PROFIBUS • PROFINET

PROFIsafe Systembeschreibung

Technologie und Anwendung

PROFIsafe

Einleitung

PROFIBUS und PROFINET sind die einzigen industriellen Kommunikationssysteme, die eine durchgängige Lösung für alle Bereiche der Fertigungs- und Prozessautomatisierung bieten. Beide Protokolle sind in der Kommunikationsprofilfamilie 3 in den internationalen Normen IEC 61158 und IEC 61784-1/-2 spezifiziert.

Eines der wichtigsten Ereignisse seit Bestehen von PROFIBUS &PROFINET International (PI) war die Veröffentlichung der ersten Spezifikation für funktional sichere Kommunikation im Jahr 1999. Dieser Schritt bedeutete einen Quantensprung in der Welt der Automatisierung und eröffnete eine Vielzahl von neuen Möglichkeiten.

Der Name dieser Technologie ist PROFIsafe. Das PROFIsafe-Logo ist untenstehend zu sehen.

Seither hat sich PROFIsafe zur weltweit führenden und durchgängigsten Technologie für funktional sichere Kommunikation entwickelt. PROFIsafe ist seit 2007 internationale Norm unter der Bezeichnung IEC 61784-3-3.

In dieser Systembeschreibung soll ein umfassender Einblick in die PROFIsafe-Technologie und verwandte Themen vermittelt werden, ohne sich dabei zu sehr in Details zu verstricken. Die vorliegende Schrift ersetzt keineswegs die angesprochenen Spezifikationen und Richtlinien. Ausschließlich diese sind maßgebend und verbindlich.

PROFIsafe wurde von TÜV und von IFA anerkannt.

Funktionale Sicherheit ist ein ernstes Thema in der Automatisierung. Daher müssen die Verbreitung, die Implementierung und der Einsatz der PROFIsafe-Technologie sorgfältig angegangen werden. Alle beteiligten Firmen und Institutionen sind dazu verpflichtet, sich zur sogenannten „PROFIsafe Policy" zu bekennen.

Diese kurze Beschreibung ist als Ergänzung und übersichtliche Zusammenfassung der offiziellen Dokumente zu verstehen.

Die Abkürzung „F" steht in diesem Dokument für „fail-safe" (ausfallsicher), „funktionale Sicherheit" oder einfach „sicherheitsgerichtet".

Inhaltsverzeichnis

1. Sicherheit in der Automatisierung

Jeder industrielle Prozess ist mehr oder weniger mit dem Risiko verbunden,

- Menschen zu verletzen / zu töten,
- die Umwelt zu zerstören,
- oder Investitionen zu schädigen.

Bei den meisten Prozessen ist es relativ einfach, Risiken ohne allzu hohe Anforderungen an die Automatisierungssysteme zu vermeiden. Es gibt aber auch typische Anwendungen mit hohen Risiken. Dazu gehören Pressen, Werkzeugmaschinen, Roboter, Förder- und Verpackungssysteme, Hochdruckverfahren, Offshore-Technik, Feuer- und Rauchmelder, Brenner, Seilbahnen usw. Solche bedürfen spezieller Vorsorge und Technologien.

Mit der Zeit sorgt der Markt dafür, dass sich die Zuverlässigkeit und Verfügbarkeit der Standard-Automatisierung auf ein gewisses wettbewerbsfähiges Kostenniveau einstellt. Die Ausfall- oder Fehlerrate der Standard-Automatisierung ist dann zwar akzeptabel für normale Einsatzszenarios, für obige Risiko-Anwendungen reicht sie aber nicht.

Dies ist vergleichbar mit dem Postsystem. Normale Postsendung soll günstig sein bei akzeptabler Zuverlässigkeit. Für wichtige Nachrichten gibt es das „Einschreiben".

1.1 Technologiewandel

In der Vergangenheit haben Mikrocontroller, Software, PCs und Kommunikationsnetzwerke einen gewaltigen Einfluss auf die Standard-Automatisierung ausgeübt und zu einer erheblichen Kostenreduzierung, höherer Flexibilität und Verfügbarkeit geführt. Die Anwendung der neuen Technologien war aber in den Sicherheits-Normen zunächst untersagt. Sichere Automatisierung musste noch „festverdrahtet" sein und auf Relais-Technik basieren (siehe Abbildung 1).

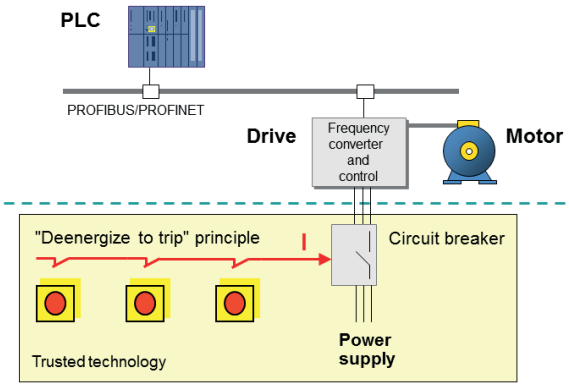

Abb. 1: Klassische Sicherheitstechnik

Dieser Zwiespalt ist verständlich. Beruht doch Sicherheit auf vertrauter Technik und bewährtem Material. Vertrauen braucht Erfahrung und diese braucht Zeit. Die Einbindung klassischer Sicherheit in moderne Automatisierung bringt aber oft nachteilige Auswirkungen. Dies sind z.B. Kosten für zusätzliche Verkabelung und Programmierung, geringere Flexibilität und Verfügbarkeit als erwartet und weitere Nachteile wie unbestimmte Haltepositionen von Maschinen und dadurch hoher Aufwand beim Wiederanlauf.

Heutzutage haben sich Mikrocontroller und Software in Millionen von Anwendungen bewährt. Die Voraussetzungen für deren Einsatz in F-Anwendungen sind mit der Veröffentlichung der internationalen Norm IEC 61508 geschaffen.

In vielen digitalen Kommunikationssystemen wurden die Mechanismen zur Fehlererkennung untersucht und vertieft. Normen wie die IEC 62280-1 halfen den Weg zu ebnen.

1.2. Realisierungen bei PI

Dies war der Auslöser für PROFIBUS & PROFINET International (PI), die PROFIsafe-Technologie als zusätzliche Schicht oberhalb der bereits existierenden PROFIBUS und PROFINET-Protokolle zu entwickeln. Dank PROFIsafe kann die Restfehlerwahrscheinlichkeit bei Datenübertragungen zwischen einem F-Host (Sicherheitssteuerung) und einem F-Device (Sicherheitsgerät) auf ein von den Normen gefordertes Maß reduziert oder sogar unterschritten werden.

PROFIsafe kann vollständig in Software implementiert werden und deckt damit, unter Verwendung von PROFIBUS und PROFINET, das komplette Spektrum an Sicherheitsanwendungen in der Prozess- und Fertigungsautomatisierung ab. PROFIsafe ist sogar für drahtlose Übertragungstechniken, wie z.B. WLAN und Bluetooth zugelassen. Unter Einbezug von IT-Sicherheitstechnik (Security) wie dem Zonenkonzept, kann es über Ethernet-Backbones angewendet werden.

PROFIsafe bietet so in der Prozessautomatisierung hohe Verfügbarkeit und geringen Energieverbrauch und in der Fertigungsautomatisierung kurze Reaktionszeiten im Bereich von ms.

Moderne F-Devices wie Laserscanner oder Antriebe mit integrierter Sicherheit können sich nun frei entfalten. So erleichtert ein ausgeklügelter iPar-Server die Verwaltung der individuellen Sicherheitsparameter (iParameter). Er umfasst Schnittstellen für F-Device-Tools (z.B. das Tool Calling

Interface) sowie Optionen zur Speicherung und zum Wiederladen von iParametern (iPar-Server). Es sei hier darauf hingewiesen, dass die Schnittstellen zu Tools und die iPar-Server-Option auch in nicht-sicherheitsgerichteten Geräten verwendet werden können.

Die Norm IEC 61508 fordert u.a. eine höhere elektromagnetische Störfestigkeit, ohne Einzelheiten festzulegen. Die ergänzende Richtline „PROFIsafe Environment" füllt diese und andere Lücken und fördert so die Entwicklung und den Einsatz von F-Devices und F-Hosts.

Bei PI besteht die Regel, dass in PROFIBUS- und PROFINET-Netzwerken nur nach IEC 61508 zertifizierte F-Devices und F-Hosts zulässig sind. Die Konformität mit dem PROFIsafe-Protokoll muss in akkreditierten PI Testlabors überprüft und von PI zertifiziert werden. Eine ergänzende „PROFIsafe Test-Spezifikation" legt die Rollen und Aufgaben der Zertifizierungsstellen (z.B. TÜV) und der PI Testlabors fest.

Für aktuelle Informationen über PROFIsafe besuchen Sie bitte www.profisafe.net. Für allgemeine Informationen über PROFIBUS und PROFINET besuchen Sie bitte www.profibus.com.

1.3. Internationale Normen

In den meisten Ländern regulieren nationale Gesetze den Schutz von Mensch und Umwelt. In Europa z.B. sind die Niederspannungsrichtlinie, die EMV-Richtlinie und die Maschinenrichtlinie typische Beispiele für eine solche Gesetzgebung. Die Gesetze verweisen wiederum auf „gelistete" internationale Normen.

In Abbildung 2 finden Sie eine Auswahl an relevanten IEC- und ISO-Normen zu den Themen „Sicherheit" und „Feldbusse" und deren Zusammenhänge.

Die Grundnorm für funktionale Sicherheit ist die IEC 61508, in der funktionale Sicherheit von elektrischer Ausrüstung und grundlegende Prinzipien und Verfahren abgedeckt werden. Sie liefert einen quantitativen Ansatz zur Berechnung der Restwahrscheinlichkeit für gefährliche Fehler in sogenannten Sicherheitsfunktionen (Safety Integrity Levels - **SIL**). Dies ist besonders für Entwickler von F-Devices und F-Hosts hilfreich. Die Sektornorm IEC 62061 beschreibt spezielle Sicherheitsaspekte für Maschinenanwendungen in der Fertigungsautomatisierung. Diese Norm betrachtet Systeme, Subsysteme und einzelne Elemente und wie deren Kombinationen in Sicherheitsfunktionen zu beurteilen sind. ISO 13849 ist der Nachfolger der EN 954-1 (zurückgezogen

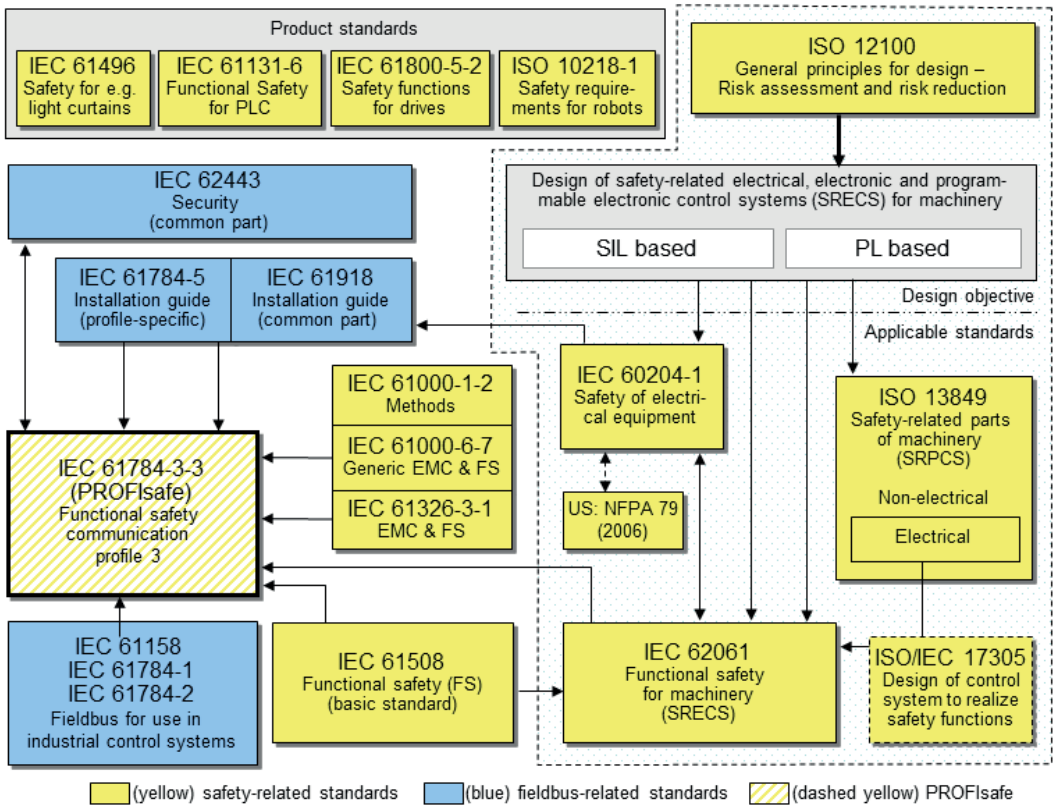

Abb. 2: Feldbus- und Sicherheitsnormen für Fabrikautomatisierung

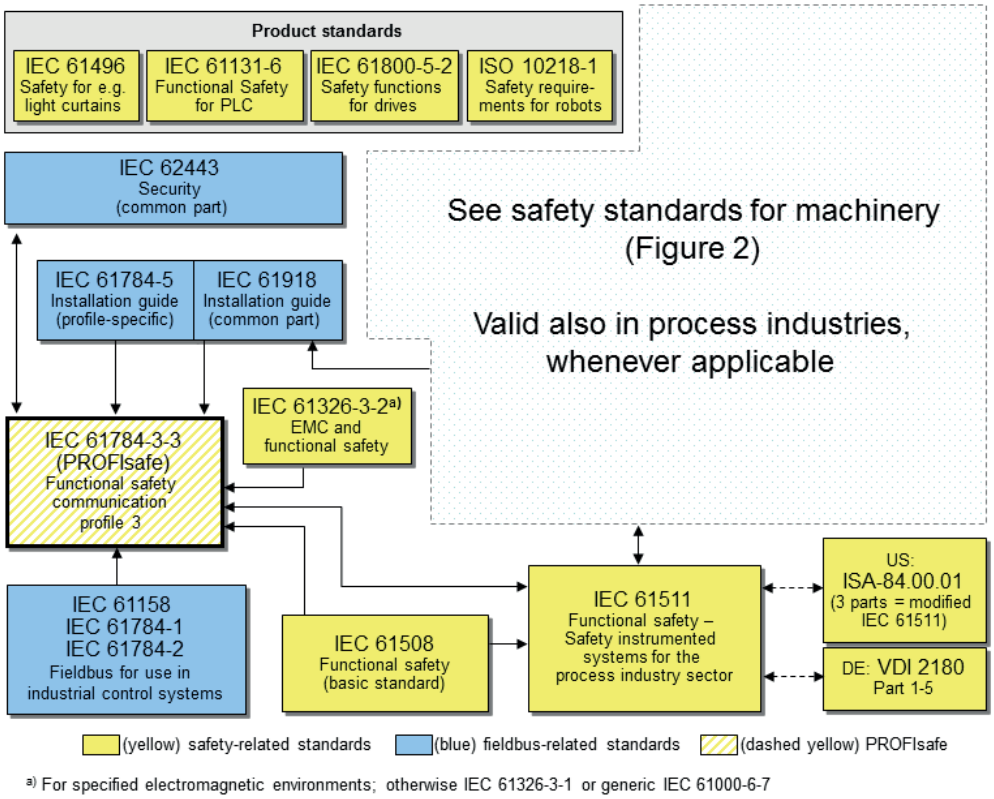

Abb. 3: Feldbus- und Sicherheitsnormen für Prozessautomatisierung

in 2011) mit ähnlichem Zweck. Sie führt aber ein leicht abgewandeltes Berechnungsmodell (Performance Levels - **PL**) ein und deckt auch nicht-elektrische Geräte wie z.B. hydraulische Ventile ab. In der Maschinensicherheit werden in der ISO 12100 sowohl die Basis-Terminologie und Entwurfsmethoden als auch die Risikobewertung und Risikoverringerung definiert. Die IEC 60204-1 spezifiziert allgemeine Anforderungen und Empfehlungen zur elektrischen Ausrüstung von Maschinen. Hierzu zählen Themen wie die Spannungsversorgung, Schutz vor elektrischem Schlag, Not-Halt, Leitungen und Kabel usw. Produktnormen wie IEC 61496, IEC 61800-5-2, IEC 61131-6 und ISO 10218-1 beschreiben die Anforderungen an individuelle Produktfamilien.

Im Anhang der europäischen Maschinenrichtlinie werden die Maschinen und Teile aufgelistet, die laut Gesetz einer Zertifizierung z.B. durch eine akkreditierte Stelle (IFA, TÜV, FM - Factory Mutual, usw.) bedürfen. Bei harmonisierten Produktnormen (z.B. IEC 61496) kann eine Herstellererklärung reichen.

Die Anforderungen an F-Devices und F-Hosts für höhere EMV-Festigkeit sind in IEC 61326-3-1 festgelegt. Bewertungskriterien wie DS („defined state") bei funktionaler Sicherheit lassen Funktionsabweichungen unter speziell erhöhter elektromagnetischer Störbelastung zu. Das Prüfobjekt (EUT) muss in diesen Fällen jedoch mindestens in einen sicheren Zustand übergehen.

Die Feldbusnormen sind in IEC 61158 und IEC 61784-1 spezifiziert. Varianten für Echtzeit-Ethernet, wie z.B. PROFINET IO sind in IEC 61784-2 definiert. Allgemeine Festlegungen der Installationsrichtlinien sind in IEC 61918 zusammengefasst, profilspezifische in IEC 61784-5. Allgemeine Security-Richtlinien gibt es in der IEC 62443, profilspezifische sind geplant für eine zukünftige IEC 61784-4.

In Abbildung 3 ist eine ähnliche Auswahl an IEC- und ISO-Normen zu finden, die an die Gegebenheiten der Prozessautomatisierung angepasst wurden. Hier beschreibt die Sektornorm IEC 61511 die Situation der Langzeiterfahrung (Betriebsbewährung) im Bereich der höchst sensiblen Prozessinstrumentierung in einer definierten elektromagnetischen Umgebung. Die Sektornorm IEC 61326-3-2 berücksichtigt dementsprechend die EMV-Anforderungen für diese Umgebungen.

2. Anforderungen erfüllt

Von Beginn an war PROFIsafe darauf ausgerichtet, dem Entwickler von F-Geräten und dem Endanwender eine umfassende und effiziente Lösung zur Verfügung zu stellen.

Das PROFIsafe-Protokoll hat keine Rückwirkungen auf PROFIBUS- und PROFINET-Netzwerke. Sicherheits-Nachrichten können daher über die Buskabel zusammen mit Standardnachrichten übertragen werden (Abbildung 4).

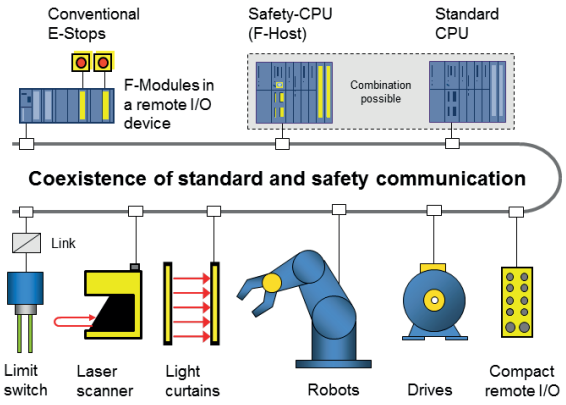

Abb. 4: Der „Single Channel"-Ansatz

Diese „Single-Channel"-Lösung erlaubt auch den Einsatz einer Standard-SPS mit integrierter, aber logisch getrennter F-Verarbeitung. Optional kann so Medien-Redundanz für Hochverfügbarkeit realisiert werden. Für Anwender, die Standard- und F-Kommunikation lieber physisch trennen möchten, stellt PROFIsafe kein Hindernis dar. Selbst Anwender von separierten Netzwerken profitieren dennoch von der einheitlichen Technologie.

Das PROFIsafe-Protokoll hat keine Rückwirkung auf die Standard-Busprotokolle. Es soll so unabhängig wie möglich vom jeweiligen Übertragungskanal sein, gleich ob Kupferkabel, Lichtwellenleiter, Rückwandbus oder drahtlos. Weder die Übertragungsraten noch die jeweilige Fehlererkennung spielen eine Rolle. Für PROFIsafe sind die Übertragungskanäle lediglich „Black Channels" (Abbildung 5).

Das PROFIsafe-Protokoll erspart dem Anwender die Sicherheitsbeurteilung seines individuellen Rückwandbussystems oder anderer Kanäle über PROFINET und PROFIBUS hinaus. Es gewährleistet daher die funktionale Sicherheit des kompletten Pfades, vom Sender eines F-Signals (z.B. F-Modul in einem entfernten Busterminal) bis zum Empfänger (F-Host) und umgekehrt (Abbildung 6).

Das PROFIsafe-Protokoll kann für sicherheitsgerichtete Anwendungen bis SIL3 gemäß IEC 61508 / IEC 62061 oder PL „e" / Kategorie 4 gemäß ISO 13849 eingesetzt werden.

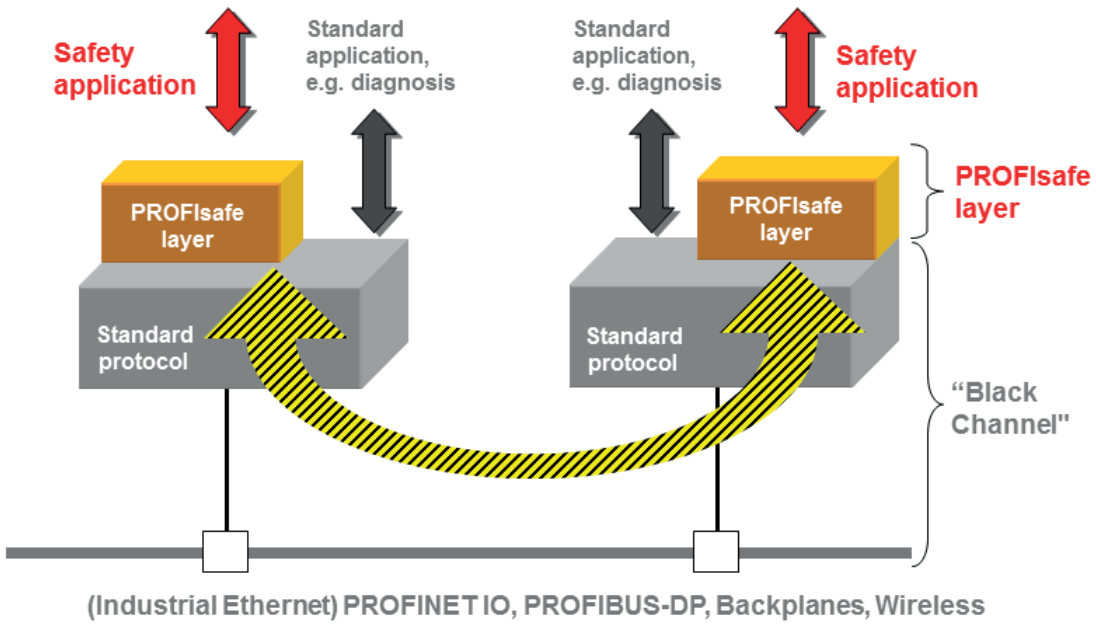

Abb. 5: Das „Black Channel"-Prinzip

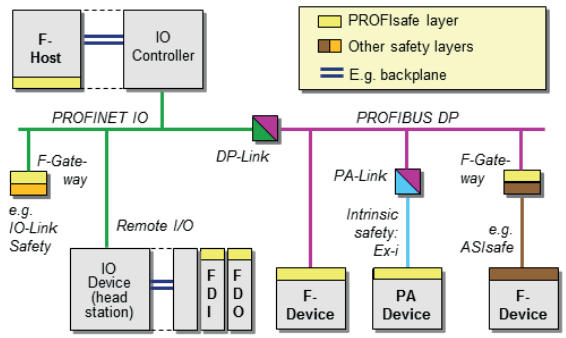

Abb. 6: Der vollständige Sicherheitskommunikationspfad

Die Parameter des PROFIsafe-Protokolls sind nach den Vorgaben von PROFIBUS bzw. PROFINET handzuhaben, z.B. über GSD. Sie sind jedoch während des Speicherns, der Auswertung, der Wertzuweisung und des Transfers vom Konfigurationstool über den IO-Controller bzw. DP-Master bis zum F-Device zu sichern. Alle F-Devices oder F-Module in entfernten Busterminals haben den gleichen PROFIsafe-(Protokoll)-Parametersatz (sogenannte F-Parameter) zu verwenden, um eine einheitliche Verwaltung zu ermöglichen.

Die individuellen Sicherheitsparameter (iParameter) von F-Devices sind technologiespezifisch, z.B. bei Antrieben mit integrierter Sicherheit, Laserscannern, usw. Diese iParameter per GSD zu verwalten wäre extrem aufwändig und brächte unnötige Abhängigkeiten. Daher ist es den Entwicklern von F-Devices zu ermöglichen, ihre individuellen Konfigurations-, Parametrier-, und Diagnose-Tools (CPD-Tools) über entsprechende Schnittstellen in Engineering-Tools integrieren zu können. Dies erleichtert die Navigation und Kommunikation zu einzelnen F-Devices oder F-Modulen.

Zum schnellen Tausch von F-Devices im Fehlerfall hat das System ein zentrales Speichern und Abrufen von individuellen Sicherheitsparametern (iPar-Server) zu ermöglichen. Dies kann durch die Steuerung geschehen, die für die GSD-basierte Startparametrierung des Busses sorgt.

In ergänzenden Anleitungen sind alle Aspekte für den Einsatz von PROFIsafe-Geräten festgelegt, so z.B. die Anforderungen an:

- Installation
- Elektrische Sicherheit
- Spannungsversorgungen
- Elektromagnetische Verträglichkeit
- IT-Sicherheit (Security)

Schließlich erhalten Entwickler von PROFIsafe F-Devices oder F-Modulen bestmögliche Unterstützung durch PROFIsafe-Development-Kits sowie durch Kompetenz- und Testzentren.

In der aktuellen Version erfüllt PROFIsafe all diese Anforderungen. Dennoch bleibt das Konzept einfach und ist leicht zu verstehen.

Bevor PROFIsafe im Detail betrachtet wird, werden bestimmte Voraussetzungen und Randbedingungen beschrieben.

3. „Black Channel" Vorgaben

Obwohl PROFIsafe das Black-Channel-Prinzip nutzt, gibt es gewisse grundlegende Eigenschaften von PROFIBUS und PROFINET, die bei der Entwicklung von PROFIsafe berücksichtigt wurden.

3.1. Basisfunktionen

Die zyklische Kommunikation zwischen einem Bus-Controller und seinen Feldgeräten (Ansprache und Antwort-Prinzip) ist eine dieser Basisfunktionen. Das Prinzip spürt jedes defekte Gerät unmittelbar auf. PROFIsafe baut auf dieses Prinzip.

Eine weitere Funktion ist die 1:1 Kommunikationsbeziehung zwischen einem Bus-Controller und seinen zugeordneten Feldgeräten. PROFIsafe baut auf dieses Prinzip, um die Authentizität von Nachrichten zu gewährleisten.

3.2. Netzwerkkomponenten

Ein „Black Channel" kann mehrere transparente Netzwerkkomponenten umfassen, wie z.B. Switches, Router, Links und Funkübertragungsstrecken. Für PROFIsafe gibt es geringfügige Restriktionen zur Erfüllung der SIL3-Anforderungen.

So sind alle Arten von Switches zulässig, jedoch maximal nur 100 Switches in Serie. Der Kennungsraum („Codename") einer PROFIsafe-Insel muss eineindeutig sein. Verbundene Inseln mit überlappendem Kennungsraum müssen durch Multi-Port-Router voneinander getrennt sein. Es gibt keine Einschränkungen für Netzübergänge von PROFINET über PROFIBUS hin zur eigensicheren Version MBP-IS (Abbildung 6).

3.3. Drahtlose Übertragung

Eine drahtlose Übertragung ist zulässig, solange eine ausreichende Verfügbarkeit (keine Fehlauslösungen) und IT-Sicherheit (Security) gewährleistet sind.

PROFIsafe spezifiziert bestimmte Anforderungen an die IT-Sicherheit für drahtlose Übertragungssysteme sowie für leitungsgebundene Netzwerke, die an industrielle Ethernet-Backbones oder das Internet (sogenannte offene Netzwerke) angeschlossen sind.

3.4. Datentypen

Feldbuskommunikation kennt verschiedene Datentypen zum Informationsaustausch (siehe Literatur). Zur Verringerung der Komplexität bietet PROFIsafe eine sinnvolle Untermenge an.

3.5. Selektive Passivierung

Die PI-Schrift „Remote I/O for Factory Automation (RIO for FA)" spezifiziert den Prozessdaten zugeordnete Wertstatus-Bits, um deren Gültigkeit anzuzeigen. Dadurch sind individuelle Benutzerreaktionen pro Prozessdatum möglich. PROFIsafe bietet hierzu einen konfigurierbaren Schutz vor automatischem Wiederanlauf.

4. PROFIsafe – Die Lösung

Ziel der F-Kommunikation zwischen zwei Partnern ist die Übergabe von

- aktuellen und unverfälschten Daten (Integrity),
- an den geplanten Empfänger (Authenticity),
- zur rechten Zeit (Timeliness).

Bei der Nachrichtenübertragung in komplexen Netzwerktopologien können mancherlei Fehler auftreten, sei es durch Hardwareausfälle, elektromagnetische Störungen oder andere Einflüsse. Nachrichten können verloren gehen, eingeschleust werden, wiederholt, verspätet oder in falscher Reihenfolge auftreten und/oder verfälschte Daten zeigen. Im Fall von F-Kommunikation kann es zu falscher Adressierung kommen: eine Nachricht erreicht fälschlicherweise ein F-Device und gibt sich als korrekte F-Nachricht aus. Unterschiedliche Übertragungsraten können außerdem zu Speichereffekten in den Buskomponenten führen. Aus den zahlreichen Gegenmaßnahmen in der Literatur konzentriert sich PROFIsafe auf die vier in Abbildung 7.

Measure: / Error:	Monitoring Number (sign of life)	Time-out (with receipt)	Codename (for sender and receiver)	Data Consistency Check (CRC)
Data corruption				X
Unintended repetition		X		
Incorrect sequence	X			
Loss	X	X		
Unacceptable delay		X		
Insertion	X		X	
Masquerade (standard message mimics failsafe)				X
Incorrect adressing	X		X	
Out-of-sequence	X			
Loopback of messages	X			

Abb. 7: Fehlertypen und Sicherheitsmaßnahmen

4.1. Sicherheitsmaßnahmen

Die Sicherheitsmaßnahmen umfassen:

- die Nummerierung von F-Nachrichten (Aufdeckung von Reihenfolgefehlern genutzt für „Timeliness")
- eine Zeiterwartung mit Quittung (Aufdeckung von Zeitüberschreitung für „Timeliness")
- eine Kennung (Codename) zwischen Sender und Empfänger („Authentifizierung")
- eine Datenintegritätsprüfung (CRC = zyklische Blockprüfung)

Anhand der Monitoring-Nummer kann der Empfänger nachvollziehen, ob er die Nachrichten vollzählig und in der richtigen Reihenfolge erhalten hat. Mit der Quittung gelangt die Monitoring-Nummer zur Prüfung zurück zum Sender. Eigentlich wäre ein simples „Toggle-Bit" hier ausreichend gewesen. Da aber einige Buskomponenten, wie z.B. Switches, über einen Zwischenspeicher verfügen, wurde für PROFIsafe eine 32-Bit Monitoring-Nummer gewählt.

In der F-Technik kommt es nicht nur auf die Übermittlung von korrekten Prozesssignalen und -werten an, sondern auch auf deren Aktualisierung innerhalb einer Prozessfehlertoleranzzeit. Hierdurch kann ein F-Device bei Zeitüberschreitung selbständig die vordefinierten Sicherheitsmaßnahmen auslösen, z.B. Stoppen einer Bewegung. Das F-Device benutzt dazu einen Watchdog-Timer, der neu gestartet wird, wenn eine F-Nachricht mit neuer Monitoring-Nummer eingetroffen ist.

Die 1:1 Kommunikationsbeziehung zwischen F-Host und F-Device vereinfacht die Erkennung von fehlgeleiteten F-Nachrichten. Dazu benötigen Sender und Empfänger eine eineindeutige Kennung (Codename) im gesamten Netzwerk, die der Überprüfung der Authentizität von F-Nachrichten dient. Bei PROFIsafe wird der Codename auch „F-Address" genannt.

Zur Erkennung von fehlerhaften Datenbits spielt die zyklische Blockprüfung (CRC) eine Schlüsselrolle. Für die notwendigen Betrachtungen der Restfehlerwahrscheinlichkeiten werden die Festlegungen der IEC 61508 herangezogen, die die zulässige Wahrscheinlichkeit von gefährlichen Fehlern (SIL) von Sicherheitsfunktionen beziffert. PROFIsafe orientiert sich an den Festlegungen dieser Norm (Abbildung 8).

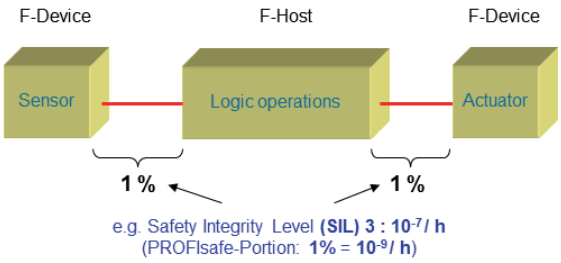

Abb. 8: Sicherheitsfunktion und SIL

Gemäß IEC 61508 umfasst ein Sicherheitskreis alle Sensoren, Aktoren, Übertragungselemente und die Logikverarbeitung, die in eine Sicherheitsfunktion involviert sind. Die IEC 61508 definiert Versagenswahrscheinlichkeiten für verschiedene Safety-Integrity-Level (SIL). Für SIL3 ist dies z.B. 10^{-7}/h. PROFIsafe setzt ein sorgfältig ausgewähltes 32-Bit CRC-Generatorpolynom ein, welches eine Wahrscheinlichkeit für gefährliche Ausfälle pro Stunde von weniger als 10^{-9}/h sicherstellt. Dieser Wert wird unabhängig vom unterlagerten „Black Channel" gewährleistet. Somit wird selbst bei SIL3-Anwendungen von PROFIsafe weniger als 1 % des gesamten Betrags von 10^{-7}/h einer Sicherheitsfunktion in Anspruch genommen. Damit bleiben 99 % für Ausfälle in Sensoren, Aktoren oder in der Logikverarbeitung.

4.2. PROFIsafe-Formate

F-Nachrichten zwischen einem F-Host und seinem F-Device werden als Nutzfracht in PROFIBUS- oder PROFINET-Telegrammen transportiert. Im Fall eines modularen F-Devices mit mehreren F-Modulen besteht die Nutzfracht aus mehreren F-Nachrichten. In Abbildung 9 ist das Format einer „Safety Protocol Data Unit (SPDU)" dargestellt.

F-Input/Output data	Status / Control Byte	CRC signature
		across F-Parameter, F-I/O data, Status/Control Byte, Monitoring Number
1 to 12/13 (max. 123) bytes	1 byte	4 bytes

Abb. 9: PROFIsafe SPDU-Format

Die SPDU besteht aus drei Feldern. Das erste enthält die F-Ein-/Ausgabedaten unter Berücksichtigung des erwähnten Datentypen-Subsets. Die Datenstruktur eines bestimmten F-Devices ist in der zugehörigen GSD-Datei (General Station Description) definiert. Fertigungs- und Prozessautomatisierung stellen unterschiedliche Anforderungen an ein F-System. Erstere arbeitet mit kurzen Signalen („Bits"), die sehr schnell verarbeitet werden müssen. Die andere arbeitet mit längeren Prozesswerten („Gleitkomma"), die etwas langsamer sein dürfen. PROFIsafe empfiehlt die Verwendung von 1 bis 12/13 Bytes F-Ein-/Ausgabedaten in der Fertigungsautomatisierung, da die F-Hosts diese Datenlängen unterstützen müssen. Die Sicherheitsmaßnahmen von PROFIsafe sind allerdings so ausgelegt, dass Datenlängen bis zu 123 Bytes nutzbar sind.

Das zweite Feld besteht aus einem Steuer-Byte, wenn die SPDU vom F-Host kommt oder einem Status-Byte, wenn sie vom F-Device kommt. Beide dienen der Synchronisierung der PROFIsafe-Protokollmaschinen.

Das dritte Feld einer PROFIsafe SPDU beinhaltet eine 32-Bit CRC-Signatur.

Die Monitoring-Nummer wird nicht mit der PROFIsafe SPDU übertragen. Sender und Empfänger verfügen jeweils über eine eigene Monitoring-Nummer-Berechnung, die beide mit Hilfe des Steuer- und des Statusbytes synchronisiert werden. Die korrekte Synchronisierung wird durch Einbezug des Monitoring-Nummer-Wertes in die CRC-Signaturberechnung überwacht. Die Berechnung basiert auf einem effizienten Pseudo-Zufallszahlengenerator. Für jede Verbindung wird ein eigener Startwert („Seed") in der Berechnung verwendet, der sich aus dem zugehörigen Codename („F-Address") ableitet.

4.3. PROFIsafe-Dienste

Sender und Empfänger von PROFIsafe SPDUs arbeiten in Schichten oberhalb des „Black Channel" (Abbildung 5). Diese PROFIsafe-Layer sind als Software realisiert („Treiber"). Herzstück des PROFIsafe-Layers ist eine Zustandsmaschine für die reguläre zyklische Verarbeitung der PROFIsafe SPDUs sowie für seltenere Operationen, wie z.B. Systemstart, Ein- und Ausschalten, CRC-Fehlerbehandlung usw. In Abbildung 10 ist dargestellt, wie die PROFIsafe-Layer mit der individuellen F-Device-Technologie und dem F-Host Anwenderprogramm zusammenarbeiten.

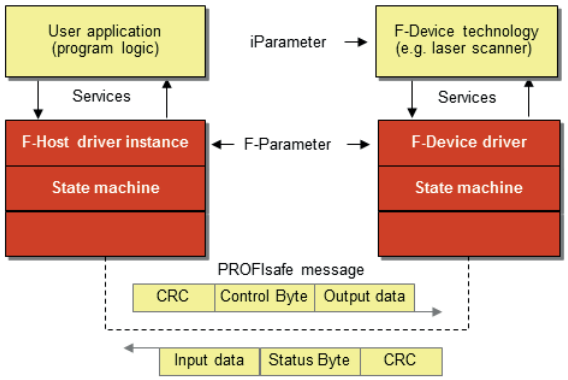

Abb. 10: PROFIsafe-Schichten in F-Host und F-Device

F-Host-Dienste

Die F-Host-Dienste sorgen vor allem für den Austausch von F-Ein-/Ausgabedaten. Beim Hochfahren oder im Fehlerfall werden die realen Prozesswerte durch voreingestellte Failsafe-Werte (FV) ersetzt. Sie haben den Wert „0", um den Empfänger in einen sicheren Zustand zu versetzen (z.B. energielos).

Den F-Devices, bei denen „Abschalten" nicht der einzige sichere Zustand ist, wie beispielsweise Brennerventilatoren, stellt PROFIsafe einen zusätzlichen Dienst in Form eines Flags „activate_FV" im Steuer-Byte zur Verfügung. Ein F-Device kann seinerseits über ein Flag „FV_activated" im Status-Byte das Anwenderprogramm über seinen sicheren Zustand informieren.

F-Kommunikationsfehler zwingen den F-Host-Treiber in den sicheren Zustand zu schalten. In der Regel darf eine Sicherheitsfunktion nicht automatisch und ohne menschliches Zutun vom sicheren Zustand in den Normalbetrieb umschalten. Um das Anwenderprogramm über die Notwendigkeit des Bediener-Eingriffs und einer Quittung zu informieren, bietet PROFIsafe einen zusätzlichen Dienst „OA_Req". Außerdem informiert PROFIsafe auch das F-Device über eine ausstehende Quittung, die es per LED optional anzeigen kann. Die Quittung des Bedieners kann das Anwenderprogramm durch einen entsprechenden Dienst „OA_C" an den F-Host-Treiber übergeben.

Die technologiespezifischen Parameter eines F-Devices werden iParameter genannt. Sollte ein F-Device zur Laufzeit einen Wechsel der iParameter benötigen, dann hilft PROFIsafe auch hier. Der Dienst „iPar_EN" erlaubt dem Anwenderprogramm die Freischaltung des F-Devices zum Empfang von neuen iParametern. Der Partnerdienst „iPar_OK" signalisiert dem Anwenderprogramm die Bereitschaft zur Wiederaufnahme des sicherheitsbezogenen Betriebs.

F-Device-Dienste

Die PROFIsafe-Dienste für die F-Devices ermöglichen den Austausch von F-Ein-/Ausgabedaten, das Setzen von sicheren Zuständen und die Meldung hierüber, die Verwaltung der iParameter und die bereits erwähnte Quittungsanfrage beim Bediener.

Außerdem kann die F-Device-Technologie eventuelle Fehler dem F-Host über ein „Device_Fault"-Flag im Status-Byte melden.

Die Dauer der Anforderung einer Sicherheitsfunktion durch ein F-Device muss lang genug sein für die Übertragung mit PROFIsafe (mindestens zwei Inkremente der Monitoring-Nummer). Ein spezieller Dienst unterstützt dies durch Information über neue Monitoring-Nummern.

Diagnosedaten des PROFIsafe-Layers gehen an den technologiespezifischen Teil des F-Devices.

Der F-Parameter übergibt das F-Device an den PROFIsafe-Layer. Es hat diese F-Parameter neben allen anderen Parametern während des Hochlaufs des Bussystems erhalten. Bleibt die Frage, was es mit diesen F-Parametern auf sich hat.

F-Parameter

Die F-Parameter enthalten Informationen, um den PROFIsafe-Layer an bestimmte Kundenvorgaben anzupassen und die Parametrierung auf einem separaten Weg (diversitär) zu überprüfen. Die wichtigsten F-Parameter sind:

- F_S/D_Address (kurz: „F-Address")
- F_WD_Time
- F_SIL
- F_iPar_CRC
- F_Par_CRC

Die „F_Address" ist eine eineindeutige Verbindungskennung für F-Geräte innerhalb einer PROFIsafe-Insel und entspricht dem „Codename". Der Technologie-Teil des F-Devices vergleicht den Wert von Micro-Schaltern vor Ort oder einer sonstwie zugewiesenen Information, um die Authentizität der Verbindung zu überprüfen.

F_WD_Time spezifiziert die Millisekunden für einen Watchdog-Timer. Der Timer überwacht die Dauer bis zum Empfang der nächsten gültigen PROFIsafe-SPDU.

F_SIL gibt den SIL an, den der Anwender vom jeweiligen F-Device erwartet. Er wird mit der lokal gespeicherten Angabe des Herstellers verglichen.

F_iPar_CRC ist eine Prüfsumme, die aus allen iParametern des technologiespezifischen Teils des F-Devices berechnet wird.

Schließlich bietet F_Par_CRC eine CRC-Signatur über alle F-Parameter. Sie stellt die fehlerfreie Übertragung der F-Parameter sicher.

Soweit der Überblick über das PROFIsafe-Protokoll.

5. Wie implementieren?

Zunächst sollte die nötige und ergänzende Literatur zu PROFIsafe beschafft werden (siehe Literaturhinweise). Es sollten nur die hier angegebenen oder neueren Versionen sein. Eine frühe Version V1.30 der PROFIsafe-Spezifikation ist inzwischen zurückgezogen worden.

Als nächstes ist eine Einarbeitung in die Sicherheitsgrundnorm IEC 61508 zu empfehlen oder eine entsprechende Beratung in Anspruch zu nehmen, um zu erfahren, was beim Entwicklungsprozess und der Organisation zwecks Erzielen der erforderlichen Gerätesicherheit beachtet werden muss. Allgemein gilt: die Implementierung von PROFIsafe macht aus einem Standard-Gerät kein F-Gerät. PROFIsafe schützt vor Übertragungsfehlern, nicht aber vor Gerätefehlern. Die Architektur der „Technologie" des F-Devices, das Protokoll und die Art und Weise wie beides implementiert sind, bestimmen den erreichten Safety Integrity Level (SIL) des Gerätes.

5.1. Sicherheitsklassen

Obwohl PROFIsafe für Sicherheitsfunktionen bis SIL3 geeignet ist, ist es nicht zwingend notwendig das F-Device ebenfalls für SIL3 zu entwickeln. Die geforderte Sicherheitsklasse hängt von der Endanwendung und von der Definition der Sicherheitsfunktionen ab. Es kann mit F-Devices einer niedrigeren Sicherheitsklasse durch Redundanz oder andere Maßnahmen ein höherer SIL erreicht werden (siehe „PA-Devices").

5.2. F-Devices

Zusätzlich zur Möglichkeit, die PROFIsafe-Spezifikation direkt zu implementieren, gibt es noch den Einsatz eines am Markt erhältlichen Starter-Kits. Der Produktleitfaden auf der PI-Webseite bietet nähere Information. Die Vorteile eines Starter-Kits liegen auf der Hand: vorzertifizierte Treibersoftware, zusätzliche wertvolle Informationen, Tools und technischer Support.

Für die Schnittstellen zu PROFIBUS und PROFINET sind alle verfügbaren ASICs und Kommunikations-Stacks einsetzbar. Die PROFIsafe-Treibersoftware ist entsprechend anzupassen.

Sichern der GSD

In PROFIBUS- oder PROFINET-Netzen muss jedes Gerät über eine GSD-Datei verfügen. Nach dem Festlegen der allgemeinen Parameter eines F-Devices in der GSD müssen die F-Parameter codiert werden. Dieser F-Parameterblock wird durch eine spezielle CRC-Signatur „F_ParamDescCRC" gegen Datenverfälschung auf den Speichermedien geschützt. Ein Konfigurationstool kann die Datenintegrität des F-Parameterblocks anhand der darin enthaltenen speziellen CRC-Signatur überprüfen.

Sichern der E/A-Datenstruktur

Die GSD beschreibt auch das Format der F-Ein-/Ausgabedaten. Zur Sicherung dieses Abschnitts der GSD dient eine weitere CRC-Signatur „F_IO_StructureDescCRC".

iParameter

Die vielen unterschiedlichen Technologien der F-Geräte bedingen eine Vielzahl von individuellen Sicherheitsparametern (iParameter).

Die Menge von iParametern reicht von wenigen Bytes für F-Module bis hin zu mehreren 10 kBytes für einen Laserscanner. Für die meisten F-Geräte existieren bereits Softwaretools zur Konfiguration, Parametrierung und Diagnose (CPD-Tool). Daher ist es wenig sinnvoll, die iParameter über die GSD abzuwickeln.

PROFIsafe empfiehlt die Verwendung des neuen sogenannten Universal-Parameter-Servers (iPar-Server). Für die Bereitstellung des iPar-Servers sind die F-Host-Hersteller verantwortlich. Der Server kann sich entweder im nicht-sicherheitsbezogenen Teil des F-Hosts, d.h. dem Parametrier-Master befinden oder in einer untergeordneten Steuerung, wie z.B. einer SPS oder einem Industrie-PC im selben Netzwerk.

Abbildung 11 zeigt die grundsätzlichen Schritte des iPar-Server-Mechanismus anhand eines Beispiels. Zusammen mit der Netzwerkkonfiguration und der F-Parametrierung wird der i-Par-Server für das F-Device initiiert (1). Im sicheren Zustand (FV) kann ein F-Device in den zyklischen Datenaustausch gehen. Vom Engineering-Tool aus wird ein CPD-Tool über die jeweils passende Schnittstelle (2), z.B. TCI (Tool Calling Interface) oder FDT (Field Device Tool), gestartet. Dabei wird mindestens die Netzadresse des konfigurierten Gerätes mitgegeben. Das CPD-Tool ermöglicht dann die Parametrierung, Inbetriebnahme und den Test (3). Nach Beendigung dieser Vorgänge wird die iPar_CRC-Prüfsumme berechnet und in hexadezimaler

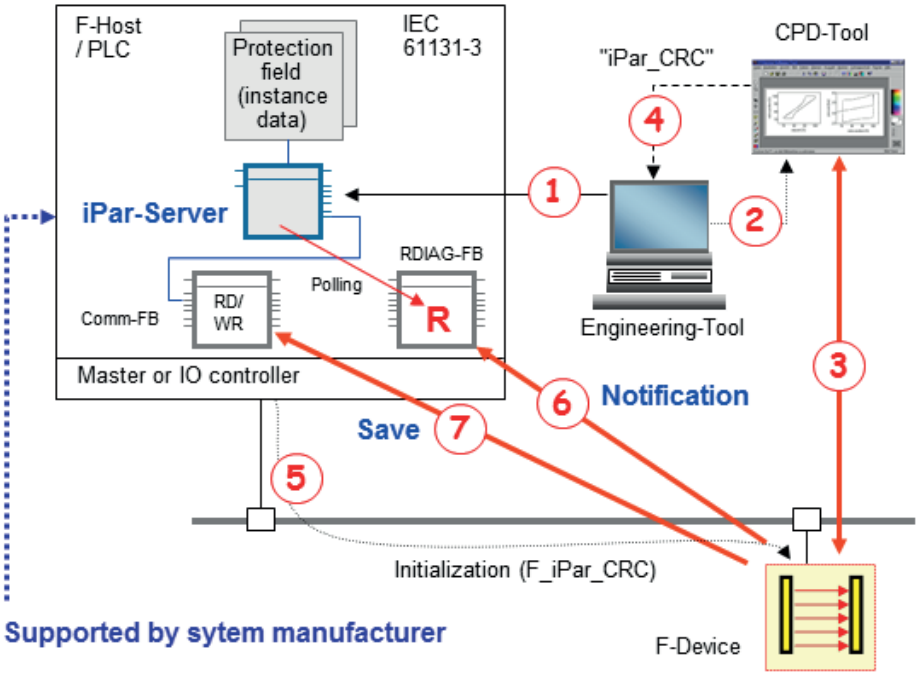

Abb. 11: Das iPar-Server Konzept

Form angezeigt. Der Wert wird in das Eingabefeld „F_iPar_CRC" im Konfigurationsteil des Engineering-Tools übernommen (4). Ein Neustart versorgt das F-Device auch mit dem F-Parameter „F_iPar_CRC" (5). Nach einer abschließenden Verifikation ist das F-Device befähigt, den Upload zu seiner iPar-Server-Instanz anzufordern. Es bedient sich dabei einer speziellen Diagnosemeldung. Der iPar-Server fragt die Diagnose-Information ab (z.B. RDIAG FB), liest die Upload-Anfrage (R) aus und startet den Upload-Prozess (7). Dabei werden die iParameter, unter Verwendung von azyklischen Diensten (Read Record), als Instanz-Daten im iPar-Server gespeichert.

Wurde ein defektes F-Device ersetzt, so erhält das neue F-Device seine F-Parameter direkt beim Hochlauf inklusive „F_iPar_CRC". Da neue F-Devices oder auch F-Devices mit flüchtigem Speicher nicht über die passenden iParameter verfügen, erkennt das neue F-Device einen Fehler beim Abgleich der Prüfsumme „F_iPar_CRC". Als Konsequenz fordert es den Download der iParameter bei der iPar-Server-Instanz an, wobei wieder die Standard-Diagnose bemüht wird. Der iPar-Server liest die Anfrage (R) aus der Diagnose-Information und startet den Download-Prozess (Write Record). Dank dieses Transfers erhält das F-Device auf einfachem Weg die ursprüngliche Funktionalität ohne CPD-Tools oder weiteren Engineering-Aufwand.

PROFIdrive

Die IEC 61800-5-2 definiert Sicherheitsfunktionen für Antriebe mit integrierter Sicherheit. Hierzu zählt eine Reihe von Stoppfunktionen:

- Sicher abgeschaltetes Moment
- Sicherer Stopp 1
- Sicherer Stopp 2
- Sicherer Betriebshalt

Und eine Gruppe von weiteren Sicherheits-unterfunktionen:

- Sicher begrenzte Beschleunigung
- Sicher begrenzte Geschwindigkeit
- Sicher begrenztes Moment
- Sicher begrenzte (absolute) Position
- Sicher begrenztes Inkrement
- Sichere Bewegungsrichtung
- Sicher begrenzte Motortemperatur

Abbildung 12 zeigt, wie herkömmliche Elektromechanik durch elektronische, sichere Stopp- und Überwachungsunterfunktionen ersetzt werden. Ein Hauptziel besteht darin, die Funktion der Antriebssteuerung zu überwachen und nur bei Ausfällen abzuschalten. Der PI-Arbeitskreis „PROFIdrive" spezifizierte einen Teil dieser Funktionen in einer Erweiterung zur PROFIdrive-Spezifikation (siehe Literatur).

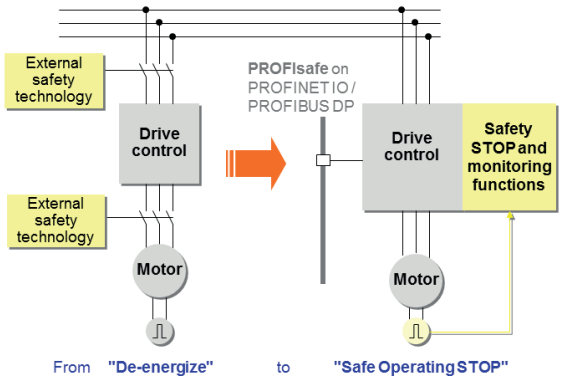

Abb 12: Antriebe mit integriertem STOPP und Überwachungsunterfunktion

PA Devices

F-Devices für die Prozessautomatisierung richten sich nach der Sektornorm IEC 61511 und dem Aspekt „Betriebsbewährtheit". Ein PA-Gerät kann unter bestimmten Umständen ein höheres SIL erreichen, wenn es als betriebsbewährt eingestuft ist. In der Regel werden PA-Geräte gemäß IEC 61804 entwickelt. Hier spielt die Gerätebeschreibung (EDD) eine wichtige Rolle. Daher hat der PA Arbeitskreis „PA Devices" eine Erweiterung ihrer PA-Gerätespezifikation erstellt, worin der Einsatz der PROFIsafe-Plattform für PA-Geräte, sowie Methoden zur Parametrierung geregelt sind (siehe Literatur).

I&M-Funktionen

Seit 2005 müssen alle PROFIBUS-Geräte mit azyklischen Diensten die sogenannten I&M-Funktionen anbieten. I&M steht für „Identification and Maintenance". Sie erlauben das standardisierte Auslesen des Hersteller-Codes des Geräts, seine Katalog- und Seriennummer sowie die Hard- und Softwareversion. Anhand des Hersteller-Codes und zusätzlichen Informationen vom PI-Webserver kann der Anwender direkt zu den neuesten Produktinformationen auf der Hersteller-Website weitergeleitet werden, wie in der „Profile Guideline Part 1" beschrieben (siehe Literatur).

Diagnose

Ein Hauptvorteil von PROFIBUS und PROFINET liegt in der Möglichkeit für Feldgeräte, den Betreiber in Ausnahmesituationen wie Ausfällen oder Fehlfunktionen mit Informationen zu versorgen. Mittels guter Diagnosen lassen sich Stillstandszeiten von Anlagen reduzieren und somit auch Kosten. Das Diagnosekonzept berücksichtigt neben der Codierung der Informationen auch unterschiedliche Sprachen und Hilfe-Texte, was im Einzelfall zu tun ist, wie in der „Profile Guideline Part 3" beschrieben (siehe Literatur).

Literatur

- PROFIsafe Policy V1.5; Best.-Nr. 2.282
- PROFIsafe – Profile for Safety Technology on PROFIBUS DP and PROFINET IO, V2.6.1; Best.-Nr. 3.192
- PROFIsafe – Environmental Requirements, V2.6; Best.-Nr. 2.232
- PROFIsafe – Test Specification for F-Slaves, F-Devices, and F-Hosts, V2.2; Best.-Nr. 2.242
- PROFIsafe for PA-Devices, V1.0.1; Best.-Nr. 3.042
- PROFIdrive on PROFIsafe, V3.00.4; Best.-Nr. 3.272
- Specification for PROFIBUS Device Description and Device Integration, Volume 1: GSD, V5.1; Best.-Nr. 2.122
- GSDML Specification for PROFINET IO, V2.3.2; Best.-Nr. 2.352
- Profile Guideline, Part 1: Identification & Maintenance Functions, V2.0; Best.-Nr. 3.502
- Profile Guideline, Part 2: Data Types, Programming Languages, and Platforms, V1.0; Best.-Nr. 3.512
- Profile Guideline, Part 3: Diagnosis, Alarms and Time Stamping, V1.0; Best.-Nr. 3.522
- Profile Guideline, Part 4: Universal Parameter Server, V1.0.1; Best.-Nr. 3.532
- Diagnosis for PROFINET IO, V1.1; Best.-Nr. 7.142
- Rapid way to PROFIBUS DP; Best.-Nr. 4.071
- Industrial Communications with PROFINET; Best.-Nr. 4.181

5.3. F-Host

Abhängig von der Strategie der Hersteller sind unterschiedliche Architekturen für F-Hosts mit PROFIsafe-Kommunikation denkbar: unabhängige F-CPUs oder auch integrierte, aber logisch getrennte Sicherheitskonzepte mit Standard-CPUs.

Mögliche Strukturen

Sichere Verarbeitung kann auf vielfältige Weise realisiert werden: z.B. Hardware-Redundanz mit Diskrepanzprüfung, Software-Redundanz, Schutzeinrichtungen oder bereits existierende diversitäre Hardware-Plattformen. Starter-Kits sind verfügbar.

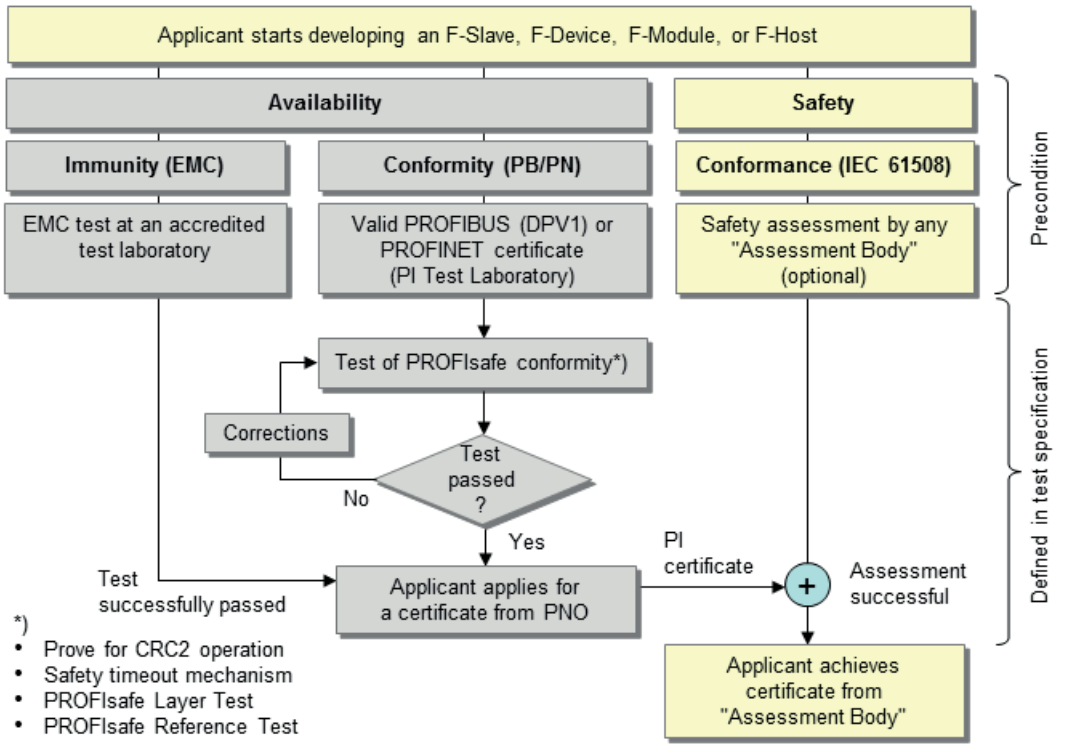

Abb. 13: Test- und Zertifizierungsprozeduren

Conformance Classes

Um das korrekte Zusammenspiel zwischen allen F-Devices und allen am Markt erhältlichen PROFIsafe F-Hosts garantieren zu können, spezifiziert PROFIsafe sogenannte Conformance Classes für F-Hosts. Die Erfüllung dieser Anforderungen ist die Voraussetzung für eine Zertifizierung durch PI (Abbildung 13).

6. Zertifizierung

Unterschiedliche Produkte von diversen Herstellern kommunizieren innerhalb einer PROFIsafe-Insel. Damit dies korrekt funktioniert, müssen die Produkte gemäß PROFIsafe-Spezifikation implementiert worden sein. In der Regel wird die Konformität aufgrund von Testberichten akkreditierter Testlabors durch ein Zertifikat der Zertifizierungsstelle von PI bescheinigt.

6.1. Die PROFIsafe-Tests

Das PROFIsafe-Protokoll basiert auf endlichen Zustandsmaschinen. Daher bestand die Möglichkeit des mathematischen Nachweises der ordnungsgemäßen Funktion von PROFIsafe selbst bei mehr als zwei voneinander unabhängigen Fehlern oder Ausfällen. Dies wurde durch das systematische Generieren aller erdenklichen Funktions- und Belastungsszenarien erreicht. Diese Szenarien wurden für die Entwicklung eines vollautomatischen PROFIsafe-Layer-Tests herangezogen, welcher nun dazu dient, F-Devices und F-Hosts auf Konformität mit PROFIsafe zu überprüfen. Dies ist Teil eines dreistufigen Verfahrens innerhalb der gesamten Sicherheitszertifizierung gemäß IEC 61508 durch Prüfstellen (Abbildung 13).

6.2. Sicherheitsbeurteilung

Es sei hier angemerkt, dass die Testlabors von PI die PROFIsafe-Layer-Tests im Auftrag von Prüfstellen durchführen. Dies sind z.B.:

- TÜV (weltweit)
- IFA (Deutschland)
- SP (Schweden)
- SUVA (Schweiz)
- HSE (Großbritannien)
- FM, UL (USA)

Dies sind die einzig zugelassenen Stellen, die eine Sicherheitsbeurteilung gemäß IEC 61508 durchführen dürfen.

Für jedes einzelne F-Device ist ein Sicherheitshandbuch vorgeschrieben, welches Informationen über den SIL-Anspruch SIL_{CL} (claim limit), den Performance Level (PL) und die Kategorie (Cat) sowie den PFH_d (Wahrscheinlichkeit eines gefährlichen Fehlers pro Stunde) enthalten muss.

PROFIsafe stellt eine Spezifikation für Test und Zertifizierung von Geräten bereit (Literatur). Derzeit gibt es weltweit vier Testlabors, die für PROFIsafe-Tests von PI akkreditiert sind (siehe www.profibus.com/test-labs).

7. Einsatz von PROFIsafe

Der PI-Leitfaden „PROFIsafe - Environmental Requirements" (siehe Literatur) beschäftigt sich mit sämtlichen Umfeldaspekten des PROFIsafe-Kommunikationsprotokolls. Er beantwortet Fragen wie beispielsweise:

- Muss ein F-Device vor sehr hohen Spannungen geschützt werden, die unbekannte Quellen über das Bus-Kabel einspeisen könnten?
- Kann für F-Devices dieselbe 24V-Versorgung wie für die Standardgeräte im Netzwerk verwendet werden?
- Wie soll die gemäß IEC 61508 geforderte „erhöhte Störfestigkeit" am F-Device getestet werden?
- Was muss bei der Installation beachtet werden?
- Welche IT-Sicherheit (Security) ist zu gewährleisten?

Die nachfolgenden Kapitel fassen den Inhalt dieses Leitfadens kurz zusammen.

7.1. Elektrische Sicherheit

Die Feldbusnormen IEC 61158 und IEC 61784-1/-2 fordern von allen Geräten im Netzwerk die Einhaltung der gesetzlichen Anforderungen des Landes, in dem sie eingesetzt werden (angezeigt z.B. durch CE). So müssen in industriellen Anwendungen die Schutzmaßnahmen gegen elektrischen Schlag entsprechend des IEC 61010-x-Teils getroffen werden, der zum jeweiligen Gerätetyp passt. Sie werden PELV (Protected Extra Low Voltage) genannt und begrenzen die zulässige Spannung in einem Fehlerfall auf ein für Menschen ungefährliches Maß. Dank dieser gewöhnlich gesetzlich vorgeschriebenen Forderung wird der Schutzaufwand in F-Devices und F-Hosts „erträglich".

7.2. Spannungsversorgung

Für F-Devices / F-Hosts und Standardgeräte kann dieselbe 24V-Versorgung genutzt werden. In beiden Fällen muss per Gesetz PELV gewährleistet sein.

7.3. Erhöhte Störfestigkeit

Für F-Anwendungen muss die entsprechende Spezifikation der Sicherheitsanforderungen (SRS) bestimmte Grenzwerte für die elektromagnetische Störfestigkeit festlegen (IEC 61000-1-1), die für die elektromagnetische Verträglichkeit einzuhalten sind. Die Grenzwerte sind so festzulegen, dass sowohl die Phänomene der IEC 61000-2-5 als auch die erforderlichen SIL berücksichtigt sind.

Für allgemeine Industrieanwendungen definiert die generische Norm IEC 61000-6-7 bzw. die Sektornorm IEC 61326-3-1 die Störfestigkeitsanforderungen für Geräte die Sicherheitsfunktionen ausführen bzw. dafür vorgesehen sind.

Produktnormen wie die IEC 61496-1 (z.B. Laserscanner) legen für einzelne Phänomene andere (höhere) Testpegel fest.

Die Umgebungsbedingungen in der Prozessindustrie können im Vergleich zu allgemeinen Industrieumgebungen durchaus unterschiedlich sein. Daher können für PA-Geräte die spezifischen Anforderungen und Verhaltenskriterien der IEC 61326-3-2 herangezogen werden.

Für PROFIsafe ist ein spezieller EMV-Testaufbau definiert.

7.4. Hochverfügbarkeit

Bei funktionaler Sicherheit geht es darum, Menschen vor Verletzungen zu schützen, z.B. durch Abschalten von gefährlichen Geräten. Eine charakteristische Größe für solche Sicherheitsfunktionen ist der Safety Integrity Level (SIL). Er gibt die Wahrscheinlichkeit für gefährliche Ausfälle einer Sicherheitsfunktion pro Stunde an, z.B. 10^{-7}/h bei SIL3.

Bei Hochverfügbarkeit (Fehlertoleranz) hingegen geht es um die Aufrechterhaltung der Automatisierung auch bei Ausfällen. Eine charakteristische Größe für Hochverfügbarkeit ist die Betriebsbereitschaft eines Gerätes bezogen auf die Gesamtbetriebsdauer (z.B. 99,99%). Unter anderem bestimmt vor allem Redundanz die Fehlertoleranz eines Systems.

	PROFIsafe	Redundancy	PROFIsafe and Redundancy
Application	Factory and process automation: Presses, robots, level switches, shutdown valves, as well as burner control and cable cars	Process automation; Tranportation infra-structure Chemical or pharma-ceutical productions, refineries, offshore; tunnels	Process automation; Transportation infra-structure Chemical or pharma-ceutical productions, refineries, offshore; tunnels
High Availability	-	No downtimes at best (fault tolerance)	No downtimes at best (fault tolerance)
Safety	No dangerous failures (required by law or insurances)	Redundancy by itself does not provide safety	No dangerous failures (required by law or insurances)

Abb. 14: Funktionale Sicherheit und Hochverfügbarkeit (Fehlertoleranz)

PROFIsafe kann mit oder ohne Redundanz eingesetzt werden. Abbildung 14 zeigt mögliche Kombinationen.

7.5. Installationsrichtlinien

Ziel von PROFIsafe ist es, funktional sichere Kommunikation in Standard-Netzwerke zu integrieren ohne die bestehenden Installationsrichtlinien zu beeinflussen. Für einen zuverlässigen Betrieb und die Erfüllung gesetzlicher Vorgaben wird die Einhaltung der PROFIsafe-Spezifikationen und -Richtlinien jedoch dringend empfohlen. Wichtige und zu beachtende Themen sind im Folgenden angesprochen.

Voraussetzungen

Alle Standardgeräte und F-Devices in einem Netzwerk müssen laut 7.1. elektrische Sicherheit aufweisen.

Alle F-Devices müssen nach IEC 61508 zertifiziert sein, bei F-Devices für die Prozessautomatisierung nach IEC 61511. Eine PROFIsafe-Konformität muss von akkreditierten PI-Testlabors getestet und bestätigt sein.

Alle anderen Standardgeräte in einem PROFIsafe-Netzwerk müssen ihre Konformität zu PROFIBUS oder PROFINET anhand eines entsprechenden Zertifikats von PI oder gleichwertigen Nachweisen unter Beweis stellen.

Randbedingungen

Bei PROFIBUS DP sind Stichleitungen nicht zulässig. Für PROFINET IO gelten folgende Regeln:

- Maximal 100 Switches in Reihe
- Nur ein F-Host pro Submodul
- Alle Netzwerkkomponenten müssen industrietauglich sein (z.B. gemäß IEC 61131-2)
- Router zur Trennung von PROFIsafe-Inseln erforderlich (gekennzeichnet durch eineindeutige „F-Address/Codename")

Verkabelung

PROFIBUS und PROFINET schreiben geschirmte Kabel vor mit beidseitiger Schirmauflage auf den Steckergehäusen für bestmögliche elektromagnetische Störfestigkeit. In der Regel ist ein Potenzialausgleich erforderlich. Ist dies nicht möglich, helfen Lichtwellenleiter weiter.

In Fällen definierter EMV und geringen Störeinflüssen dürfen Anwender unter Inkaufnahme häufigerer Fehlauslösungen auch Kabel ohne Schirmung verwenden.

Verfügbarkeit

Selbst bei geschirmten Kabeln kann die Datenleitung durch Signalrauschen gestört sein, wenn z.B. die Zwischenkreisspannung eines Frequenzumrichters nicht ausreichend gefiltert ist. Signalstörungen können auch durch fehlende Abschlusswiderstände entstehen. Dies ist keine Frage der Sicherheit sondern der Verfügbarkeit. Ausreichende Verfügbarkeit der Automatisierung ist eine notwendige Voraussetzung für

Sicherheit. Sicherheitsfunktionen in Anlagen mit ungenügender Verfügbarkeit tendieren zu ungewolltem Auslösen (Nuisance Trips). Dies wiederum verführt Produktionsleiter dazu, die Sicherheitsfunktionen außer Kraft zu setzen mit unter Umständen verheerenden Folgen.

Mitgliedsfirmen von PI bieten zahlreiche Tools, Verfahren und Checklisten für die Untersuchung der Übertragungsqualität in Netzwerken.

„Not-Halt"-Aspekte

PROFIsafe ist der Bahnbrecher für viele F-Geräte, insbesondere für Antriebe mit integrierter Sicherheit. Heutzutage können Antriebe sichere Zustände ohne Abschalten des Motors einnehmen (Not-Halt). Beispielsweise hält die neue Sicherheitsunterfunktion SOS (sicherer Betriebshalt) den Motor unter Regelung in einer definierten Position. Diese neue Möglichkeit erfordert beim Anwender einen Paradigmenwechsel. Früher wurde durch einen „Not-Aus"-Taster die Stromversorgung physisch vom Motor getrennt. Daher bestanden beim Motortausch keinerlei elektrische Gefahren für eine Person.

Die neue IEC 60204-1 beschreibt Maßnahmen gegen elektrischen Schlag mit Hilfe von abschließbaren Motorschutzschaltern, Leistungs- und Hauptschaltern mit Sicherungen (Abbildung 15). Sie spezifiziert außerdem ein 5-Leiter-System (TN-S) mit getrennten Neutralleitern „N" und Schutzleitern „PE", sowie geschirmte Kabel zwischen den Antrieben und Motoren. Für viele Sicherheitsfragen ist die IEC 60204-1 eine äußerst wertvolle „Fundgrube". In der entsprechenden US-Norm NFPA 79 wurden einige Anpassungen für den Nordamerikanischen Markt vorgenommen (Abbildung 3).

7.6. Funkübertragung

Immer mehr Anwendungen, wie z.B. fahrerlose Transportsysteme (AGV), rotierende Maschinen, Portalroboter und Bedienterminals, nutzen die drahtlose Übertragung für die Anbindung an Feldbusse. PI unterstützt WLAN- und Bluetooth-Lösungen. PROFIsafe ist mit seiner Tauglichkeit für eine Bitfehlerwahrscheinlichkeit von 10^{-2} für alle möglichen „Black Channels" zugelassen. Es sind jedoch die nachstehend aufgeführten Überlegungen zur IT-Sicherheit (Security) zu berücksichtigen.

7.7. IT-Sicherheit (Security)

PROFINET auf Basis von Industrial Ethernet, einem offenen Netzwerk, wirft insbesondere bei drahtloser Übertragung zwangsläufig Fragen zur IT-Sicherheit (Security) auf.

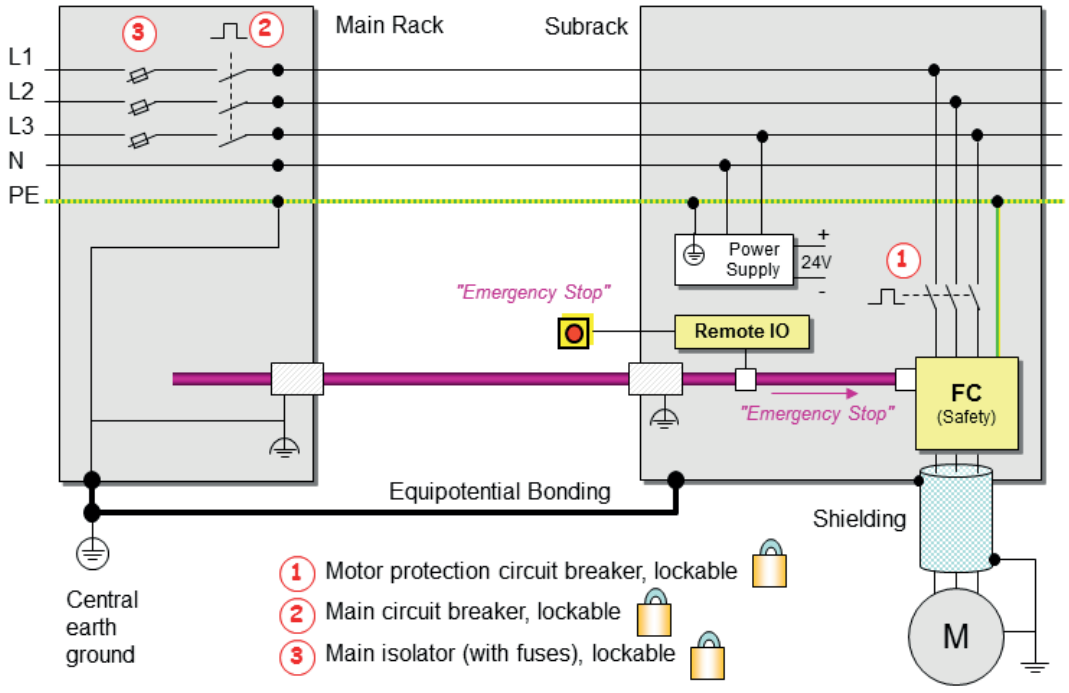

Abb. 15: „Not-Halt"-Konzept der IEC 60204-1

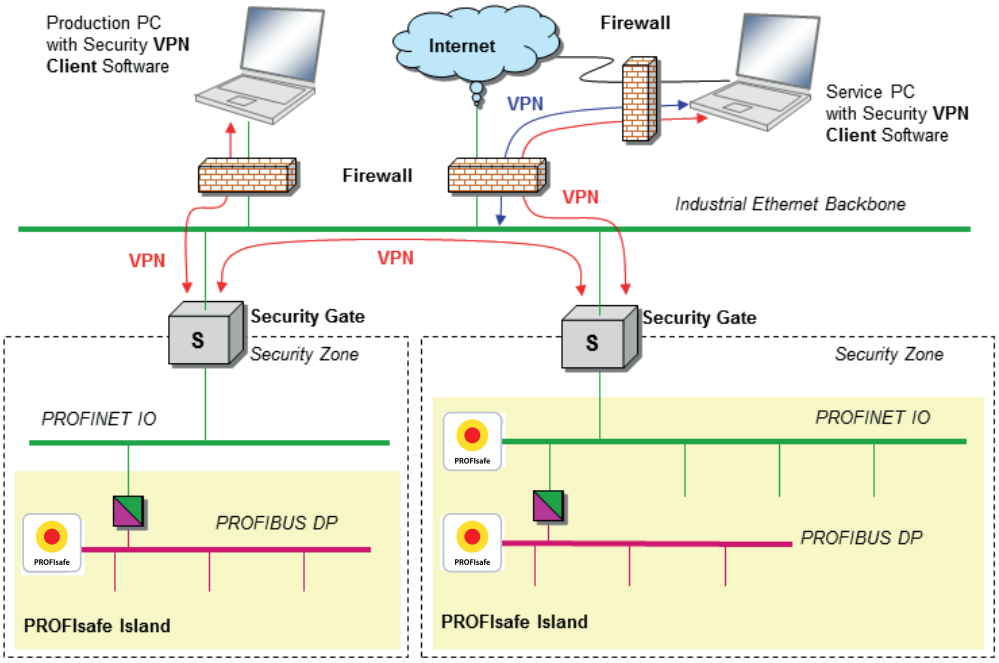

Abb. 16: Security-Konzepte für „geschlossene" und „offene" Netzwerke

PI verfolgt das Konzept der sogenannten Security-Zonen, die als geschlossene Netzwerke betrachtet werden können (Abbildung 16). Die einzige Möglichkeit, über ein offenes Netzwerk wie Industrial Ethernet von einer Security-Zone in eine andere zu gelangen, führt durch sogenannte Security-Gates. Diese bedienen sich bewährter Sicherheitstechniken wie VPN (Virtual Private Network) und Firewalls, um sich vor unerlaubtem Zugriff zu schützen. PROFIsafe-Netzwerke müssen sich immer in Security-Zonen befinden und durch Security-Gates geschützt werden. Wenn Verbindungen zu offenen Netzwerken unvermeidbar sind, dann hilft der PROFINET Security-Leitfaden, V2.0; Best.-Nr. 7.002 weiter.

IEEE 802.11 spezifiziert für drahtlose Übertragung die notwendigen IT-Sicherheitsmaßnahmen in PROFIsafe-Netzwerken. Es ist nur der Betrieb im Infrastruktur-Modus zulässig; der Adhoc Modus ist nicht erlaubt. Details beschreibt die PROFIsafe-Spezifikation (Literatur).

7.8. Reaktionszeit

In der Regel sind die Antwortzeiten herkömmlicher Steuerungsfunktionen auch kurz genug für Sicherheitsfunktionen. Dennoch gibt es F-Anwendungen mit kritischen Antwortzeiten für Sicherheitsfunktionen (SFRT). Pressen mit Lichtgittern als Schutzvorrichtung sind hier ein Beispiel. Ein Maschinendesigner muss bereits in einem frühen Entwicklungsstadium wissen, wie weit ein Lichtgitter mindestens von der gefährlichen Presse entfernt sein muss. Eine allgemein gültige Regel besagt, dass eine Hand mit maximal 2 m/s bewegt wird. Der minimale Abstand lässt sich somit aus s = 2 m/s x SFRT berechnen, wenn die Auflösung des Lichtgitters hoch genug ist, um einen einzelnen Finger zu erkennen (EN 999). Andernfalls sind Korrektursummanden nötig.

Das Modell in Abbildung 17 veranschaulicht die Berechnung der SFRT. Es besteht aus einem Sensor, einer F-Übertragung, der Signalverarbeitung, einer weiteren F-Übertragung und einem Aktuator. Alle Bestandteile haben ihre eigenen statistischen Schwankungen für den Signaldurchlauf. Die maximale Laufzeit TWCDT für die Durchquerung des Systems ist die Verzögerungszeit im ungünstigsten Fall, d.h. alle Elemente des Systems benötigen ihre maximale Zeit. Im Sicherheitsfall kommt noch hinzu, dass eines der Bestandteile zum Zeitpunkt des Signaldurchlaufs versagt. Daher muss beim ausgefallenen Teil noch eine Differenzzeit bis zum Ansprechen des Watchdog addiert werden (von mehr als einem Ausfall muss nicht ausgegangen werden). Die SFRT setzt sich also aus TWCDT und der eben erwähnten Differenzzeit zusammen.

Bei jedem einzelnen F-Device müssen die Informationen über die Verzögerungszeiten gemäß PROFIsafe-Spezifikation im Sicherheitshandbuch stehen, um Engineering-Tools die Abschätzung von SFRTs zu ermöglichen.

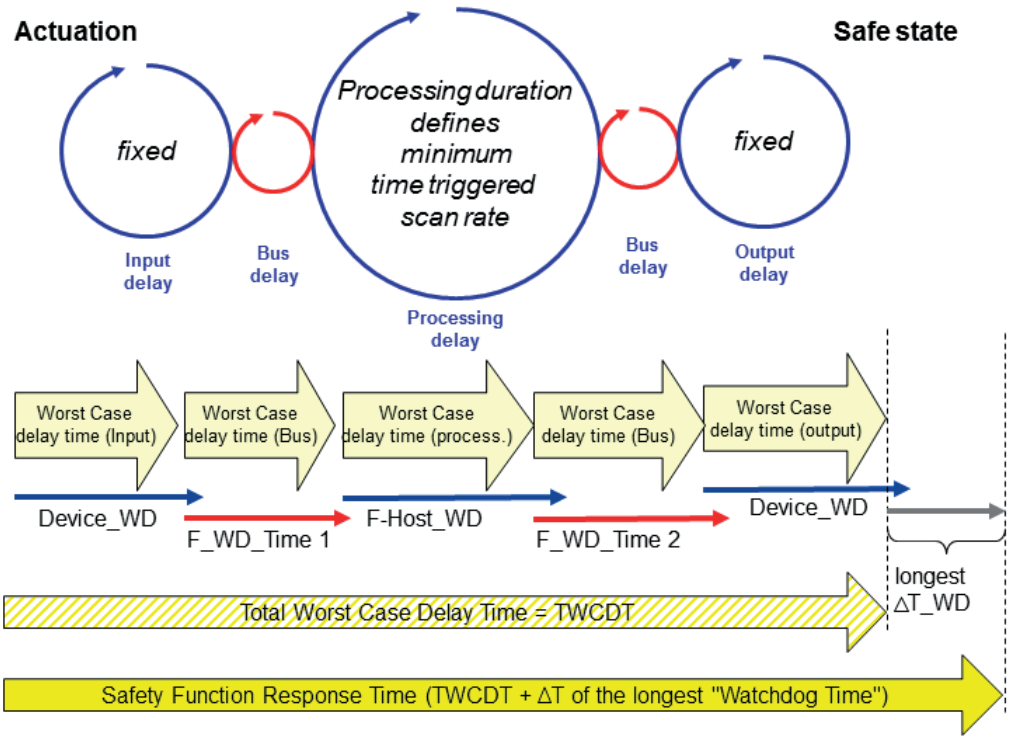

Abb. 17: Safety Function Response Time (SFRT)

8. Für Integratoren

8.1. Richtlinien & Normen

In vielen Ländern sind die Sicherheitsanforderungen für gefährliche Maschinen gesetzlich geregelt. In der EU gilt dies für die Maschinenrichtlinie 2006/2/EC. Sie enthält eine Liste mit sogenannten harmonisierten Normen. Für einen Maschinenhersteller gilt die Konformitätsvermutung zu den Richtlinien, wenn die relevanten Normen erfüllt sind.

Relevante Normen in Bezug auf PROFIsafe sind z.B. IEC 62061, ISO 13849 und ISO 12100-1 (siehe 1.3. und Abbildung 2).

8.2. Risikominderung

Es ist immer besser, eine Maschine mit inhärenter Sicherheit so zu entwickeln, dass sie Gefahren vermeidet. Im ersten Teil der ISO 12100 werden alle Arten möglicher Gefahren aufgelistet. Im zweiten Teil zeigt sie eine iterative Methode zur Reduzierung des Risikos von Automatisierungstechnik anhand einer Risikobeurteilung. Diese setzt sich aus einer Risikoanalyse und einer Risikobewertung zusammen:

- Spezifiziere die Grenzen und die vorgesehene Verwendung der Maschine
- Ermittle die Gefahren und die Gefährdungssituationen für den kompletten Lebenszyklus
- Schätze das Risiko für jede ermittelte Gefahr und Gefährdungssituation ein
- Bewerte das Risiko und entscheide über die Notwendigkeit einer Risikominderung

Mit Hilfe der „3-Schritt-Methode"

- inhärent sichere Konstruktionsmaßnahmen,
- Schutzeinrichtungen und ergänzende Schutzmaßnahmen,
- Aufklärung des Anwenders über das Restrisiko,

kann der Konstrukteur Gefahren vermeiden oder durch Schutzmaßnahmen Risiken mindern.

Schutzeinrichtungen und ergänzende Schutzmaßnahmen bilden die Grundlage von Sicherheitsfunktionen wie z.B. Lichtgitter, zugehörige logische Verknüpfung und Motorschütz.

8.3. Anwendung der IEC 62061

Die IEC 62061 und die ISO 13849 bieten Methoden zum Umgang mit Sicherheitsfunktionen. Während die IEC 62061 sehr gut die PROFIsafe-Technologie und die F-Hosts abdeckt, behandelt ISO 13849 zusätzlich die hydraulischen, pneumatischen, elektrischen und mechanischen Komponenten.

IEC 62061 fordert einen Sicherheitsplan für den gesamten Lebenszyklus einer Maschine mit Design, Bediener-Rollen und Verantwortungen, Inbetriebnahme, Austausch und Wartung bis zur Demontage.

ISO und IEC bemühen sich, die beiden Verfahren der IEC 62061 und ISO 13849 im gemeinsamen Projekt „ISO/IEC 17305" zu harmonisieren und zu verbessern (siehe Abbildung 2).

8.4. Risikobewertung

Beide Normen beschreiben, basierend auf der ISO 12100, ein ähnliches Konzept der Risikobewertung von Sicherheitsfunktionen:

Risiko = Ausmaß eines Schadens und die Eintrittswahrscheinlichkeit

Die Eintrittswahrscheinlichkeit setzt sich aus Aufenthaltsdauer, deren Häufigkeit und der Möglichkeit zur Gefahrenabwendung zusammen.

8.5. SIL/PL/Cat-Bestimmung

Beide Normen IEC 62061 und ISO 13849 bieten berechenbare Kenngrößen. Zum einen der erforderliche SIL und zum anderen der erforderliche PL und die Cat (siehe 1.3). Eine Kenngröße kann in die andere umgerechnet werden. Langfristig dürften die Unterschiede „verblassen", wenn die Risikobeurteilungen in Engineering-Tools interaktiv abgefragt werden. Es wird erwartet, dass die künftige ISO/IEC 17305 hierbei Hilfe bietet.

8.6. Sicherheitsfunktion

Die IEC 62061 definiert sogenannte sicherheitsbezogene elektrische Steuerungssysteme (SRECS) mit Subsystemen für Erfassung, Verarbeitung und Ausgabe. Subsysteme bestehen aus Elementen (z.B. Schalter).

Der eleganteste Weg zur Sicherheitsfunktion führt über zertifizierte oder vorzertifizierte F-Devices (Sensoren, Aktuatoren) und F-Hosts, die über PROFIsafe verbunden sind.

8.7. Erreichter SIL

Die F-Devices liefern in ihrem Sicherheitshandbuch die Informationen zur Bestimmung des von einer Sicherheitsfunktion erreichten SIL. In einem ersten Schritt wird der geringste SIL_{CL} aller F-Geräte (F-Devices, F-Hosts) ermittelt. Dieser bestimmt das maximal erreichbare SIL der gesamten Sicherheitsfunktion. In manchen Fällen bieten Hersteller Systemsupport, um durch Redundanz von F-Devices und zugehöriger Systemsoftware ein höheres SIL zu erzielen.

In einem zweiten Schritt werden die PFH_d-Werte der F-Geräte addiert und mit den für ein bestimmtes SIL zulässigen Werten verglichen. Der geringste SIL-Wert aus beiden Berechnungen bestimmt den maximal erreichbaren SIL der Sicherheitsfunktion.

In den folgenden Abschnitten wird gezeigt, wie F-Module in Remote I/Os mit klassischen F-Geräten, wie Not-Halt-Schalter, Sicherheits-Türschalter, usw. gemäß Abbildung 4 kombiniert werden können.

8.8. Elektromechanik

IEC 62061 definiert vier Subsystem-Architekturen A, B, C und D samt Berechnungsformeln für die Anbindung klassischer F-Geräte. Mit Hilfe der B_{10}-Werte für mechanische Schalter, der geschätzten Zahl an Schaltzyklen, der Diagnoseabdeckung und dem CCF-Faktor (Common Cause Failure) kann die Wahrscheinlichkeit von gefährlichen Ausfällen anhand der Formeln berechnet und zur Bestimmung des SIL herangezogen werden.

8.9. Nichtelektrische Teile

ISO 13849-1 definiert sogenannte Safety-Related Parts of Control Systems (SRP/CS) für elektrische, aber auch für hydraulische, pneumatische und mechanische Teile. Dank der Norm können auch für nicht-elektrische Teile ein PL- und ein PFH_d-Wert ermittelt werden, die dann für die Bestimmung des SIL einer Sicherheitsfunktion gemäß IEC 62061 verwendet werden.

8.10. Validierung

IEC 62061 macht einen Validierungsplan als Teil des gesamten Sicherheitskonzepts erforderlich. Eine Maschine muss gemäß diesem Plan getestet, überprüft und dokumentiert werden.

9. F-Device Familien

Die PROFIsafe-Technologie hat den Standard- und F-Geräten völlig neue Möglichkeiten eröffnet. Das Kapitel gibt einen kurzen Überblick über einige wichtige F-Devices und typische Anwendungen.

9.1. Remote-I/O

Standard-Remote-I/Os können nun F-Module beinhalten, ohne Rückwirkung auf die Kopfstationen. Dies macht F-Module wie z.B. digitale und analoge Ein-/Ausgaben, Leistungsmodule, Motorstarter oder Frequenzumrichter mit integrierter Sicherheit verfügbar. Die F-Module können in Gruppen angeordnet und somit auch gruppenweise abgeschaltet werden.

Not-Halt-Taster verursachen wegen der Einzelprüfung kostspielige jährliche Inspektionen. Die neue Technologie ermöglicht ein einfaches Aufzeichnen aller Betätigungen während eines Jahres. So müssen lediglich die verbleibenden unbetätigten Schalter überprüft werden, d.h. eine enorme Kostenersparnis.

9.2. Optischer Sensor

Optische F-Sensoren wie Lichtgitter oder Laserscanner sind in der IEC 61496 spezifiziert. Optische Sensoren eignen sich hervorragend für die flexible Absicherung von Entry/Exit-Portalen. Das Beispiel in Abbildung 18 zeigt, wie PROFIsafe ergänzend zu den Sicherheitsfunktionen von Laserscannern und Antrieben mit integrierter Sicherheit arbeitet (siehe 9.3.).

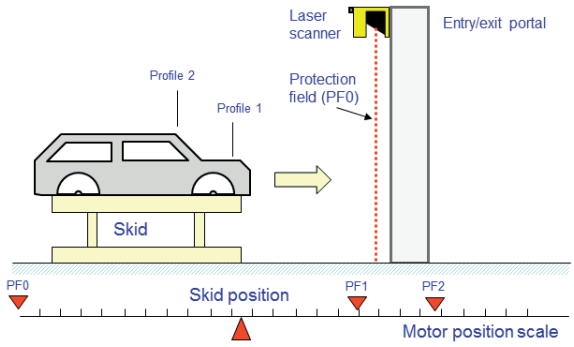

Abb. 18: Software "Muting-Sensoren" für Laserscanner

9.3. Antrieb

Die Sicherheitsunterfunktionen von Antrieben sind in der IEC 61800-5-2 spezifiziert. In der Regel werden hier für die Sicherheitsunterfunktionen F-Positionsgeber benötigt. Dessen Werte werden dem Anwender über PROFIsafe zugänglich gemacht, wodurch auf physische Endlagenschalter oder Mutingsensoren verzichtet werden kann. Wie in Abbildung 18 zu erkennen ist, bestimmt die Motorposition das Schutzfeld des Laserscanners am Entry/Exit-Portal der Fertigungszelle unter Berücksichtigung des Profils der jeweiligen Fahrzeugkarosserie.

In Abschnitt 5.2. sind weitere Sicherheitsunterfunktionen gelistet, die in nächster Zukunft zu revolutionären Anwendungen führen werden.

9.4. Roboter

Sicherheitseinrichtungen für Roboter sind in ISO 10218 spezifiziert. Die neuen Sicherheitsunterfunktionen für Antriebe können auch in Robotern integriert werden und ermöglichen so neue Funktionen, wie z.B. „kollaborative Roboter", die Hand in Hand mit Personen arbeiten.

9.5. F-Gateway

Es gibt F-Gateway-Geräte zwischen PROFIsafe und ASIsafe (AS-Interface Safety-at-work). Hierdurch können die Vorteile beider Sicherheitskonzepte kombiniert werden. Während ASIsafe problemlos die Signale am Kabel angeklemmter Not-Halt-Taster erfassen kann, bietet PROFIsafe Vorteile im Umgang mit intelligenten F-Devices, wie Antrieben mit integrierter Sicherheit.

9.6. PA-Gerät

Es wurde bereits erwähnt, dass es für Sicherheit in der Prozessautomatisierung eine eigenständige Sektornorm gibt. NAMUR hat als Normungsorganisation für u.a. die Chemie- und Pharmaindustrie die Begleitnorm NE97 veröffentlicht, in der die F-Kommunikation mit F-Feldgeräten spezifiziert ist. Danach verfügt ein „betriebsbewährtes" PA-Gerät mit einer PROFIBUS MBP-IS-Schnittstelle über einen PROFIsafe-Treiber, der aktiviert oder deaktiviert werden kann. Im Modus „AUS" handelt es sich um ein Standard-PA-Gerät, im Modus „EIN" um ein F-Device (Abbildung 19).

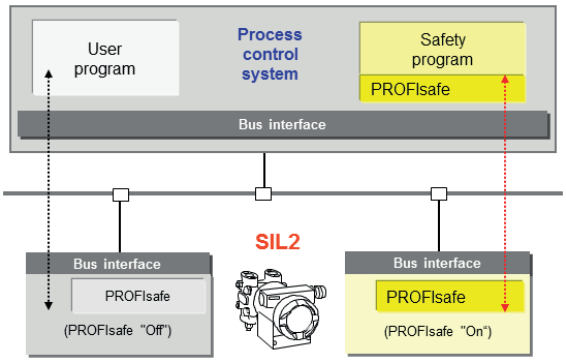

Abb. 19: PROFIsafe und NE97 für PA-Geräte

NAMUR hat mit der Norm VDI 2180 eine weitere Begleitnorm ins Leben gerufen, welche die Entwicklung von F-PA-Geräten erleichtert.

Derzeit werden für die meisten PROFIsafe-Anwendungen in der Prozessautomatisierung Remote I/Os mit F-Modulen für 4-20mA- oder HART-Systeme eingesetzt. Abbildung 20 zeigt die beiden Einsatzmöglichkeiten von PROFIsafe für „betriebsbewährte" PA-Geräte. Dies stellt einen gelungenen Kompromiss dar, obwohl die Vorteile von direkter Feldbusanbindung, wie z.B. Weitbereichsmessung, Parametrierung und ausgeklügelte Diagnostik, hier nicht zum Tragen kommen.

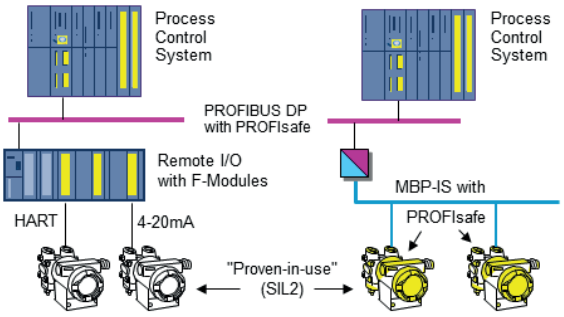

Abb. 20: Zwei Möglichkeiten für PROFIsafe und PA-Geräte

Füllstandsüberwachung

Auch Füllstandsschalter für Tanks profitieren von der PROFIsafe-Technologie. PROFIBUS PA mit den eigensicheren Übertragungen MBP-IS und RS485-IS eignen sich hervorragend für diese Art von F-Devices. PROFIsafe sorgt hier für die sicherheitsgerichtete Übertragung der Abschaltsignale, während der Anwender den Status der Sensoren über den Standard-Diagnosekanal abrufen kann.

ESD-Ventil

Auch für Electronic-Shut-Down-Ventile (ESD) können durch PROFIsafe erhebliche Verbesserungen erzielt werden. Hier besteht das Hauptziel darin, die Ventilfunktion durch „partial valve strokes" periodisch zu überprüfen und den Weg bis zur Endposition sowie die dafür benötigte Zeit im Trend zu überwachen. Dies kann automatisch durch F-Hosts realisiert werden und ermöglicht eine planbare Instandhaltung. Die RS485-IS-Schnittstelle ermöglicht zusammen mit Barrieren ein schnelles Abschalten, auch in Exi-Bereichen.

Drucktransmitter

Sicherheitsgerichtete Drucktransmitter führen die beiden Funktionen Füllstandsmessung und Überfüllsicherung eines Tanks durch einen Sollwertvergleich kombiniert aus.

Gas- und Feuermelder

Gas- und Feuermelder werden z.B. auf unbemannten Ölplattformen eingesetzt. Zusätzliche Positionsinformationen machen es möglich, die Brandabschnittstüren nur an den betroffenen Stellen automatisch zu schließen.

10. Anwendernutzen

Inzwischen sind mehr als 5 Millionen PROFIsafe-Knoten weltweit installiert.

Die installierte Basis von PROFIBUS beträgt heute weit mehr als 50 Mio. Geräte und die von PROFINET mehr als 10 Millionen.

Oberstes Entwicklungsziel bei Erweiterungen war und ist daher die vollständige Kompatibilität zu den bereits am Markt eingesetzten Geräten.

Dank des unabhängigen Kommunikationsprotokolls für funktionale Sicherheit von PROFIsafe und dem „Black-Channel-Prinzip" ist selbst der Umstieg von PROFIBUS nach PROFINET ohne besondere Umstände möglich. Die identische PROFIsafe-Treibersoftware kann in PROFINET- und PROFIBUS-Geräten verwendet werden.

Die Einführung von PROFIsafe bedeutete einen Quantensprung in 3 Schritten:

- Von sicherheitsgerichteter Relaislogik zu programmierbarer Logik
- Von Parallelverdrahtung zu funktional sicherer serieller Kommunikation
- Von isoliert arbeitenden zu kooperierenden F- Geräten

Die folgenden Aussagen sind eine treffende Zusammenfassung der Vorteile von PROFIsafe aus unterschiedlichen Blickwinkeln.

10.1. Integrator und Anwender

- Die gleichen Kosteneinsparungen wie bei der Einführung von Standard-PROFIBUS: reduzierte Verdrahtung, flexible Konfiguration, Parametrierung und Diagnose
- Einfaches und kosteneffizientes Systemdesign mit breitem Produktspektrum vieler Hersteller
- Keine besonderen Installations-Restriktionen
- Hoch innovative F-Anwendungen durch einfache Kommunikation zwischen intelligenten F-Devices

- Hohe Flexibilität bei Retrofit sowie bei Erweiterung und Umbau bestehender Anlagen
- Integrierte Technologie für Fertigungs- und Prozessautomatisierung
- Schulung, Dokumentation und Wartung nur für eine Bustechnologie erforderlich
- Programmierung von Standard- und F-Anwendungen mit nur einem Tool und zertifizierten F-Funktionsbausteinen
- Einfache Dokumentation von F-Konfiguration und F-Anwenderprogramm
- Kostensparende breite Akzeptanz der Systeme dank zertifizierter Geräte
- Internationale Akzeptanz durch IEC 61508-konforme Technologie
- Zertifikate von IFA und TÜV

10.2. Gerätehersteller

- TÜV-zertifizierte Software ermöglicht einfache Implementierung und kosteneffiziente Reproduzierbarkeit einer PROFIsafe-Lösung
- PROFIsafe-Kommunikation passt in unterschiedlichste Architekturen von programmierbaren F-Steuerungen
- PROFIsafe ist Wegbereiter für neue innovative Gerätefunktionen

10.3. Künftige Investitionen

- Riesige installierte Basis von PROFIBUS- und PROFINET-Geräten
- PROFIBUS &PROFINET-Organisationen und Support-Center weltweit präsent
- Alle von PI herausgegebenen bestehenden und zukünftigen Spezifikationen nutzbar auch für F-Anwendungen
- PROFIsafe ist internationaler Standard als IEC 61784-3-3 und GB/T-Standard in China
- Zukünftige Software wird den Lebenszyklus einer F-Anwendung vom Design über die Bewertung und Validierung bis hin zur Dokumentation begleiten und damit den Aufwand weiter verringern

11. PROFIBUS & PROFINET International (PI)

Offene Technologien bedürfen zu ihrer Pflege, Fortentwicklung und Verbreitung am Markt einer unternehmensunabhängigen Institution als Arbeitsplattform. Für die Technologien PROFIBUS und PROFINET wurde zu diesen Zwecken im Jahre 1989 die PROFIBUS Nutzerorganisation e.V. (PNO) als eine nonprofit Interessensvertretung von Herstellern, Anwendern und Instituten gegründet. Die PNO ist Mitglied im 1995 gegründeten internationalen Dachverband PI (PROFIBUS & PROFINET International). Mit mehr als 25 regionalen Vertretungen (RPA) und ca. 1.400 Mitgliedern ist PI auf allen Kontinenten vertreten und stellt die weltweit größte Interessengemeinschaft auf dem Gebiet der industriellen Kommunikation dar (Abbildung 21).

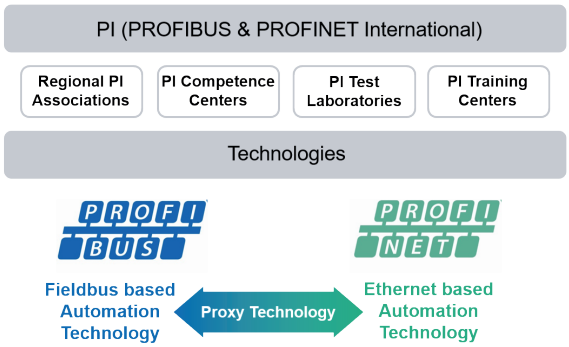

Abb. 21: PROFIBUS & PROFINET International (PI)

11.1. Aufgaben von PI

Die wesentlichen Aufgaben von PI sind:

- Pflege und Weiterentwicklung von PROFIBUS und PROFINET
- Förderung der weltweiten Verbreitung von PROFIBUS und PROFINET
- Investitionsschutz für Anwender und Hersteller durch Einflussnahme auf die internationale Normung
- Interessensvertretung der Mitglieder gegenüber Normungsgremien und Verbänden
- Weltweite technische Unterstützung von Unternehmen durch PI Competence Center (PICC)
- Qualitätssicherung durch Produktzertifizierung auf Basis von Konformitätstests in PI Testlabors (PITL)
- Etablierung eines weltweit einheitlichen Ausbildungsstandards durch PI Training Center (PITC)

11.2. Technologieentwicklung

PI hat die Technologieentwicklung an die PNO Deutschland übertragen. Der Beirat (Advisory Board) der PNO steuert die Entwicklungsaktivitäten. Die Technologie-Entwicklung findet in über 50

Arbeitskreisen statt, in denen über 500 Experten, vorwiegend aus den Entwicklungsabteilungen der Mitgliedsfirmen aktiv sind.

11.3. Technischer Support

PI unterhält weltweit mehr als 50 akkreditierte PICC. Diese Einrichtungen beraten und unterstützen die Anwender und Hersteller vielfältig. Als Einrichtung von PI bieten sie ihre Dienste im Rahmen des vereinbarten Regelwerkes firmenneutral an. PICC werden regelmäßig auf ihre Eignung hin in einem für sie zugeschnittenen Akkreditierungsprozess überprüft. Aktuelle Adressen sind auf der Website zu finden.

11.4. Zertifizierung

PI unterhält weltweit 10 akkreditierte PITL für die Zertifizierung von Produkten mit PROFIBUS- bzw. PROFINET-Schnittstelle. Als Einrichtung von PI bieten sie ihre Dienste im Rahmen des vereinbarten Regelwerkes firmenneutral an. Die Qualität der Testdienstleistungen der PITL wird regelmäßig in einem strengen Akkreditierungsprozess überprüft. Aktuelle Adressen sind auf der Website zu finden.

11.5. Ausbildung

Zur Sicherstellung eines weltweit einheitlichen Ausbildungsstandards für Ingenieure und Techniker wurden PITC etabliert. Die Akkreditierung der Training Center und deren Experten sichert die Qualität der Ausbildung und damit die der Engineering- und Aufbau-Dienstleistungen für PROFIBUS und PROFINET. Für PROFIsafe gibt es ein dreitägiges Training zum „PROFIsafe Certified Designer". Aktuelle Informationen sind auf der Website zu finden.

11.6. Internet

Aktuelle Informationen über PI und die Technologien PROFIBUS und PROFINET sind auf der PI-Website www.profibus.com verfügbar. Dazu gehören unter anderem ein Online-Product-Finder, ein Glossar, verschiedene Webinare und der Download-Bereich mit Spezifikationen, Profilen, Installations-Richtlinien und anderen Dokumenten.

PROFIsafe Systembeschreibung
Technologie und Anwendung

Version April 2016
Bestellnummer 4.341

Herausgeber:

PROFIBUS Nutzerorganisation e. V. (PNO)
PROFIBUS & PROFINET International (PI)
Ohiostraße 8 · 76149 Karlsruhe · Deutschland
Tel.: +49 721 98 61 97 0 · Fax: 721 98 61 97 11
E-Mail: info@profibus.com
www.profibus.com · www.profinet.com

Haftungsausschluss

Mit PI weltweite Unterstützung!

Regional PI Association (RPA)

Regional PI Associations (RPAs) repräsentieren PI rund um die Welt und sind Ihr persönlicher Ansprechpartner vor Ort. Sie verantworten das lokale Marketing für die Verbreitung von PROFIBUS, PROFINET und IO-Link, indem sie u. a. Messeauftritte, Seminare, Workshops, Pressekonferenzen durchführen und die Öffentlichkeitsarbeit wahrnehmen.

PI Competence Center (PICC)

Die PI Competence Center (PICCs) arbeiten eng mit den RPAs zusammen und sind Ihr erster Ansprechpartner bei technischen Fragen. Beim Entwickeln von PROFIBUS- oder PROFINET-Geräten, der Inbetriebnahme von Systemen sowie durch Anwendersupport und -schulung stehen die PICCs Ihnen bei Bedarf unterstützend zur Seite.

PI Training Center (PITC)

PI Training Center (PITCs) unterstützen Sie als Anwender oder Entwickler dabei, mehr über die Technologien PROFIBUS und PROFINET und deren Einsatzmöglichkeiten zu erfahren. Nach einer erfolgreich absolvierten Abschlussprüfung eines Kurses zum Certified Installer oder Engineer erhalten Sie ein von PI ausgestelltes Zertifikat.

PI Test Lab (PITL)

PI Test Labs (PITLs) sind von PI autorisiert, Zertifizierungstests für PROFIBUS und PROFINET durchzuführen. Nach einem erfolgreich bestandenen Test erhalten Sie von PI ein Zertifikat für Ihr Produkt. Das Zertifizierungswesen spielt eine große Rolle für die nachhaltige Qualitätssicherung der Produkte und sichert damit ein hohes Maß an Fehlerfreiheit und Verfügbarkeit der im Einsatz befindlichen Systeme.

PROFIBUS Nutzerorganisation e. V. (PNO)
PROFIBUS & PROFINET International (PI)
Ohiostraße 8 • 76149 Karlsruhe • Deutschland
Tel.: 721 98 61 97 0 • Fax: +49 721 98 61 97 11
E-Mail: info@profibus.com
www.profibus.com • www.profinet.com