

SISTEMA – Softwareassistent zur Bewertung von sicherheitsbezogenen Maschinensteuerungen

Was kann SISTEMA?

Mit dem Software-Assistenten SISTEMA (Sicherheit von Steuerungen an Maschinen) steht Entwicklern und Prüfern von sicherheitsbezogenen Maschinensteuerungen eine umfassende Hilfestellung bei der Bewertung der Sicherheit im Rahmen der DIN EN ISO 13849-1 zur Verfügung. Das Windows-Tool bietet dem Benutzer die Möglichkeit, die Struktur der sicherheitsbezogenen Steuerungsteile (SRP/CS, Safety-Related Parts of a Control System) auf der Basis der sogenannten vorgesehenen Architekturen nachzubilden und erlaubt schließlich eine automatisierte Berechnung der Zuverlässigkeitswerte auf verschiedenen Detailebenen einschließlich des erreichten Performance Levels (PL).

Über Eingabemasken werden relevante Parameter wie die Risikoparameter zur Bestimmung des erforderlichen Performance Level (PL_r), die Kategorie des SRP/CS, die Maßnahmen gegen Fehler gemeinsamer Ursache (CCF) bei mehrkanaligen Systemen, die mittlere Bauteilgüte ($MTTF_d$) und die mittlere Testqualität (DC) von Bauelementen bzw. Blöcken Schritt für Schritt erfasst. Nachdem die geforderten Daten in SISTEMA eingetragen wurden, sind die berechneten Ergebnisse sogleich sichtbar. Praktisch für den Benutzer: Jede Parameteränderung wird in ihrer Auswirkung auf das Gesamtsystem über die Programmoberfläche direkt angezeigt. Das umständliche Nachschlagen in Tabellen und Ausrechnen von Formeln (Bestimmung der $MTTF_d$ nach der Parts Count Methode, Symmetrisierung der $MTTF_d$ für jeden Kanal, Abschätzung des DC_{avg} , Ermittlung von PFH und PL etc.) wird durch die Software übernommen und entfällt daher weitestgehend. Dies ermöglicht es dem Nutzer, Parameterwerte zu variieren, um so die Auswirkung von Änderungen zu beurteilen, ohne dabei großen Aufwand zu treiben. Die Resultate werden schließlich in einem druckbaren Report zusammengefasst.

Wie wird SISTEMA verwendet?

SISTEMA verarbeitet sogenannte Grundelemente aus insgesamt sechs verschiedenen Hierarchiestufen:

- das Projekt (PR),
- die Sicherheitsfunktion (SF),
- das Subsystem (SB),
- den Kanal (CH)/Testkanal (TE),
- den Block (BL) und
- das Element (EL).

Deren Zusammenhang ist in Abbildung 1 kurz dargestellt.

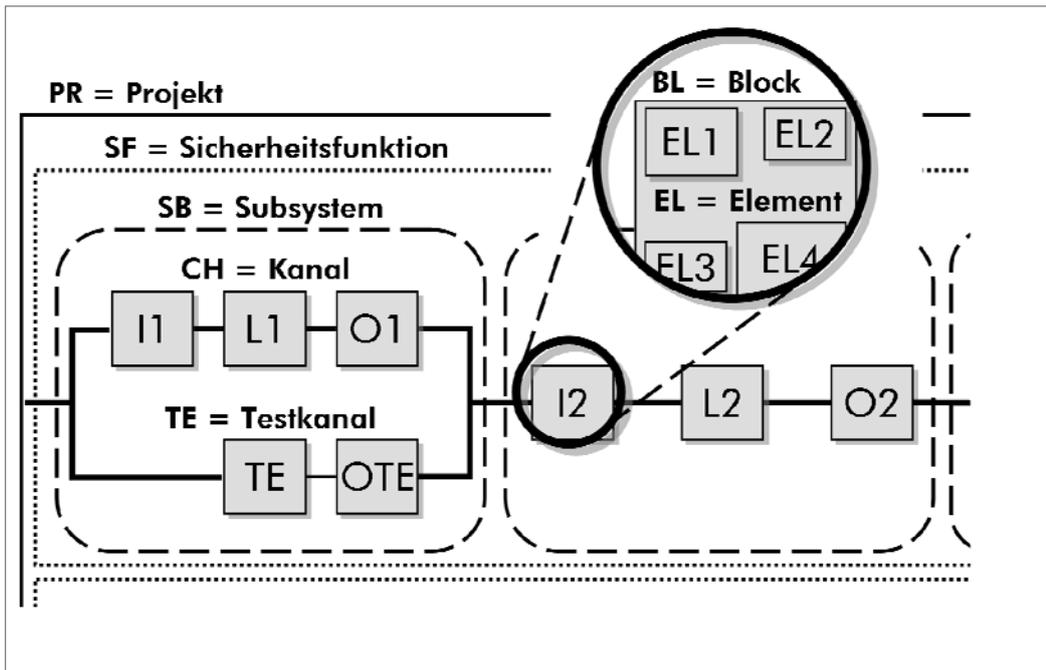


Abbildung 1: Die in SISTEMA betrachteten Hierarchieebenen

Der Benutzer eröffnet zunächst ein Projekt und kann darin die Maschine bzw. die Gefahrenstelle, die weiter betrachtet werden soll, definieren. Dem Projekt werden schließlich alle erforderlichen Sicherheitsfunktionen zugewiesen. Diese können durch den Benutzer festgelegt und dokumentiert sowie mit einem PL_r belegt werden. Der tatsächlich erreichte Performance Level (PL) des parametrisierten SRP/CS wird automatisch aus den Subsystemen ermittelt, die – in Serie geschaltet – die Sicherheitsfunktion ausführen. Den Subsystemen liegt jeweils – in Abhängigkeit zu der gewählten Kategorie – eine sogenannte vorgesehene Architektur aus der Norm zugrunde. Aus der Architektur bestimmt sich unter anderem, ob die Steuerung einkanalig, einkanalig getestet oder redundant ausgelegt ist und ob bei der Auswertung ein spezieller Testkanal zu berücksichtigen ist. Jeder Kanal kann sich wiederum in beliebig viele Blöcke unterteilen, für die der Benutzer entweder direkt einen $MTTF_d$ -Wert und einen DC-Wert einträgt oder aber auf der niedrigsten Hierarchieebene die Werte für die einzelnen Bauelemente einträgt, aus denen sich der Block zusammensetzt.

Weiterhin runden komfortable Bibliotheksfunktionen den Leistungsumfang von SISTEMA ab. Viele Hersteller von Komponenten und Bauteilen bieten SISTEMA-Bibliotheken mit Daten ihrer Produkte an. Auf den Internetseiten des IFA sind Links zu diesen Bibliotheken gelistet. Der Benutzer kann aber auch eigene Bibliotheken erstellen, in denen er selbst entwickelte Subsysteme oder häufig verwendete Bauteile abspeichern kann. Bibliotheken können lokal beim Benutzer, aber auch zentral auf Servern abgelegt sein.

Die Benutzerschnittstelle von SISTEMA

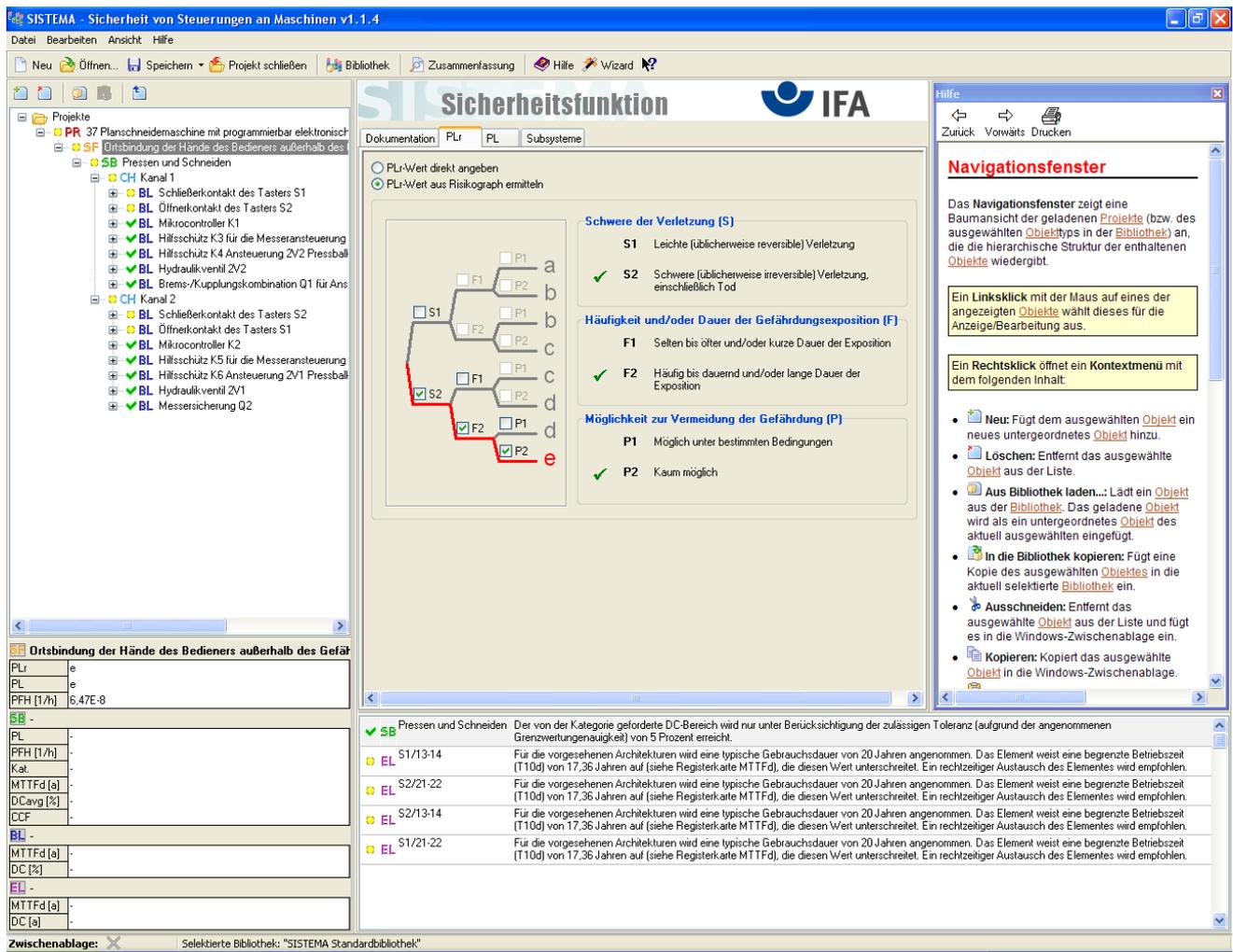


Abbildung 2: Die Programmoberfläche von SISTEMA

Die Programmoberfläche von SISTEMA gliedert sich in vier Bereiche (siehe Abbildung 2). Den größten Anteil der Fläche nimmt der Arbeitsbereich auf der rechten Seite ein. Er enthält je nach aktiver Sicht eine editierbare Eingabemaske oder einen Abschnitt aus dem Übersichtsdokument. Der Inhalt der jeweiligen Sicht ist durch das ausgewählte Grundelement aus der weiter oben genannten Hierarchie bestimmt und wird über die Selektion in einer Baumansicht auf der linken Seite festgelegt. Jede Verzweigung in der Baumansicht steht für ein Grundelement. Über den Baum lassen sich auch Grundelemente auf den verschiedenen Ebenen neu erzeugen, entfernen, verschieben oder kopieren. Die Details des angewählten Grundelements werden in der Editieransicht über die Eingabemaske eintragen. Jede Eingabemaske ist selbst über Register in verschiedene Bereiche untergliedert. Die jeweils letzte Registerkarte enthält eine Tabelle, die alle untergeordneten Verzweigungen zusammenfasst und die wichtigsten Informationen auflistet. Hat der Benutzer beispielsweise einen Block in der Baumansicht markiert, so zeigt diese Tabelle alle darin enthaltenen Elemente mit ihren MTTF_d- und DC-Werten an.

Ferner enthält die Baumansicht zu jedem Grundelement eine Statusinformation durch eine farbliche Markierung in Form eines Symbols neben der Verzweigung. Ein rotes Kreuz zeigt an, dass eine Bedingung der Norm nicht erfüllt ist, ein Grenzwert überschritten ist oder eine allgemeine Inkonsistenz vorliegt, durch die ein erforderlicher Wert nicht berechnet werden kann. In diesem Fall wird

eine Warnung ausgegeben. Gelb bedeutet, dass ein unkritischer Hinweis vorliegt (z. B. wenn ein Grundelement noch unbenannt ist). Alle anderen Grundelemente werden mit grünen Haken gekennzeichnet. Eine Farbkennzeichnung vererbt sich immer auch auf die übergeordneten Verzweigungen, wobei rot die höchste und grün die niedrigste Priorität hat. Alle Warnungen und Hinweise zu dem aktiven Grundelement werden im Meldungsfenster unterhalb des Arbeitsbereiches aufgeführt.

Der Bereich unterhalb der Baumansicht zeigt die wichtigsten Kontextinformationen des ausgewählten Grundelementes an. Diese bestehen aus PL , PFH , $MTTF_d$, DC_{avg} und CCF des übergeordneten Subsystems sowie PL_r , PL und PFH der übergeordneten Sicherheitsfunktion (das gilt natürlich nur für Grundelemente, die in tieferen Hierarchieebenen liegen). So sieht der Benutzer laufend, wie sich seine Änderungen in den angezeigten Parametern bemerkbar machen.

Neben ihrer Flexibilität zeichnet sich die Programmoberfläche von SISTEMA durch eine komfortable und intuitive Bedienbarkeit aus. Kontextspezifische Hilfetexte sollen den Einstieg erleichtern. Zusätzliche Unterstützung bietet der mit der Anwendung ausgelieferte Wizard – ein Assistent, der den Einsteiger Schritt für Schritt bei der virtuellen Nachbildung seiner Steuerung begleitet und ihm einen schnellen Zugang gewährleistet.

Wo sind SISTEMA und die Benutzeranleitungen zu erhalten?

Das Programm SISTEMA kann nach Registrierung kostenlos unter der Internetadresse www.dguv.de/ifa über den Webcode [d11223](#) heruntergeladen werden. Die Weitergabe an Dritte ist erlaubt. Eine Veränderung von SISTEMA ist aber nicht gestattet. SISTEMA enthält folgende Sprachversionen: Deutsch, Englisch, Französisch, Italienisch und Finnisch. Weitere Sprachversionen werden folgen. Anleitungen zur Benutzung von SISTEMA bieten die SISTEMA-Kochbücher (Webcode [d109240](#)) sowie die installierte Hilfedatei. Informationen und Hilfen zur EN ISO 13849-1 finden Sie über den Webcode [d18471](#) sowie über die Internetadresse www.dguv.de/ifa/13849.

Ansprechpartner:

Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA)
Referat 5.1
Dr. Michael Huelke
Alte Heerstraße 111
53757 Sankt Augustin
E-Mail: sistema@dguv.de