

ASPICE und ISO 26262

Prozess trifft Inhalt

Warum Prozessreife und funktionale Sicherheit nur gemeinsam funktionieren – ein Leitfaden für ASPICE-Assessoren und Safety-Ingenieure

Die Ausgangsfrage

In fast jedem Automotive-Projekt taucht irgendwann die Frage auf:

„Machen wir jetzt ASPICE oder ISO 26262?“

Die Antwort: **Beides. Und zwar zusammen.** Wer die beiden Rahmenwerke als Alternativen betrachtet, hat ihre Grundlogik noch nicht verstanden.

Der fundamentale Unterschied

Automotive SPICE	ISO 26262
Bewertet die Qualität von Entwicklungsprozessen	Definiert inhaltliche Anforderungen an sicherheitskritische Systeme
<i>Fragt: Wie gut ist das, was wir tun?</i>	<i>Fragt: Was müssen wir tun, um funktionale Sicherheit nachzuweisen?</i>
Sind Anforderungen rückverfolgbar? Werden Reviews durchgeführt? Ist der Prozess wiederholbar?	Welche Analysen, Dokumente und Verifikationsschritte sind für welchen ASIL erforderlich?

- ASPICE sagt, **wie** ein guter Prozess aussieht.
- ISO 26262 sagt, **was** inhaltlich geliefert werden muss.

Wo überschneiden sie sich?

Die Überschneidungen sind erheblich – und gewollt. ISO 26262 fordert einen strukturierten Entwicklungsprozess mit Planung, Verifikation, Konfigurationsmanagement und Problemlösung. Genau diese Prozesse bewertet ASPICE in seinen Prozessreferenzmodellen.

Konkrete Parallelen

SYS.2 / SWE.1 – Anforderungsmanagement

ISO 26262 fordert vollständige, konsistente Safety Requirements auf System- und Softwareebene. ASPICE bewertet, ob der Anforderungsprozess das strukturiert liefert.

SWE.3 / SWE.4 – Detailentwurf und Verifikation

ISO 26262 schreibt methodenspezifische Verifikation vor – abhängig vom ASIL. ASPICE prüft, ob Verifikationsprozesse systematisch geplant und durchgeführt werden.

SUP.8 – Konfigurationsmanagement

Für ISO 26262 ist lückenlose Rückverfolgbarkeit von Anforderungen bis zum Test keine Option – sie ist Pflicht. ASPICE SUP.8 bewertet genau diesen Prozess.

SUP.9 – Problemlösungsmanagement

Safety-relevante Fehler müssen nach ISO 26262 systematisch erfasst, bewertet und verfolgt werden. ASPICE SUP.9 liefert den Prozessrahmen dafür.

Was passiert ohne Verzahnung?

Zwei häufige Fehler in der Praxis:

Fehler 1: ASPICE als Selbstzweck

Teams optimieren Prozessreife auf Capability Level 2 oder 3 – aber die Safety-Artefakte sind inhaltlich leer. Gute Prozesse, schlechte Ergebnisse.

Fehler 2: ISO 26262 ohne Prozessreife

Safety-Dokumente werden erstellt – aber nicht kontrolliert, nicht versioniert, nicht rückverfolgbar verknüpft. Im Audit fehlen Nachweise, die eigentlich vorhanden sein sollten.

Beide Fehler sind teuer. Und beide sind vermeidbar.

Was funktioniert in der Praxis?

1. Gemeinsame Planung – Safety Plan und SPICE-Prozessplanung von Anfang an aufeinander abstimmen. Nicht zwei separate Dokumente – ein integrierter Projektrahmen.

2. Artefakte doppelt nutzen – Ein gut strukturiertes Software Requirements Specification-Dokument erfüllt gleichzeitig ASPICE SWE.1 und ISO 26262 Part 6 Anforderungen. Einmal richtig machen – doppelt profitieren.

3. Reviews integrieren – Safety Reviews und ASPICE-konforme Peer Reviews schließen sich nicht aus. Mit der richtigen Checkliste erfüllen sie beide Anforderungen gleichzeitig.

4. Assessments koordinieren – ASPICE-Assessment und Functional Safety Audit sollten koordiniert stattfinden – nicht als unabhängige Parallelveranstaltungen.

Fazit

ASPICE und ISO 26262 sind keine Konkurrenten.

ASPICE gibt der funktionalen Sicherheit das Prozessgerüst, das sie braucht, um reproduzierbar und nachweisbar zu sein.	ISO 26262 gibt ASPICE den inhaltlichen Fokus, der aus Prozessqualität echte Produktsicherheit macht.
---	---

Wer beides versteht, entwickelt effizienter – und besteht Audits souveräner.

Wie ist das in euren Projekten – ASPICE und ISO 26262 integriert oder noch in getrennten Silos?

Über den Autor

Markus Steinmetz ist als Auditor und Assessor bei der TÜV NORD CERT GmbH im Geschäftsfeld Spezifische Managementsysteme tätig, mit Schwerpunkt auf IT- und Informationssicherheits-Managementsystemen. In dieser Funktion führt er Audits und Assessments nach Standards wie ISO 27001, ISO/SAE 21434 und IEC 62443 durch.

Unabhängig von dieser Tätigkeit arbeitet Markus als freiberuflicher Spezialist in den Bereichen funktionale Sicherheit und Cybersecurity, mit besonderem Fokus auf die Verknüpfung von funktionaler Sicherheit und Cybersecurity in integrierten Entwicklungsprogrammen.

Die in diesem Whitepaper dargestellten Inhalte und Ansichten spiegeln seine persönliche fachliche Expertise und Erfahrung wider und stehen in keinem Zusammenhang mit der TÜV NORD CERT GmbH oder verbundenen Unternehmen.

Kontakt

E-Mail: markus@steinmetz-security.de

Website: <https://steinmetz-security.de>

LinkedIn: www.linkedin.com/in/markus-steinmetz-78052817