SparxSystems CE: Enterprise Architect unterstützt funktionale Sicherheit nach ISO26262

Im Jahr 2007 stand man bei einem Automobilzulieferer vor der Herausforderung, die Anforderungen des kommenden Standards ISO26262 zur Entwicklung sicherheitskritischer Systeme (Functional Safety Management, FSM) erfüllen zu müssen. Dr. Oliver Alt, ehemaliger Enterprise Architect Trainer, begleitete das Unternehmen in verschiedenen Rollen über mehrere Jahre bei der Umsetzung der modellbasierten Systementwicklung mit der Modellierungs-Plattform.

Dr. Oliver Alt

Die ISO26262 stellt zusätzliche Anforderungen an die Entwicklung, die über klassische Entwicklungsprozessanforderungen wie CMMI oder Automotive SPICE hinausgehen, und bei der Entwicklung sicherheitskritischer Systeme beachtet werden müssen. Sie basiert auf der allgemeinen Industrienorm für sicherheitskritische Systeme IEC/ISO61508. Mit Inkrafttreten in den Jahren 2011/2012 muss jedes sicherheitskritische System im Auto diese Norm erfüllen, um eine Straßenzulassung zu erhalten.
Mit der damals eingesetzten dokumentenzentrierten Entwicklung, bei der vorwiegend Textdokumente mit Abbildungen zum Einsatz kommen, sah man sich dieser Herausforderung nicht mehr gewachsen. Eine zentrale Anforderung der neuen Norm ist nämlich die Nachverfolgbarkeit (Traceability) aller Entwicklungsartefakte. Daher machte man sich auf die Suche nach einem neuen Ansatz.

Modellbasierte Entwicklung: Die optimale Lösung zur Umsetzung der ISO26262
Dabei stieß man bald auf die modellbasierte Entwicklung. Sie nutzt neue Entwicklungsmethoden und Modellierungssprachen wie UML (Unified Modeling Language) für die Softwaremodellierung bzw. SysML (Systems Modeling Language) für die Modellierung von Gesamtsystemen. Dieser Ansatz wurde als optimal dafür angesehen, um den Herausforderungen der Entwicklung von sicherheitskritischen Systemen im Automobil nach ISO26262 auch langfristig gewachsen zu sein.
Neben der Entscheidung für SysML als Modellierungssprache wurde daher ein geeignetes Modellierungswerkzeug gesucht, das die Anforderungen an Stabilität, Erweiterbarkeit und Multi-User-Fähigkeit erfüllt.
Einzelne Mitarbeiter aus der Softwareentwicklung des Unternehmens hatten Enterprise Architect bereits im Rahmen der Mitarbeit in AUTOSAR[1]-Gremien kennen und schätzen gelernt. Die Modellierungs-Plattform wird nämlich im AUTOSAR-Umfeld gerne und häufig eingesetzt. Da sie sich durch die hohe Stabilität, großen Funktionsumfang und geringen Anschaffungspreis auszeichnet, waren im Unternehmen bereits einige Lizenzen verteilt im Einsatz. So bot es sich an, Enterprise Architect auch für die geplante Systemmodellierung mit SysML zu evaluieren.
Schon nach kurzer Zeit erhielt das Werkzeug eine sehr positive Beurteilung und das Unternehmen kaufte etwa 100 Lizenzen an. Zugleich vertiefte sich ein eigenes Team in die neuen Themen Modellierungsmethodik und SysML, um damit die ISO26262 sowie Automotive SPICE umsetzen zu können.

1 AUTOmotive Systems Architecture – Ein Standard für flexible Softwarearchitektur im Automobilumfeld.

Aufbau einer passenden Infrastruktur

Zunächst musste eine Infrastruktur für die modellbasierte Entwicklung entstehen. Als Basis diente eine zentrale Datenbank, zunächst auf Open-Source-Basis. Diese wurde später durch ein anderes System ersetzt, das von der Unternehmens-IT besser unterstützt wird. Der Umstieg von einer Datenbank zur anderen erwies sich als problemlos, da Enterprise Architect Funktionen wie „Project Transfer“ beinhaltet und die Datenbank-Schemata systemübergreifend kompatibel sind.

Neben der Datenbank wurde die Sicherheitsfunktion aktiviert, die es ermöglicht, Benutzern verschiedene Rechte innerhalb eines Modells zu erteilen. So erhalten z.B. einzelne Benutzer nur Leserechte, andere aber erweiterte Rechte. Durch die Kopplung der internen Benutzerverwaltung mit dem Windows Active Directory konnte sogar ein Single Sign-On für das Modell erreicht werden. So müssen sich die Anwender nur einmal bei Windows anmelden, der Zugriff auf die Enterprise Architect Datenbank erfolgt vollautomatisch mit allen benötigten Rechten.

Wie sieht es nun aber mit der Performance von Modellierngs-Plattform aus: Erlaubt sie auch bei großen Modellen noch ein flüssiges Arbeiten? Dazu erstellten wir ein Testprogramm, das über die Programmierschnittstelle (Enterprise Architect Application Interface, EA-API) automatisch eine Million Elemente in der Modelldatenbank anlegt. Danach öffnete ein Benutzer das Modell und beurteilte die Reaktionsgeschwindigkeit. Der Test endete so positiv, dass man sich auch für kommende Modellgrößen gerüstet sah.

Nutzung der Erweiterungsmöglichkeiten

Schon früh in der Nutzung von Enterprise Architect erwiesen sich die Erweiterungsmöglichkeiten als äußerst hilfreich und zielführend. So erlaubt das erwähnte EA-API, die Plattform durch Software fernzusteuern oder per Plug-In‘s neue Funktionen hinzuzufügen. Darüber hinaus lassen sich sogenannte UML-Profile nutzen: Sie ermöglichen die Erweiterung von Modellierungssprachen zur Anpassung an die eigenen Bedürfnisse. Damit gelang es, in die Modelle auch Aspekte der funktionalen Sicherheit zu integrieren. Komponenten können etwa mit dem in ISO26262 spezifizierten ASIL-Level (Automotive Safety Integrity Level) versehen werden, was sowohl grafisch wie auch farblich sichtbar ist. Diese Funktion wird bei der in der ISO26262 beschriebenen „ASIL-Dekomposition“ oft und gerne genutzt.

Die Modellierungssprachen wurden mit Hilfe von Profilen viel besser auf die Bedürfnisse und Vorkenntnisse der Nutzer zugeschnitten. Dies führte letztlich zu einer höheren Akzeptanz von Enterprise Architect und der modellbasierten Entwicklung.

Integration von Enterprise Architect in den Prozess

Ab einer gewissen Projekt- und Unternehmensgröße wird leicht verständlich, das Enterprise Architect nur Teil einer größeren Werkzeugkette sein kann. Daher sollte er nahtlos in die Kette integriert werden. Dafür stehen Mittel wie Excel Im-/Export, Dokumentengenerierung oder XMI-Im-/Export zur Verfügung. Will man über diese Möglichkeiten hinausgehen, so lassen sich über die umfangreiche EA-API im Prinzip beliebige (externe) Daten mit dem Modell integrieren. Im Unternehmen entstanden über die letzten zehn Jahre daher spezielle Plug-Ins und Anwendungen, um Daten mit anderen Entwicklungswerkzeugen auszutauschen oder diese ins Modell zu integrieren.

Zentral war dabei die Integration mit dem schon existierenden Anforderungsmanagement-Werkzeug. Nun werden die Anforderungen so in das Modell integriert, dass diese als (SysML-)Anforderungsmodellelement zur Verfügung stehen und mit anderen Modellelementen in Enterprise Architect grafisch verknüpft werden können. Dies löst die Herausforderung der umfassenden Nachverfolgbarkeit (Traceability) der Entwicklungsartefakte auf elegante Weise.
Weitere Integrationen betreffen die Nutzung von Daten aus dem Modell für die bei sicherheitskritischen Systemen extrem wichtige FMEA (Fehler-Möglichkeits- und -Einflussanalyse) sowie anderen Verfahren der Entwicklung sicherheitskritischer Systeme und zugehöriger Werkzeuge.
Ein weiterer Aspekt ist die automatisierte Erzeugung von Variantenbeschreibungen aus den Modellen. Sowohl die Modelle als auch die Definition von bestimmten Produktvarianten liegen in elektronischer Form vor und sind maschinell zu verarbeiten. Eine darauf aufbauende Erweiterung generiert automatisch Variantenbeschreibungen in unterschiedlicher Form aus dem entsprechend vorbereiteten Modell. Das führte zu einer deutlichen Verkürzung der Entwicklungszeit für die Spezifikation einer Kundenvariante. Die Entwicklung bzw. Beschaffung der beschriebenen Integrationslösungen und Erweiterungen erfolgte sowohl im Unternehmen als auch durch externe Dienstleister.

Enterprise Architect gehört heute zu den zentralen Entwicklungswerkzeugen
Das Unternehmen zieht nach mehreren Jahren Einsatz von Enterprise Architect für die modellbasierte Entwicklung von sicherheitskritischen Systemen im Automobilbereich ein sehr positives Fazit. Das Modell umfasst inzwischen mehrere 100.000 Elemente und ein Vielfaches an Verbindungselementen (Konnektoren). Was zunächst nur für ein Projekt pilotiert war, ist inzwischen zu einem standort- und länderübergreifenden, etablierten Entwicklungsverfahren geworden.
Begleitend zur Werkzeugeinführung machten sich die Modellierer und Nutzer in internen und externen Schulungen mit Werkzeug und Methodik vertraut. Inzwischen arbeiten mehrere hundert Nutzer mit Enterprise Architect, die Plattform konnte also ihre Alltagstauglichkeit unter Beweis stellen. Die Modelle ermöglichen den Nutzern eine ausgezeichnete Übersicht über die täglich wachsenden Systeme. Auch die Herausforderungen bei der Entwicklung sicherheitskritischer Systeme bleiben mit der Plattform handhabbar und lassen sich wesentlich effizienter meistern. Die Aspekte der modellbasierten Entwicklung wurden darüber hinaus auch bei externen Audits der Entwicklungsprozesse gelobt und stets positiv bewertet.
Enterprise Architect hat sich in diesen Jahren und mit jeder neuen Version im Hinblick auf Performance und Funktionsumfang verbessert. Die Plattform ist damit zu einem nicht mehr wegzudenkenden Teil in der Kette der wichtigen Entwicklungswerkzeuge im Unternehmen geworden.