

Standardisierung sicherheitsgerichteter SPS-Applikationssoftware durch PLCopen

Erstmals Standard für „sichere“ Software

Im Rahmen der Hannover Messe 2005 wurde von der PLCopen eine Spezifikation zur Standardisierung von sicherheitsbezogenen Programmierumgebungen und Funktionsbausteinen als Entwurf erstmals öffentlich vorgestellt. Die Vorteile verdeutlicht ein Programmiersystem mit zertifizierten Softwarekomponenten, für das noch in diesem Jahr eine Bibliothek mit entsprechenden Funktionsbausteinen vorliegen soll.



Compliance-Logo „Safety“ der PLCopen

Die bereits zertifizierten sicherheitsbezogenen Softwarekomponenten von KW-Software erfüllen heute schon diesen internationalen Qualitätsstandard der PLCopen. Am Beispiel des sicheren Programmiersystems Safeprog werden nachfolgend die wichtigsten Inhalte der Spezifikation erläutert.

Warum Standardisierung?

In der Vergangenheit wurden durch die Zertifizierungsstellen bereits die Embedded-Software (Laufzeitsystem, Betriebssystem) und die Hardware einer sicherheitsgerichteten Automatisierungslösung intensiv geprüft.

DER AUTOR



Dipl.-Wirtsch.-Ing. Volker Sasse, Sales Manager für den Bereich sichere Softwarekomponenten bei der KW-Software GmbH in Lemgo (www.kw-software.de)

PRAXIS PLUS

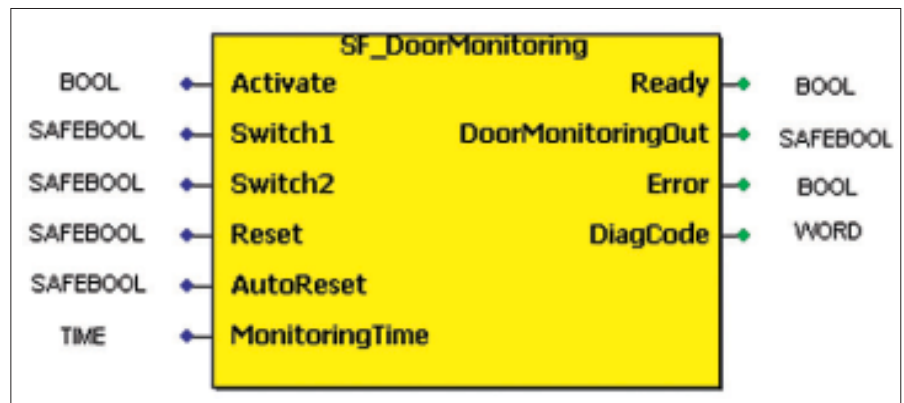
Durch die PLCopen-Safety-Spezifikation ist ein Meilenstein zur Standardisierung von sicherheitsgerichteter Applikationssoftware erreicht worden. Die Anwender können Software, die die Anforderung dieses Safety-Standards erfüllt, leicht am PLCopen-Compliance-Logo erkennen. Entsprechende Software ist durch einen hohen Qualitätsstandard gekennzeichnet. Mit dem Programmiersystem Safeprog von KW-Software ist bereits eine Engineering-Software im Markt verfügbar, die diese Anforderungen vollständig unterstützt.

Dies führt dazu, dass heute eine Vielzahl von Engineering-Software mit uneinheitlicher Bedienung und unterschiedlichen Ausprägungen der Sicherheitsfunktionen existieren. Erschwerend kommt hinzu, dass die existierende Engineering-Software meist nicht den aktuellen Qualitätsstandards der Sicherheitstechnik z.B. der IEC 61508 genügt. Dies liegt daran, dass im Rahmen der früheren Normen DIN VDE 0801 und EN 954-1 die Applikationssoftware kaum betrachtet wurde. Als Folge müssen sich sowohl SPS-Programmierer als auch Prüfungsstellen immer wieder mit unterschiedlichen Ausprägungen der Sicherheitslogik auseinandersetzen. Die Definition eines einheitlichen Standards für sicherheitsbezogene Applikationssoftware ist daher aus Sicht des Anwenders ein richtiger und wichtiger Schritt.

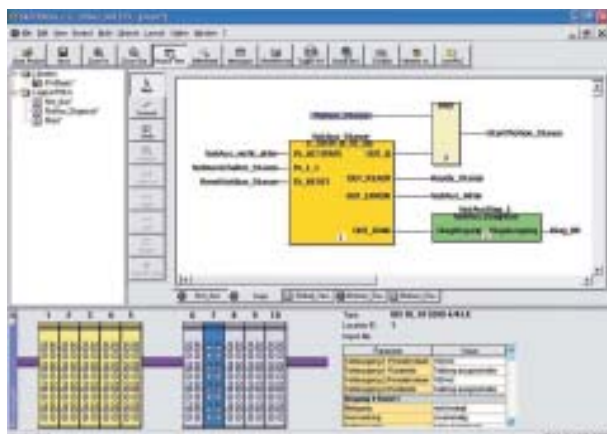
PLCopen-Safety-Spezifikation

Die Funktionalität einer Sicherheitssteuerung erschließt sich dem Anwender aber erst vollständig durch entsprechende Engineering-Software. Aber gerade im Bereich der sicherheitsgerichteten Applikationssoftware gibt es keine durchgängigen Anforderungen.

Im Rahmen der PLCopen wird von deren Mitgliedern – darunter fast alle führenden Hersteller von Sicherheitssteuerungen und der verwendeten Programmierertools – sowie externen Organisationen (BGIA, TÜV Rheinland) eine



Beispiel gemäß PLCopen-Spezifikation des sicheren Funktionsbausteins Schutztür mit den definierten Datentypen der Ein- und Ausgänge



Der grafische Editor im Safeprog



Die sichere Software-Plattform von KW-Software

Spezifikation zur Standardisierung der sicherheitsbezogenen Applikationssoftware erarbeitet. Erstmals wurde auf der Hannover Messe eine Vorab-Version vorgestellt. Ziel ist es, dass bis zur SPS/IPC/Drives (22. bis 24. November in Nürnberg) diese Spezifikation von der BGIA und dem TÜV Rheinland freigegeben wird.

Die Spezifikation geht im Wesentlichen auf die Standardisierung von sicheren Funktionsbausteinen sowie die standardisierte Nutzung dieser Bausteine in einer Engineering-Software ein. Im Folgenden wird auf die wichtigsten Inhalte exemplarisch eingegangen. Diese sind:

- Sichere Funktionsbausteine,
- Sicherheits-Datentypen,
- Empfehlung für Programmierrichtlinien und
- abgestufte User-Level.

Herstellerunabhängige Projektierung erleichtert

Im Rahmen der PLCopen-Arbeitsgruppe sind nach aktuellem Stand 19 Sicherheits-Funktionsbausteine hinsichtlich der Ein-/Ausgänge, der Zustandsmaschine, Fehlererkennung

und Fehlerbehandlung spezifiziert worden. Darunter sind die wichtigsten Sicherheitsfunktionen wie Not-Aus, Schutztür, Betriebsartenwahlschalter, 2-Handkontrolle enthalten. Auf Basis der PLCopen-Spezifikation wird es Anbietern von sicheren Automatisierungssystemen deutlich erleichtert, diese Bausteine zu implementieren und zu zertifizieren. Die beispielhaft genannten Bausteine sind bereits heute Bestandteil des sicheren Programmiersystems Safeprog von KW-Software, das im Rahmen der Interbus-Safety-Plattform von Phoenix Contact mit Erfolg zertifiziert worden ist.

Die korrekte Verwendung der sicheren Funktionsbausteine gemäß PLCopen wird dem SPS-Programmierer durch die Hersteller übergreifende Funktionalität erleichtert. Dazu zählen der geringere Schulungsbedarf und die einfachere Übertragung von programmierten Sicherheitsfunktionen auf verschiedene SPS-Systeme. Ein weiterer Vorteil ist der geringe Aufwand für die Validierung des SPS-Programms durch den

Inbetriebnehmer, wenn Teile der Sicherheitslogik auf bereits zertifizierten Softwarebausteinen beruhen. KW-Software wird als eines der ersten Unternehmen mit der Implementierung der sicheren Funktionsbausteine gemäß der PLCopen beginnen. Zehn sichere Softwarebausteine sollen noch in diesem Jahr als Bibliothek im Programmiersystem Safeprog angeboten werden.

Sichere und nicht sichere Funktionen eindeutig trennen

Um eine mögliche Verwechslung von sicheren und nicht sicheren Datentypen (Variablen) zu vermeiden, wurde der Datentyp Safebool in der PLCopen-Spezifikation definiert. Dieser Datentyp kann nur im Zusammenhang mit den sicherheitsgerichteten Softwarebausteinen eingesetzt werden. Entsprechende Plausibilitätsprüfungen sollten – wie im Safeprog – durch das Programmiersystem durchgeführt werden.

Um den Programmierrichtlinien der PLCopen-Spezifikation gerecht zu werden, sollte der grafische Editor der Engineering-Software durch

geeignete Maßnahmen die sicherheitsgerichtete Programmierung unterstützen. Dies kann durch eine farbliche Kennzeichnung der unterschiedlichen Typen von Funktionsbausteinen, Kennzeichnung von nicht sicheren Datentypen (Variablen) und weitere Plausibilitätsprüfungen im grafischen Editor erreicht werden.

Abgestufte User-Level für verschiedene Anwendungen

Im Rahmen der PLCopen-Spezifikation wurden verschiedene User-Level identifiziert, die auf eine unterschiedliche Erfahrung und Verantwortung des Anwenders für die Erstellung des SPS-Programms abzielen:

- Basic-Level: Anwendung von zertifizierten Bausteinen,
- Expert-Level: Verwendung von zertifizierten Bausteinen und Erstellung eigener Sicherheitslogik,
- System-Level: Erstellung von zertifizierten Funktionsbausteinen durch den Anbieter.

Abhängig vom User-Level wurde der Umfang an Standardfunktionen und Standard-Funktionsbausteinen unterschiedlich definiert. Im Basic-Level ist es dem Anwender nur durch die Verschaltung mit den Funktionen (und, oder) bereits zertifizierter Funktionsbausteine unter der Verwendung elementarer Zeit- und Zählerbausteine möglich, die Sicherheitslogik zu erstellen. Umfangreichere Möglichkeiten stehen ihm im Expert-Level zur Verfügung. Entsprechend der unterschiedlichen User-Level der PLCopen bietet KW-Software zwei Ausprägungen für die Programmierung einer Sicherheits-SPS an. Safeconf bezieht sich auf den Basic-Level und Safeprog deckt den Expert-Level ab. Safeprog wird Anbietern von Sicherheitssteuerungen in einer gesonderten OEM-Version im System-Level zur eigenen Erstellung sicherer zertifizierter Funktionsbausteine für Bibliotheken zur Verfügung gestellt.

eA-INFO-TIPP

Die Innovation der nach IEC 61508 (SIL3) zertifizierten Softwarelösung Safeprog/Safeos hat sich auch bei der Vergabe des Automation Award 2004 gezeigt, und zwar mit dem sehr guten zweiten Platz. Das gesamte Ranking der zehn anlässlich der SPS/IPC/Drives 2004 nominierten Produkte finden Sie unter:
 • www2.ea-online.de/ea/live/automation_award/liste.html