Agile und sicherheitsgerichtete Softwareentwicklung – Widerspruch oder Chance?

Gudrun Neumann, 15.10.2015

SGS TÜV SAAR

WHEN YOU NEED TO BE SURE

SGS

AGENDA

- Definitionen
- Werte agiler Softwareentwicklung
  - Menschen und Interaktionen stehen über Prozessen und Werkzeugen
  - Funktionierende Software steht über einer umfassenden Dokumentation
  - Zusammenarbeit mit dem Kunden steht über der Vertragsverhandlung
  - Reagieren auf Veränderung steht über dem Befolgen eines Plans
- Zusammenfassung

SGS-TÜV SAAR GMBH

- SGS-TÜV Saar GmbH / Funktionale Sicherheit
  - Joint-Venture zwischen SGS-Gruppe und TÜV Saarland
  - Global Competence Center - Funktionale Sicherheit
    - Zentrale in München, Zweigstelle in Dortmund
    - Lokale Expertenteams in Japan, China, Taiwan und Korea
    - Gem. ISO/IEC 17025 akkreditierte Prüfstelle für Funktionale Sicherheit
    - Mitglied bei den relevanten Standardisierungsgremien, wie z.B. IEC 61508, ISO 26262 und E-Mobilität

SICHERHEITSGERICHTETE ENTWICKLUNG
(DIN EN 62304:2007)

- 3.21 SICHERHEIT
  - Freiheit von unvertretbaren RISIKEN
- 3.16 RISIKO
  - Kombination der Wahrscheinlichkeit des Auftretens eines Schadens und des Schweregrades dieses Schadens
- 3.12 MEDIZINPRODUKTE-SOFTWARE
  - ein Software-System, das entwickelt wurde, um in das in der Entwicklung befindliche Medizinprodukt integriert zu werden, oder das für die Benutzung als selbständiges Medizinprodukt vorgesehen ist.

AGILE PROZESSE

- www.duden.de: Suche nach **AGIL** ergibt
  - von großer Beweglichkeit zeugend; regsam und wendig
  - Betriebsam, beweglich
- Das Fundament der agilen Prozess-Philosophie bilden vier Grundwerten:
  - Menschen und Interaktionen stehen über Prozessen und Werkzeugen
  - Funktionierende Software steht über einer umfassenden Dokumentation
  - Zusammenarbeit mit dem Kunden steht über der Vertragsverhandlung
  - Reagieren auf Veränderung steht über dem Befolgen eines Plans

AGENDA

- Definitionen
- Werte agiler Softwareentwicklung
  - Menschen und Interaktionen stehen über Prozessen und Werkzeugen
  - Funktionierende Software steht über einer umfassenden Dokumentation
  - Zusammenarbeit mit dem Kunden steht über der Vertragsverhandlung
  - Reagieren auf Veränderung steht über dem Befolgen eines Plans
- Zusammenfassung

Verfahren für Menschen und Interaktionen
(DIN EN ISO 13845:2012)

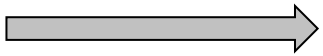
- 5.5.1 Verantwortung und Befugnis
  - Die oberste Leitung muss sicherstellen, dass die Verantwortungen und Befugnisse festgelegt, dokumentiert und innerhalb der Organisation bekannt gemacht werden. Die oberste Leitung muss die gegenseitigen Beziehungen aller Personen festlegen, …
- 5.5.3 Interne Kommunikation
  - Die oberste Leitung muss sicherstellen, dass geeignete Prozesse der Kommunikation innerhalb der Organisation eingeführt werden und dass eine Kommunikation über die Wirksamkeit des Qualitätsmanagementsystems stattfindet.
- 7.3.1 Design- und Entwicklungs-…
  - Die Organisation muss die Schnittstellen zwischen den verschiedenen an dem Design und der Entwicklung beteiligten Gruppen leiten und lenken, um eine wirksame Kommunikation und eine klare Zuordnung der Verantwortung sicherzustellen.

WERKZEUGE FÜR MENSCHEN UND INTERAKTIONEN (DIN EN 60601:2007)

- 14.6.2 Risikobeherrschung
  - … Für die Implementierung jeder Maßnahme der Risikobeherrschung müssen angemessen validierte Werkzeuge und Verfahren ausgewählt und festgelegt werden.
- 14.10 Verifizierung
  - die Auswahl und die Anwendung von Verifizierungswerkzeugen;

AGENDA

- Definitionen
- Werte agiler Softwareentwicklung
  - Menschen und Interaktionen stehen über Prozessen und Werkzeugen
  - Funktionierende Software steht über einer umfassenden Dokumentation
  - Zusammenarbeit mit dem Kunden steht über der Vertragsverhandlung
  - Reagieren auf Veränderung steht über dem Befolgen eines Plans
- Zusammenfassung



FUNKTIONIERENDE SOFTWARE
(DIN EN 62304:2007)

- 5.6.4 Inhalt der Integrationsprüfung
  - Bei der Prüfung der Software-Integration muss der Hersteller darauf achten, ob die integrierte Softwarekomponente wie beabsichtigt funktioniert.
- 5.7.1 Festlegung von Prüfungen für Software-Anforderungen
  - Der Hersteller muss einen Satz von Prüfungen festlegen und durchführen, die durch Angabe von Eingabewerten, erwarteten Ausgaben, Pass/Fail-Kriterien und Verfahren zur Durchführung von Softwaresystem-Prüfungen so beschrieben sind, dass alle Software-Anforderungen abgedeckt werden.

DOKUMENTATION
(DIN EN 62304:2007)

- 5.7.5 Inhalte der Aufzeichnungen der Software-System-Prüfungen
  - Der Hersteller muss:
    a) das Prüfergebnis dokumentieren (Pass/Fail und eine Liste der Anomalien),
    b) genügend Aufzeichnungen aufbewahren, um die Wiederholung von Prüfungen zu erlauben, …
- 5.1.8 Planung der Dokumentation
  - Der Hersteller muss Informationen über die Dokumente, die während des Software-Entwicklungszyklus erzeugt werden sollen, in den Software-Entwicklungsplan mit einschließen oder in diesem referenzieren. …

AGENDA

- Definitionen
- Werte agiler Softwareentwicklung
  - Menschen und Interaktionen stehen über Prozessen und Werkzeugen
  - Funktionierende Software steht über einer umfassenden Dokumentation
  - Zusammenarbeit mit dem Kunden steht über der Vertragsverhandlung
  - Reagieren auf Veränderung steht über dem Befolgen eines Plans
- Zusammenfassung

ZUSAMMENARBEIT MIT DEM KUNDEN

- DIN EN 60601:2007; 14.7 Anforderungsspezifikation
  - … Die Anforderungsspezifikation für ein System oder Subsystem muss diejenigen wesentlichen Leistungsmerkmale und Maßnahmen der Risikobeherrschung enthalten und unterscheiden, die durch dieses System oder Subsystem verwirklicht werden.
- DIN EN 62304:2007; 5.2.2 Inhalt der Software-Anforderungen
  - Soweit angemessen muss der Hersteller in die Software-Anforderungen für die Medizinprodukte-Software
  - Folgendes einschließen:

    a) Anforderungen an die Funktionalität und die Leistungsfähigkeit; z.B. Notwendigkeit der Kompatibilität mit Nachrüstungen …

VERTRAGSVERHANDLUNGEN

- DIN EN ISO 13845:2012; 7.2.2 Bewertung der Anforderungen in Bezug auf das Produkt
  - **...** Wenn der Kunde keine dokumentierten Anforderungen vorlegt, müssen die Kundenanforderungen vor der Annahme von der Organisation bestätigt werden.
- Gesetzliche Anforderungen, wie z.B. MPG, sind zu beachten
- Aus Haftungsgründen sind vertragliche Vereinbarungen sehr zu empfehlen

AGENDA

- Definitionen
- Werte agiler Softwareentwicklung
  - Menschen und Interaktionen stehen über Prozessen und Werkzeugen
  - Funktionierende Software steht über einer umfassenden Dokumentation
  - Zusammenarbeit mit dem Kunden steht über der Vertragsverhandlung
  - Reagieren auf Veränderung steht über dem Befolgen eines Plans
- Zusammenfassung

BEFOLGEN EINES PLANS (DIN EN 62304:2007)

- 5.1.1 Software-Entwicklungsplan
  - … Der Plan muss folgende Punkte umfassen:
  - a) die Prozesse, die bei der Entwicklung des Software-Systems verwendet werden
  - b) die zu liefernden Ergebnisse der Aktivitäten und Aufgaben;
  - c) Rückverfolgbarkeit zwischen System-Anforderungen, Software-Anforderungen, Software-System Prüfungen und Risikokontroll-Maßnahmen, die in Software implementiert werden
  - d) Software-Konfigurations- und Änderungsmanagement, einschließlich „Software Of Unknown Provenance“ (SOUP) - Konfigurationselementen und Software, die zur Entwicklungsunterstützung verwendet wird
  - e) Software-Problemlösung und Behandlung von Problemen, …

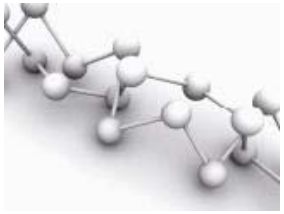
REAGIEREN AUF VERÄNDERUNG

- 6.2.1.2 Dokumentation und Evaluation von Rückmeldungen
  - Rückmeldungen müssen dokumentiert und daraufhin evaluiert werden, ob ein Problem in einem freigegebenen Softwareprodukt besteht. Jedes Problem muss als Problembericht aufgezeichnet werden.
- 6.2.1.3 Evaluation von Problemberichten auf Auswirkungen auf die Sicherheit
  - Jeder Problembericht muss evaluiert werden um festzustellen, inwieweit die Sicherheit eines freigegebenen Softwareprodukts betroffen ist, und ob eine Änderung des freigegebenen Softwareprodukts erforderlich ist, um das Problem zu adressieren.

AGENDA

- Definitionen
- Werte agiler Softwareentwicklung
  - Menschen und Interaktionen stehen über Prozessen und Werkzeugen
  - Funktionierende Software steht über einer umfassenden Dokumentation
  - Zusammenarbeit mit dem Kunden steht über der Vertragsverhandlung
  - Reagieren auf Veränderung steht über dem Befolgen eines Plans
- Zusammenfassung

ZUSAMMENFASSUNG



- Im Mittelpunkt sicherheitsgerichteter Software-Entwicklung steht der Mensch
- Jedes Teammitglied muss den Regeln für die Kommunikation und Zusammenarbeit zustimmen
- Dokumentation ist notwendig um sich auf neue Projekte konzentrieren zu können
- Vertragliche Vereinbarungen sind wegen der gesetzlichen Anforderungen notwendig (Produkthaftung)

Keep It Simple and Safe

= KISS

Danke für Ihre Aufmerksamkeit

IHR PARTNER ZUR FUNKTIONALEN SICHERHEIT

SGS-TÜV Saar GmbH

Functional Safety

Hofmannstrasse 50

D-81379 Muenchen

Germany

www.sgs-tuev-saar.com/fs

Gudrun Neumann

Product Manager Functional Safety Software

Industrial Functional Safety Expert IFSE

Automotive Functional Safety Expert AFSE

E-Mail: gudrun.neumann@sgs.com

Phone: +49 89 787 475 -216

Fax: +49 89 787 475 -217