Die Zertifizierung des Modellierungswerkzeugs ASCET nach der IEC 6 15 08

Peter Dencker und Tilman Glötzner

ETAS GmbH
Borsigstrasse 14
70469 Stuttgart
Tilman.Gloetzner@etas.com

Abstract: Im Folgenden wird die Zertifizierung des Modellierungswerkzeugs ASCET nach der IEC61508 beschrieben. Nach einer Kurzbeschreibung von ASCET und der Norm wird die Motivation für eine Zertifizierung beleuchtet und ihr Nutzen für den Werkzeuganwender. Danach folgt eine Erklärung des Zertifizierungsprozess und der dabei entstehenden und zu prüfenden Dokumente.

1 Einleitung

Dieser Beitrag beschreibt die Zertifizierung des Modellierungstools ASCET nach der IEC 6 15 08 als „Fit for purpose“.

Im ersten Teil wird kurz die Funktion und der Aufbau von ASCET erläutert. Danach wird der IEC 6 15 08 und seine Zielsetzung beleuchtet. Der nächsten Teil geht auf die Motivation für die Zertifizierung eines Codegenerators ein. Dann wird die Zertifizierung für den Codegenerator an Hand des allgemeinen Vorgehensmodells erklärt. Der letzte Teil beinhaltet einen Ausblick auf die wachsende Bedeutung von Sicherheitsstandards.

2 ASCET

ASCET ist ein Modellierungswerkzeug, das sich an Funktionsentwickler und Softwareingenieure in der Automobilindustrie wendet. Es unterstützt einen iterativen Entwicklungszyklus nach dem V-Modell im Wesentlichen durch 5 Funktionen: Modellierung, Rapid Prototyping, Codegenerierung, Integration, Dokumentengenerierung. Codegenerierende Modellierungswerkzeuge verschieben die Funktionsentwicklungsaktivitäten von der Code-Ebene auf die abstrakte Modellebene. Sie erzwingen dabei einen Ablauf in einer Richtung, nämlich vom Modell zum Seriencode. Das Modell wird mittels Simulation und Rapid Prototyping immer tiefer überprüft und schrittweise verfeinert.

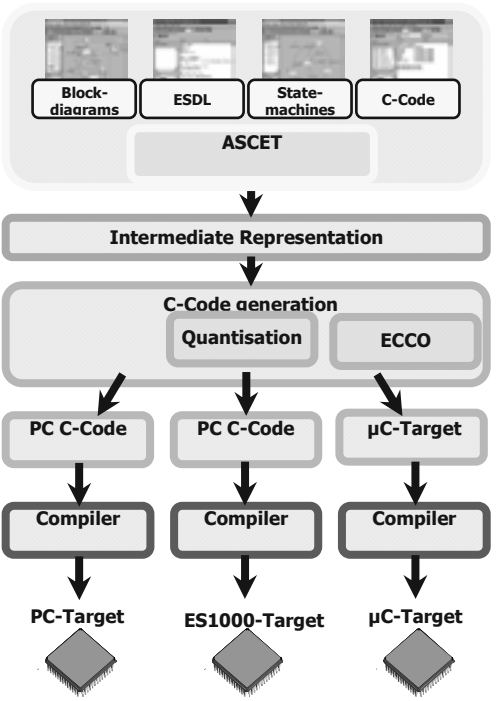

Abbildung 1: Funktionsdiagramm von ASCET

Die Effizienz der Softwareentwicklung steigt dadurch bei abnehmenden Entwicklungsrisiken und Entwicklungsaufwand.

Abbildung 1 zeigt den funktionalen Aufbau von ASCET. Die Modellkomponenten in den verschiedenen Notationen werden zuerst in eine Zwischendarstellung überführt, aus der nach einer Optimierung C-Code generiert wird. Soll das Modell in Fließkomma-Arithmetik auf dem PC simuliert werden, wird die im linken Ast dargestellte Compilerkette verwendet. Festkomma-Arithmetik wird mit der Quantisierungskomponente durch den mittleren Ast abgedeckt. Im rechten Ast erkennt man zusätzlich die Codegenerierung für die Zielplattform. Die mit ECCO bezeichnete Komponente führt während der C-Code-Generierung zusätzliche Optimierungen und Anpassungen für Zielplattform durch.

3 Die IEC 6 15 08

Die IEC 6 15 08 bietet eine systematische Herangehensweise an die funktionale Sicherheit von elektrischen, elektronischen und programmierbaren elektronischen Systemen in einem sicherheitsrelevantem Kontext an. Ausgehend von den Risiken, die durch Fehlfunktionen von einem System ausgehen können, fordert die Norm die Implementierung von Sicherheitsfunktionen. Um ein korrektes Funktionieren im Bedarfsfall zu gewährleisten, formuliert sie Methoden und Ziele im Lebens- und Entwicklungszyklus des Systems. Sie repräsentiert den derzeitigen Stand der Technik und des wirtschaftlich Sinnvollen.

Der „Safety Integrity Level (SIL)“ ist ein zentraler Begriff in der Norm. Er formuliert eine Anforderung an die funktionale Sicherheit eines Systems. Der SIL wird in 4 diskreten Stufen nach akzeptierten Auswirkungen von „Leichte Verletzungen einiger Personen, Sachschäden“ (SIL 1) bis „Tod vieler Personen (Katastrophe)“ (SIL 4) angegeben.

Erfüllt das Werkzeug und sein Entwicklungsprozess die Anforderungen des SIL n, so kann es nach „SIL n, fit for purpose“ zertifiziert werden. Damit ist das Werkzeug geeignet, Entwicklungen von Steuergeräten bis zu dem SIL n zu unterstützen.

Im Automobilbereich gibt es derzeit keinen branchenspezifischen Standard, so dass man direkt auf die IEC 6 15 08 zurückgreift. Typischer Weise kommen SIL2 oder SIL3 zu Anwendung. Für einen elektrischen Fensterheber wird SIL 2 ausreichend sein. Für ein ESP-Steuergerät, das aktiv in die Querdynamik des Fahrzeugs eingreifen kann, wird man SIL 3 erreichen wollen.

4 Motivation für eine Zertifizierung

Eine Zertifizierung nach IEC 6 15 08 wird häufig als Maßnahme zur Risikominimierung von Haftungsfällen angestrebt. Klagen aufgrund von **grober Fahrlässigkeit** gegen einzelne Personen werden sich eigentlich immer ausschließen lassen. In **Produkthaftungsfällen** wird das Zertifikat in der Regel die Nachweispflicht umkehren können, d.h. der Kläger (und nicht der Beklagte) wird nun nachweisen müssen, dass die Unternehmung ihrer Sorgfaltspflicht bei der Produktentwicklung nicht nachgekommen ist. Die Wahrscheinlichkeit eines Haftungsfalls und die dafür gebildeten Rückstellungen können verringert werden.

Zusätzlich kann man bei Steuergerätezertifizierung durch Verwendung eines zertifizierten Codegenerators auf zeitintensive, fehleranfällige und teure manuelle Reviews des aus dem Modell generierten Quellcodes verzichten. Die Reviews werden auf die abstraktere und übersichtlichere Modellebene verschoben. Auch Modultest, statische Codeanalyse und formale Reviews des autogenerierten Codes werden überflüssig. Bei großen Projekten mit viel autogeneriertem Quellcode verringert sich der Aufwand drastisch.

5 Die Zertifizierung

Die letzte Zertifizierung von ASCET war die dritte ihrer Art. Man verständigte sich daher auf eine „Delta-Zertifizierung“, bei der man sich auf Änderungen seit der letzten Prüfung durch den TÜV Nord konzentrierte. Von der ersten Anfrage bis zum Zertifikat vergingen fast 15 Monate. Der Projektverlauf lässt sich in 6 Abschnitte teilen:

1. Definitionsphase

   In diese Phase wird der Umfang der Zertifizierung mit TÜV Nord als zertifizierende Organisation abgestimmt. Im Fall von ASCET bestimmten ETAS und der TÜV Nord dabei die Transformation des Modells zum C-Code, d.h. den Codegenerator, als sicherheitsrelevante Funktion. Ausserdem verständigte man sich auf eine bestimme Konfiguration bzw. Version von ASCET. Auch der grobe Zeitrahmen des Zertifizierungsprojektes wurde festgesetzt.

2. Vorbereiten der Zertifizierung

   In dieser Phase wurden ein Zertifizierungsplan (Projektplan), ein Prüfplan und ein Bewertungsplan erarbeitet. Der **Prüfplan** listet die Anforderungen der

Norm, gegen die ASCET und sein Entwicklungsprozess geprüft wurden. Der **Bewertungsplan** hingegen beschreibt einen Maßstab, mit dem der Erfüllungsgrad der Anforderungen bestimmt wurde. Die Erfüllungsgrade der individuellen Anforderungen fließen gewichtet in ein Endergebnis ein, das über den Erfolg der Zertifizierung entscheidet. Auch das ist im Bewertungsplan dokumentiert.

3. Erstellen von Dokumentation

   In diesem Arbeitspaket wurde die für ASCET vorhandene Produkt- und Prozessbeschreibungen sowie Prozessartefakte, wie z.B. Testresultate, mit den Anforderungen aus IEC61508 in Beziehung gesetzt, um ihre Erfüllung zu begründen. Dieses war die aufwändigste Phase des Zerifizierungsprojekts.

4. Prüfung bzw. Audit

   Der TÜV Nord sichtete die übergeben Dokumentation, und führte mehrere Audits vor Ort durch. Bei diesen wurden Detailfragen, die sich aus den Dokumenten ergaben, geklärt, und Interviews mit Entwicklern und Produktmanagern durchgeführt.

5. Auswertung der Prüfergebnisse

   Der TÜV Nord wertete die Prüfergebnisse mittels des zuvor aufgestellten Bewertungsplans aus. Basierenden darauf entschied sich der TÜV für eine Zertifzierung.

6. Projektabschluss

   Mit Ausstellung und Übergabe des Zertikates wurde das Projekt abgeschlossen.

6 Ausblick

Die Anwendung der IEC 6 15 08 breitet sich derzeit schnell aus. Mehr und mehr Sicherheitsfunktion finden ihren Weg in das Auto und werden durch Steuergeräte implementiert. Das verstärkt die Notwendigkeit systematischer und risikobasierter Ansätze, wie sie die IEC 6 15 08 anbietet. Die Norm und der daraus abgeleitete branchenspezifische Standard ISO WD 26262, der gegenwärtig entwickelt wird, dürften in den nächsten Jahren in der Automobilindustrie stark an Bedeutung gewinnen.

Die IEC 6 15 08 hat viel mit den qualitäts- und prozessorientierten Standards wie CMMI oder ISO 9001 gemein. Konformität zur IEC 6 15 08 sollte deswegen nicht als zusätzlicher Prozessaufwand gesehen werden. Sie ist vielmehr eine Maßnahme, die Qualität und die Effizienz der Entwicklung und des Produktes selbst nachhaltig zu verbessern. Zertifizierte Entwicklungswerkzeuge unterstützen diese Ziele durch deutliche Verringerung des Zertifizierungsaufwands beim Automobilhersteller.