ZERTIFIZIERUNG VON SICHERHEITSKRITISCHEN GALILEO ANWENDUNGEN – ANWENDUNG EINES TRANSMODALEN ANSATZ

M. Endrich (m.endrich@tu-bs.de), A. Jasch (a.jasch@tu-bs.de)
Stephan Kocks (s.kocks@tu-bs.de) T. Feuerle (t.feuerle@tu-bs.de), P. Hecker (p.hecker@tu-bs.de)

TU Braunschweig, Institut für Flugführung
in Kooperation mit
TÜV NORD CERT GmbH

Zusammenfassung

Das Institut für Flugführung der TU Braunschweig (IFF) ist in verschiedenen Forschungsaktivitäten im Bereich der Satellitennavigation tätig. Ein spezieller Forschungsbereich sind dabei sicherheitskritische Anwendungen. Hier besteht eine enge Partnerschaft mit der TÜV Nord Cert GmbH.

Das IFF war u.a. Partner im GALCERT Projekt, das durch die Europäische GNSS Supervisor Authority (GSA) finanziert wurde. Im Rahmen dieses Projektes wurde ein Grünbuch für die Zertifizierung des Galileo Signal in Space (SIS) erstellt. Aktuell ist das IFF im Rahmen eines Folgeprojekts, dem GAUSS Basisprojekt, tätig. Das Projekt wird zum Teil durch das Niedersächsische Ministerium für Wissenschaft und Kultur und zum Teil durch das Niedersächsische Ministerium für Wirtschaft, Arbeit und Verkehr finanziert. Während GALCERT die Systemseite untersuchte, liegt der Fokus in GAUSS auf der Seite der Anwendungen. Ein Ziel des Projektes ist es, einen harmonisierten, transmodalen Zertifizierungsprozess für sicherheitskritische Satellitennavigationsanwendungen für alle Transportdomänen zu entwickeln.

Die Zertifizierungsprozesse in den verschiedenen Transport-Domänen sind in der Regel historisch gewachsen und unterscheiden sich infolge dessen oft deutlich. Dies beginnt bereits bei Definition und Nutzung der Begrifflichkeiten. Eine der ersten Aufgaben in der Entwicklung eines transmodalen Prozesses ist daher die Erstellung eines firmenübergreifenden Vokabulars.

Zur Entwicklung eines transmodalen Zertifizierungsprozess werden die spezifischen Zertifizierungsprozesse der einzelnen Domänen sowie ihre technischen Bauvorschriften in einzelne Artefakte aufgeteilt. Diesen werden bestimmte Attribute zugeordnet. Auf diese Weise wird eine einfachere Vergleichbarkeit der Anforderungen und Prozesse der einzelnen Transportdomänen erreicht. Vergleichbare Artefakte werden im weiteren Verlauf zu einem Artefakt zusammengefasst. Hierbei wird jedoch darauf geachtet die Verweise zu den ursprünglichen domänentypischen Artefakten nicht zu verlieren. Am Ende wird so ein generischer Prozess geschaffen, der die Zertifizierung der einzelnen Domänen in einer Prozesskette abbildet und dabei die Möglichkeit des domänenspezifischen Ergebnisses offen lässt.

Die bisher erzielten Ergebnisse zeigen, dass trotz der oberflächlich betrachtet großen Unterschiede im Detail viele Gemeinsamkeiten in den Transportdomänen existieren. Auf der einen Seite lassen sich auf der Ebene der Prozesse viele kleine Schritte zwischen den Domänen aufeinander abbilden. Die einzelnen Anforderungen und Bauvorschriften auf der anderen Seite sind in Ihrer Ausprägung zwar oft unterschiedlich, basieren aber oft auf gleichen Annahmen. Zudem werden zumeist ähnliche Anforderungen an den Nachweis der erfüllten Anforderungen gestellt.

Dieser Artikel illustriert den entworfenen Ansatz zur Entwicklung eines transmodalen Zertifizierungsprozesses und die ersten erzielten Ergebnisse beim Vergleich der domänenspezifischen Zertifizierungsumgebungen.

1.INSTITUT FÜR FLUGFÜHRUNG

Das Institut für Flugführung der TU Braunschweig (IFF) ist in verschiedenen Forschungsbereichen der Satellitennavigation aktiv. Ein spezieller Unterbereich ist dabei die Nutzung von globalen Satelliten-navigationssystemen (GNSS) für sicherheits-kritische Anwendungen. Hier arbeitet das IFF u.a. partnerschaftlich mit der TÜV Nord Cert GmbH zusammen.

2.HINTERGRUND

Heute sind die verfügbaren GNSS Systeme GPS und GLONASS als stand-alone Lösungen nicht in der Lage, die für viele potentielle sicherheitskritische Anwendungen notwendige Leistung zu liefern. Dies gilt insbesondere für Integritätsinformationen. Neben anderen sind Satellite (SBAS) und Ground (GBAS) based Augmentation Systems oft verwendete Techniken, um die Leistungsmerkmale der GNSS zu verbessern. Diese Systeme liefern bereits viel versprechende Ergebnisse, bleiben allerdings mit hohen Kosten verbunden und müssen zudem noch beweisen, ob sie die hohen Anforderungen von sicherheitskritischen Anwendungen tatsächlich erfüllen können. Ein Vorteil des zukünftigen europäischen Systems Galileo werden die garantierten Genauig- und Verfügbarkeiten sein. Diese werden die grundlegenden Anforderungen vieler sicherheitskritischer Anwendungen erfüllen.

Das IFF war an der Europäischen GALCERT Studie im Auftrag der GNSS Supervisor Agency (GSA) beteiligt. Ziel der Studie war ein Grünbuch für die Zertifizierung des Galileo Signal-in-Space (SIS). Aktuell ist das IFF Partner im GAUSS Projekt, einem GALCERT Folgeprojekt, das von den Niedersächsischen Ministerien für Wirtschaft und für Wissenschaft gefördert wird. Während sich GALCERT auf das Galileo SIS konzentrierte, betrachtet das GAUSS Projekt darauf aufbauend die Anwendung selbst. Ein Ziel des Projektes ist der Entwurf eines harmonisierten, domänenübergreifenden Zertifizierungsprozess für sicherheitskritische Galileo-Anwendungen. Hierzu arbeiten verschiedene Partner aus den verschiedenen Transportdomänen im Projekt mit. Die beteiligten Partner kommen dabei sowohl aus Wissenschaft und Forschung als auch aus Industrie und Wirtschaft.

2.1.Zertifizierungsprozesse

Zertifizierungsprozesse in den verschiedenen Transportdomänen haben sich im Allgemeinen historisch entwickelt und unterscheiden sich stark untereinander. Eine der Lehren aus GALCERT ist, dass innerhalb der Domänen zum Teil unterschiedliche Vokabulare und Definitionen verwendet werden. So kann ein Begriff in zwei verschiedenen Domänen völlig unterschiedliche Bedeutungen haben. Ein erster Schritt hin zu einem transmodalen Prozess ist daher die Definition eines gemeinsamen, in allen Domänen kompatiblen und gültigen Vokabulars.
Mit ihren sehr individuellen Charakteristiken wäre es ein schwieriges Unterfangen, die verschiedenen Zertifizierungsprozesse zu einem tatsächlich in allen Domänen akzeptierten Prozess zu vereinheitlichen. Es ist sicher eine interessante Herausforderung, auf legislativer Ebene auf eine Harmonisierung der Zertifizierungsvorschriften für sicherheits-kritische GNSS Anwendungen in den verschiedenen Transportdomänen hin zu arbeiten. Hierbei handelt es sich allerdings um einen vornehmlich politischen Prozess. Angesichts der verschiedenen beteiligten Akteure angefangen von Behörden und Institutionen bis hin zu Herstellern und Nutzern erscheint es auch auf lange Sicht praktisch nicht umsetzbar. Anstelle dieses top-down Ansatzes verfolgt das IFF mit seinen Partnern daher eine bottom-up Strategie, die in der vorliegenden Arbeit vorgestellt wird.

3.TRANSMODALER ANSATZ

Um von den domänenspezifischen zu einem transmodalen Zertifizierungsprozess zu

kommen, werden im Wesentlichen die folgenden vier Schritte durchgeführt:

1)*Analyse* der domänenspezifischen Situation
2)*Aufspaltung* der domänen-spezifischen Regeln in logische, unteilbare Einheiten
3)*Vergleich* der domänenspezifischen Einheiten zwischen den Domänen und *Identifizierung* der Überlappungen
4)*Fusion* der Ergebnisse in ein transmodales Metamodell bei gleichzeitiger *Reduktion* der redundanten Teile

Um den Prozess zu vereinfachen wird die Gesamtthematik Zertifizierung zunächst in zwei Teilbereiche aufgeteilt. Auf der einen Seite die formale Prozessebene, in der die übergeordnete Zertifizierungsprozesskette und die dazugehörigen Teilprozesse beschrieben sind. Auf der anderen Seite die konkreten Zertifizierungsanforderungen wie funktionale, technische und qualitative Anforderungen an das zu zertifizierende Produkt. Da Zertifizierungsprozesse in der Regel von strikten Vorgaben durch domänenspezifische Behörden bestimmt sind, ist davon auszugehen, dass die Gemeinsamkeiten zwischen den Domänen eher im Bereich der konkreten Anforderungen zu finden sind.

Im Folgenden werden die im Prinzip ähnlichen aber im Detail leicht differierenden Ansätze für die beiden Teilebenen Prozesse und Anforderungen vorgestellt.

3.1.Prozesse

Im ersten Schritt wird eine ausführliche Detailanalyse der Zertifizierungsregeln und Prozeduren in jeder betrachteten Domäne durchgeführt. In dieser Phase werden die verschiedenen domänenspezifischen Zertifizierungsrichtlinien gesammelt und analysiert. Darauf aufbauend wird die typische Prozesskette anhand eines Beispiels visualisiert.

Im zweiten Schritt wird der Zertifizierungsprozess dort, wo es die Vorschriften erlauben, in logische und dann unteilbare Einheiten aufgespalten. Diese Einheiten werden in ein vorher definiertes Template mit einem vordefinierten Satz von Attributen überführt. Zu diesen Attributen gehören z.B. Beschreibung des Schritts, Dokumente, Verantwortlichkeiten, Vorbedingungen, Nachbedingungen, Vorgänger- und Nachfolgeprozesse. Die Transformation in ein einheitliches Template erleichtert den Vergleich untereinander im nächsten Schritt.

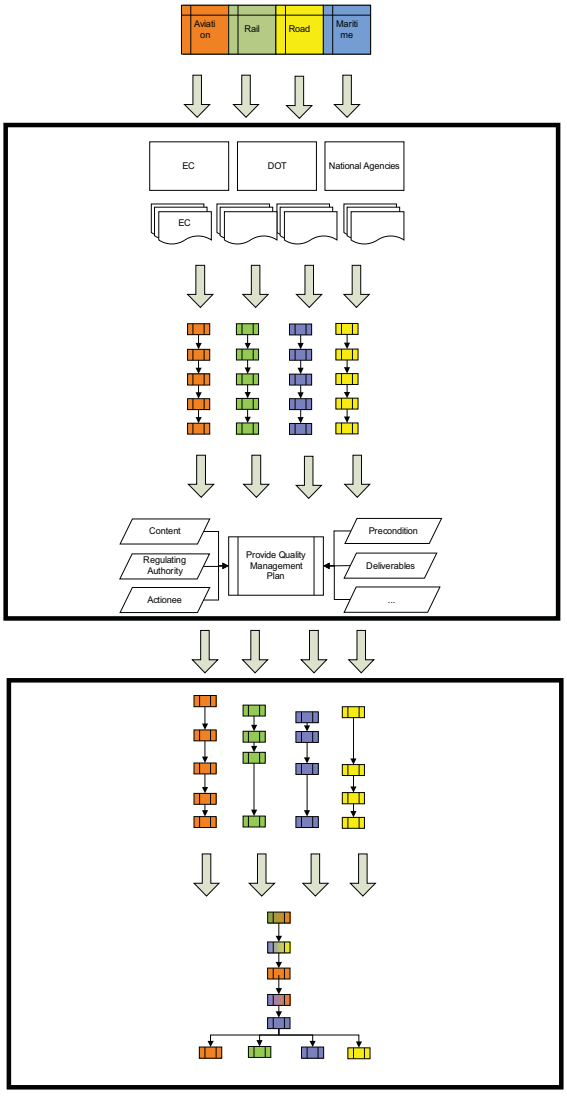

BILD 1. Prozess Methodik

Im dritten Schritt werden alle Prozessschritte anhand ihrer Attribute sortiert und untereinander verglichen. Bei Übereinstimmungen untereinander werden sie zusammengelegt, so dass die Menge der

Schritte insgesamt reduziert wird.
Im letzten Schritt werden die einzelnen Prozessschritte in einer gemeinsamen, transmodalen Prozesskette vereint. Diese Kette beinhaltet dann zum einen alle kombinierten sich überschneidenden, zum anderen alle nicht kombinierbaren Schritte, die nur für eine einzelne Domäne gültig sind. Die Architektur der Prozesskette ist insofern modular aufgebaut, dass die einzelnen Prozessschritte als austauschbare Module strukturiert sind.
Als Basis dient ein abstrakter, übergeordneter Zertifizierungsprozess mit genau definierten Schnittstellen zwischen den Modulen. Eine wichtige Voraussetzung für die Gültig- und damit verbundene Anwendbarkeit eines solchen Prozesses ist die absolute Konformität mit allen Regeln in jeder spezifischen Domäne, in der er eingesetzt werden soll.

3.2.Anforderungen

Für die Anforderungsebene werden zunächst wieder alle domänenspezifischen Richtlinien und Zertifzierungsdokumente identifiziert und analysiert. Neben diesen werden auch nicht domänenspezifische, allgemeine Vorschriften wie z.B. die Norm 61508 der International Electrotechnical Commission (IEC-61508) untersucht.

Im zweiten Schritt wird ein Anforderungs-Template mit verschiedenen Attributen definiert. Zu diesen Attributen gehören unter anderem Inhalt, Bereich, Handelnde und Kritikalitätslevel. Aus den Vorschriften werden dann alle einzelnen Anforderungen extrahiert, in unteilbare logische Einheiten aufgespalten und in das einheitliche Template überführt.

Der dritte Schritt ist die Erstellung einer Kreuzmatrix, die die Anforderungen jeder Domäne gegen die Anforderungen aller anderen Domänen referenziert. Bei diesem Schritt müssen insbesondere die feinen Unterschiede und Charakteristiken der einzelnen Domänen berücksichtigt werden. Zudem existieren durch verschiedene gültige Standards oft schon innerhalb einer Domäne Redundanzen von Anforderungen, die in diesem Schritt direkt aufgelöst werden können. Das Ergebnis dieses Schrittes ist eine konsolidierte Liste aller Anforderungen aus allen Domänen und die identifizierten Überschneidungen untereinander.

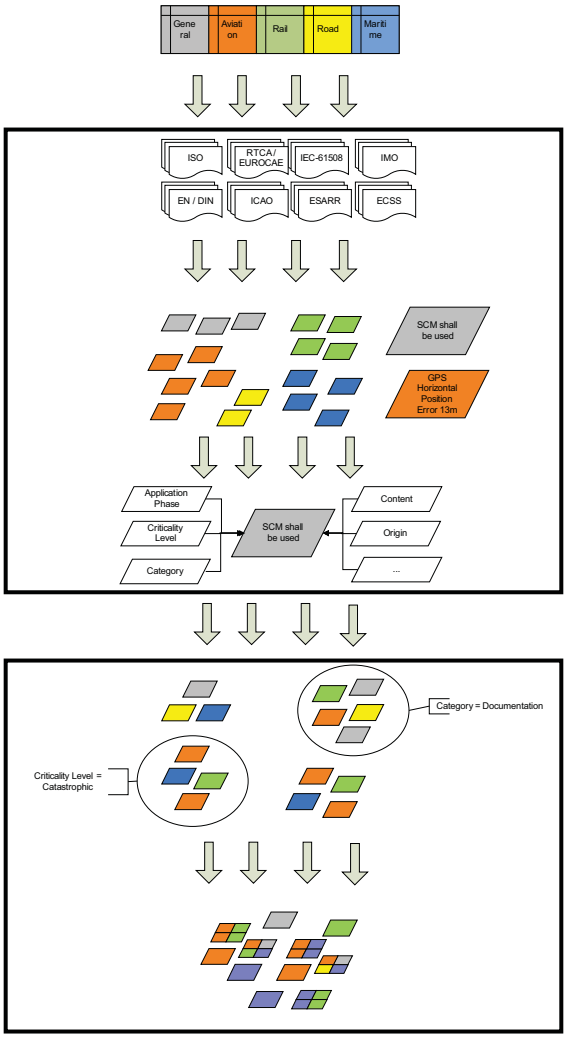

BILD 2. Anforderungs Methodik

4.ANWENDUNG DES ANSATZES

Die ersten Ergebnisse bei der Anwendung des beschriebenen Ansatzes hin zu einem modularen, transmodalen Zertifizierungsprozess sind viel versprechend. Auch wenn es nicht möglich ist, einen einzelnen, allgemein gültigen Zertifizierungsprozess für alle

Transportdomänen zu definieren, finden sich doch viele gemeinsame Bereiche und Überscheidungen zwischen den Domänen, die zunächst nicht offensichtlich sind.
Der transmodale Ansatz liefert zudem eine vereinheitlichte, modulare Prozesskette und eine Datenbank mit domänenübergreifenden Anforderungen.

Wie erwartet, gibt es allerdings fundamentale Unterschiede zwischen den Domänen, die nicht mit einer einfachen bottom-up Strategie ausgeräumt werden können. Diese Unterschiede betreffen allerdings fast ausschließlich die formale Prozessebene.

Eine der größten Herausforderungen ist die unterschiedliche Struktur der verantwortlichen Behörden und Institutionen. Dazu gehört unter anderem auch die Frage, ob die Zertifizierung größtenteils nationalen oder internationalen Autoritäten unterliegt. Während Zertifizierung und Akkreditierung in manchen Transport-Domänen wie z.B. der Luftfahrt (EASA / FAA) auf internationaler Ebene harmonisiert sind, sind diese in anderen Domänen wie z.B. der Eisenbahn oft vor allem national bestimmt.

Ein Unterschied in der Anforderungsebene zwischen den Domänen ist zudem die Tatsache, ob überhaupt differenzierte Richtlinien existieren. Während allgemeine Richtlinien für Soft- und Hardware in praktisch allen Transportdomänen existieren, gibt es mit Ausnahme der Luftfahrt bisher kaum Richtlinien für die Verwendung von GNSS für sicherheitskritische Anwendungen.

5.ABSCHLIESSENDE BEMERKUNGEN UND NÄCHSTE SCHRITTE

Die vorliegende Arbeit beschreibt die fortlaufenden Forschungsarbeiten des IFF zu einem transmodalen Zertifizierungsprozess für zukünftige sicherheitskritische Galileo-Anwendungen. Zu den aktuellen Ergebnissen dieser Arbeiten gehören Templates für Anforderungsartefakte und Prozessschritte, eine stetig erweiterte Datenbank mit tatsächlichen Anforderungsartefakten aus verschiedenen Transportdomänen und ein erstes Metamodell für eine transmodale Prozesskette. Die ersten Ergebnisse haben gezeigt, dass ein solches Metamodell angewandt werden kann und ein, bis zu einem bestimmten Grad einheitlicher Ansatz für die Zertifizierung von sicherheitskritischen Galileo Anwendungen möglich ist.

Diese vielversprechenden Ergebnisse sind die Basis für zukünftige Schritte. Die nächsten, vertiefenden Arbeiten umfassen zum einen die kontinuierliche Erweiterung der Anforderungsdatenbank und das Verifizieren der Templates. Zum anderen wird der Fokus auf der Detailspezifikation des Metamodells für den Prozess liegen.

Um sowohl das Prozessmodell als auch die Anforderungsdatenbank zu verifizieren und zu validieren, sind zudem verschiedene Beispielzertifizierungen geplant. Mögliche Kandidaten für eine solche Zertifizierung reichen von einer einzelnen Komponenten wie zum Beispiel eines Galileo Referenz-Empfängers bis zu kompletten System wie zum Beispiel GBAS basierte Landeunterstützungssysteme für CAT-II/III Anflüge. Zur Verifikation des Ansatzes müssen die Ergebnisse dieser Beispielzertifizierung dann gegen die Ergebnisse einer domänenspezifischen Standardzertifizierung evaluiert werden.

6.DANKSAGUNGEN

Diese Arbeit wurde teilweise vom Niedersächsischen Ministerium für Wissenschaft und Kultur gefördert. Sie beinhaltet Beiträge der Partner des IFF im GAUSS Projekt. Das GAUSS Projekt wird gefördert durch die Niedersächsischen Ministerien für Wissenschaft und Kultur auf der einen Seite und Wirtschaft auf der anderen Seite. Teile dieser Arbeit wurden im Rahmen einer Partnerschaft des IFF mit der TÜV Nord Cert GmbH durchgeführt.