



»SAFEGRID« besitzt als sichere Softwarekomponente alle Funktionalitäten für die sichere Geräteparametrierung.

Besser sicher parametrieren

Sicherheitskonzept – Funktionale Sicherheit in Geräten und Reglern erfordert eine Sichere Parametrierung. Eine zertifizierte Softwarekomponente hilft weiter.

Im Folgenden wird die Funktionsweise dieser Softwarekomponente, die sich herstellernerneutral anpassen und einfach in existierende Softwaretools integrieren lässt, beschrieben. Funktionsprinzip ist ein vierstufiges Sicherheitskonzept, welches kein Rücklesen und Vergleichen der übertragenden Parameter erfordert. »Safegrid« bietet darüber hinaus viele Komfortfunktionen, die die Parametrierung nicht nur sicher, sondern auch einfach gestalten.

Funktionale Sicherheit

Die Aspekte der funktionalen Sicherheit für elektrische oder elektronische Systeme – auch programmierbar – sind in der Normenreihe IEC 61508 beschrieben. In modernen Systemen wie Maschinen, Anlagen, Geräten etc. besteht die Herausforderung bezüglich der funktionalen Sicherheit darin, die korrekten Funktionen von komplexen programmierbaren Systemen sicherzustellen. Wichtig ist die Methoden- und Sachkompetenz zur Vermeidung systematischer Fehler. Diese sind in der Regel menschlicher Natur und entstehen z.B. bei der Spezifikation oder der Implementierung. Auch physikalische Phänomene, die zu Störungen und Ausfällen führen können, gilt es zu beherrschen. Ein Antriebsregler mit integrierter Sicherheitsfunktion stellt eines dieser modernen Systeme dar.

Herstellerneutrale Softwarekomponente

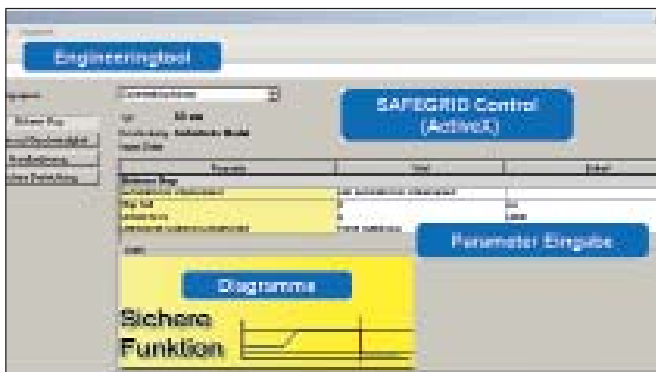
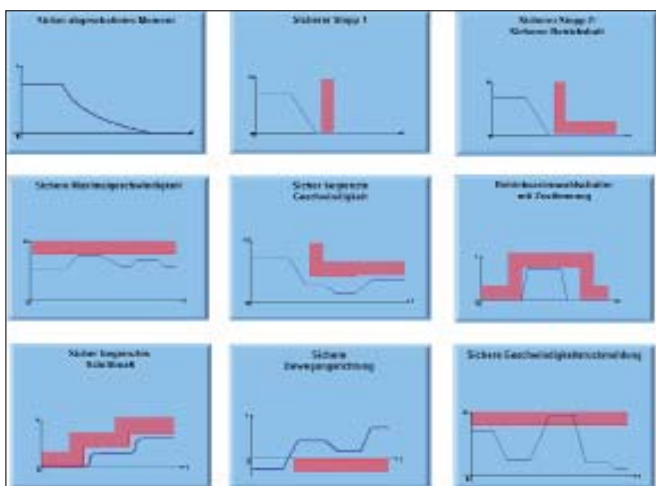
Safegrid ist eine sichere, nach IEC 61508 zertifizierte Softwarekomponente. Die Integration erfolgt in die Rahmenan-

wendungen, also in das Engineering-Tool der Geräteherstellung als visuelles ActiveX oder .Net Control Element. Die primäre Anforderung einer Geräteparametrierung nach den Vorgaben der Sicherheitstechnik erfüllt Safegrid durch sein integriertes Konzept. Die individuelle Gestaltung der Parametrierungs-Oberfläche, als sekundäre Anforderung, in Bezug auf das zu parametrierende Gerät, erfolgt über die Gestaltung einer Beschreibungsdatei. Die Gerätebeschreibungs-Datei definiert flexibel die Inhalte des Safegrid. Die Inhalte des Safegrid werden herstellerspezifisch in einer Gerätebeschreibungs-Datei für ein sicheres Automatisierungsgerät beschrieben (z.B. XML). Auf diese Weise können später unabhängig von der KW-Software sehr flexibel weitere Parameter, Funktionen oder Sprachversionen hinzugefügt werden. Die Gerätebeschreibungs-Datei wird durch eine Checksumme gesichert und im File-System des PC abgelegt.

Sicherheitskonzept in vier Stufen

Safegrid lässt sich durch einen Container (Safegrid Frame) in bereits existierende Engineering-Tools auf Basis Windows 32 bit Technologie oder .Net leicht integrieren. KW-Software bietet als Unterstützung für die Integration des Safegrid sowie für die Definition der Gerätebeschreibungs-Datei einen Integration Guide an.

Durch das vierstufige Sicherheitskonzept des Safegrid ist das Rücklesen der einzelnen Parameter mit der expliziten Bestätigung durch den Anwender nicht mehr notwendig. Es wird lediglich die Checksumme



Sicherheitsfunktionen eines Antriebsreglers (oben). Die Oberfläche von Safegrid gestaltet eine einfache Integration in bestehende Tools.

des entsprechenden Parametersatzes vom sicherheitsgerichteten Automatisierungsgerät im Hintergrund zurück gelesen. Der Anwender wird anschließend über den Status der Parametrierung per Dialog informiert.

Vier Schritte zur Sicherheit

Schritt 1: Die gesicherte Eingabe der über die Tastatur eingegebene Werte im Stringformat wird nach Bestätigung zunächst als Binärwert im RAM, also im Arbeitsspeicher des Rechners gespeichert. Der eingegebene Wert wird auf dem Bildschirm gelöscht und der im RAM gespeicherte Wert, wieder auf Stringformat gewandelt, zur Anzeige gebracht. Dies hat die Sicherheit, dass die Daten der Eingabe, der Anzeige und des Speicherinhaltes konsistent sind. Ein Fehler bei der Eingabe wird unmittelbar durch den Anwender erkannt und korrigiert.

Schritt 2: Die gesicherte Datenhaltung wird über entsprechende Checksummen im Arbeitsspeicher sichergestellt. Nur der zu parametrierende Wert liegt außerhalb der Checksumme und wird nach Bestätigung Teil dieser, durch eine neue CRC(cyclic redundancy check)-Berechnung. Nicht nur der Parametersatz, sondern auch die XML-Konfiguration, welche eindeutig einem Gerätetyp zugeordnet ist, wird gesamtheitlich durch CRC gesichert und auf Datenträger wie Festplatte gespeichert.

Schritt 3: Die gesicherte Erzeugung des Parametersatzes erfolgt diversitär. Dies bedeutet konkret, dass der später auf das Zielgerät zu übertragende Byte-stream nach zwei unterschiedlichen Algorithmen erzeugt wird. Für beide Datensätze wird eine Checksumme berechnet. Sowohl die Datensätze als auch die Checksummen werden verglichen. Um hier mögliche Fehler aufzudecken, wird der diversitär erzeugte Parametersatz mit der Checksumme kombiniert. Auf dem Zielgerät wird dann durch die erneute Checksummengenerierung ein eventueller Fehler erkannt.

Schritt 4: Der gesicherte Datentransfer zum Zielgerät kann aufgrund der Datensicherheit mittels Standardkommunikation über Ethernet, USB, WLAN

etc. erfolgen. Ein - nicht notwendiges - Rücklesen vom Parametersatz als Bestätigung der sicheren Übertragung schließt den Vorgang.

Ein Blick auf die Oberfläche von Safegrid zeigt neben dem wirklichen Sicherheitskonzept eine Reihe von professionellen Funktionen, die die Parametrierung von sicheren Geräten für den Anwender komfortabel gestalten.

Komfortable Bedienung

Einzeln vordefinierte Parametergruppen, strukturiert in

Gruppen, ermöglichen die Bereitstellung ganzer Funktionen. Auswahlfelder zeigen die definierten Parameter bzw. Parameterbereiche. Um dem Anwender eine weitere einfache Hilfestellung zu bieten, erfolgt eine farbliche Zuordnung zwischen gültigen und ungültigen Parametern. Durch einen Farbumschlag bei der Eingabe von korrekten Parametern in Blau und nicht korrekten Parametern in Rot, sieht der Anwender sofort, welche Werte zulässig und welche Werte abgelehnt werden. Darüber hinaus sind Plausi-

bilitätsprüfungen definierbar. Sind mehrere Parameter im Widerspruch zueinander, werden diese abgelehnt. Jedem Feld kann in der Eingabemaske zur besseren Erläuterung ein Tool-Tip zugeordnet werden. Zur besseren Verdeutlichung des Parameterwertes können zusätzlich Grafiken eingebunden werden. Selbstverständlich können Parametersätze importiert und exportiert werden.

Thorsten Behr, KW-Software



BAUMER IVO VILLINGEN-SCHWENNIN/?/ (Index: 0) 149 x 202 mm