Peter Maurer

(E-Mail: p.maurer@maurer-treutner.de)
begleitet seine Kunden seit vielen Jahren bei der Einführung von agilen Methoden, in letzter Zeit verstärkt auch im Bereich sicherheitskritscher Systementwicklung.
Er ist seit 1995 Geschäftsführer bei Maurer & Treutner.

Sicherheitskritische Systeme agil entwickeln!

Wenn wir uns ins Auto setzen, durch eine Drehtür gehen, unser Haus mit Gas heizen oder in der Umgebung eines Atomkraftwerks wohnen – täglich müssen wir uns darauf verlassen können, dass die Systeme, die dabei für unsere Sicherheit verantwortlich sind, korrekt entworfen wurden und auch in jeder Situation einwandfrei funktionieren.

Damit das gewährleistet ist, müssen bei der Entwicklung sicherheitskritischer Systeme eine Reihe von Normen eingehalten werden. Die Norm IEC 61508 mit dem Titel „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbar elektronischer Systeme“ wird insbesondere auf Systeme angewendet, bei denen Fehlfunktionen eine Gefahr für Mensch und Umwelt darstellen (http://www.iec.ch/zone/fsafety/Preview.htm).

Diese Norm bezieht sich nicht auf spezielle Anwendungsbereiche, sondern macht allgemeine Vorgaben für Systeme mit funktionaler Sicherheit. Mit der IEC 61508 sind wiederum eine ganze Reihe von weiteren Normen verbunden, die sich eingehend mit sicherheitskritischen Systemen in den verschiedensten Anwendungsbereichen beschäftigen. Als Beispiele seien die Normen IEC 61511 (Prozessindustrie), IEC 62061 (Sicherheit von Maschinen) und für die Kerntechnik die Normen IEC 61513, IEC 62138 sowie IEC 60880 erwähnt.

Das Ziel dieser Normen ist es, Fehler im Entwurf und in der Implementierung zu vermeiden, aufgetretene Fehler rechtzeitig im Entwicklungsprozess zu erkennen und die Auswirkungen möglicher Fehler oder fehlerhafter Bauteile zu begrenzen. Um diese Ziele erreichen zu können, stellen die Normen nicht nur Anforderungen an Entwurf und Implementierung von sicherheitskritischen Systemen, sondern auch an den Entwicklungsprozess und die dabei eingesetzten Methoden. Im Wesentlichen werden eine kontinuierliche Dokumentation der sicherheitsbezogenen Anforderungen, eine Validierung und Verifikation parallel zur Entwicklung sowie ein dokumentierter Entwicklungsprozess verlangt. Eine iterative Entwicklung in vertikalen Ausschnitten ist möglich – dabei muss natürlich gewährleistet sein, dass die sicherheitsbezogenen Anforderungen jederzeit nachvollziehbar sind.

Wie passen nun agile Entwicklungsmethoden mit den Anforderungen der Sicherheitsnormen zusammen? Kann man die agilen Prinzipien so umsetzen, dass gleichzeitig die Sicherheitsaspekte zufriedenstellend berücksichtigt werden?

Um diese Frage beantworten zu können, lohnt sich ein Blick auf die Werte, die im Agilen Manifest (http://agilemanifesto.org/) beschrieben sind:

Individuals and interactions over processes and tools

Im Vordergrund steht bei der Entwicklung sicherheitskritischer Systeme die Aufgabe Fehler zu vermeiden, durch die Schaden oder Gefahr entstehen kann. Um dies zu erreichen ist es nach unserer Erfahrung wichtig, dass zwischen allen beteiligten Entwicklern eine offene und effiziente Kommunikation stattfindet – genau wie es im Agilen Manifest ausdrücklich gefordert wird. Natürlich sind daneben auch prozessorale Maßnahmen und Tools notwendig, die dabei helfen dieses Ziel zu erreichen. Diese können aber nur dann erfolgreich eingesetzt werden, wenn sie einen echten Mehrwert für das Projekt bringen.

Working software over comprehensive documentation

Für die Entwicklung sicherheitskritischer Systeme wird eine ausführliche Dokumentation gefordert, die es insbesondere erlaubt, sicherheitsbezogene Anforderungen über alle Projektschritte hinweg zu validieren und verifizieren. Dies steht nicht im Widerspruch zum Agilen Manifest – zum Nachweis, dass ein sicherheitskritisches System allen Sicherheitsanforderungen genügt, ist die Dokumentation dieser Anforderungen und ihre Validierung unbedingt erforderlich. Sie gehört also zu einer „working software“ unabdingbar dazu.

Customer collaboration over contract negotiation

Bei einer Entwicklung gemäß der IEC 61508 ist es das oberste Ziel zu gewährleisten, dass die Sicherheit von Mensch und

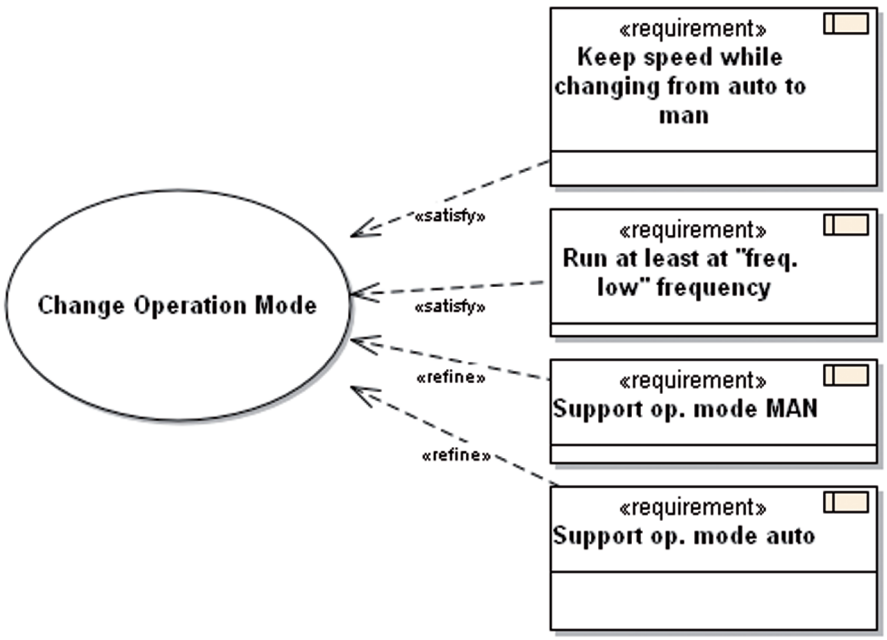

Abbildung 1: Use Case mit Beziehungen zu Requirement

Umwelt nicht gefährdet wird. Dazu ist eine enge und partnerschaftliche Zusammenarbeit zwischen Auftragnehmern und Auftraggeber absolut erforderlich.

Responding to change over following a plan

Auch bei der Entwicklung von sicherheitskritischen Systemen führen immer kürzere Produktlebenszyklen und Konkurrenzdruck dazu, dass sich Anforderungsänderungen während der Entwicklung gar nicht vermeiden lassen. Laut der IEC 61508 muss dabei darauf geachtet werden, dass die Änderungen validiert und verifiziert werden, die Anforderungen dürfen in Hinblick auf die Sicherheit dadurch nicht gefährdet werden. Wird dies erfüllt, spricht nichts dagegen, neue und veränderte Requirements aufzunehmen. Im Gegenteil – tiefere Kenntnis der Materie führt ja gerade zu mehr Sicherheit!

Die Vorteile einer agilen Vorgehensweise werden noch deutlicher, wenn wir nun einige Prinzipien, die hinter dem Agilen Manifest stehen, betrachten und uns überlegen, wie sie bei der Entwicklung sicherheitskritischer Systeme umgesetzt werden können.

Our highest priority is to satisfy the customer through early and continuous delivery of valuable software.

Dieses Prinzip schafft die Grundlage eines vertrauensvollen Verhältnisses zwischen dem Kunden und dem Entwickler. Gerade bei Systemen mit sicherheitsbezogenen Funktionen ist das besonders wichtig, denn hier müssen eventuelle Missverständnisse so früh wie möglich aufgedeckt und ausgeräumt werden. Zu einer wertvollen Software gehören für diese Systeme auch die in den Sicherheitsnormen geforderten Dokumentationen. Hier ist insbesondere wichtig, dass ein Requirements-Management erfolgt, das die Anforderungen an die Traceability berücksichtigt. Zum Einsatz gelangen an dieser Stelle klassische Requirements-Management-Tools wie DOORS oder CaliberRM. In Bereichen, in denen diese Tools nicht explizit verlangt werden, ist es aber auch möglich, das Requirements-Management auf Basis der SysML-Requirements in einem entsprechenden UML-Tool durchzuführen.

Neben der Dokumentation der Requirements ist es in unseren Augen für die Validierung sicherheitskritischer Systeme unumgänglich, auch die essenziellen Use Cases mit ihren Beziehungen zu den Requirements im Rahmen eines UML-Modells zu dokumentieren.

Welcome changing requirements, even late in development. Agile processes harness change for the customer's competitive advantage

Werden alle notwendigen Validierungs- und Verifikationsschritte durchlaufen, spricht grundsätzlich nichts dagegen, auch späte Änderungen an den Requirements auch bei der Entwicklung sicherheitskritischer Systeme zu ermöglichen. Trotzdem empfiehlt es sich, frühzeitig ein möglichst vollständiges Requirements-Modell zu haben, da die Validierung neuer Requirements im Zusammenhang mit sicherheitsbezogenen Anforderungen ziemlich aufwändig ist.

Deliver working software frequently, from a couple of weeks to a couple of months, with a preference to the shorter timescale.

Dieses Prinzip beinhaltet ein iteratives Vorgehen bei der Entwicklung, wie es z.B. in den Sprints von Scrum umgesetzt wird. Für die Entwicklung sicherheitskritischer

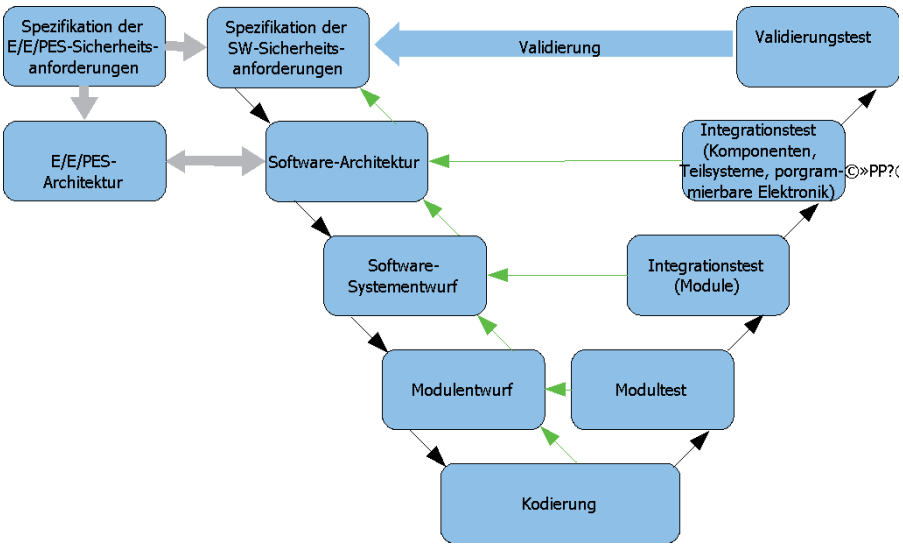

Abbildung 2: Die im Rahmen einer Iteration notwendigen Schritte des V-Modells

Systeme ist es dabei unumgänglich, dass in jedem Iterationsschritt die wesentlichen Elemente des V-Modells durchlaufen werden. Insbesondere an den Test werden dadurch sehr hohe Anforderungen gestellt. Dies lässt sich auf der Ebene der Module entsprechend dem Test Driven Development (wie es zum Beispiel auch im Rahmen von eXtreme Programming beschrieben wird) verwirklichen. Auf der Grundlage von Unit-Tests haben wir in unseren Projekten die Anweisungsüberdeckung gemessen und dokumentiert – so können wir durch die Entkopplung beim Test einen sehr hohen Überdeckungsgrad erreichen. Diese Informationen sind wertvoll für die gesamte Verifikation des Systems. Die Ergebnisse der Unit-Tests sind natürlich Teil der Dokumentation. Das alles kann natürlich Integrations- und Systemtests nicht ersetzen, stellt aber eine wertvolle Ergänzung dar.

Business people and developers must work together daily throughout the project

Der Begriff Business People erscheint im Zusammenhang mit der Entwicklung von Embedded Systems zunächst ungewohnt – wir verstehen darunter die Experten, die mit dem Einsatz der Systeme vertraut sind. Gerade bei der Analyse der Sicherheitsanforderungen spielen sie eine herausragende Rolle, da sie aus ihrer Praxis die kritischen Punkte meist am besten beurteilen können. Wir halten es daher für unumgänglich, solche Anwender eng in die Entwicklung einzubinden. Auch hier fördert Agilität Vorgehensweisen, die im Endeffekt zu größerer Sicherheit beitragen!

Build projects around motivated individuals. Give them the environment and support they need, and trust them to get the job done.

The most efficient and effective method of conveying information to and within a development team is face-to-face conversation.

Sehr oft spielen bei sicherheitskritischen Systemen Aspekte der Konstruktion, Elektronik und Software eng zusammen. Deshalb empfiehlt es sich Teams zu bilden, in denen Experten aus allen Bereichen zusammenarbeiten. Durch die gemeinsame Arbeit wächst bei allen das Verständnis für das Gesamtsystem und es ist möglich, Probleme gemeinsam zu analysieren und an der richtigen Stelle zu lösen. Allerdings treten gerade zu Beginn in interdisziplinären Teams häufig Verständigungsprobleme auf, da unterschiedliche Begriffswelten aufeinanderstoßen. Am Anfang der Teamarbeit steht deshalb immer eine Begriffsklärung. Wir empfehlen dazu ein gemeinsames Projektglossar, in dem die Verwendung der Fachbegriffe des Projekts definiert und das über die gesamte Entwicklungszeit fortgeschrieben wird.

Allerdings erweist sich der hohe Grad an Expertentum oft als Problem, da es sich nicht vermeiden lässt, dass bestimmte Mitarbeiter mit speziellem Know-how gleichzeitig in mehreren Projekten eingesetzt werden. Es ist deshalb erforderlich, die Iterationen aller Projekte innerhalb einer Organisation zu synchronisieren und die entsprechenden Mitarbeiter zwischen den Projektteams zu teilen. Als vorteilhaft hat es sich dabei erwiesen, wenn ein Mitarbeiter innerhalb eines Iterationsschrittes nur in einem Projekt arbeitet, da dadurch Zielkonflikte zwischen den Projekten vermieden werden.

Working software is the primary measure of progress.

Wie oben ausgeführt, gehören die durch die Sicherheitsnormen geforderten Dokumente zu jeder Auslieferung dazu. Ein Problem bei der iterativen Entwicklung von Embedded Systems (nicht nur für sicherheitskritische Systeme) stellt die unterschiedliche Geschwindigkeit in den verschiedenen Disziplinen dar. Die lauffähige Software, die am Ende einer Iteration präsentiert wird, muss deshalb gerade in frühen Phasen häufig auf Evaluierungsplattformen laufen. Neben der lauffähigen Software sind auch die Zwischenresultate aus der Elektronikentwicklung und der Konstruktion (z.B. Schaltpläne, Schaltungslayouts, 3-D-Modelle, verschiedene Prototypen) ein wichtiges Maß für den Projektfortschritt und können zur Präsentation von Iterationen mit herangezogen werden.

Continuous attention to technical excellence and good design enhances agility.

Simplicity – the art of maximizing the amount of work not done – is essential.

Agiles Vorgehen zeichnet sich dadurch aus, dass nur die Dinge getan werden, die für das Produkt einen Mehrwert bringen. Wie schon weiter oben ausgeführt gehören für sicherheitskritische Systeme unbedingt auch Modelle dazu, aus denen die Architektur und ihr Bezug zu den sicherheitsbezogenen Anforderungen hervorgehen. Die Forderung nach Einfachheit darf nicht dazu führen, dass für die Sicherheit des Systems wichtige Elemente verloren gehen.

Fazit:

Agilität und Anforderungen an sicherheitskritische Systeme passen sehr gut zusammen, wenn man dabei alle kritischen Punkte im Auge behält und das Prinzip Agilität nicht über alles andere stellt.

Gerade die Forderung nach einer engen Zusammenarbeit sowohl innerhalb des Entwicklungsteams als auch zwischen Kunden und Lieferant sorgt für ein tiefes Verständnis der Aufgabe und kann damit ein wichtiger Baustein für die Einhaltung der in den Normen geforderten Sicherheitskriterien sein.

Sind Sie interessiert an diesem Thema? Wir begleiten unsere Kunden seit Jahren bei der Einführung von agilen Methoden und habe dabei auch umfangreiche Erfahrungen bei der Entwicklung von Systemen mit sicherheitsbezogenen Funktionen gesammelt. Wenn Sie Fragen haben – sprechen Sie uns an! ■