solcept
electronics • software

Vom funktionierenden zum sicheren Produkt

ein Erfahrungsbericht zur
Einführung von funktionaler Sicherheit

Andreas Stucki, Solcept AG

Was erwartet Sie?

Wie sind wir zu Safety gekommen?

Was haben wir generell gelernt?

Was haben wir bezüglich Fähigkeiten gelernt?

Was haben wir bezüglich Werkzeugen gelernt?

Was haben wir bezüglich Management gelernt?

Was möchten Sie noch wissen?

Ausgangslage: Steuerungen
2003..jetzt

Entwicklungsdienstleister mit 17 Mitarbeitern

Schlüsselthemen

- **Systemanforderungen**
- **Funktion (und nicht-funktionale Anforderungen)**

CMMI-DEV Level 2
2011

Schlüsselthemen

- **adäquat**
- **strukturiertes Projektmanagement (inkl. Risikomanagement)**
- **Prozess-Fokus statt Produkt-Fokus**

CMMI-DEV Level 2
2011

Änderungen

- **Feedback-Schleifen: kontinuierliche Verbesserung/ Peer Qualitätssicherung**
- **systematisches Herangehen an Prozesse**

Entscheide

- **Management Commitment: „go for it“**

Avionik
2013

Schlüsselthemen

- **Engineering**
- **Software Design („High Level Requirements“)**
- **Hardware**

Avionik
2013

Änderungen

- **Anforderungsmanagement: Traceability, 3 Stufen: System, High Level, Low Level**
- **EASA: Stages of Intervention**

Entscheide

- **Prozesse Industrie-agnostisch („If you use the standard after writing processes and plans, you have a Problem“ Hilderman)**

Medizintechnik
2014

Schlüsselthemen

- **Design**
- **statische Code Analyse**

Medizintechnik
2014

Änderungen

- **einige Umbenennungen**

Entscheide

- **ad-hoc, projektspezifisch implementiert**

CMMI-DEV Level 3
2016

Schlüsselthemen

- **Technische Umsetzung**
- **Organisationsfokus: Prozesse der Organisation**

CMMI-DEV Level 3
2016

Änderungen

- **Peer Qualitätssicherung verbessert**
- **Training**

Entscheide

- **keine (Entwicklung der Prozesse seit Level 2)**

Automotive
2016

Schlüsselthemen

- **Software Low Level**
- **Sicherheitsanalysen**

Automotive
2016

Änderungen

- **Safety Plan/ Safety Case**
- **Development Interface Agreement**
- **Rollen**

Entscheide

- **TÜV als Qualitätssicherung (Conformation Measures)**

Was erwartet Sie?

Wie sind wir zu Safety gekommen?

Was haben wir generell gelernt?

Was haben wir bezüglich Fähigkeiten gelernt?

Was haben wir bezüglich Werkzeugen gelernt?

Was haben wir bezüglich Management gelernt?

Was möchten Sie noch wissen?

Generell: Missverständnisse

Funktionale Sicherheit: Einfache ein weiteres Feature?

- **wenige Buchstaben führen zu viel Aufwand**

Was ist „normal“?

- **QM/ DAL E... ist mehr als „normale“ Industrie-Software**

Man wird doch wohl etwas abkürzen können!

Was erwartet Sie?

Wie sind wir zu Safety gekommen?

Was haben wir generell gelernt?

Was haben wir bezüglich Fähigkeiten gelernt?

Was haben wir bezüglich Werkzeugen gelernt?

Was haben wir bezüglich Management gelernt?

Was möchten Sie noch wissen?

Fähigkeiten: Anforderungsmanagement

Anforderungen & Design schreiben

- **Abstraktionsebene adäquat**
- **Ingenieurs-Job?**

Anforderungs-Architektur

- **angepasst an das Produkt**
- **Software, HDL-Code, System, Schnittstellen...**

Fähigkeiten: Änderungsmanagement

Issue-Tracker basiert

- **Workflow**
- **CCB**

Dokumentations-, Review- und Releaseplanung

- **früh, als Startpunkt für Änderungsmanagement**
- **von Gesamtintegration & Verträgen abhängig**

Fähigkeiten: Sicherheitsanalysen

Typen

- **FME(D)A, FTA, PHA...**

Bereich

- **System, Software, Hardware**
- **Produkt, Design**
- **sinnvolle Software-FMEA**

Fähigkeiten: Design

Abstraktion

Mindset

Was erwartet Sie?

Wie sind wir zu Safety gekommen?

Was haben wir generell gelernt?

Was haben wir bezüglich Fähigkeiten gelernt?

Was haben wir bezüglich Werkzeugen gelernt?

Was haben wir bezüglich Management gelernt?

Was möchten Sie noch wissen?

Werkzeuge: Generell

A fool with a tool is still a fool... (R. Weinstein)

- **Nicht immer von Fähigkeiten zu trennen**

Wichtiger als bei „normalen“ Projekten

- **mehr automatisierbare Qualitätssicherung**

Open Source & Qualifizierbarkeit

Werkzeuge sind sehr unterschiedlich in Qualität

Werkzeuge: Anforderungen

Für den ganzen Lebenszyklus

- **Schreiben**
- **Review**
- **Änderungen**
- **Coverage/ Traceability**

Werkzeuge: Konfigurationsmanagement

Vor allem gute Prozesse

- **Wie wird das Werkzeug verwendet**

Planung

- **Ein Repository für alles unter Konfigurationsmanagement**
- **Welche Repositories für was (z.B. Wiki)**

Was erwartet Sie?

Wie sind wir zu Safety gekommen?

Was haben wir generell gelernt?

Was haben wir bezüglich Fähigkeiten gelernt?

Was haben wir bezüglich Werkzeugen gelernt?

Was haben wir bezüglich Management gelernt?

Was möchten Sie noch wissen?

Management: Commitment

Ressourcen bereitstellen

- **Prozesse (entwickeln und warten)**
- **Training**
- **Projekte (mehr als „normal“)**

Mindset

- **Haftung vs. „Effizienz“ (es läuft ja schon!)**

Management: Sicherheitskultur

Der Fisch stinkt vom Kopfe...

Gratwanderung Haftung-Effizinz

Systematische Fehler gibt es, ausser natürlich bei uns

Paradigmen-Wechsel für alle

- **Ingenieur – Projektleiter – Produktmanager - Geschäftsführung**

Management: Zusammenarbeit mit Dritten

Development Interface Agreement

Aufgabe	Ergebnis	Format/ Tool	Verantwort-lichkeiten Partei 1	Verantwort-lichkeiten Partei 2	Verantwort-lichkeiten Partei 3
System Design					
System Definition	System Requirement Specification (“Lastenheft”)	PDF/ ODF	Consult	Review & Release	Responsible
System Design	System Specification (“Pflichten-heft”) System Architecture	PDF/ ODF	Uninvolved	Audit/ Inform	Responsible

Management: Externer Support

Gap Analysen

- **Standards sind nicht immer so klar...**
- **Acceptable Level of Compliance**

Qualitätssicherung

- **TÜV/ notified body/ EASA**
- **Unabhängigkeit/ Liability**

Was erwartet Sie?

Wie sind wir zu Safety gekommen?

Was haben wir generell gelernt?

Was haben wir bezüglich Fähigkeiten gelernt?

Was haben wir bezüglich Werkzeugen gelernt?

Was haben wir bezüglich Management gelernt?

Was möchten Sie noch wissen?

Fragen?
Diskussion

kontaktieren Sie mich:

Andreas Stucki, Solcept AG

a.stucki@solcept.ch

+41 (0)43 477 40 63

Änderungsverzeichnis

Version	Entwurf/ für Review/ Freigegeben	Datum	Verant-wortlich	Kommentare/ Änderungsverlauf
00.01	Entwurf	2018-08-17	a2s	first draft
01.00	Freigegeben	2018-08-22	a2s	kleine Änderungen nach Paper, Typos