ProSafe-RS ハードウエアの特徴

Hardware Features of the ProSafe-RS

山　城　　靖　彦*1
YAMASHIRO Yasuhiko

当社の安全システムProSafe-RSを構成するハードウエアは，SIL3という高い安全度水準をシングル及び冗長化の両方のモジュール構成で実現している。ハードウエアは市場で大きな実績のあるCENTUM CS 3000の高い信頼性技術と資産をベースに，機能安全規格IEC61508で規定されている種々の安全設計要求事項をクリアした設計となっている。特に今回の開発では，マイクロプロセッサの二重化技術を，CPUモジュールだけでなくI/Oモジュールにも適用することで，シングル及び冗長化の両方の構成でSIL3を実現した。

The new hardware of our ProSafe-RS safety system offers single and dual-redundant module configurations, both of which have achieved a safety integrity level (SIL) of 3. Based on the technological heritage and reliability of the CENTUM CS 3000, which has a proven track record in the hardware market, the ProSafe-RS is designed to meet all the safety design requirements of IEC61508, an international functional safety standard. The main feature of the newly developed ProSafe-RS hardware is the application of dual microprocessor technology, not only to the CPU module, but also to the I/O module. This feature affords an SIL of 3 in a single configuration as well as in a dual-redundant configuration.

1. は じ め に

機能安全規格IEC61508の安全度水準SIL3を達成した安全システムは既に市場で複数存在しているが，モジュールの二重化や三重化で実現しているものが殆どである。この方式だと，モジュールが1つ故障すると安全性は劣化（ディグレード）してしまうため，安全性維持のためには一定時間内に修復しなければならない。また，モジュールの多重化が必要なことから，コストも割高になりがちである。シングル構成でSIL3が実現できれば，システムコストを低く抑えることができ，さらに冗長化が可能であれば，高い稼動率を得ることができる。

本稿では，市場実績のあるCENTUM CS 3000の高信頼技術をベースに，シングルモジュール構成でSIL3の安全度を達成し，さらにフレキシブルな冗長化も可能とした安全システムProSafe-RS（**図1**）の主にハードウエアについて紹介する。

2. 安全設計アーキテクチャと信頼性

（1）SIL3適合のための要件
シングル構成にてSIL3の安全ループに適用可能とす

図1　ProSafe-RS 外観（冗長化構成時）
上段：セーフティコントロールユニット
下段：セーフティノードユニット

*1 IA事業部システム事業センター 安全システム部

るためには，ProSafe-RSのPFD(Probability of Failure on Demand)値を，SIL3 の安全ループ全体のPFD 値(10^{-3}～10^{-4})の15%(1.5×10^{-4})以下に収めなければならない。そのためには，プルーフテスト(定期点検で行う動作試験)を 10 年とした場合，ProSafe-RSを構成するハードウエアにおける検出不能危険故障率(λ_{DU})を3.4fit(10^9時間中に起きる故障が3.4回という確率)以下という極小な値に収める必要がある。

また，SFF(Safe Failure Fraction:((全故障率－λ_{DU})÷全故障率)×100%)が 99% 以上であることとIEC61508で規定されている。これは，あらゆる自己診断を駆使して，検出不能危険故障率を1%未満に抑えなければならないことを意味する。

(2) 安全設計アーキテクチャ

SIL3を実現するに当たっては，いかに自己診断を充実させるかが重要なポイントであるが，IEC61508では，マイクロプロセッサは単体での自己診断率を90%以上にはできないとされており，99%以上を達成するためには，2つのマイクロプロセッサを使用して演算結果を比較するなどの手段が必要となる。そのため，ProSafe-RSのプロセッサモジュールでは，CENTUM で実績のあるマイクロプロセッサの二重系照合方式“ Pair & Spare 方式 ”を採用した。入出力モジュールにおいても，CS 3000 の FIO をベースにマイクロプロセッサをペアで使用し，さらに入出力回路の多系統化と系統間比較，および入出力回路の活性化診断を行い，高い故障検出率を達成した。また，プロセッサモジュールと入出力モジュール間のデータ通信を行うI/O バス(ESB/SB バス)においても，SIL3の安全性を保証する必要がある。そのため，V ネットでの安全通信と同様に，プロセッサモジュールと入出力モジュールの両者にセーフティレイヤーを設け，安全通信データにはCRCやシーケンス番号を付加して厳密にチェックを行い，安全性を保証している。

(3) 安全性の検証

SIL3 に適合していることの確認は，FMEDA(Failure Modes Effects and Diagnostic Analysis)という手法によって，全ての構成部品に対してその部品の故障率と故障モード，故障で引き起こされる影響を分析することにより行った。その分析から，それら故障のうち，自己診断によって検出できない危険故障率(λ_{DU})を定量的に見積もってPFD値を算出し，目標の1.5×10^{-4}以下であることを確認した。そして，その見積もりが正しいことを，安全認証機関TÜV立会いの下で，フォルトインサーションテストなどの実機検証にて証明した。

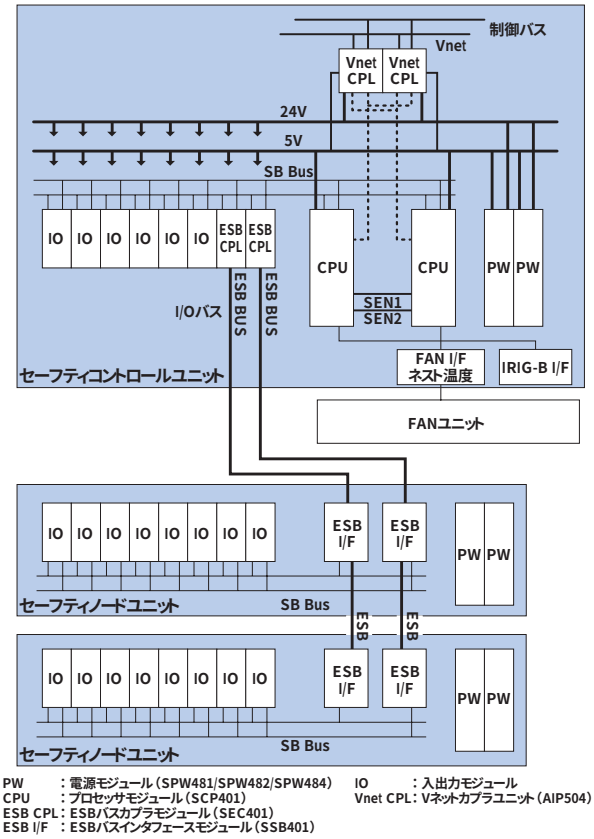

図2　SCS の構成

(4) 高信頼性

SIL3の安全性を維持したまま，高い信頼性と高い稼働率を実現するために，モジュール単位で実施可能な CS 3000 の冗長化技術を採用した。プロセッサモジュール，入出力モジュール，電源モジュール，通信バスの全てが冗長化可能であるが，電源モジュールと通信バスは標準で冗長化構成とし，プラットフォーム部分の信頼性を高めている。また，耐環境性においても，一般のDCSより厳しいテスト条件が求められるIEC61131-2(Programmable Controllers–Equipment requirements and test)，EN298(バーナマネジメント規格)，EN54-2(防消火システム規格)の要件をクリアし，さらに耐腐食性はANSI/ISA S71.04 の G3 仕様を標準としている。

3. SCS ハードウエア構成

SCS(Safety Control Station)は1台のセーフティコントロールユニットと，最大 9 台まで拡張可能なセーフティノードユニットで構成され，制御バスとI/Oバスには，CENTUM CS 3000 と同じ V ネットおよび ESB/SB バスを採用している。**図2**に，ProSafe-RSのSCSの構成を示す。

開発に当たっては，高い安全性と信頼性は元より，

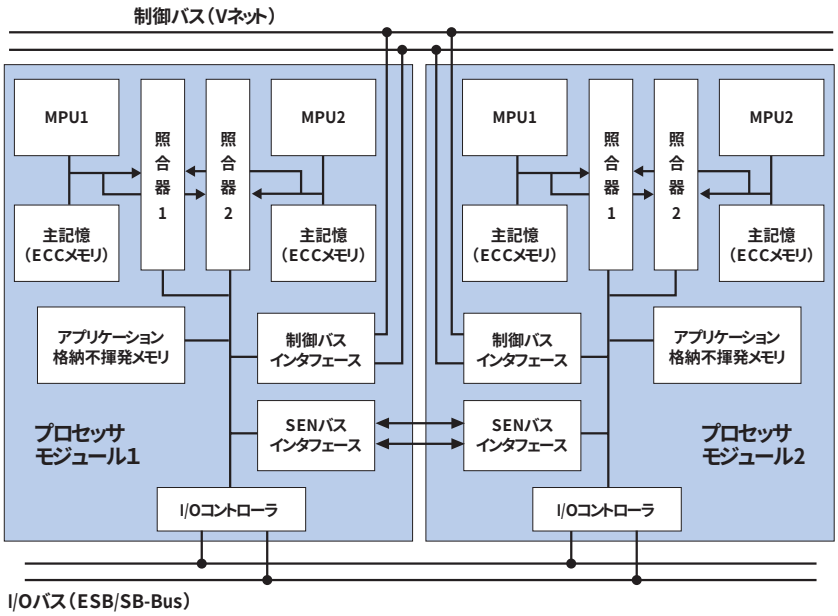

図3　プロセッサモジュールの構成（冗長化時）

CS 3000との統合化運用および保守性，生産性を考慮して，CS 3000のFFCSとFIOをプラットフォームとした。そのため，外形寸法はFFCSやFIOと同じである。

3.1 ユニット構成

セーフティコントロールユニットは，プロセッサモジュールの他に8枚の入出力モジュールを実装して，ユニット単独でSCSを構成することができる。または入出力モジュールは6枚とし，ESBバスカプラモジュール（SEC401）を実装してセーフティノードユニットを拡張する構成もとることができる。セーフティコントロールユニットの動作周囲温度は−20℃～50℃が標準であるが，上限70℃まで対応可能な，冷却ファン付きの広温度対応仕様も用意している。

また，SCS間での高精度時刻同期を実現するためのIRIG-B（GPS接続）インタフェースもオプションで用意している。

セーフティノードユニットには，最大8枚までの入出力モジュールを実装することができ，標準で−20℃～70℃の温度環境に対応している。

3.2 I/O バス

I/Oバス（ESB/SBバス）の仕様は，CENTUMと同じである。前述のセーフティレイヤーにより，同一バス上で安全通信と非安全通信のアイソレーションが実現できているため，従来のFIOを同じバスに接続して使用することも可能である。但し，安全機能に非干渉であることのTÜV認証を取得する必要があり，現在はRS通信モジュールのみ接続可能としている。

3.3　プロセッサモジュール

図3にプロセッサモジュールの構成を示す（冗長化構成時）。プロセッサモジュールは，二重系照合方式（Pair & Spare）を採用しているCS 3000 FFCSのプロセッサモジュール（CP401）をベースに開発した。CP401の二重系照合方式では，2つのプロセッサが同一の演算を行い，その演算結果を1つの照合器により信号線レベルで比較して，一過性の演算エラーを検出できる。これだけでも十分に高い信頼性を得ているが，ProSafe-RSでは，照合器と主記憶および関連するレジスタ群やWDTなども完全に二重化して，共通原因故障となり得るものを徹底的に排除し，検出不能危険故障率（λ_{DU}）を極小とする設計としている。これらの機能をCP401と同じサイズに収めるため，高集積度のASICを新規に開発し，マイクロプロセッサ（MPU）や主記憶（ECCメモリ）を除いた二重化関連機能の殆どを，この1チップのASIC上に搭載している。このASICの設計に関してもIEC61508で規定されている種々の安全設計要件を満たしたものとなっている。

また，CP401では停電時の主記憶バックアップは充電可能な二次電池を使用しているが，バックアップ可能な時間は48時間ほどである。しかし，IEC61131-2では，アプリケーションプログラムの保持時間を通常温度下で1,000時間以上，高温度下でも300時間以上を要求している。この要求に対応するため，アプリケーションプログラムは不揮発メモリ（フラッシュメモリ）に格納する方式を採用した。

3.4　入出力モジュール

今回，FIOをベースに4種類のSIL3適合入出力モジュールを新たに開発し，既存FIOの2種類の通信モジュールを安全非干渉モジュールとして，同一SCSへ実装できるようにした。**表1**に，入出力モジュールの種類を示す。

表1　入出力モジュールの種類

形　名	モジュール種類	仕　様
SAI143	アナログ入力モジュール	4-20 mA, 16 ch
SAV144	アナログ入力モジュール	1-10 V, 16 ch
SDV144	デジタル入力モジュール（SOE機能付き）	無電圧接点, 16 ch
SDV531	デジタル出力モジュール	24 VDC, 8 ch, 0.6 A/ch
ALR111*	RS232通信モジュール	2ポート
ALR121*	RS422/485通信モジュール	2ポート

*SCSへ実装して使用できるが，安全ループへの適用はできない。

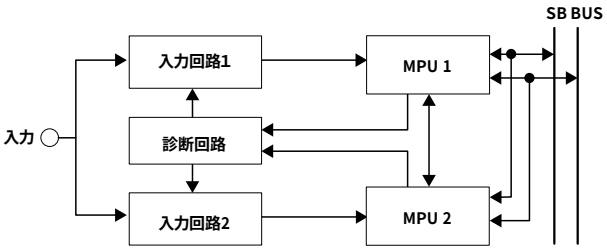

図 4　入力モジュール

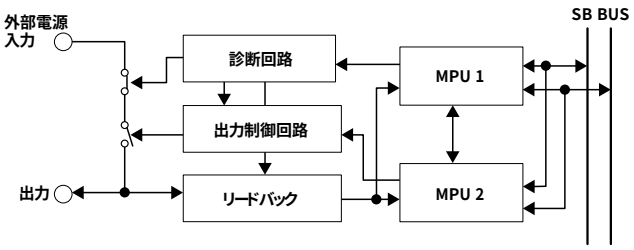

図 5　出力モジュール

図 4 に入力モジュール，**図 5** に出力モジュールの構成概略を示す。それぞれの入出力モジュールには MPU が 2 つ搭載されており，プロセッサモジュールからのコマンドや入出力データの健全性を，MPU間で比較照合しあいながら動作している。入出力モジュールにおけるMPU間の比較照合動作は，プロセッサモジュールのようにハード的な比較器で行うのとは異なり，それぞれのMPUに搭載されているファームウエアによって MPU 間通信を行い，高度に同期を取りながら照合動作を実現している。この方式は安全入出力モジュールの大きな特長の一つである。

3.4.1 入力モジュール

入力モジュールは 2 つのプロセッサ（MPU）と，1 チャネル当たり 2 系統の入力回路，そして入力回路部や周辺回路の診断を行う回路で構成されている。フィールドからの入力信号は，独立した2つの入力回路を経由して2つの MPU に入力される。MPU はそれぞれに入力されたデータが一致しているかどうかを相互に照合しあうことで，入力回路およびMPU自身の健全性を保証している。データが一致していれば，そのデータはファームウエアで構築されたセーフティレイヤーを通してプロセッサモジュールへ送信される。また，安全システムで扱う入力信号はシャットダウン要求が発生しない限り変化することがないことから，もし入力チャネルの回路部品が固着故障した場合にそれを検出できないと，いざデマンドが発生した場合に出力をシャットダウンすることができない。そのような危険状態に陥らないため，入力チャネル回路を定期的に活性化して，常に固着故障の有無を診断している。

3.4.2 出力モジュール

出力モジュールでは，プロセッサモジュールから I/O バス経由で送られてくる出力指示コマンドを2つのMPUで受信し，セーフティレイヤーによってそのコマンドの健全性を各MPUでチェックし，さらにその結果を，MPU間で比較する。コマンドの健全性が確認できたら，指示値を出力する。出力値は 2 つの MPU で読み返しを行い，指示値と合っているかどうかを常に診断している。また，出力信号もシャットダウン要求が発生しない限り変化することがないため，出力スイッチや読み返し回路が固着故障していないかどうかを，回路の定期的な活性化により診断している。もしも出力スイッチが ON に固着故障してしまった場合は，出力スイッチと直列に配置されているもう一方のスイッチをOFFにして，出力を強制的に OFF にすることができるようになっている。

3.4.3 フィールド配線診断

ProSafe-RSとフィールド機器とを接続するための配線の健全性も，安全ループを構成する上での重要なポイントとなる。ProSafe-RS自身が健全であったとしても，配線が短絡または断線していると，安全ループとして正しく機能することができない。そのため，ProSafe-RSの入出力モジュールでは，配線の短絡や断線を検出する機能を実装しており，異常を検出した場合はアラームによりオペレータに通知し，復旧を促すことができるようになっている。

4. おわりに

本稿では，ProSafe-RS SCSのハードウエア構成と設計アーキテクチャを紹介した。今後，市場では，安全ループのPFD値の大きな部分を占めるセンサやアクチュエータの安全性，信頼性を向上する技術の開発が加速されていくものと考えられる。

ProSafe-RSも，それらフィールド機器に対応可能な入出力モジュールのラインナップを充実させ，より高度な安全ソリューションをユーザに提供してゆく所存である。

参考文献

(1) IEC61508 First Edition：Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems

(2) 小宮浩義 他，“ CENTUM CS 3000 R3コンパクト制御ステーション FFCS ”，横河技報，Vol. 48，No. 4，2004，p. 149-152