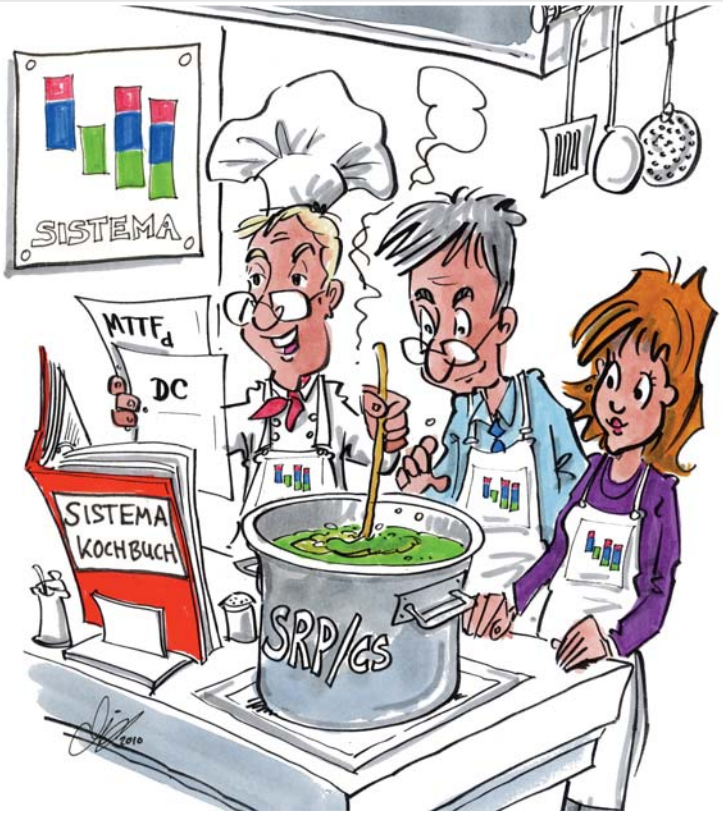

Software-Assistent Sistema:

Berechnung und Bewertung der Maschinensicherheit

Die lizenzfreie Software Sistema gilt mit fast 30.000 registrierten Nutzern als globaler De-facto-Standard bei der Bewertung der Sicherheit von Maschinensteuerungen im Rahmen der DIN EN ISO13849-1. Die Anwendung der Norm erfordert u.a. die Berechnung der Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (PFH) für jede Sicherheitsfunktion an einer Maschine.

Bevor die Berechnung erfolgen kann, muss der Maschinenkonstrukteur – egal welches Tool er verwendet – aus seinem Schaltbild ein sicherheitsbezogenes Blockdiagramm erstellen. Dieses stellt die Ausführung der Sicherheitsfunktion in ihren logischen Zusammenhängen dar. Das Sistema-Kochbuch 1 (Bild 1) behandelt in einer Schritt-für-Schritt-Anleitung diesen ungewohnten Prozess der Abstraktion sowie den Folgeschritt, das Übertragen der Blöcke (d.h. der Bauteile) in die Software und das Eintragen ihrer Kennwerte. Über Eingabemasken werden die Risikoparameter zur Bestimmung des erforderlichen Performance Level (PLr), sowie die Kategorie, die Maßnahmen gegen Fehler gemeinsamer Ursache (CCF) bei mehrkanaligen Systemen, die mittlere Bauteilgüte (MTTFd) und die mittlere Testqualität (DC) von Bauelementen bzw. Blöcken Schritt für Schritt erfasst. Die Auswirkung jeder Parameteränderung auf das Gesamtsystem kann direkt angezeigt und als Report ausgedruckt werden.

Schnittstellen zu Sistema

Sistema bietet zwei Schnittstellen auf Basis der beiden Dateitypen (Bild 2): die Bibliotheksdatei (*.slb), die Datensätze von Bauteilen oder kompletten Steuerungsteilen enthält, sowie die Projektdatei (*.ssm), die den projektspezifischen Nachweis vom Performance Level der Sicherheitsfunktionen enthält. Eine darüber hinaus gehende Programmier- oder Funktionsschnittstelle (API) ist derzeit nicht implementiert. Die Installation der Software lässt sich mit den Parametern des eingesetzten Installers 'Inno Setup' begrenzt steuern, z.B. mit dem 'silent install'. Für Hersteller von Bauteilen und Komponenten der Sicherheitstechnik bietet das Programm die Möglichkeit, für die Anwender eine SQL-Datenbank der Zuverlässigkeitswerte der Bauteile in Form einer Bibliothek bereitzustellen (Bild 2, Pfad A). Das IFA prüft diese Bibliotheken jedoch nicht und betreibt keinen zentralen Bibliotheksserver. Der Anwender kann aus der Software heraus eine IFA-Webseite mit einer aktuellen Liste von Hyperlinks auf die Downloadseiten der Hersteller aufrufen. Der dargestellte Pfad B – die Entwicklung eines Importfilters zur Konvertierung von Bibliotheken – ist aufgrund der Urheberrechte an den Herstellerbibliotheken nicht zulässig. Die graphische Oberfläche (GUI) ermöglicht es dem Anwender, neue Bibliotheken aus dem lokalen Dateisystem oder vom Datenbankserver einzubinden oder zwischen bereits registrierten Bibliotheken zu wechseln. Auch eigene Bibliotheken lassen sich mit Hilfe der GUI anlegen und verwalten. In eigene Bibliotheken kann der Anwender die benötigten Datensätze

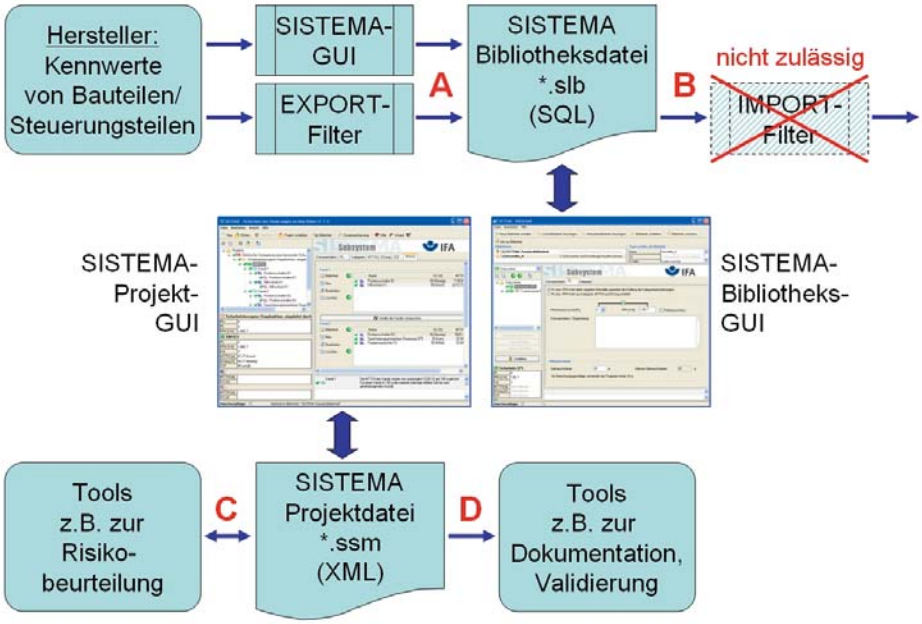

Bild 2: Sistema bietet Schnittstellen für Bibliotheksdateien, die Datensätze von Bauteilen bzw. Steuerungsteilen enthalten, sowie Projektdateien, die den Nachweis vom Performance Level der Sicherheitsfunktionen enthalten.

der Hersteller eintragen, für die es keine Herstellerbibliotheken gibt, sondern ein Produktdatenblatt. Oft ist es effizienter, anstatt bei der Projektierung durch die vielen umfangreichen Original-Bibliotheken zu browsen, besser einmalig die gelisteten oder häufig eingesetzten Bauteile in eine eigene 'Sammel'-Bibliothek zu kopieren. Diese dann auf einem Datenbankserver abgelegt und regelmäßig aktualisiert, spart allen Anwendern im Unternehmen viel Zeit. Eine Besonderheit der Lösung ist aber die Fähigkeit, vorprojektierte Steuerungsteile der Anwender für die Weiterverwendung in anderen Projekten in Bibliotheken zu speichern – ähnlich wie die Makros von CAD-Programmen. Dabei werden nicht nur das Endergebnis (PFH und Performance Level) abgespeichert, sondern die komplette Struktur und Information aller enthaltenen Bauteile. Dies kommt der Praxis entgegen: Nicht immer können solche Makros 1:1 wiederverwendet werden, weil einzelne Bauteile ersetzt werden müssen. Diese Redesigns aber unterstützt Sistema. Die Grenzen des integrierten Editors sind jedoch schnell erreicht. Für sehr große Bauteilesortimente bietet es sich an, die Generierung einer Bibliothek zu automatisieren, z.B. als Exportfilter aus einer Produktdatenbank. Interessierte Hersteller oder Softwarehäuser können beim IFA die Dokumentation der Bibliotheken und Projektdateien anfragen. Eine andere Schnittstelle zur Software stellt die Projektdatei im lesbaren XML-Format dar. Solch eine Projektdatei kann von anderen Tools erzeugt oder auch weiterverarbeitet werden, um dadurch effiziente Toolketten zu erzeugen (Bild 2, Pfade C/D). So haben die bekanntesten Programme zur Risikobeurteilung inzwischen eine Kopplung zu Sistema: Der Anwender bewertet Risiken an der Maschine und definiert beispielsweise steuerungsbasierte Schutzmaßnahmen (Sicherheitsfunktionen). Aus diesen Informationen werden Projektdateien generiert, damit dort der Projekteur die verwendeten Steuerungsteile eintragen kann. Mehrarbeit und Fehler werden vermieden.

Netzwerkbibliotheken und Software auf Terminalserver

Sistema wurde ursprünglich als reine Client-Anwendung für den Betrieb auf einem PC für einen Nutzer konzipiert. Bis zu der Version 1.1.2 musste die für den Start von der Anwendung benötigte interne Standard- und Normendatenbank zwingend auf der lokalen Festplatte liegen, da für den Zugriff auf diese Datenbankdateien bisher ausschließlich die offene Datenbanktechnologie 'Firebird Embedded' eingesetzt wurde. Zudem war aufgrund dieses Datenbankzugriffes die zeitgleiche Nutzung einer Bibliothek aus zwei Anwendungen heraus nicht gestattet. Ab der Version 1.1.3 wurde die Unterstützung des 'Firebird Servers' hinzugefügt. Die Verwaltung der Bibliotheken obliegt bei dieser Variante einem Datenbankserver, der es ermöglicht, Herstellerbibliotheken zentral abzulegen und diese von mehreren Anwendern über ein Netzwerk gleichzeitig zu nutzen. Eine Anleitung dazu stellt das IFA mit dem Sistema Kochbuch 2 bereit. Neben den Bibliotheken können aber auch die internen Datenbankdateien auf diesem Datenbankserver abgelegt werden. Die Beschränkung des exklusiven Zugriffs beim 'Firebird Embedded' entfällt, was es ermöglicht, mehrere Instanzen parallel auf einem Rechner zu starten. Dies ist besonders relevant beim Einsatz von der Software auf einem Terminalserver. Das IFA hat ein weiteres Sistema-Kochbuch 3 veröffentlicht, das diesen Modus und die notwendigen Konfigurationen beschreibt. Das Programm ist kostenlos auf der Website des Instituts in den Sprachen Deutsch, Englisch, Französisch, Italienisch und Finnisch erhältlich. Weitere Sprachen sind in Vorbereitung. ■

www.dguv.de/ifa

Autor: Dr. Michael Huelke, Referatsleiter 'Neue Technologien, Mensch und Technik', Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA)

Autor: Andy Lungfiel, Entwickler, Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA)