# Nicht-SIL-Komponenten in einem SIL-Gesamtsystem

*Mit der IconTrust-Softwaretechnik ist es möglich, in einer sicherheitskritischen Gesamtfunktion nicht-sicherheitsrelevante HMI-Komponenten zu nutzen*

UWE HÄUSSER *

Kontinuierlich werden in den letzten Jahren immer mehr funktionale Einzelgeräte miteinander vernetzt, Daten erfasst, ausgewertet und visualisiert. Dies betrifft inzwischen nicht mehr nur Server und PCs, sondern erfolgt bis zu kleinsten Steuerungen und Sensoren. Mit weitreichenden Folgen: Plötzlich sollen nicht-sicherheitsrelevante Komponenten für eine sicherheitsrelevante Gesamtfunktion verwendet werden.

Der Anwender verlangt inzwischen verstärkt vom Zulieferer der Systemkomponenten entsprechende Eignungsnachweise, aus denen für ihn ersichtlich ist, ob eine Systemkomponente in seinem sicherheitsrelevanten Anwendungsfall einsetzbar ist oder nicht. Ein Eignungsnachweis kann z.B. ein Gutachten nach DIN EN 50126 / 50126 / 50129, IEC 61508 o.ä. sein, das die Eignung der Systemkomponente für ein bestimmtes Einsatzszenario und einen geforderten SIL (Safety Integrity Level) mit einem einzuhaltenden Restrisiko bescheinigt. Was bedeutet das für den Zulieferer hinsichtlich Entwicklungsprozess einer Systemkomponente und deren Produktdesign?

Die o.g. Normen definieren das von einem System ausgehende Restrisiko nach dem MEM-Prinzip (Minimum Endogenous Mortality). Das heißt, dass ein Ausfall der sicherheitsrelevanten Funktion der Systemkomponente die natürliche Sterblichkeitsrate des Menschen ($2 \times 10^{-4}$ Todesfälle pro Jahr und Person) nicht signifikant erhöhen soll. Das Restrisiko wird in der IEC 61508 als $PFD_{avg}$-Wert (Average Probability of dangerous Failure on Demand) und/oder PFH-Wert angegeben (Average Frequency of dangerous failure per hour). Aus diesen Werten kann ein SIL abgeleitet werden. Normalerweise macht diese Risikoanalyse der Kunde und gibt dem Zulieferer ein maximal zulässiges Restrisiko und den benötigten SIL für ein bestimmtes Einsatzszenario vor.

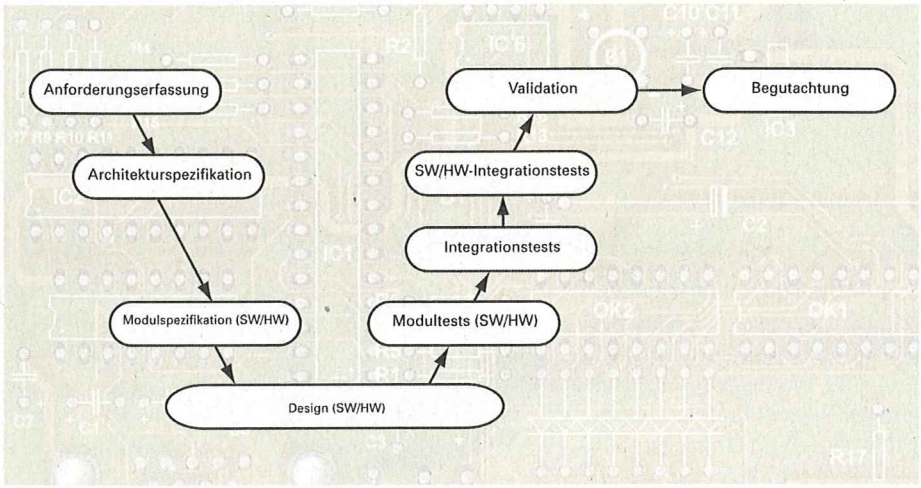


***Bild 1:*** *Der SIL-Entwicklungsprozess für die Hersteller von Komponenten*

## Der Entwicklungsprozess EC 61508 in der Praxis

In der IEC 61508 ist ein generischer Entwicklungsprozess beschrieben, der Neueinsteiger schnell überfordert. Reduziert man den Prozess auf das für Komponentenhersteller notwendige Maß, ergibt sich ein recht schlanker Entwicklungsprozess (Bild 1: Entwicklungsprozess für Komponentenhersteller). Ist ein passender Entwicklungsprozess in der Firma erst einmal eingeführt, lassen sich Projekte recht schematisch umsetzen, sodass systematische Fehler schon allein durch das „Leben" des Prozesses verringert werden. Die Durchführung der Produktentwicklung für verschiedene SIL unterscheidet sich dann größtenteils nur noch durch die notwendige Teamstruktur, Systemarchitektur, Test- und Nachweistiefe.

Dafür muss der Hersteller noch nicht einmal unbedingt alle „alten" Prozesse über Bord werfen. Meist reicht es die bestehenden Prozesse neu zu gruppieren und geringfügig anzupassen. Um die Kommunikation zwischen dem Hersteller, dem Gutachter und weiteren externen an dem Projekt beteiligten Akteuren zu verbessern, sollten die Bezeichnungen der IEC 61508 für Prozessschritte, Artefakte, Kennwerte u.s.w. übernommen werden.

## Präzise Definition der Sicherheitsanforderung

Eine sicherheitsrelevante Entwicklung nach IEC 61508 ist anforderungsgetrieben. Daher ist es immens wichtig, die Sicherheitsanforderungen bei Projektbeginn präzise zu erfassen und möglichst im Projektverlauf nicht mehr zu ändern. Unpräzise, sich widersprechende oder zu komplexe Anforderungen an die Sicherheitsfunktionen eines Systems verteuern und verlängern die Entwicklung signifikant. Jedweder unnötige Ballast sollte vermieden und in einer Abgrenzung des Systems erfasst werden. Hierbei spielen folgende Fragen eine zentrale Rolle: Wann werden Sicherheitsanforderungen erfüllt bzw. nicht erfüllt (EMV, Klima, mechanische Belastungen etc)? Was ist der sichere Zustand des Systems? Gibt es zeitliche Vorga-

* Uwe Häußer
... *ist Business Development Manager bei DEUTA-WERKE, Bergisch Gladbach*


***Bild 2:*** *IconTrust ist in der Lage, alle Daten unabhängig von der verwendeten Hardware zu überwachen*

ben (Reaktionszeiten, Prüfintervalle u.a.m.), die eingehalten werden müssen?

Sind die Sicherheitsanforderungen erst einmal alle bekannt, muss ein Sicherheitsplan erstellt werden, in dem eine, dem SIL-Level angemessene, Auswahl und Umsetzung der in der IEC 61508 geforderten Maßnamen festgelegt wird. Anschließend muss ein Projektteam zusammengestellt werden, das dem Sicherheitsplan genügt.

In dieser Phase sollte schon der Anforderungstestplan und die Anforderungstestspezifikation erstellt werden. Diese Dokumente sind die Basis für die abschließende Validation der Anforderungen. Es zeigt sich bei der Erstellung dieser Dokumente schnell, ob noch weitere Anforderungen an das System, bedingt durch das Testen, existieren und ob alle Anforderungen konsistent und testbar sind.

Sobald diese Aspekte geklärt sind, sollte ein Konzept entwickelt werden, das sicherheitsrelevante Anforderungen möglichst intelligent von nicht-sicherheitskritischen Anforderungen trennt und auf unterschiedliche Subkomponenten aufteilt, somit (beispielsweise durch Mehrkanaligkeit) eine Reduktion des benötigten SIL für die einzelnen Subkomponenten ermöglicht. Hierbei ist darauf zu achten, dass Fehler gemeinsamer Ursache (CCF, Common Cause Failure) vermieden werden. Es muss für eine Rückwirkungsfreiheit zwischen den Komponenten gesorgt werden, da sonst die Reduktion des SIL für eine Subkomponente nicht oder nur bedingt nachgewiesen werden kann. Ein intelligentes Konzept trägt erheblich zur Reduktion der Kosten und der Entwicklungszeit bei, was das Beispiel IconTrust zeigt (IconTrust überwacht dedizierte Bereiche auf dem TFT-Panel und unterscheidet dabei zwischen sicherheitsrelevanten und nicht-sicherheitsrelevanten Informationen). Ist das Konzept erst einmal festgelegt, muss das Restrisiko abgeschätzt und bereits in dieser Phase Kontakt mit dem Gutachter aufgenommen werden. Jetzt kann man sich beispielsweise das Sicherheitskonzept prüfen lassen und gegebenenfalls dieses frühzeitig um fehlende Sicherheitsmechanismen erweitern.

Modulspezifikation, Design, Implementierung, Test und Begutachtung - die ersten drei Phasen sollten für die meisten Hersteller nichts neues sein: Es werden Hard- und/oder Softwaremodule spezifiziert und deren Funktion und Interaktion festgelegt. Danach folgen Erstellung und Kodierung.

Der größte Unterschied zwischen den SIL-Stufen zeigt sich in dem Aufwand, den man für das Testen veranschlagen muss, da von der IEC 61508 das automatische Testen teilweise explizit gefordert wird. Ein intelligentes Architekturkonzept zahlt sich in dieser Phase durch massive Einsparungen beim benötigten Testaufwand aus. Neben den Tests ist ggf. noch eine Sicherheitserprobung im Zielsystem notwendig.

## Beispiel: Ein flexibles Safety-Konzept mit IconTrust

Zu guter letzt werden alle Ergebnisse der Verifikations- und Validationstests sowie aller anderen qualitätssichernden Maßnahmen in einem technischen Sicherheitsbericht zusammengefasst. Dieser enthält zusätzlich die inzwischen berechneten sicherheitsrelevanten Kennwerte des Systems. Der Gutachter prüft dann, ob das Entwicklungsteam alle nach dem SIL-Level geforderten Maßnahmen umgesetzt hat und der angestrebte SIL-Level erreicht wurde. Das Ergebnis dieser Prüfung wird in einem offiziellen Gutachten festgehalten.

Es soll ein Statusmonitor neben vielen nicht-sicherheitsrelevanten Anzeigen auch einige wenige sicherheitsrelevante Daten anzeigen. In einem konventionellen Sicherheitskonzept muss die gesamte Kette aus Applikation, Betriebssystem, CPU, Grafikkarte und Display als sicherheitsrelevant angesehen werden und dementsprechend entwickelt worden sein – mit sehr hohem Aufwand und Entwicklungskosten sowie einer geringen Flexibilität, da für jede Änderung eine neue Begutachtung notwendig ist.

Das IconTrust-Konzept erleichtert die Entwicklung des Statusmonitors erheblich. Die IconTrust-Subkomponente prüft, ob auf den als sicherheitsrelevant definierten Anzeigebereichen, die korrekte Information angezeigt wird. Dafür muss sie nur einmalig konfiguriert werden. Passen Anzeige und Statusdaten nicht zusammen wird ein erkennbar sichere Zustand wie z.B. „Monitor aus“ eingenommen. Die gesamte Kette aus Applikation, Betriebssystem, CPU und Grafikkarte kann so als nicht-sicherheitsrelevant betrachtet werden. Dies bringt folgenden Vorteile hinsichtlich Flexibilität und Obsoleszenz (Veralterung) von PC-Komponenten ohne Einfluss auf den Sicherheitsnachweis.

Zunächst die Flexibilität: Aufgrund der Unabhängigkeit können jeder PC oder eine ähnliche Plattform zur Erzeugung der grafischen Signale eingesetzt werden. Sogar bereits vorhandene Anwendungen lassen sich leicht aktualisieren. Selbst Standard-Betriebssysteme dürfen nun verwendet werden. Die Nutzung von Standard-Grafikwerkzeugen und -bibliotheken ermöglicht weiterhin die drastische Reduzierung des Zeitaufwands und damit der Entwicklungskosten. Keinerlei weitere Begutachtung ist bei Änderungen der grafischen Benutzerschnittstelle außerhalb der überwachten Bereiche notwendig. Selbst wenn das Layout der grafischen Benutzerschnittstelle innerhalb des vordefinierten Bereichs verändert wird, genügt es, die Konfiguration anzupassen. Die Obsoleszenz von PC-Komponenten ist ohne Einfluss auf den Sicherheitsnachweis: Die Unabhängigkeit von IconTrust gilt auch für alle zukünftigen Revisionsstände der PC-Plattform. So kann das Konzept den Entwicklungsaufwand verringern und die SIL-Zulassung vereinfachen. // KU

**DEUTA-WERKE** +49(0)2202 958100

## InfoClick

- Die IconTrust-Technik von Deuta

**www.elektronikpraxis.de** **InfoClick** 2826255