Integration der Normen zur Funktionalen Sicherheit in ein organisationsspezifisch angepasstes V-Modell XT und die Projektpraxis

Dipl.-Physikerin Margit Fries, Dipl.-Wirtschaftsing. (FH) Herbert Dietrich

Abteilung MO-E
Elektroniksystem- und Logistik GmbH
Livry-Gargan-Straße 6
82256 Fürstenfeldbruck
info@esg.de

Abstract: Der Vortrag stellt im ersten Teil zunächst die wichtigsten Grundprinzipien der organisationsspezifischen Anpassung des V-Modell XT vor. Im zweiten Teil wird darauf aufbauend die Erweiterung des organisationsspezifisch angepassten V-Modell XT um die in den Sicherheitsnormen IEC 61508 und ISO 26262 beschriebenen Anforderungen zur Funktionalen Sicherheit beschrieben.

Darauf folgt die operative Umsetzung beispielhaft gezeigt an zivilen (Automobilindustrie) und militärischen Entwicklungsprojekten (Geschütz). Der Vortrag geht darauf ein, welche Klippen beim ersten sicherheitsgerichteten Projekt zu umschiffen sind und welche Ansätze sich über mehrere Projekte hinweg bewährt haben. Den Abschluss bildet ein Ausblick, wie ein Projektteam vom bloßen Erfüllen der Anforderungen der Funktionalen Sicherheit zur aktiven Gestaltung in der täglichen Praxis kommt.

1 Engineering Prozesses auf Basis einer organisationsspezifischen Anpassung des V-Modell XT

Die ESG erbringt als eines der führenden System- und Softwarehäuser Deutschlands einen Großteil ihrer Leistungen auf den Gebieten Systementwicklung Embedded und Systementwicklung IT, so dass es nahelag, das V-Modell XT als Quasi-Standard für Militär, Behörden und Industrie als Basis eines State-of-the-Art-Vorgehensmodells zu definieren.

Das V-Modell XT betrachtet zwar in seiner ursprünglichen Form nur System-entwicklungsprojekte, ist jedoch aufgrund seines Baukastenprinzips und der Möglichkeit bzw. Notwendigkeit einer organisationsspezifischen Anpassung sehr flexibel und berücksichtigt zudem den Ausschreibungs- und Angebotsprozess.

Da die ESG neben der Systementwicklung Embedded/ IT auch Beratung, Logistik, Technische Dienstleistung, Training und IT-Services anbietet, nutzte sie das Baukastenprinzip und die Flexibilität des V-Modell XT intensiv für vielfältige, organisationsspezifische Ergänzungen bzw. Erweiterungen.

Durch die Unterteilung des Vorgehensmodells gelang es, ein für alle Leistungen gleiches oberes V („Projekt-V“) zu definieren und gleichzeitig den spezifischen Unterschieden und Besonderheiten verschiedenartiger Leistungen in mehreren unteren V‘s („Leistungs-V“) gerecht zu werden.

Zusätzlich wurden auf Basis der Best Practices u.a. mehr als die im V-Modell XT genannten Durchführungsstrategien für Projekte zugelassen sowie ESG-spezifische Entscheidungspunkte, Aktivitäten, Produkte und Rollen definiert.

Da das V-Modell XT im Wesentlichen Aussagen zu den Fragen "Was (Produkt)?", "Wann (Entscheidungspunkt)?" und "Durch Wen (Rolle)?" macht, die in Form einer Verfahrensanweisung dokumentiert wurden, war es notwendig, auch das "Wie (Methode)?" und "Womit (Tool)?" detailliert zu beschreiben. Diese Themen wurden in mehreren Arbeitsanweisungen dokumentiert. Dabei wurden auch Forderungen aus den Qualitätsnormen (z.B. ISO 9001, EN 9100) integriert.

Zur Unterstützung des projektspezifischen Tailorings entwickelte die ESG ein eigenes Tailoring-Tool, das als Web Applikation über das firmenweite Intranet zur Verfügung gestellt wird. Dieses Tailoring-Tool tailort auf Produktebene und stellt zur Unterstützung der Projektdurchführung Produktvorlagen und einen Projektplan zur Verfügung. Es ist verpflichtend für alle Projekte der ESG anzuwenden und enthält heute das Tailoring von über 2.000 Projekten.

2 Integration der Funktionalen Sicherheit (Safety) in den Engineering Prozess

In sicherheitskritischen Projekten, d.h. im Falle der ESG, in Projekten, in denen Systeme oder Software entwickelt werden, durch die eine mögliche Gefährdung für Mensch und Umwelt ausgehen könnte, ist die Berücksichtigung entsprechender domänenspezifischer Sicherheitsnormen notwendig, um dem Anspruch gerecht zu werden, nach Stand von Wissenschaft und Technik zu entwickeln.

Im Hinblick auf das Leistungsportfolio der ESG sind insbesondere die beiden Normen IEC 61508, als Grundnorm für alle sicherheitsbezogenen Systeme, die elektrische, elektronische oder programmierbar elektronische Komponenten (E/E/PES) enthalten, und deren Ausfall ein maßgebliches Risiko für Mensch oder Umwelt bedeutet, sowie die ISO 26262 als entsprechende Ableitung für den Automotive-Bereich von Interesse.

Basierend auf der organisationsspezifischen Anpassung des V-Modell XT wurde diese deshalb um die in den beiden Safety-Normen IEC 61508 und ISO 26262 beschriebenen Anforderungen und Vorgaben erweitert.

Dazu wurden die Anforderungen der Normen einzeln betrachtet, analysiert und so umgesetzt, dass sie vollständig und integrativ im Engineering Prozess der ESG abgebildet werden konnten.

Diese Abbildung bildet die Grundlage des Safety-Managementsystems der ESG, dessen Anwendung in sicherheitskritischen Projekten die Anforderungen der zugrundeliegenden Normen umsetzt, ohne dass sich die Mitarbeiter explizit mit diesen auseinandersetzen müssen. Diese Vorgehensweise erleichtert die Arbeit in Safety-relevanten Projekten enorm.

Zur Projektdurchführung auf Basis der organisationsspezifischen Anpassungen des V-Modells XT sowie zur Integration der Safety-Normen in diesen Entwicklungsprozess wurde ein Schulungskonzept erarbeitet. Im Rahmen dieses Schulungskonzeptes finden in der ESG für alle Mitarbeiterinnen und Mitarbeiter regelmäßige Schulungen statt.

3 Beispielhafte Umsetzung des Engineering Prozesses in der Projektpraxis

In die Ertüchtigung des Vorgehensmodells für die Entwicklung sicherheitskritischer Software und Systeme flossen direkt die Erfahrungen aus laufenden Projekten ein. Dazu wurden die Ergebnisse aus den bereits etablierten Prozessen für Lessons Learned, interne und externe Audits und der Austausch in Netzwerken für die verschiedenen Unternehmensrollen (z.B. Software-Entwickler, Projektleiter, Qualitätsbeauftragte und Qualitätssicherungsverantwortliche) genutzt. Diese Prozesse profitierten ihrerseits wiederum durch Konkretisierungen und Ergänzungen für ihre Arbeitsmittel (z.B. Auditbericht) sowie die festgestellten Best Practices und erste Grundlagen für die Entwicklung unternehmensspezifischer Kennzahlen. Dadurch war es möglich, bereits erprobte Prozesse zu nutzen oder neue Prozesse direkt hinsichtlich ihrer Angemessenheit und Zielorientierung sowie des daraus folgenden Arbeitsaufwandes zu überprüfen. Großer Wert wurde darauf gelegt zu untersuchen, ob die für die Projektpraxis unumgängliche Flexibilität gewahrt wurde. In diesem Rahmen werden Best Practices, sofern sie allgemein für die heterogene Projektlandschaft tauglich sind, direkt in das Regelwerk aufgenommen bzw. für spezifische Ausprägungen über Multiplikatoren, Qualitätsicherungsverantwortliche und Experten den Projekten zur Verfügung gestellt.

3.1 Erfahrungen und Herausforderungen

Alleine aus einem Projekt heraus sind die Anforderungen der Sicherheitsnormen nicht nur an die Projektergebnisse sondern vor allem auch an den Entwicklungsprozess kaum zu schaffen. Entscheidungen, die sich zu Anfang als sinnvoll und angemessen präsentieren, können über den Projektverlauf zu hohem Aufwand führen und zu einem großen Anteil an repetitiven Tätigkeiten, die gleichzeitig dennoch hohe Konzentration und Sorgfalt verlangen.

Der Vortrag stellt dar, wie sich solche „falschen Freunde“ frühzeitig erkennen lassen und wie beim Projektteam die Kreativität nicht in einer Flut von Dokumentation, Änderungsschleifen und mechanischem Abarbeiten untergeht. Darüber hinaus macht er deutlich, wie ein um die Aspekte der Funktionalen Sicherheit erweitertes Vorgehensmodell, in welches ein konkretes Projekt eingebettet ist, dabei hilft, dass sich Projektteams auf die Lösung der Projektaufgabe konzentrieren können. Und das, ohne dass die Gefahr besteht, Anforderungen aus den Normen zu übersehen. Dadurch bleiben unliebsame Überraschungen zum Projektende aus und Audits können mit Zuversicht und Selbstsicherheit angegangen werden.

3.2 Gestaltungsmöglichkeiten

Sicherheitskritische Projekte haben jederzeit unsere volle Aufmerksamkeit verdient. Auf den ersten Blick macht es die Vielzahl der Anforderungen aber schwer, nicht in Bürokratismus zu verfallen und die Motivation und Freude daran, etwas zu erschaffen aufrecht zu erhalten.

Der Vortrag zeigt, wie ein Projektteam diesen Schock überwinden kann und die Gestaltungsmöglichkeiten innerhalb der Normen nutzt, um Arbeitsmittel zu entwickeln (z.B. Dokumentationsvorlagen, Dictionaries, Argumentationskataloge) und Regeln zu definieren, die den Safety Engineering Process immer flüssiger laufen lassen und so mit angemessenem Aufwand die Wirksamkeit der eingesetzten Methoden optimiert.

Dies können ganz einfache Dinge sein, wie die Proof-of-Concept-Implementierung zur Absicherung der Spezifikation oder die strukturierte Sammlung von Notizen für die nächste Spezifikationstiefe oder Dokumentenversion. Ausnahmen- und Begründungskataloge ermöglichen darüber hinaus eine einheitliche, konsistente Dokumentation und bringen so Erleichterungen über den kompletten Entstehungszyklus von der Erstellung über Review und Freigabe bis hin zum internen und externen Audit.

Dadurch können alle Projektbeteiligten bereits dann kontinuierlich Erfolgserlebnisse erleben, wenn das Projektziel noch weit entfernt scheint und auf dem Weg dorthin noch eine Menge Arbeit zu erledigen ist. Wenn dann die Integration leicht von der Hand geht, Problemursachen schnell gefunden werden und die Auswirkungen von Änderungen offensichtlich sind, genießt das Team den Lohn ohne vorherige Fron.