Weshalb die Architektur von Safety-Systemen keine Rolle spielt

Roger Prew
Sicherheitsberater
ABB
Howard Road, St Neots, Großbritannien

Zusammenfassung

Bei der Architektur von Safety-Systemen kann „mehr“ an Sicherheit manchmal „weniger“ sein!

Als ABB Ende der siebziger Jahre seine ersten Safety-Systeme in der Nordsee einführte, war die interne Sicherheitsarchitektur des Systems von großer Bedeutung. Um nachzuweisen, dass der Entwurf das für sicherheitsrelevante Anwendungen erforderliche Integritätsniveau erzielen konnte, mussten die Systementwickler in erster Linie erläutern, inwieweit die interne Sicherheitsstruktur Redundanz gewährleistete. Begriffe wie 1oo2-, 2oo3-Voting, DMR-, TMR- und Quad-Systeme wurden im Laufe der Jahre vom Markt akzeptiert und erscheinen noch immer in Lastenheften und Zuliefererbroschüren. Seit der Einführung der Normen IEC61508 und IEC61511 ist der Begriff „Sicherheitsintegrität“ allerdings eindeutig definiert und hat zu einer neuen Systemgeneration geführt, für die die Begriffe DMR, TMR und Quad nicht gelten und keine Relevanz haben. Nach Meinung von Roger Prew, Sicherheitsberater bei ABB, ist die Kategorisierung der neuen Systemgeneration anhand ihrer Hardware-Architektur nicht mehr relevant und sollte vermieden werden.

Dokument-ID: 3BNP100416
Datum: 3. Dezember 2008

© Copyright 2008 ABB. Alle Rechte vorbehalten. Bilder, Diagramme und andere grafische Darstellungen in diesem Dokument dienen nur zur Veranschaulichung und stellen keine Produktkonfigurationen oder Produktfunktionen dar.

1. Was leistet ein Sicherheitssystem?

Ein Sicherheitssystem (*Safety System* oder *Safety Instrumented System* – SIS) hat die Aufgabe, jederzeit verfügbar zu sein, um einen gefährlichen Prozess automatisch in einen sicheren Zustand zu versetzen, falls im Prozess eine sicherheitsrelevante Funktionsstörung auftritt.

Die meisten in der Prozessindustrie eingesetzten Sicherheitssysteme sind Anwendungen, an die nur geringe Anforderungen gestellt werden, da der sichere Prozesszustand klar definiert ist und das System nur eingreifen muss, wenn ein Notfall eintritt.

Daher lauten die von einem Sicherheitssystem geforderten Funktionseigenschaften, dass es erstens für die Durchführung einer Notfallabschaltung (*Emergency Shutdown* – ESD) so lange wie möglich verfügbar bleiben muss (*High Availability MTBF*) und dass es zweitens in der Lage sein muss, auf eigene Funktionsstörungen auf eine vorher festgelegte, sichere Weise zu reagieren (*Fail Safe Action*). Fehlauslösungen aufgrund einer Funktionsstörung des Sicherheitssystems sind sowohl potenziell gefährlich als auch äußerst kostspielig für den Betreiber.

Bei den früheren Systemen waren diese beiden Eigenschaften oft nicht scharf voneinander abgegrenzt! Wenn eine Systemverfügbarkeit von 100 % garantiert werden könnte, wäre das Ausfallverhalten des Systems irrelevant, und es wäre keine interne Diagnose oder ein garantiertes sicheres Verhalten bei Ausfall (*fail-safe action*) erforderlich!

In der Praxis bemühten sich die Entwickler um hohe MTBF-Werte und setzten redundante fehlertolerante Architekturen ein, um der Tatsache entgegenzuwirken, dass die internen Diagnosemöglichkeiten begrenzt waren und gefährliche Ausfallzustände eintreten konnten (wenn auch nur selten)! Daher konnte das Triple- oder Quad-System mit inhärenter Fehlertoleranz und folglich hohem MTBF eine hohe PFD (Probability of Failure on Demand – Ausfallwahrscheinlichkeit im Anforderungsfall) mit niedrigem Diagnose-Deckungsgrad erreichen. Viele Systeme dieser Art arbeiteten mit einfachen Voting-Algorithmen wie 1oo2 (*1 out of 2* – 1 von 2) oder 2oo3 (2 von 3), um Ausfälle zu erkennen und entsprechende Maßnahmen durchzuführen. Voting-Systeme stellen zwar eine äußerst elegante Möglichkeit dar, den Ausfall des einen oder anderen Signalweges festzustellen, liefern aber nicht viele Informationen darüber, welche Ursache der Ausfall hatte und welche Maßnahme zur Beseitigung des Fehlers ergriffen werden sollte. Voting-Systeme lassen nur erkennen, dass auf einem der Signalwege eine Störung eingetreten ist. Im Gegensatz zur aktiven Echtzeit-Diagnose erfolgen Voting-Entscheidungen in der Regel nur dann, wenn ein sicherheitsrelevanter Systemanforderungsfall auftritt – und dann kann es schon zu spät sein! Außerdem kann ein konventionelles System mit dualer Redundanz entweder Verfügbarkeit gewährleisten, wenn der Voting-Algorithmus auf „1 out of 2“ eingestellt ist, oder Integrität, wenn der Voting-Algorithmus auf „2 out of 2“ eingestellt ist, aber nicht beides! Dieser Sachverhalt wird häufig falsch verstanden.

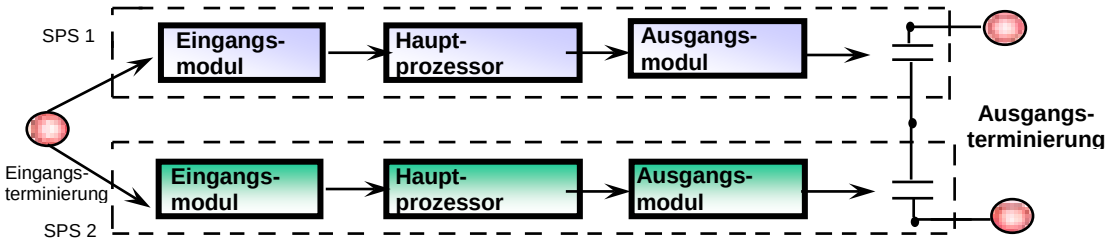


Abbildung 1 Ein duales 1oo2-System in „de-energise to trip scenario“ bietet hohe Integrität, aber geringe Verfügbarkeit

Dokument-ID: 3BNP100416
Datum: 3. Dezember 2008

© Copyright 2008 ABB. Alle Rechte vorbehalten. Bilder, Diagramme und andere grafische Darstellungen in diesem Dokument dienen nur zur Veranschaulichung und stellen keine Produktkonfigurationen oder Produktfunktionen dar.

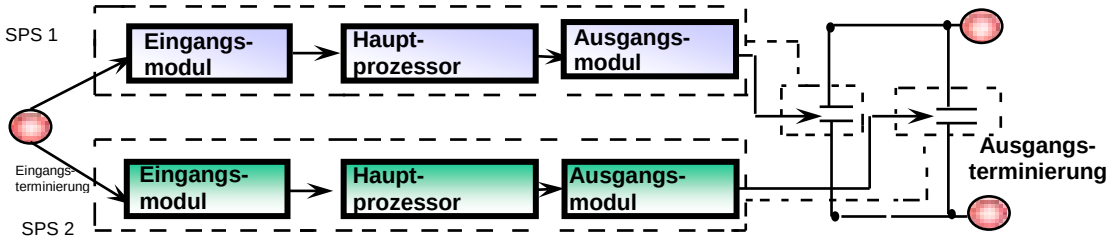


Abbildung 2 Ein duales 2oo2-System in „de-energise to trip scenario“ bietet hohe Verfügbarkeit, aber geringe Integrität

Bis zur Einführung der Standards IEC61508 und IEC61511 waren MTBF oder PFD der wichtigste Maßstab für die Qualitätsbeurteilung eines Sicherheitssystems. Dies ist jedoch eine relativ grobe Messmethode für Sicherheitssysteme die sich zu extrem anspruchsvollen Software-basierten Automatisierungssystemen entwickelt haben, und berücksichtigt nicht Aspekte wie Diagnose-Deckungsgrad, systematische Ausfälle, Common-Mode-Probleme und die Qualität und Integrität der Software.

2. IEC61508 / IEC61511

Die Verfasser dieser IEC-Normen führten eine genauere Untersuchung der Grundanforderungen durch, die erfüllt sein müssen, damit Sicherheitsintegrität[1] und Risikominderung erzielt werden können. Sie definierten vier zu messende Hauptkriterien die Sicherheitssysteme erfüllen müssen, damit der Sicherheits-Integritätslevel (SIL) als kompatibel zu dem Niveau angesehen wird, das in den Normen festgelegt ist und mittlerweile von der Branche allgemein vorausgesetzt wird. Diese Kriterien sind:

- Hardware-Sicherheitsintegrität; dieser Begriff bezieht sich auf die Fähigkeit der Hardware, die Folgen gefährlicher zufälliger Hardware-Ausfälle zu minimieren, und wird als PFD-Wert (*Probability of Failure to Danger* – Wahrscheinlichkeit eines gefährlichen Ausfalls) angegeben.
- Verhalten des Systems nach Erkennen eines Fehlerzustands. Sicherheitsrelevante Systeme müssen in der Lage sein, eine im Störungsfall sichere (*fail-safe*) Vorgehensweise auszuführen; darunter versteht man die Fähigkeit eines Sicherheitssystems, bei jedem denkbaren Ausfallzustand auf eine sichere, vorher festgelegte Weise (z. B. durch Abschaltung) zu reagieren. Dies wird in der Regel als „Safe Failure Fraction“ (SFF – Anteil ungefährlicher Ausfälle) bezeichnet und wird anhand einer Analyse des Diagnose-Deckungsgrads ermittelt, den die betreffende Applikation erreichen kann (siehe unten).
- Der wichtige neu eingeführte Parameter ist *Safe Failure Fraction* (SFF), der ein Maß für den Deckungsgrad und die Wirksamkeit der Diagnose im System darstellt. Um auch frühere Systementwürfe berücksichtigen zu können, die auf einem höheren Maß an Redundanz und einem niedrigeren Diagnose-Deckungsgrad basierten, berücksichtigt die Norm bei der Beurteilung der erreichten SIL-Bewertung die komplette Systemarchitektur. Die maximale SIL-Bewertung richtet sich nach *Safe Failure Fraction* (SFF) und *Hardware Fault Tolerance* (HFT), wie unten in Tabelle 1 dargestellt.
- Die systematische Sicherheitsintegrität bezieht sich auf Ausfälle, die aufgrund des Systementwicklungsprozesses sowie des Entwurfs und der Implementierung der Sicherheitskette erfolgen können, und beinhaltet sämtliche Aspekte seines betriebs- und instandhaltungsbezogenen Sicherheitsmanagements.

[1] „Sicherheitsintegrität“ gibt die Wahrscheinlichkeit an, mit der ein sicherheitsrelevantes System die erforderlichen Funktionen unter sämtlichen angegebenen Bedingungen innerhalb eines angegebenen Zeitraums erfolgreich ausführt [1].

Dokument-ID: 3BNP100416
Datum: 3. Dezember 2008

© Copyright 2008 ABB. Alle Rechte vorbehalten. Bilder, Diagramme und andere grafische Darstellungen in diesem Dokument dienen nur zur Veranschaulichung und stellen keine Produktkonfigurationen oder Produktfunktionen dar.

Die PFD- und SFF-Werte lassen sich für eine konkrete Systemkonfiguration aus der FMEA-Analyse (*Failure Modes and Effects Analysis*) beurteilen, und die Anforderungen zur Erfüllung der drei in der Anlagenindustrie akzeptablen SIL-Stufen sind in der folgenden Tabelle dargestellt.

Safe Failure Fraction (SFF)	**Hardware-Fehlertoleranz (siehe Anmerkung)**		
	0	1	2
< 60 %	Nicht zulässig	SIL 1	SIL 2
60 % - < 90 %	SIL 1	SIL 2	SIL 3
90 % - < 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4
Anmerkung 2: Eine Hardware-Fehlertoleranz von N bedeutet, dass N + 1 unbemerkte Fehler einen Verlust der Sicherheitsfunktion verursachen könnten.			

Tabelle 1 Hardware-Sicherheitsintegrität: architekturbedingte Einschränkungen für komplexe elektronische/programmierbare sicherheitsrelevante Teilsysteme (Quelle: IEC61508-2 Tabelle 3)

Die systematische Integrität ist eine von der Zertifizierungsstelle durchgeführte qualitative Bewertung, die betrachtet, inwieweit die Systementwickler die Maßnahmen zur Reduzierung von systematischen Ausfällen während der Entwurfsphase und im Rahmen der Systemfunktionalität interpretiert und umgesetzt haben.

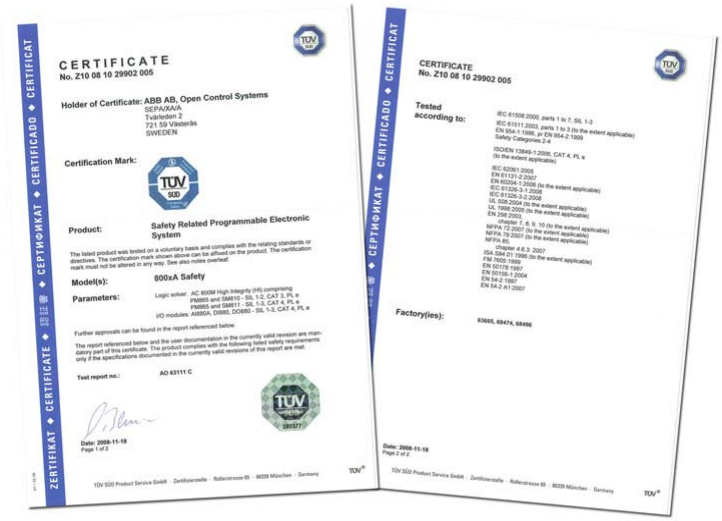
Die Norm versucht nicht speziell, die Frage von Common-Mode-Ausfällen zu beurteilen, sondern überlässt diese den Überlegungen im Rahmen der systematischen Sicherheitsintegrität. Mehrfachausfälle („Common Mode“-Ausfälle) sind allerdings problematisch bei Systemen, die identische redundante Wege verwenden, um höhere SIL-Stufen mit niedrigeren SFF-Stufen zu erreichen; aber dies wird weiter hinten noch ausführlicher behandelt.

3. Was bedeutet all das in der Praxis?

Der 800xA HI (High Integrity) SIL3-Controller von ABB ist eine Weiterentwicklung des bestehenden SIL2-Controllers, der in den letzten 3 Jahren erfolgreich vermarktet wurde. Der Controller mit SIL3-Zertifizierung hat den gleichen Geräteaufbau wie die SIL2-Version, aber mit verbesserter Firmware und Software. Ebenso wie beim SIL2-Gerät wurde auch bei diesem Controller schon in der Konzeptionsphase auf die detaillierten Anforderungen der Norm IEC61508 eingegangen.

Dokument-ID: 3BNP100416
Datum: 3. Dezember 2008

© Copyright 2008 ABB. Alle Rechte vorbehalten. Bilder, Diagramme und andere grafische Darstellungen in diesem Dokument dienen nur zur Veranschaulichung und stellen keine Produktkonfigurationen oder Produktfunktionen dar.



CERTIFICATE
No. Z10 08 10 29902 005

Holder of Certificate: ABB AB, Open Control Systems
SEPA/XA/A
Tvåridsen 2
721 59 Västerås
SWEDEN

Certification Mark:

Product: Safety Related Programmable Electronic System

The listed product was tested on a voluntary basis and complies with the relating standards or directives. The certification mark shown above can be affixed on the product. The certification mark must not be altered in any way. See also notes overleaf.

Model(s): 800xA Safety

Parameters: Logic solver: AC 800M High Integrity (HI) comprising PM865 and SM810 - SIL 1-3, CAT 3, PL e
PM865 and SM811 - SIL 1-3, CAT 4, PL e
I/O modules: AI890A, DI890, DO890 - SIL 1-3, CAT 4, PL e

Further approvals can be found in the report referenced below.

The report referenced below and the user documentation in the currently valid revision are mandatory part of this certificate. The product complies with the following listed safety requirements only if the specifications documented in the currently valid revisions of this report are met.

Test report no.: AO 63111 C

Date: 2008-11-18
Page 1 of 2

TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstrasse 65 · 80339 München · Germany

CERTIFICATE
No. Z10 08 10 29902 005

Tested according to:

IEC 61508:2000, parts 1 to 7, SIL 1-3
IEC 61511:2003, parts 1 to 3 (to the extent applicable)
EN 954-1:1996, or EN 954-2:1999
Safety Categories 2-4

ISO/EN 13849-1:2006, CAT 4, PL e
(to the extent applicable)

IEC 62061:2005
EN 61131-2:2007
EN 60204-1:2006 (to the extent applicable)
IEC 61326-3-1:2008
IEC 61326-3-2:2008
UL 508:2004 (to the extent applicable)
UL 1998:2005 (to the extent applicable)
EN 298:2003
chapter 7, 8, 9, 10 (to the extent applicable)
NFPA 72:2007 (to the extent applicable)
NFPA 79:2007 (to the extent applicable)
NFPA 85:
chapter 4 & 3: 2007
ISA 584.01:1996 (to the extent applicable)
FM 7605:1998
EN 50178:1997
EN 50156-1:2004
EN 54-2:1997
EN 54-2 A1:2007

Factory(ies): 63005, 68474, 68496

Date: 2008-11-18
Page 2 of 2

TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstrasse 65 · 80339 München · Germany

Abbildung 3 High Integrity-Zertifikat für 800xA

Der 800xA High Integrity-Controller kann in verschiedenen Architekturen als Simplex-Ausführung oder mit dualer Redundanz konfiguriert werden.

Wenn wir den einfachen SIL3-Controller betrachten, so behandelt er die vier Grundanforderungen der Norm auf sehr direkte Weise:

- PFD ist ein Maß für die Wahrscheinlichkeit eines gefährlichen (unbemerkten) Ausfalls des Systems. Die 800xA SIL2- und SIL3-Controller verwenden im Wesentlichen die gleiche Hardware. Die Grundelektronik ist auf maximale Zuverlässigkeit ausgelegt. Sie verwendet einen hohen Integrationsgrad, im praktischen Einsatz bewährte Komponenten und Produktions- und Testverfahren auf weltweitem Spitzenniveau. Der auf der Grundlage empirischer Zahlen berechnete PFD für die Elemente des Grundsystems ist in der nachfolgenden Tabelle dargestellt. Diese liegen am obersten Ende des Anforderungsbereichs für SIL 3-Systeme. Wenn wir die tatsächlichen Hardware-Ausfälle anhand der zurückgesendeten defekten Module aus den Anlagen analysieren (über 3 200 Geräte sind installiert, viele davon seit 2 Jahren), könnte sich dieser Wert noch weiter verbessern. Dieser guter, hoher Wert wird durch die veränderte Grundkonzeption erzielt und nicht durch eine Duplizierung der Hardware und einerDuplizierung von Voting-Verfahren! (In der folgenden Tabelle bezeichnet „PFH“ die Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde.)

Dokument-ID: 3BNP100416
Datum: 3. Dezember 2008

© Copyright 2008 ABB. Alle Rechte vorbehalten. Bilder, Diagramme und andere grafische Darstellungen in diesem Dokument dienen nur zur Veranschaulichung und stellen keine Produktkonfigurationen oder Produktfunktionen dar.

Variant	Including	SFF %	λdu	SIL2/SIL3	SIL2/SIL3
				PFD	PFH
PM865 Single PU		99.55%	5.74E-09	SIL2	SIL2
Processor Module	1 x PM865			1.21E-5	1.72E-10
Termination Plate	1 x TP830			SIL3	SIL3
Supervisory module	1 x SM810/SM811			8.04E-6	1.15E-10
Termination Plate	1 x TP855				
PM865 Redundant PU		99.55%	5.74E-09	SIL2	SIL2
Processor Module	2 x PM865			1.21E-5	1.72E-10
Termination Plate	2 x TP830			SIL3	SIL3
CEX-Bus interconnection Unit	2 x BC810			8.04E-6	1.15E-10
Termination Plate	2 x TP857				
Supervisory Module	2 x SM810/SM811				
Termination Plate	2 x TP855				
I/O					
Digital Input module	1ch DI880	99.98%	1.36E-10	9.52E-6	1.36E-10
Module Termination Unit(MTU)	TU842/843				

Tabelle 2 zeigt SFF, PFD und PFH für die 800xA HI-Komponenten

- Die systematische Sicherheitsintegrität des 800xA HI wird in erster Linie durch ein umfassendes Entwurfs-, Entwicklungs- und Testprogramm seitens des Systemkonstrukteurs erzielt, wobei alle Prozesse und Entwurfsmeilensteine im Rahmen eines strengen, TÜV-zertifizierten Funktionssicherheits-Managementsystems (FSMS) absolviert und in jeder Phase des Hardware- und Software-Entwicklungsprozesses von einer unabhängigen Zertifizierungsstelle wie dem TÜV genau untersucht und genehmigt werden. Natürlich sind Konstruktions- oder Systemfehler niemals ganz ausgeschlossen. Dies berücksichtigt die „integrierte Diversität“ (*Embedded Diversity*) des 800xA HI , die eine kontinuierliche aktive Prüfung auf Software-Funktionsstörungen während des Betriebs durchführt.
- Von Interesse sind dabei der SFF-Zahlenwert und das HFT-Konzept; und hier fokussiert der 800xA HI Controller im Wettbewerb mit der konventionellen architekturbasierten Analyse und entsprechender Hardware.
- Die Grundkonzeption stellt sicher, dass alle festgestellten Funktionsstörungen gemeldet werden und den Controller entweder in eine eingeschränkte (aber weiterhin sichere) Betriebsart versetzen oder einen sicheren Vorgang (Abschaltung) auslösen.

4. Ein hoher SFF-Wert weist auf eine High-Integrity-Konstruktion hin

Der Anteil ungefährlicher Ausfälle (*Safe Failure Fraction*) eines Teilsystems berechnet sich als

$$SFF = (\sum \lambda_S + \sum \lambda_{DD}) / (\sum \lambda_S + \sum \lambda_D)$$

Dabei ist

$\sum \lambda_S$ die Gesamtwahrscheinlichkeit ungefährlicher Ausfälle,

Dokument-ID: 3BNP100416
Datum: 3. Dezember 2008

© Copyright 2008 ABB. Alle Rechte vorbehalten. Bilder, Diagramme und andere grafische Darstellungen in diesem Dokument dienen nur zur Veranschaulichung und stellen keine Produktkonfigurationen oder Produktfunktionen dar.

$\sum \lambda_D$ die Gesamtwahrscheinlichkeit gefährlicher Ausfälle und

$\sum \lambda_{DD}$ die Gesamtwahrscheinlichkeit gefährlicher Ausfälle, die von den Diagnose-Tests erkannt werden.

Diese drei Arten von Ausfällen werden in der Norm klar definiert:

- Sicherer Ausfall (*Safe Failure*)
  - Das Teilsystem absolviert einen sicheren Ausfall auf, wenn es die Sicherheitsfunktion ohne Anforderung seitens des Prozesses ausführt.
- Gefährlicher Ausfall (*Dangerous Failure*)
  - Das Teilsystem absolviert einen gefährlichen Ausfall auf, wenn es seine Sicherheitsfunktion nicht auf Anforderung ausführen kann.
- Erkannter Ausfall (*Detected Failure*)
  - Ein Ausfall wird erkannt, wenn die integrierte Diagnose den Ausfall erkennen lässt. Beim 800xA High Integrity werden Ausfälle innerhalb einer Zeit von 50 ms bis 1 s erkannt.

Ausfälle können außerdem durch folgende Mechanismen erkannt werden:

- durch den normalen Betrieb – (dies führt in der Regel zu einer Fehlauslösung)
- durch regelmäßige Überprüfungen – (dieser Fall könnte sehr selten eintreten, z. B. alle 8 Jahre beim 800xA HI)
- durch die integrierte Diagnose.

Das spezielle Diagnosekonzept des 800xA HI verwendet ein hohes Maß an konventioneller aktiver Diagnose (integrierte Tests) sowie eine aktive Diskrepanzprüfung zwischen den beiden getrennten Ausführungswegen, so dass der Simplex-Controller einen SFF-Wert von fast 100 % erreicht (angegeben werden 99,8 %). Außerdem weist das SIL3-Modell dank seiner Diversitätsstruktur einen HFT-Wert von 1 für den Simplex-Controller und die Simplex-E/A auf. Aus der obigen Tabelle lässt sich entnehmen, dass der 800xA HI eigentlich die PFD- und SFF-Anforderungen für SIL4 erfüllt, obwohl er nur für SIL3 zertifiziert ist. Dies konnte erzielt werden, da der SIL2-Controller mit dem HFT-Wert 0 klassifiziert ist, aber dennoch die PFD- Anforderungen für SIL3 erfüllt. Der SIL3-Controller weist aber wegen seiner integrierten Diversitätstechnologie den HFT-Wert 1 auf, wodurch einerseits die systematische Integrität verbessert und andererseits eine gewisse Fehlertoleranz erzielt wird.

Häufig wird behauptet, dass durch eine Erhöhung des SFF-Werts lediglich gefährliche unerkannte Ausfallzustände in die Kategorie der erkannten Ausfälle verschoben werden, was wiederum eine Zunahme der Fehlauslösungen bedeutet!

Damit wir Vertrauen in unser Sicherheitssystem haben können, wünschen wir unter keinen Umständen unerkannte gefährliche Fehlerzustände! Diese vergrößern das Potenzial von langfristig unerkannten Ausfällen. Auch in einem konventionellen Dual- oder Triple-System bewirkt ein unerkannter gefährlicher Ausfall zumindest eine Beeinträchtigung des Systems, da einer der Wege im Bedarfsfall nicht funktionsfähig ist, und könnte im schlimmsten Fall – bei einem Common-Mode-Ausfall – das gesamte Sicherheitssystem in einen gefährlichen Zustand versetzen. Dies gilt insbesondere für das TMR-Konzept, bei dem ein einzelner nicht erkannter Fehler den Voting-Algorithmus „2 out of 3“, von dem seine Integrität abhängig ist, außer Funktion setzen kann!

Der 800xA HI erreicht de facto einen Diagnose-Deckungsgrad von 100 %, da keine gefährlichen Ausfallzustände bekannt sind, und kann daher effektiv die Einhaltung von SIL3 erzielen, ohne dabei auf HFT zurückgreifen zu müssen. HFT wurde in erster Linie in die Norm aufgenommen, um Legacy-Systemen, die in hohem Maße von Redundanz und Voting-Systemen abhängig waren, die Erfüllung der SIL-Anforderungen zu ermöglichen. Die Definition von HFT in der Norm ist allerdings sehr spezifisch und bezieht sich nur auf unbemerkte Ausfälle. Sie

Dokument-ID: 3BNP100416
Datum: 3. Dezember 2008

© Copyright 2008 ABB. Alle Rechte vorbehalten. Bilder, Diagramme und andere grafische Darstellungen in diesem Dokument dienen nur zur Veranschaulichung und stellen keine Produktkonfigurationen oder Produktfunktionen dar.

besagt mit Sicherheit nicht, dass ein Produkt nach der Erkennung eines Fehlers weiterhin funktioniert – was aber die meisten Anwender von einem fehlertoleranten System erwarten.

Wie sieht es mit Fehlauslösungen aus? Wenn ein Sicherheitssystem einen Diagnose-Deckungsgrad von 100 % aufweist, aber anfällig für Komponenten- oder Software-Ausfälle ist, dann erzeugt es ein inakzeptables Maß von Fehlauslösungen!

Zusätzlich zu dem hohen PFD-Wert und dem hohen SFF-Wert weisen die Simplex-Versionen des 800xA HI-Controllers und der E/A dank des hohen Integrationsgrads und der geringen Belastung und Verlustleistung der Elektronik einen inhärent hohen Zuverlässigkeitsgrad auf. Dadurch erhält der Simplex-Controller eine MTBF von fast 20 Jahren. (Somit befindet er sich auf dem gleichen Niveau wie TMR-Systeme der neuesten Generation!)

Die integrierte Diversitätsstruktur des Simplex-Controllers bewirkt eine weitere Erhöhung der statistischen MTBF (*Mean Time Between Failures*), da der SIL3-Controller damit nach dem Erkennen eines E/A-Kanalfehlers noch eine gewisse Zeit lang in einer eingeschränkten (aber zertifizierten) Betriebsart weiterarbeiten kann.

Wenn die Systemverfügbarkeit höchste Priorität hat, wie es bei zahlreichen Anwendungen in den Branchen Öl, Gas und Petrochemie der Fall ist, kann der 800xA HI für verschiedene Betriebsarten mit dualer Redundanz konfiguriert werden. Wichtig ist dabei, dass das Simplex-System und die Systeme mit dualer Redundanz genau den gleichen PFD-Wert und genau den gleichen SFF-Wert besitzen und beide den HFT-Wert 1 aufweisen. Sie verfügen über genau die gleiche Sicherheitsintegrität; der einzige Unterschied ist die MTBF (Verfügbarkeit), die sich im Vergleich zu einem ähnlichen Simplex-System um über 400 Jahre erhöhen kann.

Zuverlässigkeit, Sicherheitsintegrität und Redundanz – Begriffe, bei denen es in früheren Systemgenerationen zu großen Verwechslungen kam – sind nun wesentlich besser definiert, und durch eine Abgrenzung zwischen Zuverlässigkeit und Sicherheitsintegrität einerseits und Fehlertoleranz und HFT andererseits dürften Leistungsvergleiche zwischen Sicherheitssystemen anhand der neuen Normen erheblich einfacher werden.

Nebenbei bemerkt liegt eine gewisse Ironie in der Tatsache, dass ein Triple-System, das einen hohen Grad an Diagnose-Deckungsgrad für sich beansprucht, hinsichtlich der Integrität keinen Nutzen aus der Triple-Architektur zieht. Das 2oo3-Voting-Verfahren verbessert die Sicherheitsintegrität nicht: Da alle Kanäle die gleiche Technologie einsetzen, bewirkt das 2oo3 Vefahren weder bei der systematischen Beurteilung noch bezüglich der Common-Mode-Problematik eine Verbesserung und führt gemäß dem Ertragsgesetz (*diminishing returns*) nicht zwangsläufig zu einer Verbesserung der Verfügbarkeit gegenüber einer ähnlichen Architektur mit doppelter Redundanz.

5. Voting-Verfahren und Diagnose

Voting ist das verbreitetste Verfahren zur Erkennung von Abweichungen bei der Verarbeitung der Ergebnisse von redundanten Kanälen in mehrkanaligen Systemen. In der **Tabelle 1**, die direkt aus der Norm übernommen wurde, lässt sich erkennen, dass die Voting-Ergebnisse als Mechanismus zur Erhöhung des Diagnose-Deckungsgrades betrachtet werden können. Die Verfasser der IEC61508-Normen haben aber berücksichtigt, dass Voting-Systeme inhärente Schwächen aufweisen, wenn versucht wird, hohe Integritätsstufen zu erreichen. Wenn der Voting-Mechanismus nicht mehr verfügbar ist, da sich in einem der Kanäle ein nicht erkannter Ausfall entwickelt, kompromittiert dies die Integrität des Systems, und was noch gravierender dabei ist, ohne jemand dies bemerkt! Falls aufgrund des Voting-Verfahrens ein Ausfall erkannt wird, wechselt das System in einen eingeschränkten Betriebszustand, in dem seine Sicherheitsintegritäts-Funktionalität eventuell reduziert ist. Falls ein Ausfall nicht erkannt wird, bleibt der eingeschränkte Betriebszustand eventuell unerkannt, bis eine Anforderung an das System gestellt wird – also wenn es eventuell schon zu spät ist.

Außerdem werden einfache Voting-Systeme oft durch potenzielle Einzelfehlerstellen (*Single Point Of Failure*) im Voting-System selbst beeinträchtigt.

Die Verfügbarkeit lässt sich nur dann wirksam erhöhen, wenn das redundante System sowohl in einem vollständig redundanten als auch im eingeschränkten Modus weiterhin mit dem angegebenen SIL funktionsfähig ist. Wie

Dokument-ID: 3BNP100416
Datum: 3. Dezember 2008

© Copyright 2008 ABB. Alle Rechte vorbehalten. Bilder, Diagramme und andere grafische Darstellungen in diesem Dokument dienen nur zur Veranschaulichung und stellen keine Produktkonfigurationen oder Produktfunktionen dar.

bereits erwähnt, weist der 800xA HI sowohl in der Simplex-Ausführung als auch in der Konfiguration mit doppelter Redundanz genau die gleiche Sicherheitsintegrität auf.

Die Norm berücksichtigt die drei folgenden Arten von Systemausfällen:

- Zufällige Hardware-Ausfälle
- Systematische – konstruktions-, implementierungs- oder betriebsbedingte – Ausfälle
- Common-Mode-Ausfälle

Die Wahrscheinlichkeit, dass zufällige Hardware-Ausfälle auftreten, lässt sich anhand der vom Hersteller gelieferten Zuverlässigkeitsdaten der betreffenden Komponente beurteilen. Diese Ausfälle betreffen in einem mehrkanaligen redundanten System wahrscheinlich jeweils nur einen einzelnen Kanal. Systematische und Common-Mode-Ausfälle könnten dagegen sämtliche Kanäle eines mehrkanaligen Voting-Systems in genau der gleichen Weise betreffen. Dies könnte zu einem Totalausfall des Systems führen!

Folglich sollten Voting-Systeme mit identischen Kanälen vermieden werden, falls die Auswirkungen von systematischen und Common-Mode-Problemen reduziert werden sollen. Natürlich nutzt die Mehrzahl der Dual-, Triple- und Quad-Systeme ein Voting-Verfahren zwischen identischen Kanälen.

Dokument-ID: 3BNP100416
Datum: 3. Dezember 2008

© Copyright 2008 ABB. Alle Rechte vorbehalten. Bilder, Diagramme und andere grafische Darstellungen in diesem Dokument dienen nur zur Veranschaulichung und stellen keine Produktkonfigurationen oder Produktfunktionen dar.

6. Diversität ist besser als Quantität!

Voting-Systeme mit Diversität gibt es schon seit langem. Die im Kernenergiebereich eingesetzten Sicherheitssysteme arbeiten mit Voting zwischen verschiedenen Systemen, die oft mit verschiedenen Technologien arbeiten (Relais, Pneumatik, Elektronik etc.), von verschiedenen Unternehmen geliefert und von verschiedenen Teams in Betrieb genommen werden. Die Wahrscheinlichkeit, dass systematische oder Common-Mode-Ausfälle die Integrität des Gesamtsystems beeinträchtigen, wird daher weitgehend vermindert.

Die Simplex-Ausführungen des 800xA HI-Controllers und der E/A-Einheiten verfügen über integrierte getrennte („diverse“) Parallelverarbeitungspfade, bei denen eine aktive Diskrepanzprüfung zwischen den Pfaden die integrierte aktive Diagnose ergänzt.

Die integrierte Hardware-Diversität in der Controller-Hardware wird erreicht, indem unterschiedliche Prozessorkarten für den Controller (PM865) und das Überwachungsmodul (SM811) eingesetzt werden. Die Diversität der Software wird durch die Verwendung verschiedener Betriebssystem-Ausführungen, Compiler und Programmierungsrichtlinien sowie unterschiedlicher Programmimplementierungen im Controller- und Überwachungsmodul erzielt. Als zusätzliche Maßnahme gegen systematische und Common-Mode-Probleme wurde das Controller- und Überwachungsmodul von verschiedenen Teams entwickelt und getestet, die in zwei verschiedenen Ländern arbeiteten und sich aus Mitarbeitern mit unterschiedlichen Hintergründen und Erfahrungen zusammensetzten. Auch die E/A-Module verwenden zwei Signalwege mit einer Technologie, die integrierte Diversität aufweist, da der eine Weg mit FPGA-Technologie und der andere mit MCPU arbeitet.

Der 800xA HI entspricht nicht der konventionellen 1oo2D-Architektur und lässt sich nicht in diesen Kategorien beschreiben. Falls man es dennoch für erforderlich hält, ihm eine architekturbezogene Kennzeichnung zuzuweisen, so sollte diese Sicherheitsarchitektur beschrieben werden als **„Integrierte Diversitätstechnologie“.** Diese Diversitätstechnologie wird im **Dual**-Format eingesetzt, wenn sie in einer Einzelkonfiguration implementiert wird, und als **Quad**-Format in einer redundanten Konfiguration.

Dokument-ID: 3BNP100416
Datum: 3. Dezember 2008

© Copyright 2008 ABB. Alle Rechte vorbehalten. Bilder, Diagramme und andere grafische Darstellungen in diesem Dokument dienen nur zur Veranschaulichung und stellen keine Produktkonfigurationen oder Produktfunktionen dar.

Abbildung 4 800xA High Integrity im Dual-Format mit Einzel-E/As

Dokument-ID: 3BNP100416
Datum: 3. Dezember 2008

© Copyright 2008 ABB. Alle Rechte vorbehalten. Bilder, Diagramme und andere grafische Darstellungen in diesem Dokument dienen nur zur Veranschaulichung und stellen keine Produktkonfigurationen oder Produktfunktionen dar.

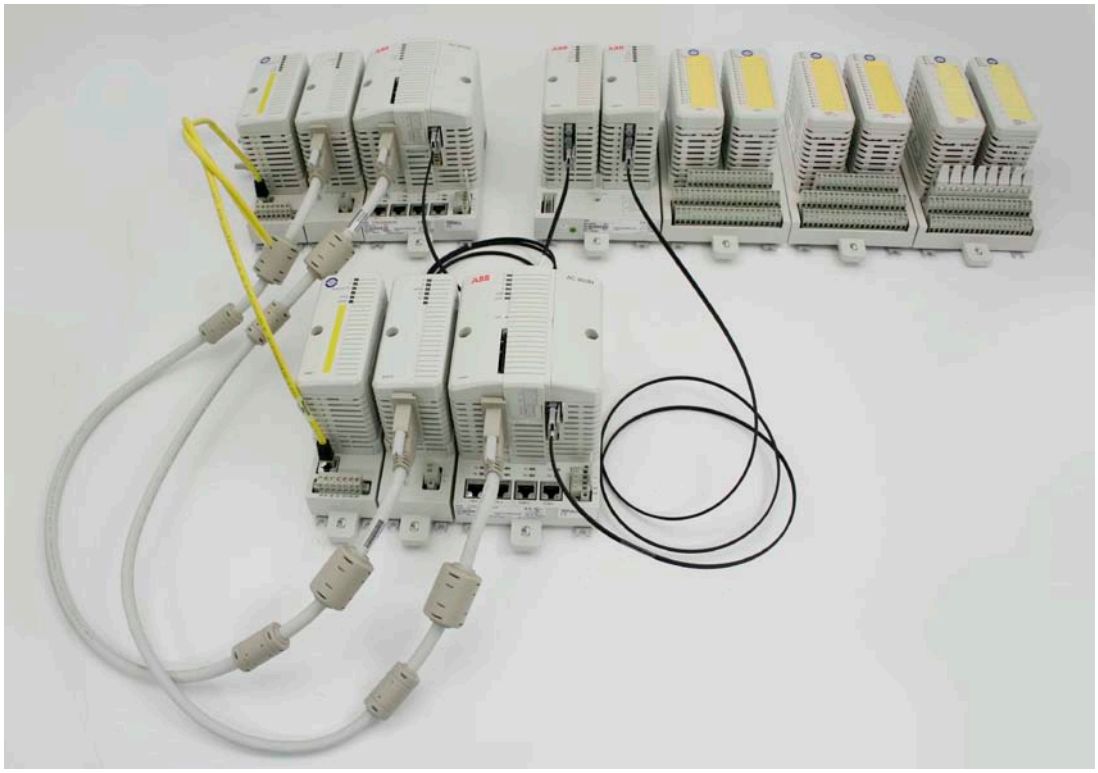


Abbildung 5 800xA High Integrity im Quad-Format mit redundanten E/As

Aufgrund des Systementwurfs und der Vorgehensweise beim Entwicklungsprozess sowie durch die Verwendung einer sicheren Firewall-Technologie, die unterschiedliche Anwendungen, die auf einem einzelnen Controller ausgeführt werden, voneinander trennt und sie schützt, kann der 800xA HI sowohl SIL3-zertifizierte als auch einfache Prozesssteuerungs-Anwendungen in demselben Controller ausführen, und zwar entweder im Simplex-Modus oder mit dualer Redundanz. Natürlich müssen Zugänglichkeit, Aufrüstungs- und Änderungsmöglichkeiten berücksichtigt werden, die in der Regel als Anforderungen an Control-Anwendungen gestellt werden und für zertifizierte Sicherheitssysteme ein Problem darstellen, aber die gewonnene zusätzliche Flexibilität ist, insbesondere bei kleineren Automatisierungsprojekten, äußerst wertvoll.

7. Active Voting oder Haupt-/Standby-System

Nachdem wir die Integritäts- von den Verfügbarkeitsanforderungen abgegrenzt haben, lässt sich nun die Effektivität der verschiedenen Entwürfe wesentlich einfacher messen.

Die Halbleiterelektronik weist inhärent eine sehr hohe Zuverlässigkeit auf, sobald die Phase der frühzeitigen Ausfälle überwunden ist. Sorgfältige Auswahl der Bauteile und Burn-in-Tests während der Fertigung stellen sicher, dass der 800xA HI – selbst bei Simplex-Betrieb – höchste Zuverlässigkeitswerte erreicht. Empirische Beurteilungen (die bei der Berechnung des erzielten SIL verwendet wurden) liegen am obersten Ende des SIL3-Bereichs, und anhand der zurückgesendeten defekten Geräte aus den Anlagen lässt sich auf der Basis von über 600 ausgelieferten Sicherheitssystemen mit über 60 000 E/A-Einheiten, die im Feld vollständig im Einsatz sind, deutlich erkennen, dass die tatsächlich erzielten Werte noch einmal um eine Größenordnung besser sind.

Da dieses Zuverlässigkeitsniveau bereits mit dem Simplex-Produkt erzielt wird, könnte man sich die Frage stellen, weshalb ein Angebot mit Dual-Redundanz überhaupt notwendig ist. Es gibt aber zahlreiche hochgradig kritische

Dokument-ID: 3BNP100416
Datum: 3. Dezember 2008

© Copyright 2008 ABB. Alle Rechte vorbehalten. Bilder, Diagramme und andere grafische Darstellungen in diesem Dokument dienen nur zur Veranschaulichung und stellen keine Produktkonfigurationen oder Produktfunktionen dar.

oder unbemannte Prozesse, bei denen die Kosten von nur einer Fehlauslösung in 20 Jahren extrem viel höher wären als die Ergänzung eines redundanten Systems.

Der 800xA HI zeichnet sich durch einen sehr charakteristischen Geräteaufbau aus, da E/A-Einheiten und Controller im redundanten Betrieb unabhängig voneinander angeboten werden können, sodass sich die Verfügbarkeit der E/A-Einheit und/oder des Controllers unabhängig voneinander erhöht. Das heißt, dass bei kritischen Prozessen, die bei Totalausfall von einem E/A-Kanal (d. h. zwei Ausfälle) weiterlaufen können, nur die Prozessoren dupliziert werden müssen. Bei den meisten Prozessen ist nur ein kleiner Teil der E/A so kritisch, dass sie 100 % Verfügbarkeit erfordert; daher können gemischte Systeme mit redundanter und nicht-redundanter E/A mit den entsprechenden Kosteneinsparungen konfiguriert werden.

Beim 800xA HI wird die Redundanz durch Hot-Standby-Betrieb, d. h. eine Quad-Konfiguration erzielt. Der eine Controller führt die Logik- und Kontrollfunktionen aus, während der andere parallel dazu läuft und seinen Betrieb mit dem ersten synchronisiert. Falls eine Funktionsstörung im Haupt-Controller eintritt, übernimmt der Standby-Controller die Arbeit übergangslos innerhalb von nur einem Abtastzyklus, und der Fehler wird gemeldet. Wenn dagegen eine Störung beim Slave-Prozessor auftritt, wird dies erkannt und gemeldet. SIL, Reparaturzeit und die gesamte Systemintegrität werden durch den Ausfall einer Seite des Systems in keiner Weise beeinträchtigt. Durch diese Struktur mit Hot-Standby-Umschaltung bleiben alle Vorteile von Voting-Systemen mit Parallelbetrieb erhalten, aber ohne die potenziellen Einzelfehlerstellen, die ein Voting-System aufweisen könnte.

Die erzielte Steigerung der Verfügbarkeit von den 99,995 % einer Einzelanwendung (d. h. Dual-Konfiguration) auf die 99,9999 % einer entsprechenden Anwendung mit dualer Redundanz (d. h. Quad-Konfiguration) mag statistisch nicht sehr signifikant sein, aber wenn durch einen unplanmäßigen Ausfall Ihres Prozesses Verluste in Millionenhöhe entstehen könnten, ist dies ein kleiner Preis, der für das Sicherheitsgefühl zu zahlen ist!

8. Vergessen Sie die Architektur – was zählt, sind die Zertifizierungsdaten

Um welche Systemkonfiguration es sich handelt – Dual, Triple, Quad, 1oo2, 2oo3 oder 2oo4 –, spielt keine Rolle mehr. Wenn wir nicht genau wissen, welchem Zweck der Architekturentwurf dienen soll, können diese Begriffe zumindest für Verwirrung sorgen, und bei der letzten Systemgeneration wurden die Definitionen für „Integrität“ und „Verfügbarkeit“ eindeutig verwechselt.

Die wichtigen Daten, aus denen die Integrität und Verfügbarkeit Ihres Sicherheitssystems hervorgeht, sind in dem „SIL Achievement Report“ enthalten, den Sie von Ihrem zertifizierten Systemintegrator oder Dienstleister (z.B. TÜV) erhalten. Dieser Bericht liefert Ihnen die folgenden Informationen:

- Berechneter PFD-Wert für Ihr System auf der Grundlage zertifizierter Zuverlässigkeitsdaten und Zuverlässigkeitsberechnungen
- Safe Failure Fraction-Wert für Ihr Sicherheitssystem, ebenfalls auf der Grundlage von zertifizierten Daten und Berechnungen für den Diagnose-Deckungsgrad
- Zertifikate zur Bestätigung der systematischen Integrität des Grundsicherheitssystems, die die Entwicklung sämtlicher sicherheitsrelevanter Teilsysteme und Elemente abdecken, siehe das angefügte Beispiel für den 800xA HI
- Zertifikate für das vom Systemintegrator verwendete Funktionssicherheits-Managementsystem (FSMS), die die Kompetenz des Projektteams und der eingesetzten Prozesse bestätigen
- ein ausführlicher „SIL Achievement Report“, der die Ergebnisse der im Verlauf des Projekts durchgeführten Funktionssicherheitsbeurteilung (Functional Safety Assessment – FSA) und die vom Team erstellten Audit-Berichte enthält

Wenn Ihnen alle diese Materialien vorliegen (die Sie von ABB erhalten können) – dann (und nur dann) können Sie zufrieden sein!

Dokument-ID: 3BNP100416
Datum: 3. Dezember 2008

© Copyright 2008 ABB. Alle Rechte vorbehalten. Bilder, Diagramme und andere grafische Darstellungen in diesem Dokument dienen nur zur Veranschaulichung und stellen keine Produktkonfigurationen oder Produktfunktionen dar.