MICRO CONSULT

Den Drachen bändigen – Sichere Software von Anfang an (Teil 3)

Das sagen die Experten

Im Zuge der Recherchen zum Beitrag „Den Drachen bändigen – Sichere Software von Anfang an“ hat MicroConsult Embedded-Experten befragt und Ratschläge wie Statements zu Qualität und Sicherheit erhalten, die wir in den folgenden Punkten zusammengefasst haben.

Die häufigsten und schwerwiegendsten Defizite zu Safety im Bereich Qualitätssicherung

1. Das Management erkennt die Wichtigkeit von Safety nicht und wälzt das Thema auf „Werkstudenten“ oder Externe ab. (Die Verantwortung für die Sicherheit sollte im Unternehmen bleiben.)
2. Technikern ist nicht bewusst, dass die Safety-Standards den Stand der Technik widerspiegeln und die Arbeit – wenn sie diesen Standards nicht gerecht wird – handwerklich bzw. ingenieurmäßig mangelhaft ist.
3. Zu den häufigsten Fehlern und Defiziten im Zusammenhang mit Sicherheit und Qualitätssicherung gehören schlechte Ausbildung, mangelhafte Fachkenntnis, fehlender Überblick, fehlende Sensibilität der Projektbeteiligten (GF, V, M, QS …)
4. Die Schnittstellen zwischen Vertrieb, Marketing, Entwicklung und Qualitätssicherung funktionieren nicht optimal.
5. Notwendigkeit und Anerkennung der QS – auch in Form von Zeit und Zuspruch – werden nicht erkannt.
6. Oft fehlt Zeit für Innovation in Form von Auswertungen der Erfahrungen, die zu Veränderungen und Verbesserungen führen.
7. Fehlende Ausbildung der Entwickler – fachlich meistens gut, doch bei der Softwareentwicklung gibt es Schwachstellen.
8. Der Stand der Technik wird nicht genügend ermittelt.
9. Die Weiterbildung der Mitarbeiter erfolgt nicht zielgerichtet.
10. Auswahl und Einsatz der Werkzeuge bzw. Methoden sind unzureichend vorbereitet.
11. Risikomanagement ist unzureichend umgesetzt, und Anforderungen und Qualitätsmerkmale sind unvollständig festgelegt.
12. Controlling der technischen Sicherheit erfolgt im Produkt-Lebenszyklus.
13. Eine Abnahme der Phasenergebnisse ist unzureichend.
14. Entspricht mein Projekt der funktionalen Sicherheit (FuSi) nach ISO 26262? Häufig wird diese Frage nicht ausreichend geklärt.
15. 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.

©MicroConsult 10-19

MICRO CONSULT

Die häufigsten und schwerwiegendsten Irrtümer zu Safety im Bereich Qualitätssicherung

Irrtum 1: Testen ist besonders wichtig, um Sicherheit zu erreichen.

Richtig ist: Qualität und Sicherheit werden nicht erprüft, sie werden konstruiert bzw. gefertigt. Oder anders: Vom Wiegen wird die Sau nicht fett, und die Elektronik und deren Software werden vom Testen nicht sicher.

Irrtum 2: Ist die Aufgabenstellung zu ungenau, wenn z.B. die Sicherheitskritikalität nicht ausgewiesen ist, liegt die Schuld (ausschließlich) beim Auftraggeber.

Richtig ist: Der Lieferant hat die alleinige Verantwortung für sein Produkt.

Irrtum 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.

Irrtum 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 werden.

Irrtum 5: Software = Code

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

Irrtum 6: Einen Qualitäts- und Sicherheitsprozess schaffe ich durch Definition von Rollen.

Richtig ist: Qualität und Sicherheit erreicht man nur durch Etablierung eines gelebten Prozesses.

Irrtum 7: Mit „Zero Defects“ erreicht man ein hohes Maß an Sicherheit.

Richtig ist: „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, sondern auch von wirtschaftlicher Vernunft.“ 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 deshalb umgesetzt werden.

©MicroConsult 10-19

Weitere Irrtümer

- Funktionale Sicherheit (FuSi) betrifft nur die Hardware.
- Der Auftraggeber hat das Projekt als nicht FuSi relevant definiert; damit sind wir aus dem Schneider.
- Funktionale Sicherheit? Darum kümmert sich unser FuSi-Manager!

Die wichtigsten Tipps und Maßnahmen von Embedded-Experten, um Defiziten entgegenzuwirken

1. Sicherheitsstandards sind Kochrezepte für den Stand der Technik und für konforme Elektronik und Software. Kochrezepte muss man für die eigene Küche anpassen und Standards begründet auf den eigenen Bedarf schaffen.
2. Sicherheit ist nicht komplett vorhanden oder fehlt völlig. Auch kleine Schritte sind – wenngleich nicht immer ausreichend – in jedem Fall 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.
4. Sparen Sie nicht an guter Ausbildung, investieren Sie in regelmäßige Weiterbildungen!

*Vielen Dank an **Dr. Günter Glöe** (Geschäftsführer CATS Software Tools, Dozent für Qualitätssicherung), Dieter Volland (MicroConsult, Dozent für Software Engineering) **Frank Listing** (MicroConsult, Dozent für Software Engineering), **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) und **Christian Nachreiner** (ehem. Geschäftsführer iNTENCE automotive electronics) für den kostbaren Input zu diesen Punkten.*

Mehr lesen

Den Drachen bändigen – Sichere Software von Anfang an:
Teil 1 „Entwickler unter Zeitdruck“

Den Drachen bändigen – Sichere Software von Anfang an:
Teil 2 „Alle Projektbeteiligten qualifizieren und informieren“

©MicroConsult 10-19

Autor: Peter Siwon

Dipl.-Ing. Peter Siwon ist freier Mitarbeiter bei MicroConsult. Er lernte die Projektarbeit im Laufe seiner beruflichen Entwicklung aus vielen Perspektiven kennen: Forschung, Entwicklung, Projektleitung, Vertrieb, Marketing und Geschäftsführung. Seit 2008 gibt er sein Wissen und seine Erfahrungen als Trainer, Coach, Lehrbeauftragter und Autor von Vorträgen, Kolumnen, Fachartikeln und Büchern weiter. Seine Vorträge und Seminare wurden bereits mehrfach ausgezeichnet. Sein Themenspektrum umfasst klassische, agile und systemische Projektmanagement-Ansätze, Kommunikation, Führung, Teamentwicklung und Konfliktlösung im Projektumfeld. Die vielen Fallbeispiele aus der Praxis seiner Kunden und Kundinnen sowie seine aktive Mitwirkung in Projekten liefern ihm immer wieder neue Impulse und Erkenntnisse für seine Tätigkeit. Darüber hinaus erweitert Peter Siwon sein Wissen durch regelmäßige Aus- und Weiterbildung - gerne blickt er dabei über den Tellerrand. Aus der Überzeugung heraus, dass die Projektarbeit maßgeblich durch menschliche Faktoren beeinflusst wird, gilt sein besonderes Interesse der menschlichen Seite des Projekterfolgs. Mehr Informationen zu Peter Siwon und Kundenmeinungen zu seiner Arbeit finden Sie unter www.systemisches-projektmanegment.info.

Weiterführende Informationen

MicroConsult Training & Coaching zum Thema Qualität, Safety & Security

MicroConsult Fachwissen zum Thema Qualität, Safety & Security

©MicroConsult 10-19