PI INTERNATIONAL

PROFIsafe
System Description

日本語版
Japanese version

Technology and Application

Open Solutions for the World of Automation

PROFIBUS

PROFINET

コミットメント

私たちは現在、そして未来においても世界の産業用オートメーションの通信分野をリードする団体でありつづけます。そして、私たちの顧客、メンバー、報道機関に最良のソリューション、利益、そして情報を提供します。

はじめに

PROFIBUS はファクトリーオートメーションとプロセスオートメーションを同時にカバーする唯一のフィールドバスです。PROFINET は標準の Ethernet をベースとして、最近特に導入が進んでいるネットワーク技術です。PROFIBUS・PROFINET ともに、その仕様は国際規格 IEC 61158 and IEC 61784-1/-2 の communication profile family 3 で規定されています。

国際プロフィバス協会（PROFIBUS and PROFINET International (PI)）の歴史の中でも、1999 年に安全通信の仕様を発表したことは大きなイベントの一つです。この発表はオートメーションの世界に大きな可能性をもたらしました。

安全通信の仕様技術とは **PROFIsafe** であり、ロゴを以下に示します。

現在、PROFIsafe は世界で最も進化し、最も利用されている安全通信技術です。PROFIsafe は同時に国際規格 **IEC 61784-3-3** となるべく活動も進めています。

本書の目的は、PROFIsafe と関連する事項を、あまり技術的に深く立ち入らずに概説することです。ですから本書は公式の規格やガイドラインに代わるものとは考えていません。規格やガイドラインは正確であり、強制力もあります。

PROFIsafe は安全機関である BGIA および TÜV に認められています。.

BGIA

安全はオートメーションの分野でも特に気をつけて扱わなければなりません。ですから PROFIsafe の普及、使用、保守は特に細心の注意をもって行われます。PROFIsafe を用いる会社、研究所は、いわゆる PROFIsafe ポリシーに従って、取り扱うことが求められます。

本書は公式の規格の補完、または要約としても利用できるでしょう。

本書における大文字の"F"は、"fail-safe", "functional safety"または単に"safety related"の省略を示します。

目次

1. オートメーションにおける安全

一般にどのような産業活動においてもなんらかリスクは存在します。

- 傷害または事故死
- 環境破壊
- 施設のダメージ

などが考えられます。

多くの場合、現場のオートメーションシステムでは特別な配慮をしなくてもリスクは回避できます。しかし、なかには高いリスクを持つアプリケーションがあります。たとえば、プレス、切断、工作機械・ロボット、コンベア、梱包機械、高圧を伴う化学工程、オフショア技術、火炎・ガスバーナー、ケーブルカーなどです。このようなケースでのリスクを回避するには特別な配慮と技術が必要です。従来は、標準のオートメーション技術を安全アプリケーションに採用するには信頼性と可要性の点から、問題があるとされました。つまり、一般的には、標準のオートメーションシステムの故障率、エラー率では、標準の制御運転でのみ使えるものであり、前に述べたようなハイリスクのアプリケーションには、十分ではありませんでした。

たとえば郵便のシステムを考えてください。通常郵便はある信頼性のレベルを提供するのですが、私たちは重要な郵便には書留を使います。

1.1 最近の考え方

最近のマイクロコントローラ、ソフトウェア、PC そして通信ネットワークの発達は標準のオートメーション技術に大きな影響を与えてきました。その結果、制御システムの価格が低下し、柔軟性が増し、信頼性が高くなりました。安全に関して言うと、今までの規格では新しい技術の使用を禁止しています。つまり、安全オートメーションはハードワイヤで結線し、リレー技術を使わなければなりません。(図 1 参照)

今までの考えは“安全は信頼できる技術、そして要素に基づく”とされています。信頼とは、つまり、長年の繰り返された経験に基づくものです。しかし、“古典的な”安全技術を、最新の制御技術の中で使い続けるのは、あまりメリットがありません。たとえば、配線コストやエンジニアリング費の増加、変更のしにくさ、予想より信頼性のないこと、他にも予想できなかった状態での機械のストップとか、一度ストップしたら再開に手間がかかるなどの欠点があるからです。

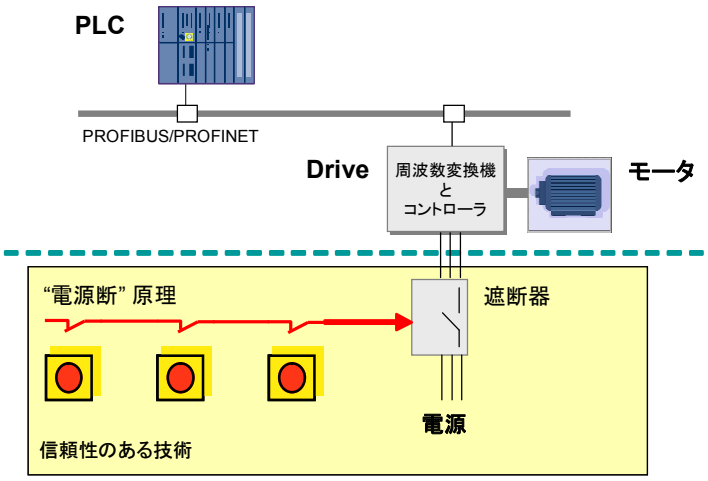

Figure 1　従来の安全対策

安全技術の状況は現在大きく変化しています。マイクロコントローラとソフトウェアは数百万システムで使われ、信頼性が証明されています。そしてマイクロコントローラとソフトウェアを安全アプリケーションに採用する前提条件・国際規格 IEC61508 がすでに成立しました。.

多くの種類のデジタル通信技術に対する故障の検出方法も研究されてきており、マーケットで受け入れられています。IEC62280-1 のような規格が使用されているわけです。

1.2 PI の活動

以上は私たちが PROFIsafe 技術を追加レイヤーとして開発し、既存の PROFIBUS と PROFINET の上位に置く理由です。PROFIsafe を使うと F-Host（安全コントローラ）と F-Device 間のデータ伝送のエラー発生の確率を要求されるレベルでかつ、関連する規格を満足するレベルまで引き下げることが出来ます。

PROFIsafe はソフトウェアだけで実現されます。ですから PROFIBUS とか PROFINET を PA、FA で使っている現場で、安全アプリケーションを容易に実現できます。PROFIsafe では、無線技術 WLAN とか Bluetooth なども採用できます。セキュリティを考慮すれば、産業用 Ethernet の幹線上でも使用できます。.

PROFIsafe はプロセスオートメーションで求められる高信頼性、低電力、ファクトリーオートメーションで要求されるミリ秒単位の速い応答のどちらにも対応できます。

その結果、レーザースキャナー、安全機能を内蔵する回転機器などの最新 F-Device が販売されています。それぞれの機器の安全パラメータ(iParameters)は効率よくサポートされます。つまり、エンジニアリングフレームワーク（たとえば、Tool Calling Interface）を使い F-Device ツールとの取り合い、そして iParameter の保存と修正機能をもつオプション (**iPar-Server**)があります。ツールのインタフェースと iPar-Server の機能は非安全機器でも使用できることに留意ください。

IEC 61508 規格では、詳細は記述せず電磁障害などに対する特別な要求を定義しています。追加資料である **"PROFIsafe Environment"** は、F-Device と F-Hosts を実際に開発、使用するときの実務方法を提供してくれます。

PROFIBUS と PROFINET の F-Device と F-Host は、IEC61508 に従って認証を受けており、安全機器として使用できます。PROFIsafe のプロトコルテストは PI テストラボで実施され、PNO オフィスで認証されます。**"PROFIsafe Test Specification"** 資料には TUV のようなアセスメントと PI テストラボの役割と仕事が記述されています。

PROFIsafe についての実際の情報は www.profisafe.net を見てください。また、一般の PROFIBUS と PROFINET については、 www.profibus.com を参照してください。

1.3 国際規格

多くの国では、その国の法律がどのように人間と環境を保護するか規定しています。ヨーロッパでは “Low Voltage Directive”, “EMC Directive”, そして“Machinery Directive”がその例です。同時に、これらの法律は国際規格も参照しています。

図 3 は安全とフィールドバスに対応する IEC 規格、ISO 規格の選択と、

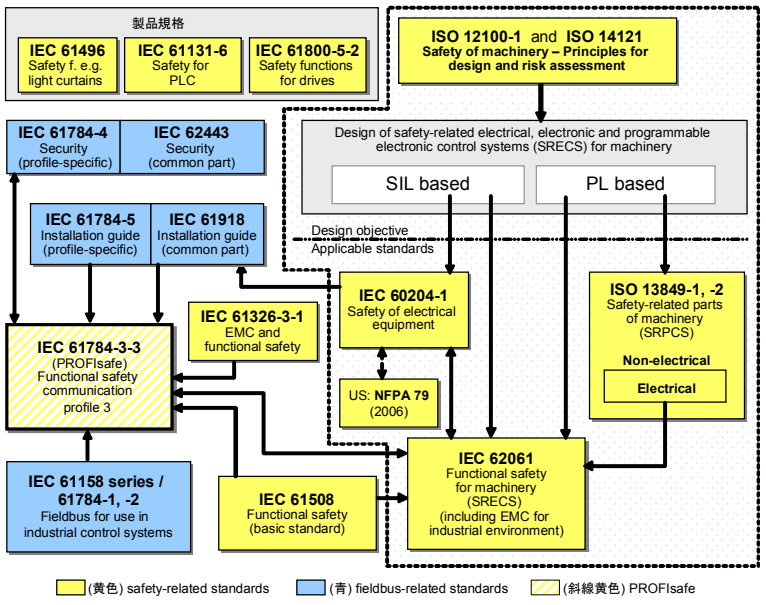

Figure 3 FA 用のフィールドバスと安全の国際規格

それらの関係を示しています。

機能安全の基本規格は IEC61508 で、電気機器の機能安全と原則と手順について記載しています。IEC61508 では安全機能が働かない場合の確率 (Safety Integrity Levels - **SIL**)を定量的に計算できるよう決めています。これは主に F-Device と F-Host の開発に役に立ちます。 IEC 62061 では、ファクトリーオートメーションで使われるような機械における安全について記述してあります。この規格は ready-to-use システム、サブシステム、そしてその要素を取り扱い、これらの組み合わせに対し、安全機能をどのように査定するかを示しています。 ISO 13849-1 は EN954-1 の後継規格であり、同じ範囲を担当します。しかし、この規格は多少異なった計算方法 (Performance Levels - **PL**)を示し、油圧バルブなど電気的でない機器をカバーします。機械の安全についての基本的な用語と方法は ISO12100-1 で定義されています。ISO 14121 はリスク計算の原則を示します。IEC 60204-1 は機械の電気機器の一般的な要求を提示します。例として、電源、電気ショックに対する保護、緊急停止、導体、ケーブルなどがあります。製品の規格（例えば IEC 61496, IEC 61800-5-2, IEC 61131-6）では個々のデバイスファミリーに対する要求を取り扱います。

ヨーロッパの"Machinery Directive" のアネックス部では"Notified Body" (BIA, TÜV, FM など)によって認証が義務付けられている機械と部品のリストが提供されています。もし、同等の製品規格があるなら（例えば IEC61496）製造業者の申告で良いとされています。

F-Device と F-Host の電磁的影響の対応については、IEC61326-3-1 に定義されています。通常のレベルより電磁影響が増加した場合の機器の動作についての記述が、特殊な機能安全 (**FS**)として、記述されています。しかしこのような場合、テスト機器(**EUT**)は安全サイドに移行しなくてはいけません。

フィールドバスの規格は IEC 61158 と IEC 61784-1 です。PROFINET IO のようなリアルタイム Ethernet 対応は IEC61784-2 に記述されています。設置ガイドラインの共通部は IEC61918 でまとまられており、そのうちプロファイルで決められる部分は IEC61784-5 に記載されています。セキュリティガイドラインの共通部は IEC62443 でまとめられ、そのうちプロファイルで決められる部分は IEC61784-4 に記載されています。

図 2 はプロセスオートメーションで要求される IEC と ISO 規格の関係を示しています。この図ではセクター規格である IEC61511 に非常にセンシティブなプロセス機器に対する長期間使用 ("proven-in-use":すでに実プロセスでの使用実績により証明済み)の件とプロセスエリアでの電磁環境について記述があります。IEC 61326-3-2 では、このような EMC の考えを取り入れています。

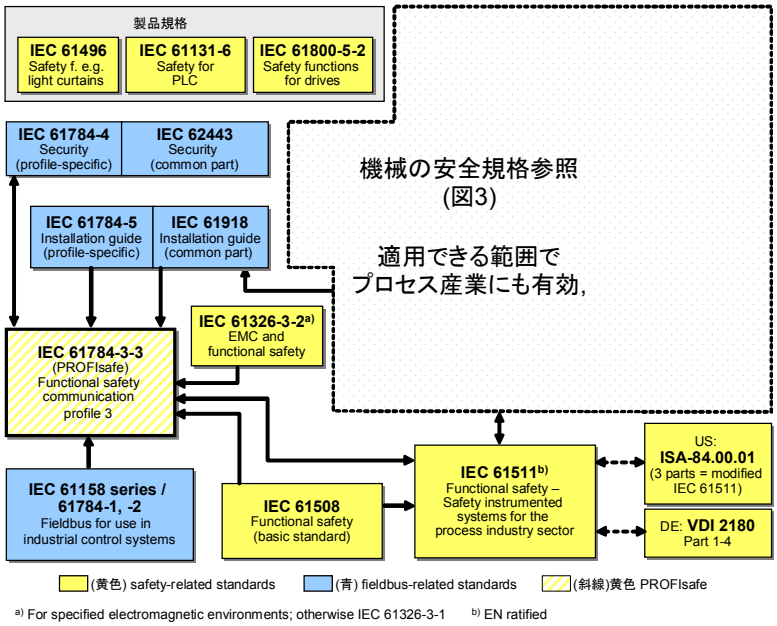

Figure 2 PA 用のフィールドバスと安全の国際規格

2. 目的

PROFIsafe は開発当初から、安全機器の製造者とユーザにわかりやすく、かつ効果的な規格であることを意識して作られています。

PROFIsafe のプロトコルは今までの PROFIBUS と PROFINET 規格を変えることなく、両方のネットワークに使えるようになっています。安全メッセージは、従来の制御メッセージが通っていた、ケーブルをそのまま使うことができます。 (図 5 参照)

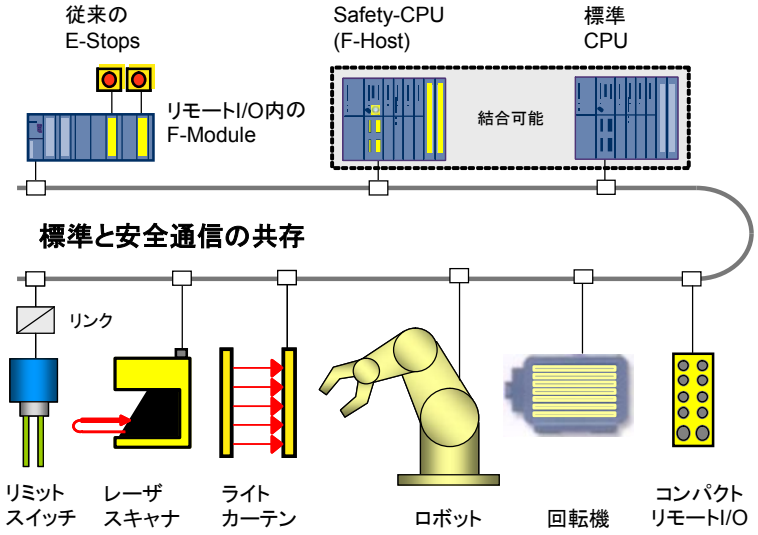

Figure 5 "Single Channel" アプローチ

この"Single Channel"アプローチ(制御と安全を一つのハードウェアにのせる)によって、論理的には別の動作で、ただしハードとしては同じ PLC を制御と安全に同時に使うことができます。オプションの冗長化をすることでさらに可用性が高くなります。制御システムと安全システムの通信を物理的に別系統で行いたい場合も PROFIsafe は問題なく対応できます。またこのようなケースでも、PROFIBUS と PROFINET を両方のネットワークに使用することができます。

PROFIsafe プロトコルを搭載しても標準のバスプロトコルに影響を与えることはありません。それだけでなく、PROFIsafe プロトコルは、伝送の物理層が銅線、光ファイバー、無線、背面板に関係なく実行できます。伝送速度もエラー検出方法も PROFIsafe には関係ありません。PROFIsafe から見ると、これらは"ブラックチャネル"と考えることができるからです。 (図 4 参照)

PROFIsafe を採用すれば、ユーザはベースである通信、または PROFINET と PROFIBUS を介した範囲で安全通信のチェックを考慮する必要がありません。PROFIsafe を使うことで、安全信号の発生元(例;リモート IO の F-Module)から、安全ロジックが実行される機器(F-Host)、そして逆方向の場合も、安全通信が確保されます。(図 6 参照).

PROFIsafe プロトコルは IEC 61508 / IEC 62061 で定義される SIL3、または EN954-1 で定義される Category 4、ISO13849-1 の PL "e"まで使用できます。

PROFIsafe プロトコルのパラメータは PROFIBUS と PROFINET で使う標準の方法(例えば GSD ファイル)を使って定義、変更、エンジニアリングできます。しかし、パラメータは、保存、設定、エンジニアリングツールから IO コントローラ、DP マスター、そして F-Device への変更の各フェーズにおいて、安全性が考慮されなければなりません。すべての F-Device、リモート IO 機器のモジュールで同じように扱えるために、同じ PROFIsafe のパラメータを使ったほうが良いといえます。

F-Device の機器でどのような安全パラメータを持つかは機器により異なります。たとえば、安全機能を持つドライブ、レーザースキャナーなどの例ですと、複雑なパラメータを GSD ファイルで取り扱うには多少無理があります。F-Device 機器について、コンフィギュレーション(C)、パラメータ設定(P)、診断(D)のツール(CPD tools)をシステムベンダーのエンジニアリングツールにまとめた方がよいでしょう。これにより特定の F-Device、F-Module が一層使いやすくなります。

故障などで F-Device を交換するときには、共通したやり方でそれぞれの安全パラメータ(iPar-Server)を取り扱うためにシステムは"Save and Restore"機能をサポートすべきです。一般に F-Host またはバスのスタートアップのパラメータ設定機能を持つコントローラはこの機能を持っています。

補足資料で PROFIsafe についての以下のような項目について説明がされています。

- 設置
- 電気安全
- 電源
- 電磁コンパチビリティ
- データセキュリティ

最後に、ベンダーは F-Device、F-Module などの PROFIsafe 機器を開発するとき、PROFIsafe 開発キッ

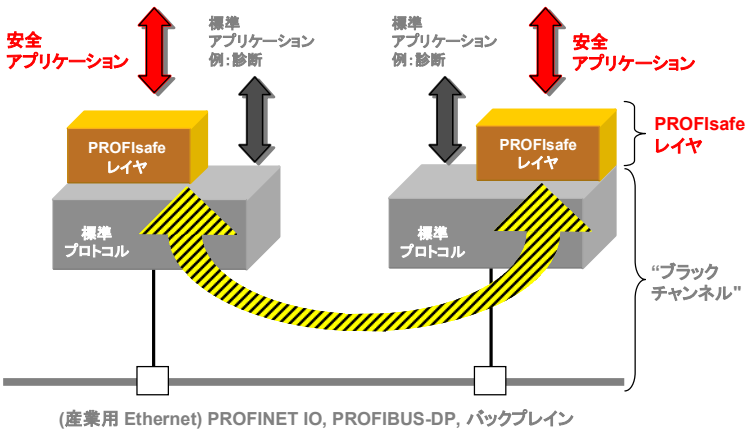

Figure 4 "ブラックチャンネル"の考え方

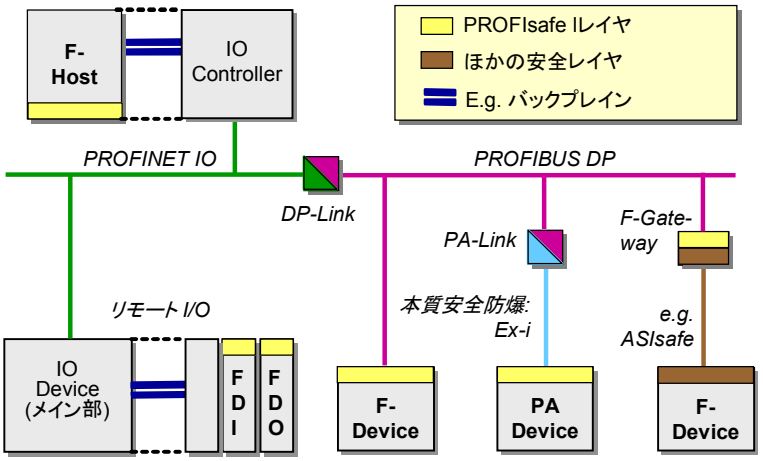

Figure 6　安全通信の通り道

ト、技術センター、そしてテストセンターからサポートを得られることを付け加えます。

現在のバージョンで PROFIsafe はこの章の最初に述べた目的をすべて満足しています。最終のコンセプトは簡単で分かりすいものです。

PROFIsafe について詳しい説明をする前に、その前提条件と制限事項についてみてみたいと思います。

3. "ブラックチャンネル" の考え方

PROFIsafe はブラックチャンネル方法を採用していますが、設計時には PROFIBUS と PROFINET のいくつかの基本的機能を考慮しなくてはなりません。

3.1 基本機能

まず、はじめにバスコントローラとそれに関連する現場機器間の周期通信(メッセージの送信・受信)があげられます。通信のポーリング動作によりデバイスの故障がすぐにわかります。PROFIsafe はこの方法を採用しているので、別途、故障チェックを入れる必要はありません。

次の点は、バスコントローラとそれに関連する現場機器の 1 対 1 通信の関係です。PROFIsafe はメッセージの確実性を増すためにこのやり方も採用しています。ただし、この方法はただ一つの F-Host がモジューラタイプである現場機器の F-Module（サブスロット）をアクセスする場合に有効です。

3.2 ネットワークコンポーネント

"ブラックチャンネル"はスイッチ、ルータ、リンク、無線など、いくつかの透過的なネットワークコンポーネントで構成されている可能性があります。PROFIsafe では、SIL3 の要求に対応するため、多少の制限を設けています。

どのようなスイッチを使用しても良いのですが、直列接続では 100 個が制限となります。PROFIsafe の集まりの中で F-Address システムはユニークでなければなりません。同じ F-Address システムを持つ集まりをつなぐ時はマルチポートルータでつなぐ必要があります。PROFINET から PROFIBUS、そして MBP-IS 本質安全機器をつなぐリンクには制限がありません。 (図 Figure 6 参照).

3.3 無線とセキュリティ

PROFIsafe では仕様の許す範囲において、無線は利用できますし、セキュリティも保証されます。

PROFIsafe は、無線を使った場合、そして産業用 Ethernet、インターネットにつながる有線ネットワーク使った場合についてセキュリティの要求点を規定しています。

3.4 データタイプ

一般にフィールドバス通信では様々なタイプのデータを使っています。(9 ページの文献を参照)取扱いを簡単にするため、PROFIsafe ではサブセットを定義しています。

4. PROFIsafe の提案

2 つの機器をつなぐ安全通信は以下の項目が求められます。

- 正確なデータを
- 正しい宛先に
- ジャストインタイムで届ける

ハードウェアの故障があったり、電磁界の影響が強かったり、他の影響で、メッセージが複雑なネットワークを移動する間に様々なエラーが起きる可能性があります。メッセージは消失するかもしれません。複数回送られるかもしれません。ほかのデータが加えられるかもしれません。または遅れ、順序違い、間違ったデータの可能性があります。安全通信の場合、不正アドレス、標準通信が間違って F-Device に配送される、または安全メッセージのふりをすることがあります。通信速度が異なるなら、バスコンポーネントが電文を保持する際のエラーが発生するかもしれません。さまざまな原因を考慮して、PROFIsafe は図 7 で示すような方法を安全確保の技術としています。

4.1 安全を確保する技術

この技術は以下のとおりです。

対策: / エラー:	シーケンス番号 (目印)	タイムアウト (受け取り応答あり)	コードネーム (送信と受信の機器用)	データ保護 (CRC)
反復	X			
欠損	X	X		
挿入	X	X	X	
不正順序	X			
衝突				X
許容できない遅れ		X		
アドレスエラー			X	
偽装 (標準メッセージが安全メッセージとなる)		X	X	X
スイッチ内のメモリ順序エラー	X			

Figure 7　通信エラーとその対策

- PROFIsafe メッセージに連続番号を振る ("sign-of-life")
- 確認を伴う期待時間値 ("watch-dog")
- 送り手と受け手間のコードネーム ("F-Address")
- データ完全性チェック (CRC = cyclic redundancy check)

連続番号を使うことで、受け手はメッセージが正しい順番で完全に来たかをチェックできます。受け手がこの番号を送り手への返答メッセージに含めれば、送り手の確認にもなります。基本的には簡単なトグルビットで十分です。しかし、PROFIsafe では、スイッチなどのバスコンポーネントのメッセージ保持も考え、24 ビットのカウンターを採用しています。

安全技術としては、メッセージが正しい値を伝送するだけでは十分ではなく、値の更新が許容時間内に行われる必要があります。これによって、それぞれの F-Device が自動的に必要な安全リアクション(例；動作をストップする)をとることができます。この目的のために、F-Device では、ウォッチドックタイマーを使います。このタイマーは更新された連続番号を持つ新しい PROFIsafe メッセージが来るたびにリスタートをします。

マスターとスレーブが 1 対 1 の関係を持つことで、あて先が違うメッセージを容易に発見できます。送り手と受け手はネットワーク内でユニークな ID(codename)を持ちます。この ID は PROFIsafe のメッセージが正しいことをチェックするために使われます。PROFIsafe では "F-Address"を codename として使います。

CRC(cyclic redundancy check)によりデータビットの間違いを発見できます。IEC61508 はあらゆる安全機能に対し故障が起こりうる可能性を規定しています。規格では、故障の可能性が定義されています。PROFIsafe はこのアプローチを採用しています。(図 9 参照).

F-Input/Output data	Status / Control Byte	CRC signature
		across F-I/O data, F-Parameter, and Consecutive Number
Maximum of 12 or 123 bytes	1 byte	3 or 4 bytes

Figure 8　PROFIsafe のメッセージフォーマット

この定義によると、安全回路には安全機能に関するすべてのセンサー、操作機、伝送機器、論理プロセスが含まれます。IEC 61508 は故障の可能性を SIL(safety integrity level)で規定します。例えば、SIL3 は 10^{-7}/h となります。伝送プロセスのである PROFIsafe はこのうち単に 1%の割合を持ちます。つまり許容される故障率は 10^{-9}/h となります。これは PROFIsafe のメッセージ長ですと CRC 多項式でカバーできる範囲です。その結果、PROFIsafe の検出できないビットエラー確率の最大値は要求される基準の 10^{-2} となります。PROFIsafe は対応する 3 から 4 バイトの CRC signature を計算するため、24 ビット、32 ビットの CRC 生成多項式を使います。選択された CRC 多項式と特殊な演算の方法での品質から、PROFIsafe は”ブラックチャンネル”で検出したエラーと無関係とされています。

4.2 PROFIsafe のフォーマット

F-Host と F-Device 間でやり取りされる PROFIsafe のメッセージは標準の PROFIBUS と PROFINET と同じ負荷となります。複数の F-Module を持つモジューラタイプの F-Device では、負荷は PROFIsafe メッセージの数により異なります。図 8 に PROFIsafe メッセージのフォーマットを示します。

最初にすでに説明したデータタイプを持つ F-Input または F-Output のデータがきます。特定の F-Device のデータ構造は通常 GSD(General Station Description)ファイルにより定義されます。一般にファクトリーオートメーションとプロセスオートメーションでは安全システムに対する要求が異なります。片方は短い(ビット)信号を高速で使う。もう一方は長い(浮動小数点)信号を幾分長い時間で取り扱います。PROFIsafe はそのため 2 つの異なったデータ構造を持つことができます。片方ではデータ長が最大 12 バイトに制限され、3 バイトの CRC データを持ちます。もう一方はデータ長が最大 123 バイトで 4 バイトの CRC データを持ちます。

F-Input または F-Output のデータに続いて、電文内に F-Host からは Control Byte が、F-Device からは Status Byte が表れます。この情報は PROFIsafe のメッセージの送り手と受け手の同期をとるために使われます。

PROFIsafe のデータは CRC チェックデータで終わります。CRC データの長さは前に述べたように F-Input または F-Output の長さで決まります。

連続番号は PROFIsafe のメッセージの中では伝達されません。送り手と受け手がそれぞれ Control byte と Status Byte を介して同期をとるカウンターを使います。CRC チェックが有効なので、カウンターの値が正しく同期しているか分ります。

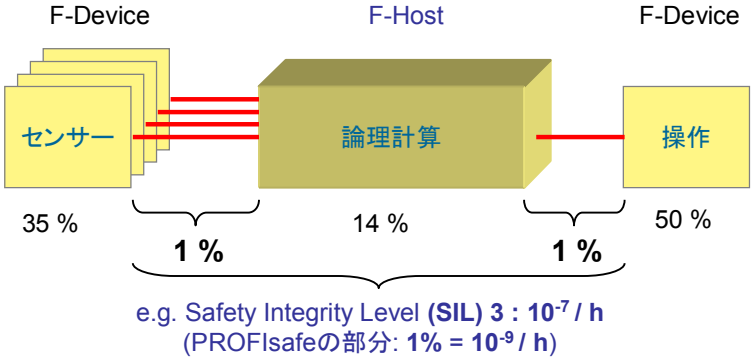

Figure 9　安全機能と SIL

"F-Address" も同様に CRC にてチェックされ、安全です。

4.3 PROFIsafe の機能

PROFIsafe メッセージの送り手と受け手はブラックチャンネルの通信レイヤーの上位に位置します。 (図 4 参照)普通はこの PROFIsafe レイヤーはソフトウェアで実現します。("drivers"). 中心となる機能は PROFIsafe メッセージの周期伝送の状態遷移の管理とスタートアップ、電源 OFF/ON 時、CRC エラー時の例外処理です。図 10 は PROFIsafe

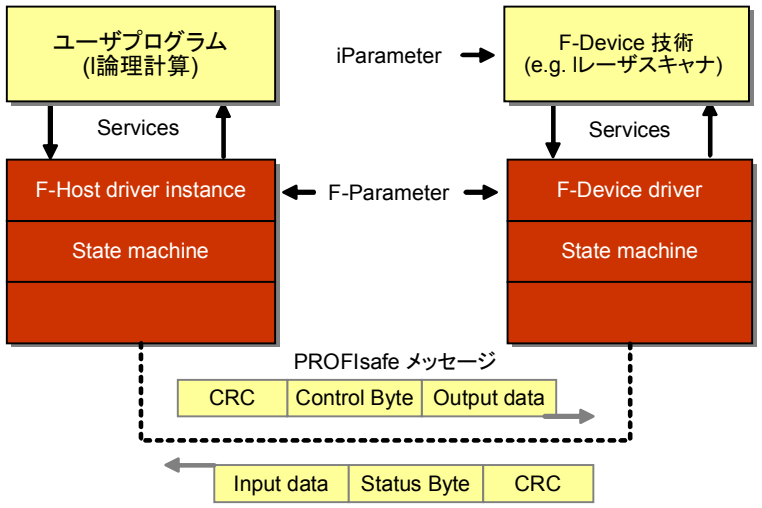

Figure 10　F-Host と F-Device 内の PROFIsafe の階層

が F-Device の主機能部分と F-Host のユーザープログラムとがどのように対応するかを示します。.

4.3.1 F-Host の機能

F-Host の主要な機能は F-Output と F-Input のデータ交換です。スタートアップの間、またはエラーが起きた時、プロセス値はデフォルトのフェールセーフ値となります。フェールセーフ値は 0 となり、受け手を安全状態とします。(非稼働状態)

別の F-Device にとっては、非稼働状態だけでなく、低スピードが安全となる場合もあります。PROFIsafe は Control Byte 内のフラグを立てるサービスを提供できます。 ("activate_FV"). その反対に、F-Device はユーザプログラムに自分が安全状態へと移行したかを Status Byte 内のフラグで知らせることができます。("FV_activated").

PROFIsafe の通信エラーも F-Host のドライバが安全状態に移行するきっかけとなります。安全状態から普通の運転状態に人の介在なしに、自動的に戻ることは一般に許されていません。オペレータの介在、確認が求められることを知らせる機能も、PROFIsafe は持っています。("OA_Req"). PROFIsafe は F-Device に待ちの要求を出すこともできます。たとえば F-Device が LED を点灯させるなどです。(オプション). オペレータの確認はユーザプログラムから、フラグ(OA_C)を介して、F-Host に伝えられます。

F-Device の技術パラメータは iParameter と呼ばれます。F-Device が運転中に iParameter を変更することもできます。F-Device が新しい iParameter を受けいれることのできるモードが用意されています。(iPar_EN"). そのほかに、ユーザプログラムに通常安全運転への準備ができたことを知らせることも出来ます。("iPar_OK").

4.3.2 F-Device の機能

F-Device の PROFIsafe 機能は、F-Output と F-Input のデータ交換のほかに、フェールセーフ値のスタートとレポート、iParameter に関する取り合い、そして前述のオペレータの要求などがあります。

さらに、F-Device は自分の故障をステータスバイト中のフラグを使って、F-Host のドライバに通知できます。 ("Device_Fault").

安全応答に対して、F-Device の命令が続く時間は、PROFIsafe の通信と比べて十分長くなければなりません。(少なくても連続番号が 2 回増加するくらい) この要求に対応するために、連続番号が新しくなったと通知する特別な機能もあります。

PROFIsafe レイヤーからの診断情報は、特殊サービスにより、伝達されます。

また、他にもいろいろ機能があるのですが、F-Parameter を PROFIsafe レイヤに伝える機能もあります。スタートアップ時に、F-Device は F-Parameter と他のパラメータを一緒に受け取ります。この F-Parameter について以下に説明します。

4.4 F-Parameter

F-Parameter は、PROFIsafe のレイヤーが特定のアプリケーションに対応するため、またエンジニアリングの間違いがないかを再チェックする情報を含んでいます。 重要な F-Parameter は以下のとおりです:

- F_S/D_Address
  (短縮して F-Address)
- F_WD_Time
- F_SIL
- F_iPar_CRC
- F_Par_CRC

F_S/D_Address は PROFIsafe システムの中でユニークなアドレスとなります。F-Device は F-Address とマイクロスイッチなどで現場で入力された値とを、コネクションが正しいかのチェックのため比較します。

F_WD_Time はミリ秒単位のウォッチドッグタイマーです。タイマーは次の有効な PROFIsafe のメッセージをチェックします。

F_SIL は特定の F-Device について、ユーザが期待する SIL 値を示します。この値は、ベンダーの値と比較されます。

F_iPar_CRC は F-device 内のすべての iParameter に対する signature です。

最後に、F_Par_CRC は F-Parameter を正しく伝達するために使われるすべての F-Parameter の signature です。

以上が PROFIsafe についての概要です。次の章で詳細な点を説明します。

5. 実装方法

最初に PI から提供されている必要かつ役に立つ資料の一覧を確認しましょう。(右のボックスを参照してください)　専用のまたは新しいバージョンを使ってください。古いバージョンの PROFIsafe の V.1.30 は参考とするだけにして、新しい製品を開発するときには使わないでください。

次に、少なくても基本規格 IEC61508 を勉強するか、新しい機器を開発するため、開発プロセスと組織に加えるべきことについて、コンサルティングを受けてください。一般のルールとして、PROFIsafe プロトコルを付加するだけでは普通の機器が安全機器となることはできません。実装されているプロトコルと方法、安全技術の構成が機器の最終的な SIL の値を決定するからです。

- PROFIsafe Policy V1.3; Order No. 2.282
- PROFIsafe - Profile for Safety Technology on PROFIBUS DP and PROFINET IO, V2.4; Order No. 3.192b
- PROFIsafe – Environmental Requirements, V2.5; Order No. 2.232
- PROFIsafe – Test Specification for F-Slaves, F-Devices, and F-Hosts, V2.1; Order No. 2.242
- PROFIsafe for PA-Devices, V1.0; Order No. 3.042
- PROFIdrive on PROFIsafe, V1.0; Order No. 3.272
- Rapid way to PROFIBUS DP; Order No. 4.072
- Industrial Communications with PROFINET; Order No. 4.182
- Specification for PROFIBUS Device Description and Device Integration, Volume 1: GSD, V5.04; Order No. 2.122
- GSDML Specification for PROFINET IO, V2.2; Order No. 2.352
- Profile Guideline, Part 1: Identification & Maintenance Functions, V1.1; Order No. 3.502
- Profile Guideline, Part 2: Data Types, Programming Languages, and Platforms, V1.0; Order No. 3.512
- Profile Guideline, Part 3: Diagnosis, Alarms and Time Stamping, V1.0; Order No. 3.522
- Communication Function Blocks on PROFIBUS DP and PROFINET IO, V2.0; Order No. 2.182

5.1 安全のクラス

PROFIsafe が SIL3 まで対応するからといって、F-Device を SIL3 に設計・開発する必要はありません。必要とされる安全のレベルは、最終ユーザのアプリケーションによって異なりますし、どのように安全機能が定義されるかにもよります。低い安全レベルの機器でも冗長化とか他の方法を使って、より高い SIL レベルとなることができます。

5.2 F-Devices

PROFIsafe のドライバーソフトを実装するには 2 つの方法があります。どちらも仕様に準拠するわけですが、最初から自分で開発するか、またはマーケットで提供される開発キットを採用するかになります。詳しくは PI の Web サイトの製品ガイドをご覧ください。開発キットを採用した場合のメリットは、すでに認定されているドライバーソフトの使用、さらに便利な情報とツールの提供、技術サポートとなります。

PROFIBUS と PROFINET のインタフェースについては、市場にある ASIC、スタックを使い、これに PROFIsafe ドライバーソフトを追加する形になります。

5.2.1 GSD のセキュリティ

GSD ファイルはすべての PROFIBUS および PROFINET の機器で必要です。F-device について GSD の共通部分の定義が終わった後、F-Parameters のコーディングをします。F-Parameters のこの部分は保管上のデータ間違いを避けるため、特別な CRC 署名("F_ParamDescCRC")で守られます。エンジニアリングツールはこの特別な署名を使って、F-Parameters の記述の整合性をチェックします。

5.2.2 コンフィギュレーションのセキュリティ

GSD には F-Input と F-Output のフォーマットも記述されます。この部分を守るために、別の CRC 署名("F_IO_StructureDescCRC") が使われます。

5.2.3 iParameter

たくさんの異なる安全機器の技術により、非常にたくさんの安全パラメータ(iParameter)が存在します。.

iParameter の数は、機器によって数バイトから、数十キロバイト（レーザスキャナー）にも上ります。多くの安全機器は、すでにパラメータ設定、診断ソフトツール(CPD-Tool)を持っています。ですからこの iParameter を GSD を介して取り扱うことはありません。

PROFIsafe は iPar-Server と呼ばれる新しい方法を推奨します。F-Host のベンダーがこの機能を提供することになります。提供形態は、パラメータ設定マスターとしての F-Host の非安全部であったり、非安全 PLC、または産業用コンピュータのようなコントロールのサブシステムとしての提供となります。

Figure 11 図では iPar-Server の考え方が示されています。F-Device のネットワーク構成、F-Parameterization と共に、iPar-Server 機能が例示されます(1)。F-Device は安全状態(FV)であり、データ交換状態に移行できます。デバイスのアドレスを設定するエンジニアリングツールから TCI (Tool Calling Interface)とか FDT (Field Device Tool)を使って、CPD ツールをスタートさせます。 パラメータ設定、コミッショニングなどは CPD tool (3)を使って行います。 その後、iPar_CRC 署名が計算され、16 進数で表示されます。この値は少なくても、エンジニアリングツール(4)の "F_iPar_CRC"の入力として使われます。"F_iPar_CRC"を F-Device に伝達するために、F-Device を再立ち上げします(5)。 最終チェックの後、F-Device は iPara-Sever に確認データを発行します(6)。これは 標準の診断メカニズムを使います。iPar-Server は診断情報(e.g. RDIAG FB)をポーリングして、要求を理解し、アップロード作業を終了します

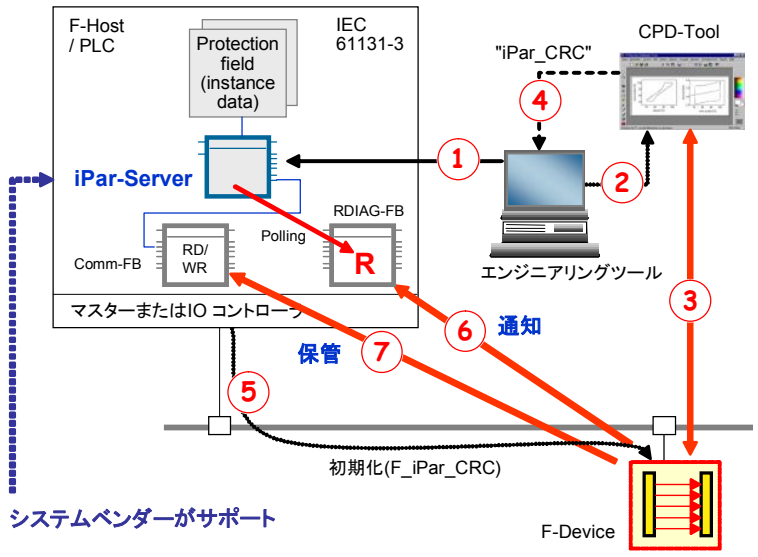

Figure 11　iPar-Server の考え方

(7)。 iParameters は非周期通信を使って、(Read Record)、iPar-Server ホスト内に保存されます。

F-Device が故障し交換するとき、新しい F-Device はスタートアップ時に "F_iPar_CRC", を含む F-Parameter を受け取ります。交換時には iParameter は設定されていないので、F-Device は自分の iParameter と "F_iPar_CRC"の違いから判断して、標準診断メカニズムを使って iPar-Server にダウンロード要求を発行します(6)。 iPar-Server は診断情報をポーリングして、要求を理解し、ダウンロードプロセスを終了させます(Write Record)。このようにして、F-Device は再エンジニアリングまたは CPD ツールなしで、システム内で自分を立ち上げることができます。

5.2.4 PROFIdrive

IEC 61800-5-2 は機能安全を使った安全機能を定義しています。これらの機能は以下の停止の機能から成り立っています。

- Safe torque off (de-energize)
- Safe stop 1
- Safe stop 2
- Safe operating stop

同時に監視の機能もあります。

- Safely limited acceleration
- Safely limited speed
- Safely limited torque / force
- Safely limited (absolute) position
- Safely limited increment
- Safe direction
- Safely limited motor temperature

Figure 12 は今までの電気機械的安全をどのようにリプレースするか記載しています。大きな目的の 1 つは回転機の運転状態を監視し、故障のときだけ、ストップさせることです。PI のワーキンググループの 1 つの PROFIdrive ワーキンググループがこれらの機能を PROFIdrive の追加機能としてまとめています。(前ページ参照).

5.2.5 PA 機器

プロセスオートメーション用の F-Device は sector standard である IEC 61511 に準拠します。ここでは特に “すでに使用されていたか” が重要になります。長年使用されてきた(Proven-in-use)場合、PA 機器はある条件のもとで、より高い SIL レベルとなります。 PA 機器は通常 IEC 61804 のデザインモデルに従います。Electronic Device Description (EDD)はこの場合、重要な役割を果たします。そのため、PI の "PA Devices" ワーキンググループは PA 機器仕様の追加として、機器とパラメータ化と PROFIsafe の関係を規定しています。(前ページ参照).

5.2.6 I&M 機能

2005 年以降、I&M 機能は非周期伝送をサポートするすべての PROFIBUS と PROFINET 機器で必須機能となっています。 I&M とは Identification and Maintenance(識別と保全)を意味し、機器製造者コード、カタログ、シリアル番号、ハードとソフトのバージョンを標準の手順でアクセスします。製造者コードと PI の Web サイト情報を使えば、ユーザは製造者の Web サイトから機器の最新情報を得ることもできます。 前ページのプロファイルガイドラインを見てください。

5.2.7 診断

PROFIBUS と PROFINET を使う大きなメリットの 1 つは、故障、エラー時に機器から診断情報を得ることがあります。適切な診断情報は設備の停止時間を短縮し、コストメリットをもたらします。この考え方は単にどのように情報をコード化するというだけでなく、わかりやすい言葉でどのように表現するか、特定の状況で次に行うアクションのような HELP 情報をどう提供するかということもあります。詳しくは関連プロファイル情報をご覧ください。(参照文献のリスト参照).

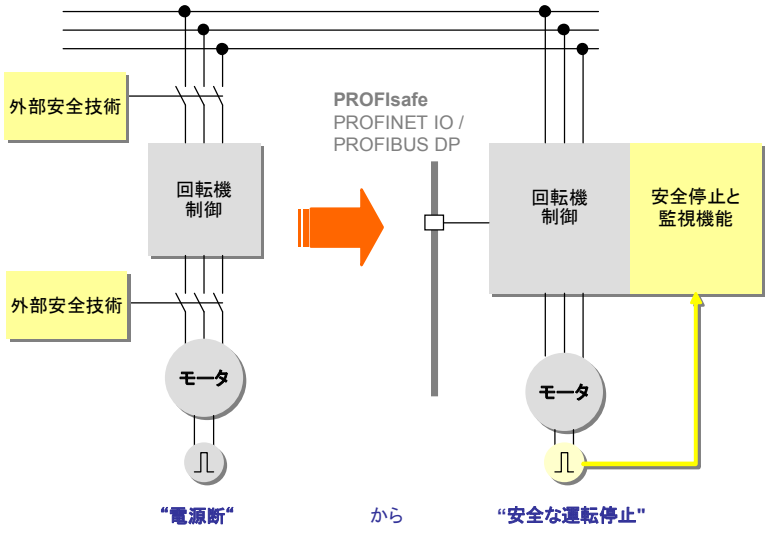

Figure 12　安全停止と監視機能を持つ回転機器

5.3 F-Host

システムベンダーの考え方により PROFIsafe に対応している H-Host をどう作るかが変わってきます。たとえば、F-CPU を独立さす。または標準 CPU 内に物理的には統合し、論理的には分離さすなどです。

5.3.1 実現方法

安全対策もさまざまな方法で実現することができます。たとえば、ハードウェアの冗長化と不一致チェック、または "ソフトウェア冗長化"、または"予防方法"、さらにはすでにある別のハードウェアを使うなどです。実現方法が複数あるため、開発キットを作るには適していません。ただし、PROFIsafe ドライバの実装はそれほど難しくはありません。

5.3.2 コンフォーマンスクラス

すべての F-Device が市場にあるすべての F-Host に接続できることを確認するため、PROFIsafe は F-Host のコンフォーマンスクラスを定義しています。PI の認定を得るために、PROFIsafe F-Hosts はコンフォーマンスクラスの要求を満たさなければなりません。 (Figure 13 参照).

6. 認証試験

PROFIsafe システム内では、さまざまなベンダーの多様な製品が通信します。通信が正しく実行されるために、製品は PROFIsafe の規格どおり設計されなければなりません。通常 PI のテストラボが認証試験を行い、製品の適合性を文書化した形で報告します。

6.1 PROFIsafe の試験

PROFIsafe のプロトコルは限られた状態マシンを元に動作します。チェックツールを使って、この状態マシンの動きを調べ、同時に 2 つ以上のエラーまたは故障が別々に発生しても PROFIsafe が正しく動作することを数学的に証明できます。つまり、システム的にすべての可能な"test-to-pass"と"test-to-fail"状態を作ります。これは、PROFIsafe レイヤテスターで自動的に実行され、F-Device と F-Host の PROFIsafe 認証試験に使われます。この試験は IEC61508 で規定される安全認証試験の 3 段階チェックの 1 部となります。(Figure 13).

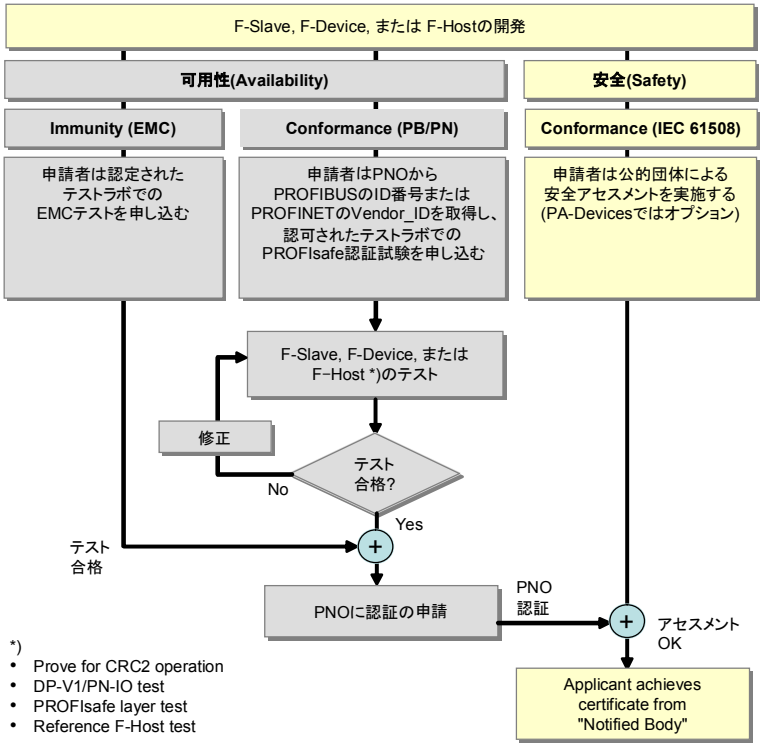

Figure 13 試験と認証の流れ

6.2 安全アセスメント

PI テストラボは以下に示すような団体の代わりに、認定された PROFIsafe のレイヤテストを実施します。

- TÜV (worldwide)
- INRS (France)
- BGIA (Germany)
- SP (Sweden)
- SUVA (Switzerland)
- HSE (United Kingdom)
- FM, UL (USA)

これらの団体は IEC61508 による安全アセスメントを担当する団体の一部です。

すべての F-Device は安全マニュアルにて、SIL_{CL} (claim limit)と PFH_d (probability of dangerous failure per hour)の情報を提供しなければなりません。

PROFIsafe ではテスト方法が決まっています。現在 2 つの PI テストラボが、PROFIsafe 機器の認証を担当しています。

7. PROFIsafe 利用について

PROFIsafe が単に通信プロトコルの規格だけであったら、完全とは言えません。たとえば F-Device について、以下のような質問があります。

- 何か異常な原因で PROFIBUS /PROFINET から高電圧が来た場合に、F-Device を守る方法を考慮すべきか?
- 標準の機器と安全機器を同じネットワークに使うとき、同じ 24V 電源を使用して良いか?
- IEC61508 で要求されている "increased immunity" について、F-Device ではどのようにテストすべきか?
- 設置規則はあるか?
- セキュリティに関する要求はあるか?

ガイドライン"PROFIsafe - Environmental Requirements"の中にこれらの質問の回答があります。

7.1 電気安全

フィールドバスの規格 IEC 61158 と IEC 61784-1, -2 では、ネットワーク内のすべての機器が "使用される国において法律を満足する“(たとえば CE マーク)を求めています。機器の種類にもよりますが、産業用の電気的衝撃に対する保護(電気安全)は IEC 61010 series または IEC

61131-2, clause 10 がベースとなっています。これらの方法は PELV (Protected Extra Low Voltage)と呼ばれ、故障時の電圧を人間に危険でない範囲に制限するようにしています。

F-Device と F-Host はこの要求を満足しなければなりません。

7.2 電源

標準機器と F-Device/F-Host が同じ 24V 電源を使っても構いません。ただし、電源は法律の要求に従い、PELV 機能を満足する必要があります。.

7.3 電磁障害

安全アプリケーションにおいて、SRS (Safety Requirements Specification)は電磁防止限界を定義しています (IEC 61000-1-1 参照)。(IEC 61000-1-1 電磁両立性を達成するために必要です) これらの制限を満たすには、電磁現象(IEC 61000-2-5 参照)と要求される SIL (safety integrity level) を考慮しなければなりません。

一般の産業用アプリケーションでは、IEC 61326-3-1 が安全関連機能で動く機器の限界レベルを定義します。

IEC 61496-1 のような製品規格 (例 レーザスキャナ)は、特定の場合についてより厳しい限界レベルを定義できます。

また、プロセス産業の機器は一般の産業機器とは別の環境条件があります。したがって、PA 機器では、要求と仕様については、IEC 61326-3-2 に記述されています。

PROFIsafe では、EMC のテストが求められます。

7.4 高可用性

安全の目的は、人間を怪我から守るための安全機能を保持し続けることです。(例 電源 OFF した危険区域の機器でも) 安全機能の指標は SIL (Safety Integrity Level)となります。SIL は安全機能が危険な故障を起こす確率を時間で記述しています。例 SIL 3 では 10^{-7}/h

反対に、高可用性（*fault tolerance:* 耐故障性*)* は、故障が起きても制御機能を保持し続けることを目的としています。高可用性の指標とは、運転時間のトータルに対し、実際に動作可能な時間の比率となります。たとえば 99.9%などです。冗長化は、この目的を達成するために用いられる方法の一つです。

	PROFIsafe	冗長性	PROFIsafe と 冗長性
アプリケーション	ファクトリーとプロセスオートメーション: プレス、ロボット、レベルスイッチ, シャットダウンバルブ バナー制御、ケーブルカー	プロセスオートメーション 交通インフラ 化学、薬品生産 製油所、オフショア トンネル	プロセスオートメーション 交通インフラ 化学、薬品生産 製油所、オフショア トンネル
高可用性	-	運転ストップなし (fault tolerance)	運転ストップなし (fault tolerance)
安全	危険な故障が発生しない (法律または保険での要請)	冗長化だけでは安全を提供できない	危険な故障が発生しない (法律または保険での要請)

Figure 14 安全と可用性 (Fault Tolerance)

PROFIsafe は対故障性を上げる冗長化を用いても良いですし、また用いなくてもかまいません。図 14 はその対応を示しています。

7.5 設置ガイド

PROFIsafe の目的は、安全通信を標準の PROFIBUS と PROFINET のネットワークに今までの設置方法に大きな影響を与えることなく統合させることです。パフォーマンスを確保し、法律を順守するためにも、PROFIsafe の仕様とガイドラインに従うことが強く求められます。その中でいくつかの大切な点を以下に述べます。

7.5.1 前提条件

7.1 で述べたように、ネットワーク内のすべての F-device は電気安全に対応していなければなりません。

すべて F-device は IEC61508 の認証が必要です。またプロセス制御では IEC61511 も必要です。そして、PI テストラボで、PROFIsafe のテストをして、認証を得なければなりません。

PROFIsafe ネットワーク内のすべての標準機器も、PROFIBUS または PROFINET について、PI の認証または同等の証明が必要です。

7.5.2 制約

PROFIBUS DP においては、スパーライン、ブランチラインを使用しないでください。

PROFINET IO は次の点を守ってください。

- 直列のスイッチは 100 個以内
- サブモジュールには 1 つの F-Host のみ
- すべてのネットワーク機器は産業環境対応であること (e.g. IEC 61131-2)
- PROFIsafe のネットワークを分割するために、シングルポートルータは使用しない。(ユニークな F-Address 仕様のため)

7.5.3 配線

PROFIBUS と PROFINET は電磁防止効果を増すために、シールドの使用と両端でシールドとコネクタのハウジングを接続するよう決められています。ですから一般に等電位ボンディングが必要です。これができない場合、光ファイバーを使用できます。

電磁的影響が小さい場合、システムの設計者は、自分のリスクで、シールドなしのケーブルを使うこともできます。

7.5.4 可用性

インバータなどの DC ラインでフィルタリングがうまくできない場合、シールドケーブルを使ってもデータラインに許容できない範囲で信号ノイズがのる時があります。また、終端抵抗をつけなかった場合も、ノイズが大きくなることがあります。これは安全の問題でなく、可用性の問題です。コントロール機能が十分に働くことは安全の前提です。うまく動かない機械を使って安全機能を実装すると、不必要な停止が多くなり、最後にはマネージャーが安全機能を

撤去するということになります。("Bhopal effect").

PI の会員からネットワークの通信の品質をチェックするツール、手順書、チェックリストが提供されています。

7.5.5 一般的な安全事項

PROFIsafe はたくさんの安全機器に新しい可能性をもたらします。特に回転機器の安全の統合化はその例です。今ではドライブはモータを止めないで安全状態となることができます。たとえば、新しい安全機能 "SOS" (safe operating stop)では、 モータをある状態に閉ループで固定します。これはユーザにとって画期的なものです。今までは緊急停止ボタンを押すと、物理的にモータの電源ラインが切断されましたから、モータから人間に電気的に危害を加えることはありませんでした。

新しい国際規格 IEC 60204-1 ではモータ保護用の遮断機、メイン遮断機、フューズ付きの絶縁機を使って、どのように電気ショック(emergency switch- off)から保護できるかが述べられています。Figure 15 はこの考えを示しています。同時に、N ライン、PE ライン、モータをドライブ間のシールドを分離する 5 線接続 (TN-S) を推奨しています。IEC 60204-1 は PROFIsafe を補完するたくさんの安全関連の事項が含まれています。北米ではこれに相当するものとして国家規格 NFPA 79 があります。 (Figure 3).

7.6 無線通信

AGV (Automated Guided Vehicles), 回転機械、ガントリロボット、指示

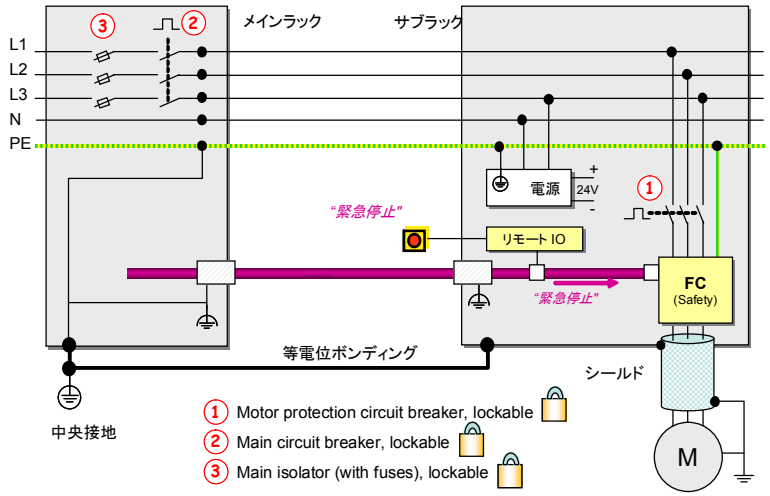

Figure 15 緊急停止の考え方 (IEC 60204-1)

パネルなど多くの 機器が PROFIBUS と PROFINET のネットワークで無線機能に対応しています。PI も WLAN と Bluetooth の利用詳細を規定する予定です。PROFIsafe, では 10^{-2} までのビットエラー確率を検出する機能を持っており、"Black Channels"となります。しかし、別途セキュリティについて考慮しなければなりません。

7.7 セキュリティ

PROFINET は産業用 Ethernet を使ったオープンネットワークであるので、無線通信とともにセキュリティの問題を考えなくてはなりません。

PI はネットワークを閉じる、いわゆるセキュリティゾーンを作るという考え方を進めています。(Figure 16). あるセキュリティゾーンからほかのゾーンにバックボーン Ethernet を介して通信するときは必ずセキュリティゲートを通ります。不法な侵入から守るため、セキュリティゲートは VPN (Virtual Private Network) とかファイヤウォールのような一般に認知された方法を使います。オープンネットワークへの接続が必要でしたら、PROFIsafe ネットワークは必ずセキュリティゾーンの中にあり、セキュリティゲートで守られます。

無線通信の場合、IEEE 802.11i 規格が PROFIsafe ネットワークに十分対応できます。ただインフラストラクチャモードだけを使い、アドホックモードは使用しません。詳細は PROFIsafe の規格を参照してください。

7.8 応答時間

多くの場合、通常の制御の応答時間は安全の場合も適用できます。しかし、時間に厳しいアプリケーションでは安全機能の応答時間(SFRT)をもっと厳密にチェックしなければなりません。ライトカーテンを使ったプレスのアプリケーションはその例です。設計者は早い段階でライトカーテンが危険なプレス機械から設置できる最小距離を計算します。通常人間の手は最速 2m/秒で動くとされています。ライトカーテンが 1 本の指でも認識できるなら、最小距離は = 2 m/s x SFRT で計算できます(EN 999)。 ほかのケースでは別途修正が必要です。

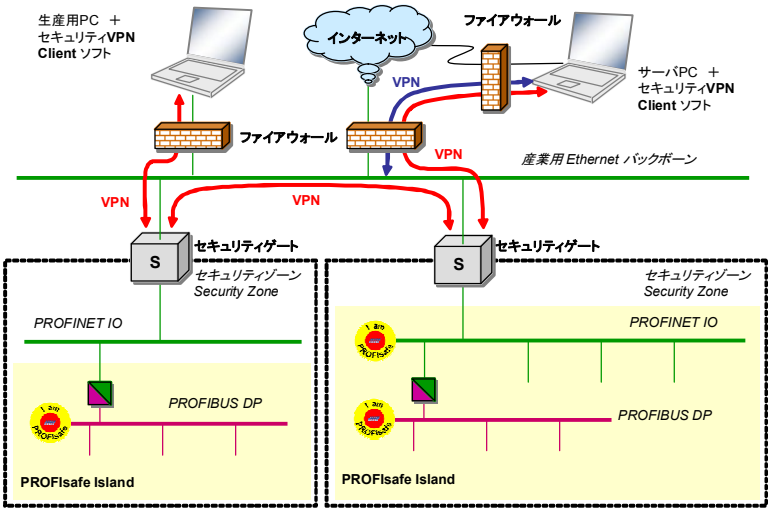

Figure 16 "クローズ"と "オープン" ネットワークに関する安全コンセプト

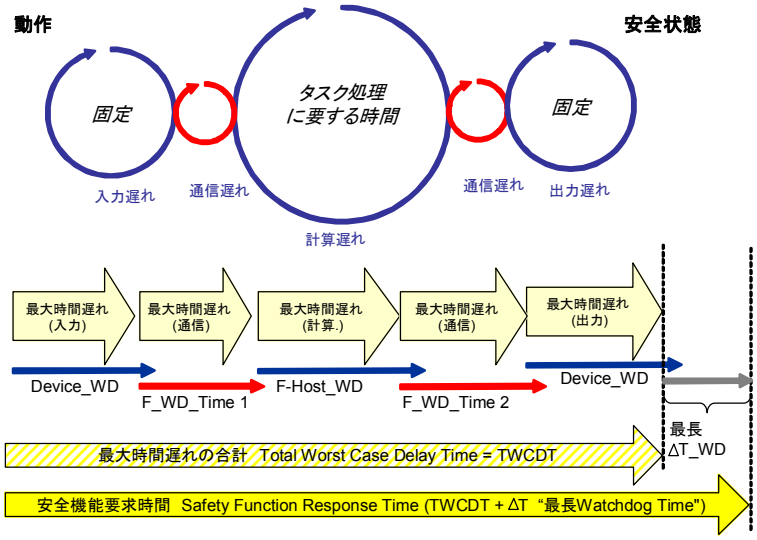

Figure 17 安全機能応答時間 Safety Function Response Time (SFRT)

SFRT について考えてみます。図 17 のモデルは、SFRT の定義を説明するときに使います。このモデルには F-Device の入力、PROFIsafe バス伝送、F-Host の信号処理、応答の PROFIsafe のバス伝送、そして F-Device の出力の各周期時間が含まれています。安全信号が要する最大時間を TWCDT (Total Worst Case Delay Time)と言い、すべてのパートで最大時間がかかるとします。安全の場合、このパートのどれかがフェイルし、信号遅れが生じた場合のケースも考えます。そのため、ウォッチドッグタイムと信号の最大時間の差分で最も大きい時間が加えられます(ある時間において 1 つ以上の故障は考慮しません)。結果として、TWCDT とこの差分時間の和が、SFRT となります。

エンジニアリングツールが SFRT を計算するため、すべての F-Device は PROFIsafe の仕様で要求される最悪の場合の遅れ時間を提示しなければなりません。

8. エンジニアリングの注意

PROFIsafe について、いろいろ説明してきました。次に安全アプリケーション、そしてその安全機能について解説します。

8.1 指令と規格

多くの国において、危険な機械についての安全要求は法律で決められています。EU では Machinery Directive 98/37/EC になります。この指令にはいわゆる対応する規格のリストが含まれています。機械製造者にとれば、相当する規格を満足しているなら、指令にも対応できているはずという仮定があります。

PROFIsafe の場合、対応する規格とは、たとえば IEC 62061, ISO 13849-1, ISO 12100-1, and ISO 14121 (see 1.3 and Figure 2)があります。

8.2 リスク低減のために

機械はもともと固有安全となるよう設計したほうが良いことは当然です。ISO12100-1 の最初のパートにはあらゆる種類の起こりうる危険がリストアップされています。2 つ目のパートでは、リスクアセスメントにより自動化機器のリスクを低減させる方法が述べられています。リスクアセスメントとは、リスク解析とリスク評価ということです。:

- 制限と機械の使われる目的を規定する
- 機械を使用する際の危険と関連する危険な状況をはっきりさせる
- それぞれの危険と危険な状況におけるリスクを計算する
- リスクを評価し、リスク低減の必要について決定する

次に述べる "3 ステップ方法" により、設計者は危険をなくしたり、保護方法を採用してリスクを軽減させたりすることができます。

- 本質的に安全な設計方法
- 安全装置(Safeguarding)、可能な保護方法
- 残余リスクについての明示

安全装置、可能な保護方法とは安全機能を実現することで、たとえばライトカーテン、相当するロジック運転、そしてモータの電源を切るブレーカなどのことを言います。

8.3 IEC 62061 の範囲

IEC 62061 と ISO 13849-1 は両方とも安全機能の取扱方法を規定しています。IEC 62061 が PROFIsafe 技術、プログラマブル安全コントローラ(F-Hosts)に適応している一方、ISO 13849-1 は油圧機器、空気圧機器、電気機器、機械部品の場合に対応します。

IEC 62061 では、設計指針、人間の役割と責任、コミッショニング、変更、保全、廃棄までをカバーする機械のライフサイクルにわたる安全計画が求められています。

8.4 リスク評価

両方の規格とも安全機能のリスク評価については同じような考えを示しています。 ISO 14121 によると:

リスク = 損害の重大さ と 損害の発生する確率

損害の発生する確率を計算するには、使用時間、頻度、危険をさける可能性を考慮します。

8.5 SIL の決定

両方の規格とも計算方法を規定しています。片方は SIL を使い、他方は PL(1.3 参照) を使います。これらは互いに他方に変換可能です。エンジニアリングツールでリスク評価を行うなら、長い目でみると、ユーザにとって、特に違いはなくなると考えます。

8.6 安全機能の設計

IEC 62061 は測定、計算、操作をおこなうサブシステムを持つ安全関連制御システム（いわゆる SRECS）について定義しています。サブシステムにはエレメント(例、スイッチなど) が含まれます。

安全機能を設計する最も簡単な方法は、認証された F-Device（センサー、操作器） と F-Host を PROFIsafe でつなぐシステムを使うことです。

8.7 達成可能となる SIL

F-Device は安全マニュアルで、安全機能を実現するための必要な情報を提供しています。最初に、安全機器（F-Device, F-Host）の中で、最も低ランクの SIL、the least SIL_{CL} (claim limit)を選びます。これがシステムとして実現できる最高の SIL となります。場合によっては、F-Device の冗長化とか特定のソフトを使うことで、SIL を上げることができます。

次に、PFH_d 値が計算され、結果が求められる SIL の範囲内にあるかがチェックされます。

これらの 2 つの値のうち、小さい SIL の値が達成可能な SIL の値となります。

次の章では、リモート IO 内の F-Module に、従来の電気機械式安全機器(図 5 の 緊急停止ボタン、ドアスイッチなど) を組み合わせるかを説明します。

8.8 従来機器との接続

IEC 62061 は従来の安全機器とつなぐために、A,B,C,D の 4 種類のサブシステム構成を規定しています。この場合の故障の可能性を計算する公式も決められています。スイッチの場合、B_{10} 値という値があり、この公式を使って、スイッチサイクルの期待値、診断の範囲、共通原因ファクター、危険な故障がおきる可能性を計算し、システムの SIIL を決定することができます。

8.9 非電気部品

ISO 13849-1 は油圧、空気圧、電気、機械部品である SRP/CS (Safety-Related Parts of Control Systems) について規定しています。これらの部品の PL と PFH_d の値をこの規格により計算でき、IEC62061 に対応する安全機能に対する SIL を決定できます。

8.10 バリデーション

IEC 62061 は全体の安全計画の一部としてバリデーション計画を要求しています。この計画により、機械はテストされ、検査され、結果が書類で残されます。

9. F-Device のファミリー

PROFIsafe を採用することで、標準機器も安全機器も新しい使い方ができるようになります。この章では重要な F-Device とそのアプリケーションについて、簡単に紹介します。

9.1 リモート I/O

リモート IO の主要部分を変えずに、安全モジュールとすることができます。安全機能を搭載した F-Module、たとえばデジタル入出力、アナログ入出力、パワーモジュール、モータスタータ、そして周波数変換機が可能になります。F-Module はグループとしてまとめることができ、グループでシャットダウンもできます。

緊急停止ボタンは毎年とても高い費用で検査しなければなりません。しかもすべてハードウェアのボタンです。新しい技術では、簡単に 1 年間のすべての駆動の履歴を収集できます。これですと駆動しなかったボタンだけテストすればよく、大きなコスト削減となります。

9.2 光センサー

ライトカーテンとか、レーザースキャナーのような光安全センサーは IEC61496 で標準化されています。光センサーはいろいろなやり方で入口、出口のチェックをするのに適しています。図 18 の例では、どのように PROFIsafe をレーザースキャナーとドライブを含めた安全システムで使うかを示しています。

9.3 ドライブ(回転機器)

ドライブの安全機能は IEC61800-5-2 で標準化されています。多くの場合は、安全位置指示機構が求められます。この値は PROFIsafe を介してユーザに伝達され、物理的な原点出し完了スイッチとかミューティングセンサーの代わりになります。図 18 に示すとおりに、車体の形によって違いはありますが、セルへの出入り時には、モータの位置によりレーザースキャナーの保護フィールドが影響されます。

5.2.4 章では、たくさんの可能な安全機能が示されています。これにより、近い将来ドライブの安全アプリケーションが大きく変わると思われます。

9.4 ロボット

ロボットの安全機能は ISO10218 に記述されています。ドライブの新しい安全機能はロボットにも生かすことができ、人間とロボットが一緒に働く、いわゆる”協調型ロボット”という新しい機能を提供します。

9.5 F-Gateway

PROFIsafe では AS-i バスの安全機能(ASIsafe)との F-Gateway が存在します。この機器は PROFIsafe と ASIsafe の利点を利用しています。ASIsafe では直列につないだたくさんの緊急停止ボタンの信号を簡単に集めることができ、PROFIsafe では統合化安全技術を使って、ドライブのような多機能の F-Device を取り扱うことができます。

9.6 PA 機器

プロセスオートメーションの安全が IEC61511 によって規定されていることは前述しました。NAMUR(ドイツの化学・製薬業界団体) は安全現場機器と安全通信をどのように行

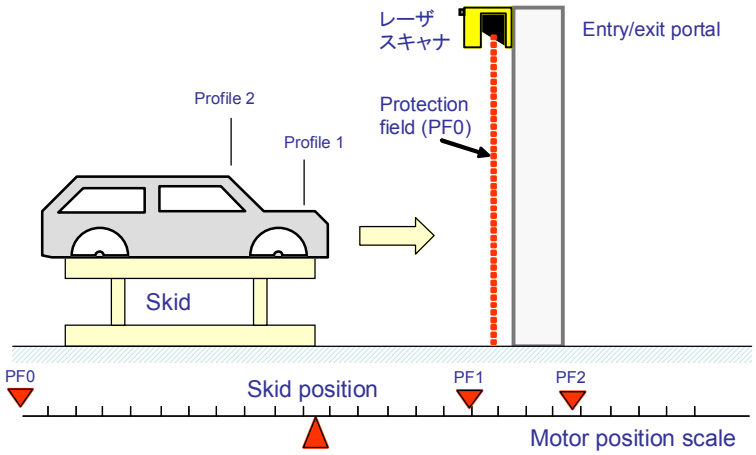

Figure 18 Software "muting sensors" for laserscanners

うかの規定 NE97 を発行しました。PROFIBUS の MBP-IS インタフェースを持つ“実績のある(Proven-in-use)” PA デバイスは、動作の”OFF”と”ON”の設定が可能な PROFIsafe ドライバを実装します。あるモードでは、その機器は標準の PA デバイスとして動作し、他のモードでは F-Device として動作します。(図 19 参照).

NAMUR はさらに別の共同規格、VDI2181、をリリースしました。この規格は、安全関連の PA 機器の開発をサポートするものです。

現在のところ、PA で使われているほとんどの PROFIsafe アプリケーションは 4-20mA または HART を使った F-Module とリモート IO の組み合わせを採用しています。図 20 では”実績のある(Proven-in-use)”PA 機器と PROFIsafe を使った 2 つの方法を示しています。広い測定レンジ、パラメータ設定、高機能の診断といったフィールドバスを利用することはできませんが、リモート IO を採用するのは、それなりにメリットがあると思えます。

9.6.1 レベルスイッチ

レベルスイッチに PROFIsafe の安全技術を使うことは、非常にメリットがあります。MBP-IS とか RS485-IS 防爆を搭載した PROFIBUS PA 機器は F-Device となることができます。標準の”black channel”がセンサーの状態を通信する一方で、PROFIsafe はシャットダウン信号を安全フレームで伝送できます。

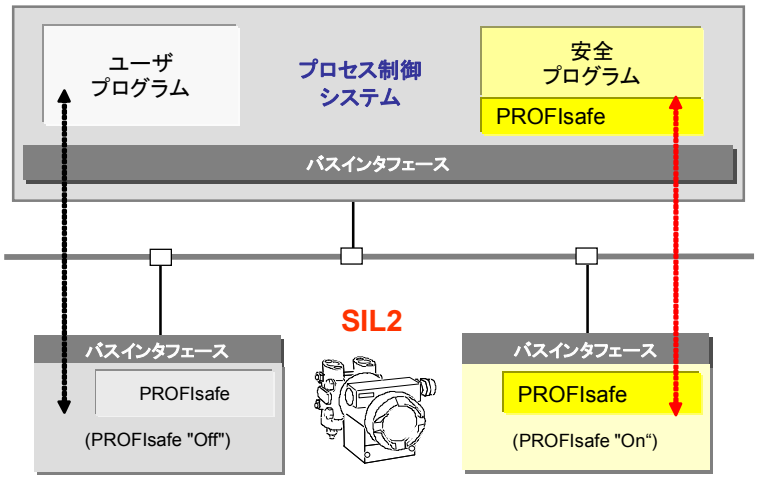

Figure 19 PA 機器に対する PROFIsafe と NE97

9.6.2 ESD バルブ

ESD (Electronic Shut-Down) バルブでも同様にメリットがあります。主な目的は、定期的に"partial valve strokes" を使ってバルブ機能をチェックすること、エンドポジションとそこまでにかかる時間をモニタリングすることです。これは F-Host を介して自動的に実行され、ユーザにとって都合が良いときに予知保全を行うことができます。バリアと RS485-IS 通信を使うと、Ex-i 環境でも高速のシャットダウンが可能になります。.

9.6.3 圧力伝送器

安全用圧力伝送器は、与えられた設定値を使って、タンクの液体注入の計測だけでなく、オーバーフローのチェック(レベルスイッチとして)を兼ねることができます。

9.6.4 ガス・炎センサー

これらのセンサーの使用例は、サービスマンがいないときの製油所などがあります。位置の情報を追加することで、ハッチを自動的に閉止することができます。

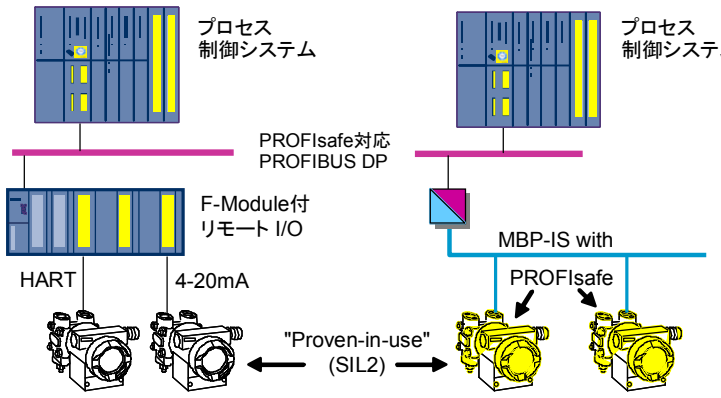

Figure 20 PROFIsafe と PA-機器の 2 つの使用例

10. ユーザのメリット

すでに世界で 2000 万台以上の PROFIBUS 機器が設置されています。したがって、現在も、今後も開発にとって大切なことは、新しい機器が既に現場で稼働している機器と完全にコンパチブルであるということです。

PROFIsafe は自律性を持ち、Black チャンネル方式を採用しているため、PROFIBUS と PROFINET をまたいで動かすこともそれほど難しくはありません。 理想的な PROFIsafe のドライバは、PROFINET の機器にも PROFIBUS の機器にも同じく利用できます。

PROFIsafe を採用することで、以下の 3 つのメリットを得ることができます:

- 今までのリレーによる安全ロジックからプログラム可能なロジックへの転換
- 多くの電線を使った配線から、シリアル通信への転換
- 単独で動く機器から、連携して動く安全機器への転換

以下の説明によって、より詳しくご理解いただけると思います。

10.1 エンジニアリング会社とユーザ

- 配線が減り、システム構成の柔軟性が増し、パラメータとかダイアログの通信ができるようになるのは、PROFIBUS を導入するのと同じコストメリットが期待できます。
- 多くのベンダーが機器を提供しているため、簡単でコストメリットのある設計が可能です。
- 多くの場合、特殊な設置制限はありません。
- 高機能の F-Device 間の通信により、最先端の安全アプリケーションを実現できます。
- 既設の拡張、レトロフィットと同じように、柔軟性をもって置き換えもできます。
- FA と PA の両方に使えます。
- トレーニング、文書、ツールも 1 つのバス技術でサポートします。
- 標準と安全関連のアプリケーションを 1 つのツールと認証された機能ブロックでプログラムできます。
- 安全関連のシステムとロジックを簡単に文書化できます。
- 認証機器を使って、システム認証のコスト削減ができます。
- IEC61508 による国際的な認定に対応
- BGIA と TÜV のアセスメントの実績

10.2 機器ベンダー

- ソフトウェアが TÜV の認証を得ているので、簡単に実装でき、開発価格を抑えることができます。
- 安全関連のコントローラが異なっても、PROFIsafe 通信は採用できます。
- 新しい革新的なデバイス機能の先駆けです。

10.3 将来への投資

- PROFIBUS と PROFINET 機器はすでに多くの設置実績があります。
- PROFIBUS/PROFINET をサポートする組織が世界中にあります。
- 現在も、これからも安全関連を含めて PI の標準規格を利用できます。
- PROFIsafe はすでに国際規格 IEC 61784-3-3 です。
- デザインからアセスメント、バリデーション、文書化を含めて、安全アプリケーションのライフサイクルをサポートするソフトウェアを計画し、よりコスト削減を目指します。

11. PI

技術の継続、さらなる開発、マーケットの拡大を考えるとオープンな技術の普及には会社に依存しないプラットフォーム的な組織が必要です。PROFIBUS と PROFINET の場合、ベンダー、ユーザ、大学に対する非営利団体として 1989 年に PNO (PROFIBUS Nutzerorganisation e.V.) が設立されました。現在 PNO は 1995 年に設立された PI (PROFIBUS & PROFINET International)のメンバーです。PI は 25 カ国に各国協会 (RPA: Regional PI Associations)を持ち、約 1,400 のメンバーが加盟しています。つまり、五大陸に広がる産業用通信の世界最大の技術普及団体となっています。

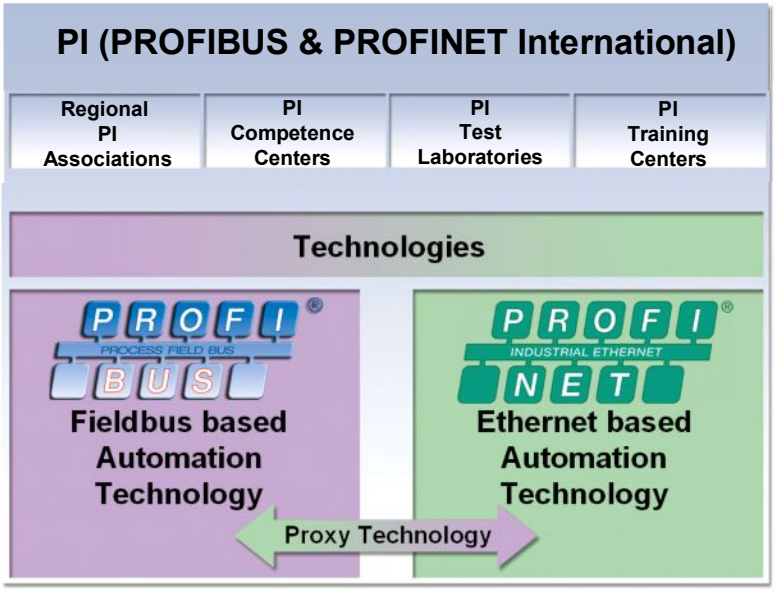

Figure 21 PROFIBUS & PROFINET International (PI)

11.1 PI の責務

PI の主な仕事は以下のとおりです:

- PROFIBUS と PROFINET 技術の保全とさらなる開発
- 世界各地での PROFIBUS と PROFINET の普及
- 標準化作業を通して、ユーザとベンダーの資産保護
- PROFIBUS と PROFINET 技術に関する標準化団体への代表
- PI 技術センター(PICC)によるメンバー・会社への技術サポート
- 認証試験をベースとした PI テストラボ(PITL)による製品認証の品質コントロール
- PI トレーニングセンター(PITC)によるトレーニングの標準化

11.2 技術開発

PI は技術開発の役目を PNO ドイツに委託しています。PNO ドイツのアドバイザリボードが開発活動のチェックをしています。実際の技術開発活動にために、500 人以上のエンジニアが 50 以上のワーキンググループで活動を続けています。

11.3 技術サポート

PI には世界中で 35 以上の PICC が存在します。PICC はユーザ、ベンダーに PROFIBUS と PROFINET に関して、あらゆる種類のアドバイスとサポートを提供します。PI の組織として、PICC は独立してサービスを提供し、この活動は規約により中立的に守られています。PICC は PI による認証により定期的にその能力がチェックされます。PICC のリストは PI の Web サイトで参照できます。

11.4 認証

PI は世界で 9 か所の PITL をサポートします。PITL は PROFIBUS /PROFINET インタフェース製品の認証をサポートします。 PI の組織として、PITL は独立してサービスを提供し、この活動は規約により中立的に守られています。PITL が試験に十分な技術、設備、規約を持って活動しているかは、定期的に厳しく PI がチェックします。PITL のリストは PI の Web サイトで参照できます。

11.5 トレーニング

PITC はエンジニアと設置技術者に対して、世界標準を確立するために設立されました。PITC とその技術者は、公式に認定されなければならず、そのため、提供されるトレーニングの品質は保証されています。これはトレーニングに関する PROFIBUS と PROFINET の技術だけでなく、関連するエンジニアリング、設置サービスについても同様です。PITC のリストは PI の Web サイトで参照できます。

11.6 インターネットによる情報提供

PI の Web サイトである www.profibus.com によって、PI の組織と PROFIBUS と PROFINET の技術を知ることができます。オンライン製品ガイド、用語解説、さまざま Web ベーストレーニングなどのほか、規格、アプリケーションプロファイル、設置ガイドラインなどのドキュメントのダウンロードエリアが用意されています。

Index

本カタログは

PROFIsafe – Safety Technology for PROFIBUS and PROFINET
System Description
Version 20 July 2007
Order Number 4.342

を日本プロフィバス協会が日本語に翻訳したものです。
日本語と原本の間に相違のあるときは原本を正とします。

特定非営利活動法人　日本プロフィバス協会
〒141-8641　東京都品川区東五反田 3-20-14　高輪パークタワー17F
電話　(03)5423-8628　　ファックス　(03)5423-8734
URL: http://www.profibus.jp
E-mail: info@profibus.jp
2010 年 3 月発行

PROFIsafe – Safety Technology for PROFIBUS and PROFINET

System Description

Version 20 July 2007

Order Number 4.342

Publisher

PROFIBUS Nutzerorganisation e.V. PNO
Haid und Neu-Str. 7
76313 Karlsruhe
Deutschland
Tel.: +49 (0)721 / 96 58 590
Fax: +49 (0)721 / 96 58 589
germany@profibus.com

PROFIBUS Trade Organisation PTO
16101 N 82nd Street, Suite 38
AZ 85260 Scottsdale
USA
Tel.: +1 480 483 2456
Fax: +1 480 483 7202
usa@profibus.com

Liability Exclusion

PNO/PTO has examined the contents of this brochure carefully. Nevertheless, errors can not be excluded. Liability of PNO/PTO is excluded, regardless of the reason. The data in this brochure is checked periodically, however. Necessary corrections will be contained in subsequent versions. We gratefully accept suggestions for improvement.

Terms used in this brochure may be trade marks and their use by third parties for any purposes may violate the rights of the owner.

This brochure is not a substitute for the standard IEC 61784-3-3 and the associated PROFIBUS and PROFINET guidelines and specifications. In case of doubt, these documents take precedence.