beispiel SHAM [9] bereit stellt. SHAM ist zur Zeit für sechs Prozessortypen verfügbar und erlaubt den Start-Stop-Betrieb des Prozessors in einer virtuellen Zeit für das Debugging der Onboard-Software. Alternativ kann ein Bord-Computer gekoppelt mit Front-Ends für die Schnittstellen des Onboard-Computers im Hardware-Loop betrieben werden. Die Front-Ends sind in diesem Fall über einen VME Bus an die System-Simulation angeschlossen. Beide genannten Möglichkeiten verwenden die gleiche Simulationsumgebung für die Dynamik- und Umgebungssimulation und den Betrieb der Testumgebung.

Das MDVE wird durch EADS Astrium in den Phasen B, C, D und E innerhalb von Raumfahrtprojekten eingesetzt, in denen EADS Astrium beteiligt ist.

4 Zukünftige Entwicklungen

Wie im vorhergehenden Abschnitt erwähnt wurde, sind die zur Zeit zur Verfügung stehenden Simulationsumgebungen nicht durchgängig über alle Projektphasen hinweg anwendbar. Entweder sind die Simulationen nicht ausreichend, um sie auf einfache Art und Weise als Testumgebung für Onboard-Software zu verwenden oder aber es existiert eine Design-Lücke zwischen den Phase A und B wie es beim MDVE von EADS Astrium der Fall ist.

Der Grund hierfür liegt in der für unterschiedliche Projektphasen benötigten Simulationsgenauigkeit und den Zeitanforderungen. Die Erfordernisse für den Aufbau einer Simulationsumgebung für die Software-Überprüfung sind andere als die Erfordernisse für den Einsatz von Simulationen in der Missionsplanung oder dem Training der Bodenmannschaft. Die Zeitgranularität der Simulation erstreckt sich hier von wenigen Millisekunden für den Softwaretest über den Sekundenbereich für das Training bis hin zu Monaten in der Missionsanalyse. Dennoch ist zu erwarten, daß sich aus der Wiederverwendung von Simulationsdaten und Simulationsmodellen über alle Projektphasen hinweg Kostenersparnisse und ein Sicherheitsgewinn ergeben.

Aus diesem Grund beabsichtigen führende Vertreter der ESA/ESTEC und der europäischen Raumfahrtindustrie eine Simulationsumgebung unter der Bezeichnung „Virtual Spacecraft“ aufzubauen, welche einen durchgängigen Gebrauch der Simulation über alle Projektphasen hinweg erlaubt. Ein wesentlicher Aspekt hierbei ist eine Modellierung der Simulation, welche für alle Projektphasen verwendbar ist.

Hierzu wird bei EADS Astrium eine Modellierung der Simulationskomponenten aufbauend auf der UML (Unified Modelling Language) durchgeführt. Als Speicherformat der Simulationsmodelle wird XMI (eXtended Metadata Interchange) verwendet, ein XML-Dialekt der Object Management Group zur Speicherung von UML-Diagrammen. Desweiteren ist angedacht, die Lücke zwischen der UML/XML-Welt und dem STEP-Standard ISO-10303 zu schließen, um Simulationsmodelle mit der Produktdatenbeschreibung von Geräten zu koppeln.

5 Literatur

[1] ESA-ESTEC Requirements and Standard Devision. *ECSS-M-30A Space Project Management, Project Phasing and Planning*. Noordwijk 19 April 1996.

[2] ESA-ESTEC Requirements and Standard Devision. *ECSS-E-40A Space Engineering, Software*. Noordwijk 13. April 1999.

[3] M. Bandecchi, B. Melton, F. Ongaro. *Concurrent Engineering Applied to Space Mission Assessment and Design*. ESA Bulletin 99. September 1999.

[4] M. Arcioni. *Simulators Rapid Prototyping in the Concurrent Design Facility*. Proceedings of 7th International Workshop on Simulation for European Space Programmes. pp 37-44. Estec, Noordwijk. November 2002.

[5] B. Ristow, J. Eickhoff. *Software Verification Facility in Satellite Development and Maintenance*. Proceedings of 7th International Workshop on Simulation for European Space Programmes. pp 45-52. Estec, Noordwijk. November 2002.

[6] B. Patin, S. Nicolas, J.F. Tilman. *Athena framework two examples of use in the aeronautic and space domain*. Proceedings of 7th International Workshop on Simulation for European Space Programmes. pp 53-60. Estec, Noordwijk. November 2002.

[7] F. Pasquier, J.M. Fournie. *SiMWARE: the ASTRIUM simulation infrastructure in support to spacecraft development, validation operations*. Proceedings of 7th International Workshop on Simulation for European Space Programmes. pp 63-70 Estec, Noordwijk. November 2002.

[8] R.H. de Vries, J. Keijzer, F. Van Lieshout, A.A. ten Dam, J.M. Moelands. *Enhancements to EuroSim*. Proceedings of 7th International Workshop on Simulation for European Space Programmes. pp 127-133. Estec, Noordwijk. November 2002.

[9] S. Mejnertson et al. *Software Validation Facility for the SPARC Micro-Processor*. DASIA 99. May 1999.