Experten-Statements und Ratschläge zu Qualität und Sicherheit

Im Zuge der Recherchen zum Artikel „Den Drachen bändigen“ in der E&E Oktober 2011 haben wir mehrere Experten befragt. Im Folgenden finden Sie eine Zusammenfassung ihrer Aussagen und Ratschläge in alphabetischer Reihenfolge der befragten Experten.

Gestellte Fragen:

A) Wo sehen Sie die häufigsten und schwerwiegendsten Defizite im Bereich Qualitätssicherung, wenn es um Safety geht?

B) Wo sehen Sie die häufigsten und schwerwiegendsten Irrtümer im Bereich Qualitätssicherung, wenn es um Safety geht?

C) Was sind Ihre wichtigsten Tipps zu Maßnahmen, um diesen Defiziten entgegenzuwirken?

Dr. Günter Glöe, Geschäftsführer CATS Software Tools GmbH , Dozent für Qualitätssicherung, MicroConsult GmbH

A) Defizite:

1. Das Management hat Safety nicht auf dem Schirm und meint, dieses als lästig empfundene Thema auf „Werksstudenten“ oder Externe abwälzen zu können. (Die Verantwortung für die Sicherheit bleibt im Unternehmen.)
2. Technikern ist nicht bewusst, dass die Safety-Standards den Stand unserer Technik widerspiegeln und unsere Arbeit – wenn wir diesen Standards nicht gerecht werden – handwerklich / ingenieurmäßig mangelhaft ist.

B) Irrtümer:

1. Testen ist besonders wichtig, um Sicherheit zu erreichen.
   Richtig ist: Qualität und Sicherheit werden nicht erprüft, sie werden konstruiert /gefertigt. Oder anders: Vom Wiegen wird die Sau nicht fett, und die Elektronik und deren Software werden vom Testen nicht sicher.
2. Wenn etwas mit der Aufgabenstellung nicht stimmt, z.B. die Sicherheitskritikalität nicht ausgewiesen ist, liegt die Schuld (ausschließlich) beim Auftraggeber, und der Lieferant muss sich nicht kümmern.
   Richtig ist: Der Lieferant hat die Verantwortung für sein Produkt.
3. Der Grobentwurf (Architectural Design) spielt keine besondere Rolle für die Sicherheit.
   Richtig ist: Im Grobentwurf werden die Weichen für ein verträgliches Miteinander von Nutzfunktion und Sicherheit - z.B. hinreichende Selbstüberwachung - gestellt.
4. Es gibt keine juristischen (gerichtlichen) Auseinandersetzungen um die Sicherheit von Elektronik und deren Software.
   Richtig ist: Es gibt sie sehr wohl, und sie können sehr langwierig und kostspielig sein.

5. Software = Code
   Richtig ist: Software besteht aus Code, Daten und der zugehörigen Dokumentation, die etwa 30 verschiedene Informationen umfasst.

C) Tipps

1. Sicherheitsstandards sind Kochrezepte für den Stand der Technik, konforme Elektronik und Software. Kochrezepte muss man für die eigene Küche anpassen und Standards begründet auf den eigenen Bedarf.
2. Sicherheit ist nicht komplett vorhanden oder fehlt völlig. Auch kleine Schritte sind – wenngleich nicht immer ausreichend – so doch nützlich.
3. Ingenieurstätigkeiten unterscheiden sich vom Basteln auch dadurch, dass sie geplant ablaufen. Die Planung der Prüfarbeiten (z.B. Test, Review) erfolgt parallel mit der Entwicklung des Arbeitsproduktes, gegen das geprüft werden soll. So erfolgt z.B. die Planung der Validierung der fertigen Elektronik / Software parallel zum Erfassen der Aufgabenstellung.

Dieter Volland, MicroConsult GmbH, Dozent für Software Engineering

A) Defizite

1) Häufigste Fehler in Zusammenhang mit Sicherheit und QS
2) Schlechte Ausbildung, mangelhafte Fachkenntnis
3) Fehlender Überblick, fehlende Sensibilität der Projektbeteiligten (GF, V, M, QS;...)
4) Es wird viel gepfuscht (Zeitdruck, Hauptsache es läuft), man ist zum Pfuschen gezwungen
5) Schnittstellen Vertrieb, Marketing, Entwicklung, Qualitätssicherung
6) Anerkennung der QS-Notwenigkeit (auch in Form von Zeit und Zuspruch)
7) MUSS statt Überzeugung
8) Wenig Zeit für Innovation, Lessons Learned, Veränderung (Erfahrung = Summe Erfahrungen)

B) Tipps

1. Gute Ausbildung
2. Unternehmensweites Verständnis für die Bedürfnisse und Notwendigkeiten der Qualitätssicherung
3. Mut zur Veränderung
4. Lessons Learned: Aus den Fehlern vergangener Projekte lernen

Frank Listing, MicroConsult GmbH, Dozent für Software Engineering

A) Defizite

1. Fehlende Ausbildung der Entwickler (fachlich meistens gut, aber bei der SW-Entwicklung gibt es Schwachstellen).
2. Unpassende oder nicht gelebte Prozesse (vor allem Vertrieb und Marketing klinken sich gerne aus – dadurch kann schon mal ein Projekt kippen).

B) Tipps

1. Regelmäßige Weiterbildungen.
2. Dokumentation von Regelverstößen, um Ursachen von Verzögerungen usw. aufzuzeigen. Ansonsten ist wieder mal die Entwicklung Schuld und nichts ändert sich.

Prof. Dr. Jürgen Mottok, Scientific Head of Laboratory for Safe and Secure Systems Faculty of Electrical Engineering and Information Technology Regensburg University of Applied Sciences

Unter „Technischer Sicherheit" wird begrifflich verstanden, dass ein technisches System, eine Anlage, ein Produkt über einen geplanten Zeitraum (gegebenenfalls die geplante Lebensdauer) hinweg die vorgesehenen Funktionen erfüllt und bei bestimmungsgemäßer Nutzung keine geschützten Rechtsgüter verletzt, d.h. weder Personen noch Sachen geschädigt werden, soweit dafür das System, die Anlage oder das Produkt ursächlich sein können. Die Zuverlässigkeit der Funktion über die vorgesehene Lebensdauer ist kein notwendiger Bestandteil der Sicherheit, sofern der Verlust der Funktion zu keinem unsicheren Zustand führt.
Quelle: Qualitätsmerkmal, „Technische Sicherheit" - Eine Denkschrift des Vereins Deutscher Ingenieure, Düsseldorf, 2007

A) Defizite

1. Ermittlung des Standes der Technik nicht durchgeführt.
2. Die Weiterbildung der Mitarbeiter ist nicht zielgerichtet.
3. Auswahl und Einsatz der Werkzeuge bzw. Methoden ist unzureichend vorbereitet.
4. Risikomanagement unzureichend umgesetzt.
5. Die Anforderungen und Qualitätsmerkmale sind unvollständig festgelegt.
6. Die Schulung der Anwender wurde vernachlässigt.
7. Controlling der Technischen Sicherheit im Produkt-Lebenszyklus
8. Eine Abnahme der Phasenergebnisse erfolgt unzureichend.
9. Es wird nicht systematisch bzw. unzureichend getestet.

B) Irrtümer

1. Definition von Rollen ergibt noch keinen Sicherheitsprozess; Etablierung eines gelebten Prozess nötig!
2. „Zero Defects" sind zwar wünschenswert, aber physikalisch nicht zu erreichen, Werner von Siemens, 1880: „Sicherheit in automatisierten Prozessen ist nicht nur eine Frage menschlicher Verpflichtung ist, sondern auch von wirtschaftlicher Vernunft."
   D.h. die Betriebssicherheit eines technischen Systems versteht sich als die Reduktion des Risikos auf ein (wirtschaftlich) vertretbares Maß. Damit verbleiben tolerierbare Restfehler in unseren technischen Systemen. Geeignete Fehlererkennung und -reaktionen müssen umgesetzt werden.

C) Tipps

1. Vollständigen Review-Prozess für sicherheitsrelevante Software etablieren, z.B. Fagan-Review
2. Formale Spezifikationstechniken einführen

3. Modellbasiertes Testen anwenden
4. W-Modell als Erweiterung des V-Modells anwenden, das man auch als einen Ansatz von Test-Driven-Development nutzen kann
5. Mitarbeiter in die Qualitätskultur des Unternehmens integrieren
6. Mitarbeiter an der Ausgestaltung des Unternehmensleitbildes integrieren
7. Eine offene Veränderungskultur ausgestalten, an der jeder Mitarbeiter partizipiert
8. Lernende Organisation, Wissen der Mitarbeiter nutzen und weiter entwickeln
9. Qualifikationsplan in der Personalführung anwenden
10. Mut und Respekt (siehe auch agile Softwareentwicklung) zur Potentialentfaltung in der Softwareorganisation nutzen
11. Mut haben, eigene Fehler offen anzusprechen
12. Respekt vor den anderen Softwareentwicklern

Christian Nachreiner, Geschäftsführer iNTENCE automotive electronics

A) Defizite

1. Ist mein Projekt FUSI (Funktionale Sicherheit, FuSi, ISO 26262)?
   Häufig wird diese Frage nicht ausreichend geklärt.
2. In fast allen Projekten ist die fehlende Verzahnung der Teststufen ein Problem. Dadurch können „weiße Flecken“ in der Testabdeckung entstehen, die in einem Safety-Projekt nicht akzeptabel sind.

B) Irrtümer

1. Der Auftraggeber hat das Projekt als nicht FUSI relevant definiert. Damit sind wir aus dem Schneider…
2. FUSI betrifft nur die Hardware..
3. FUSI, darum kümmert sich unser FUSI-Manager

C) Tipps

1. Teststufenübergreifende Testkonzepte.
2. Einführung einer Rolle in der Entwicklung, welche die Tests auf allen Ebenen von der Implementierung bis zum Prüflabor betrachtet.“

MicroConsult Trainings zum Thema

Qualität & Sicherheit

Software- & Vertragsrecht

Test & Debug

Alle Trainings und Termine sowie Coachingangebote

MicroConsult
Microelectronics Consulting & Training GmbH
Charles-de-Gaulle-Str. 6, 81737 München
Tel. +49 89 450617-71
info@microconsult.de
www.microconsult.de

Oktober 2011/Rev. 06/18