Paradigmenwechsel im Safety-Assessment – auf dem Weg zu stärkerem Einsatz physikalischer Modelle

Burkhard Münker[1]

[1]Fa. Icomod - Münker Consulting, Olper Straße 53, 57258 Freudenberg

Zeitgemäße Modellierungswerkzeuge ermöglichen eine hierarchische 1:1-Abbildung der physikalischen Einheiten des realen Systems. Intuitive, grafische Darstellungen der Komponenten und Subsysteme machen es auch nicht an der Modellerstellung Beteiligten leicht, die System-Zusammenhänge zu verstehen und ein Modell weiterzupflegen oder zu variieren. Gerade diese Natürlichkeit des komponentenorientierten Ansatzes und der Mehrwert der Modelle ist seit einigen Jahren ein maßgeblicher Motivator, entsprechende Tools in den Entwicklungsprozess einzubinden.

Ein genauerer Blick zeigt aber, dass dieser Wechsel in Mentalität und Werkzeugen zwar sehr wohl bei der System- und Funktionsentwicklung stattgefunden hat, kaum jedoch im Bereich des Safety-Assessment, also den Analysen, welche die Untersuchung der funktionalen Sicherheit eines – oft komplexen – Systems zum Ziel haben. Eine Vielzahl von zwar seit Jahrzehnten etablierten, aber oft individuellen Analysearten mit proprietären Wissens- und Ergebnis-Repräsentationen wie Fault-Tree- oder Fault-Mode-and-Effect-Analysis (FTA, FMEA) prägen hier das Bild und ebenso die Denkmuster der Verantwortlichen.

Wie gezeigt wird, lassen sich zwar die im Safety-Prozess geforderten Analyse-Ergebnisse entlang des gesamten V-Prozesses direkt aus physikalischen Bauteil-Modellen toolgestützt ableiten. Ein sanfter Paradigmenwechsel ist aber nur durch parallele Unterstützung verschiedenartiger Wissensdarstellungen in derselben Umgebung zu gewährleisten. So kann der Safety-Ingenieur mittels einer FaultTree-Bibliothek die Ausfall-Logik des Systems wie gewohnt als Fehlerbaum darstellen und gleichzeitig – graduell zunehmend - für Teilumfänge zeitgemäße Komponenten-Bibliotheken zur physikalischen Beschreibung von Nominal- und Fehlerverhalten einsetzen.