

Unterstützung bei der Anwendung der IEC 61508

Werkzeug zur Anforderungsermittlung

Die Norm IEC 61508 wird zunehmend im Bereich sicherheitskritischer Systeme und deren Software angewendet, um Zuverlässigkeit, Sicherheit und Wartbarkeit dieser Systeme zu sichern. Sie gibt mehrere hundert Maßnahmen vor, die während des Entwicklungsprozesses von sicherheitskritischen Systemen angewendet werden können. Wie verbindlich eine Maßnahme ist, hängt davon ab, welches Risiko beim Betrieb des Systems zu beherrschen ist. FRANK BÜCHNER



Die IEC 61508 ist eine allgemeine Norm und bildet die Grundlage für speziellere anwendungsspezifischere Normen, beispielsweise für Eisenbahnen und Kernkraftwerke, und ist in allen Bereichen anzuwenden, bei denen keine speziellere Norm existiert. Problematisch bei der Anwendung der IEC 61508 ist die große Anzahl von möglichen Maßnahmen und ihre variierende Verbindlichkeit in Abhängigkeit vom zu beherrschenden Risiko des Systems. Im Folgenden wird gezeigt, welche Schritte die Anwendung der Norm erfordert und wieso Werkzeugunterstützung hierbei äußerst hilfreich ist.

Anwendung der IEC 61508

Zunächst werden die Anforderungen in Bezug auf die Qualität des Systems bestimmt. Diese Anforderungen resultieren einerseits aus dem aktuellen Stand der Softwaretechnik; andererseits werden sie durch die speziellen Anforderungen an die (Software-) Qualität des fraglichen Systems festgelegt, etwa in Bezug auf Zuverlässigkeit, Sicherheit oder Wartbarkeit. Der Grad der angestrebten Qualität wiederum hängt wesentlich vom Risiko ab, den der spätere Betrieb des Systems mit sich bringen wird. Deshalb besteht der erste Schritt in der Anwendung der IEC 61508, das zu beherr-

Frank Büchner studierte Informatik an der Universität Karlsruhe (TU). Seit Abschluss seines Studiums ist er nun über ein Dutzend Jahre im Bereich der eingebetteten Systeme in unterschiedlichen Positionen tätig. Zur Zeit arbeitet er bei Hitex in Karlsruhe als Produktmanager.



Abb. 2: Die Maßnahmen aus der Hauptklasse ‚Software, Lifecycle, Design and Development‘ (senkrecht) und der Unterklasse ‚SW-Architecture – Techniques‘ (horizontal). Zueinander alternative Maßnahmen sind durch einen gemeinsamen grauen Hintergrund gekennzeichnet.



Abb. 3: Ausgewählte Maßnahmen sind angekreuzt; Maßnahmen, für die eine Notiz hinterlegt ist, sind mit einem Ausrufezeichen markiert.

schende Risiko des Systems zu ermitteln. Von diesem Risiko wird der sogenannte ‚Safety Integrity Level‘ (SIL) abgeleitet, der bestimmt, wie verbindlich die Anwendung einer Maßnahme aus der IEC 61508 ist.

Werkzeugunterstützung

Da die Norm mehrere hundert Maßnahmen enthält, die teilweise alternativ zueinander verwendet werden können und deren Verbindlichkeit vom Safety Integrity Level abhängt, ist die Verwaltung dieser Maßnahmen ohne Werkzeugunterstützung kaum handhabbar. Insbesondere da unterschiedliche Parteien, wie etwa Auftraggeber, Qualitätssicherung und Entwicklung in die Auswahl der Maßnahmen involviert sind, benötigt man die Dokumentation des fortschreitenden Entwicklungsprozesses in elektronischer Form, um die Diskussion bzw. Revision der getroffenen Entscheidungen zu ermöglichen. RiskCat ist ein Werkzeug, das den Überblick über die Maßnahmen verschafft, den Auswahlprozess systematisiert und getroffene Entscheidungen dokumentiert.

Risikobestimmung

Das projektierte System wird in Hinblick auf das Betriebsrisiko analysiert. Hierbei wird etwa untersucht, ob und mit welcher Wahrscheinlichkeit das System Menschenleben gefährden könnte, ob finanzielle Verluste, Schaden für das Image des Herstellers oder ‚nur‘ verärgerte Benutzer durch den Betrieb des Systems zu befürchten sind. Die IEC 61508 bietet drei Methoden an, um das Risiko zu ermitteln (Abb. 1): Darunter ist die Risikographmethode, die besonders in

Deutschland angewandt wird. In Großbritannien verbreitet ist die ALARP-Methode (as low as reasonable practicable). Diese beiden Methoden sind qualitative Wege zur Risikoanalyse. Als dritte Methode erlaubt die IEC 61508, das Risiko in Form von akzeptierten Versagensraten quantitativ anzugeben.

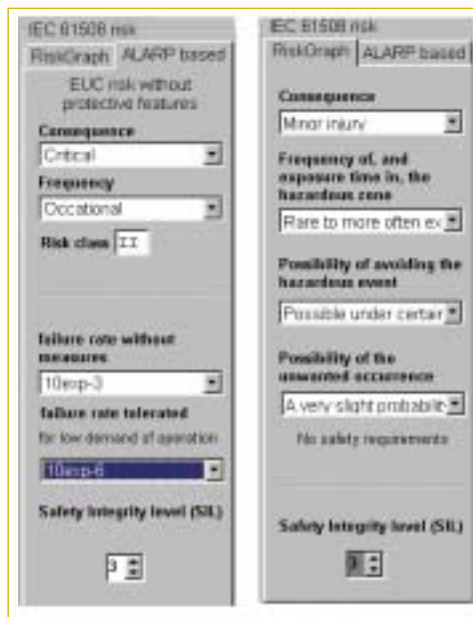


Abb. 1: Risikoermittlung in RiskCat: Links oben nach der ALARP-Methode, links unten durch Angabe der akzeptierten Versagensrate und rechts nach der Risikograph-Methode

Alle drei Methoden werden von RiskCat unterstützt. Hierbei kann man einfach unter vorgefertigten Beschreibungen auswählen.

Bestimmung des SIL

Erfolgte die Risikoanalyse nach der Risikographmethode oder indem Versagensraten angegeben wurden, so kann das Werkzeug den SIL

automatisch nach den Vorgaben der IEC 61508 bilden. Die Norm sieht vier diskrete Stufen für den SIL vor (1 bis 4), wobei bei Stufe 4 die höchsten Anforderungen gestellt werden. Der SIL kann auch manuell eingestellt werden, etwa wenn aus Marketingüberlegungen heraus ein höherer Level zugrunde gelegt werden soll als nach der Risikoanalyse notwendig. Außerdem kann ein höherer SIL die Option für den Einsatz des Systems in Umgebungen offen halten, für die es ursprünglich nicht vorgesehen war. Beispielsweise könnte ein System, das für den Einsatz in nichtöffentlichen Bereichen konzipiert ist, auch in öffentlichen Bereichen zum Einsatz kommen. In der Dokumentation, die von RiskCat erzeugt wird, sind sowohl die Vorgaben der Risikoanalyse als auch der SIL festgehalten.

Auswahl der Maßnahmen und ihrer Verbindlichkeit

Das Tool teilt die Maßnahmen der Norm IEC61508 in sechs Hauptklassen ein, die nach den Anwendungsgebieten der Maßnahmen gebildet werden. Eine dieser Hauptklassen umfasst beispielsweise alle Maßnahmen, die mit dem Design und der Entwicklung der Software im Lebenszyklus des Systems zu tun haben. Auf die Maßnahmen einer Hauptklasse wird in der Software (Abb. 2) durch vertikale Reiter auf der linken Seite des Hauptfensters zugegriffen. RiskCat unterteilt die Maßnahmen einer Hauptklasse jedoch noch weiter: Die Maßnahmen dieser Unterklassen sind durch horizontale Reiter zugänglich, die sich am oberen und unteren Rand des Hauptfensters befinden. Die Klassifikation der Maßnahmen durch das Werkzeug schafft einen Überblick über die Maßnahmen und dies ist die Voraussetzung für deren systematische Bearbeitung. Unter Um-

ständen, wenn es beispielsweise nur um die Entwicklung der Hardware des Systems geht, sind Teile der Norm nicht relevant. Mit der Software sind die interessierenden Maßnahmengruppen jedoch immer leicht zugänglich. Abhängig vom Safety Integrity Level legt die Norm IEC 61508 die Verbindlichkeit der Maßnahmen fest. Es gibt fünf Stufen für die Verbindlichkeit, nämlich ‚possible‘, ‚recommended‘, ‚highly recommended‘, ‚mandatory‘ und ‚not recommended‘. RiskCat stellt die gerade vorliegende Verbindlichkeit einer Maßnahme durch die Farbe der Maßnahme dar. Beispielsweise erscheinen ‚highly recommended‘ Maßnahmen blau, während ‚mandatory‘ Maßnahmen rot sind. Das Tool zeigt dem Anwender diese Zuordnung ständig an.

Durch die Farbkodierung ist die Relevanz der Maßnahmen immer leicht ersichtlich; die Farbkodierung empfiehlt dadurch auch die Reihenfolge, in der die Maßnahmen bearbeitet werden sollten.

Wenn der Level geändert wird, wechselt unter Umständen auch die Verbindlichkeit einer Maßnahme. Beispielsweise stuft das Erhöhen des SIL von 1 auf 2 den Einsatz der Datenflussanalyse von ‚recommended‘ auf ‚highly recommended‘ hoch; das Erhöhen des Levels von 2 auf 3 bedeutet den Übergang von einkanali gen Systemen auf redundante Systeme. Diesen Wechsel der Verbindlichkeit kann man leicht durch den damit verbundenen Farbwechsel erkennen. Somit hat man ein probates Mittel, um die Auswirkungen eines niedrigeren/höheren SIL herauszufinden. Möglicherweise fällt der Aufwand für ein System mit einem höheren SIL gegenüber den damit verbundenen Vorteilen, wie höherer Zuverlässigkeit oder erweitertem Einsatzgebiet, kaum ins Gewicht.

Bei einigen Gruppen von Maßnahmen reicht die Auswahl einer Maßnahme der Gruppe aus, um die Anforderungen der Norm zu erfüllen. Die Maßnahmen dieser Gruppen sind also alternativ zueinander zu sehen. RiskCat stellt zueinander alternative Maßnahmen zusammen dar und unterlegt sie mit einem gemeinsamen grauen Hintergrund, so dass einerseits leicht zu erkennen ist, unter welchen Alternativen gewählt werden kann und andererseits vermieden wird, dass zwei zueinander alternative Maßnahmen überflüssigerweise gleichzeitig selektiert werden.

Die Auswahl einer Maßnahme erfolgt im Tool durch einen Doppelklick auf die jeweilige Maßnahme. Ausgewählte Maßnahmen sind durch ein Kreuz gekennzeichnet.

Der Anwender entscheidet für jede Maßnahmen der (relevanten) Haupt- und Unterklassen, ob sie angewendet werden soll oder nicht. Damit legt der Anwender einerseits fest, welcher Aufwand bei der Entwicklung des Systems anfallen wird und andererseits, welche Probleme beim späteren Betrieb des Systems (nicht) zu erwarten sind. Insbesondere bei ‚recommended‘

und ‚highly recommended‘ Maßnahmen ist eine sorgfältige Abwägung anzuraten. Wird die Konformität zu IEC 61508 angestrebt, ist natürlich darauf zu achten, dass die als ‚mandatory‘ vorgeschriebenen Maßnahmen angewandt werden.

Abschließend kann das Werkzeug eine Checkliste mit allen ausgewählten Maßnahmen erzeugen. In dieser Checkliste kann zusätzlich angegeben werden, wie bzw. womit eine Maßnahme konkret durchgeführt wird. Die Checkliste bildet die Grundlage sowohl für die Entwicklung des Systems als auch für seine spätere Abnahme.

Weitere Eigenschaften

RiskCat verwaltet Notizen, die der Anwender zu einzelnen Maßnahmen hinterlegen kann (Abb. 3). Diese Notizen bieten sich zur Dokumentation von Gründen an, die zu einer Entscheidung für bzw. gegen die Anwendung einer Maßnahme geführt haben.

Der aktuelle Arbeitstand, hauptsächlich die aktuelle Auswahl der Maßnahmen, kann abgespeichert und restauriert werden. Dies bietet auch die Möglichkeit, das Werkzeug für ein neues Projekt mit einer bereits vorgefertigten Auswahl von Maßnahmen zu starten, welche beispielsweise eine firmenweite Selektion von Maßnahmen für einen bestimmten SIL darstellt, die dann nur noch wenig für das spezifische Projekt angepasst werden muss.

Im Standardlieferungsumfang ist der Text der Normteile 1 bis 3 der IEC 61508 auf englisch und französisch enthalten. Über das Kontextmenü einer Maßnahme erlaubt RiskCat dem Anwender sehr einfach, direkt den diese Maßnahme betreffenden Originaltext der Norm einzusehen.

Fazit

Die große Anzahl von Maßnahmen und die Variation ihrer Verbindlichkeit bei wechselndem Safety Integrity Level (SIL) macht den Einsatz eines Werkzeugs zur Auswahl der geeigneten Maßnahmen praktisch unabdingbar. RiskCat bietet nicht nur einen Überblick über die Maßnahmen und erlaubt eine systematische Bearbeitung, sondern dokumentiert auch die getroffenen Entscheidungen.

Anzeige