安全システムProSafe-RSのねらいと特長

Aims and Features of the ProSafe-RS Safety System

西　田　　純[*1]
NISHIDA Jun

国際安全規格IEC61508の安全度SIL3レベルに適合したシステム製品ProSafe-RSを開発した。本製品は，単独で安全計装に使用可能な各種条件を満たしているだけでなく，当社のプロセス制御システムCENTUM CS 3000との強い親和性をもち，プロセス・プラントをトータルで設計するユーザに対して，柔軟かつ統合されたトータルソリューションのためのプラットフォームを提供する。本稿では，ProSafe-RSのねらいと特長を概観する。

We have developed the ProSafe-RS, a safety system compatible with the SIL3 level of the IEC 61508 international standard. This product alone fulfills the requirements for safe instrumentation. In addition, it is highly compatible with our CENTUM CS 3000 process control system and offers a platform for flexible, comprehensive solutions to users who implement overall process plant designs. This paper outlines the aims and features of the ProSafe-RS.

1. はじめに

近年プロセス制御の分野において，事故時の社会的影響の大きさなどから，重大事故を防止することの重要性がますます認識されてきている。国際安全規格IEC61508およびIEC61511においても，重大事故を防止するために，プロセス制御系に幾層もの防護層を構築するとともに，安全計装システム(Safety Instrumented System：SIS)によるリスク低減が必須となってきている。SISに含まれる安全システムは，安全性と高信頼性の両立が求められる。一般には安全性と高信頼性は類似な意味に受け取られるが，安全システムにおける安全性とは，いざという時にプラントのシャットダウンを実行する確度の高さを意味し，自身の故障時にも，安全側であるシャットダウン方向に動作する特性を含む。一方，信頼性とは，自身の故障によってプラントを停止させる確率(誤トリップ率)が低いことを意味する。また，ユーザの視点では，プロセス制御も安全計装も，同一プラントに対して行うため，両者をトータルで考慮したソリューションが求められている。当社の安全システムProSafe-RSは，これらの要求に応えるべく，以下の特長を持つことを狙いとして開発した。

・DCSとの統合
・シングル構成で安全度水準SIL3の高安全性と高信頼性の両立
・IEC61131-3準拠のエンジニアリングツール

2. システム構成

図1に，安全システムProSafe-RSと，生産制御システムCENTUM CS 3000の統合システム構成例を示す。ProSafe-RSは，セーフティエンジニアリングPC(SENG)とセーフティコントロールステーション(SCS)を，制御バスVnetで直結した構成から成っている。

SENGは，エンジニアリング機能及び保守機能を提供するソフトウエアが動作するPCである。

SCSは，SENGで作成したアプリケーションをダウンロードすることにより，シャットダウンなどのロジックを実行する安全コントローラである。SCSの基本アーキテクチャーは，CS 3000 FCSの柔軟性を備えたアーキテクチャーを継承しており，IOモジュールおよびCPUモジュールは，1ステーションの中で二重化構成(**図1-①**)，あるいはシングル構成(**図1-②③**)をユーザの目的に合わせて選択できる。また，SCS間セーフティ通信をサポートしており，CS 3000と共通の制御バスVnet経由で，SCSをまたがったセーフティループが実現可能(**図1-④**)である。

SENGにてCS 3000タグのエンジニアリングを行い，それをSCSにダウンロードすることにより，CS 3000 HISから，CS 3000 FCSと同様の方法で，SCSを扱う統合オペレーションが可能(**図1-⑥**)となる。

*1 IA事業部システム事業センター 安全システム部

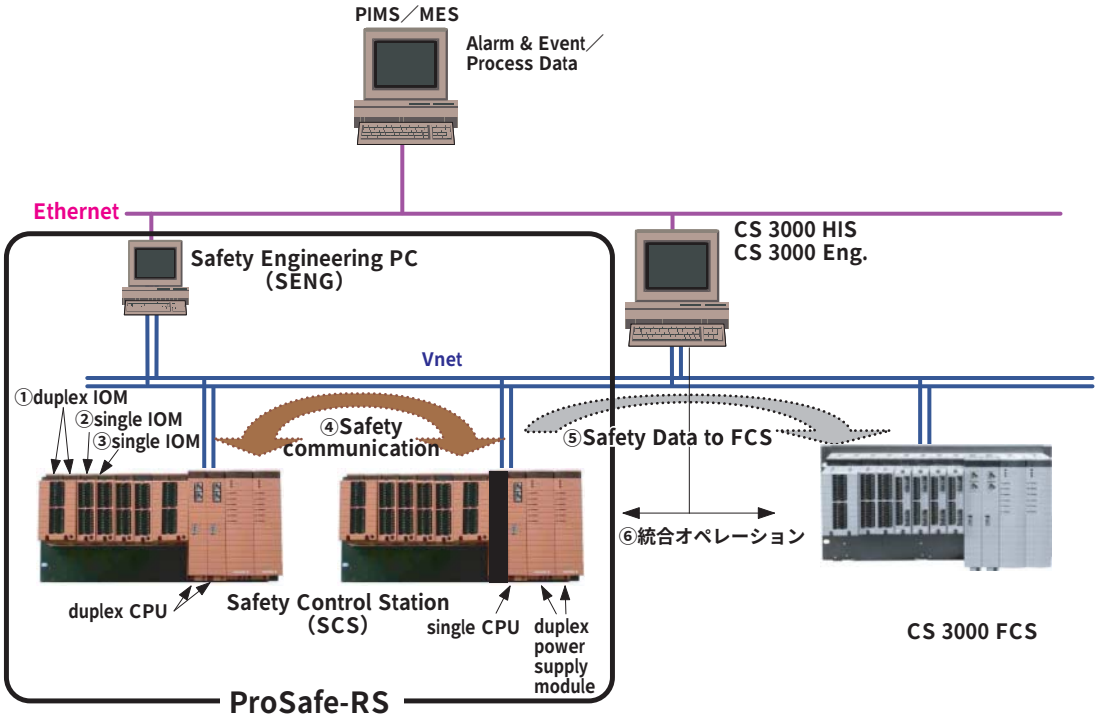

図 1　ProSafe-RS ／ CS 3000 統合システム構成例

3.　DCS との統合

3.1 アーキテクチャー統合

ProSafe-RSは，その基本アーキテクチャーとしてCS 3000と同一のアーキテクチャーをベース技術として採用している。これによって，長年に亘るDCS開発により洗練された使い易さと，CS 3000 のフィールド実績により証明された信頼性を実現している。

ユーザにとっても，CS 3000 と ProSafe-RS を同一プラントに適用することによって，ハードウエアの設置や保守の方法などの基本的な考え方がDCSとSISで共有できるという利点がある。

また，アーキテクチャー統合により，SISとDCSを共通の制御バス Vnet で接続できる構造が可能となった。これにより，システム構築や相互のインタフェース設計がシンプルになり，それらの設計コスト，設置コスト含むトータルエンジニアリング効率の大幅な改善が期待できる。

さらに，オペレータステーションHISおよびMES領域へのインタフェースをDCSとSISとで同一にする設計思想は，今後の上位の機能拡張(設備管理など)においても，本質的に DCS と SIS を区別なく扱うトータルソリューションを提供する基盤となり得る。

3.2 オペレーション統合

SISは，プラントに異常が発生して，かつDCSや人間による対応ができなくなった時に，即座にプラントを安全に停止させるためのシステムである。つまり，SISのオペレーションや監視が必要になるケースは非常に稀であり，その時のためだけに常に SIS 独自の HMI と DCS の HMI を両方監視するのは，非常に不便である。同一のHMIにてSISとDCSを操作監視ができれば，オペレータは両者のHMIの操作を覚えなくてもよい上，いざと言う時に通常使用している DCS の HMI による的確な対処が可能である。従って，SIS の通常時の監視は，DCS と同一の HMI にて実行できることが強く求められている。

ProSafe-RSでは，ユーザのこの要求を満たすため，以下のような特長を持つオペレーション統合環境を実現した。

- オペレータが，SISからくるプリアラームをCS 3000と同じ HMI にて確認できる。
- 定期点検時に，オペレータがCS 3000と同じ方法でオペレーションできる。
- SCS のデータを CS 3000 の HMI や FCS が簡単に参照できる構造になっており，DCS と SIS の統合アプリケーションが容易に構築できる。例えば，SIS と DCS のセンサ情報を DCS 側で比較して DCS 側のセンサの正当性をチェックするなど，SISのデータをDCS側でうまく利用するアプリケーションが可能である。
- OPC による上位管理を，DCS と同等に扱える。
- DCSとSISのイベント情報(Sequence of Event：SOE)を統括して分析することにより，プラント全体での異常原因解析が可能である。

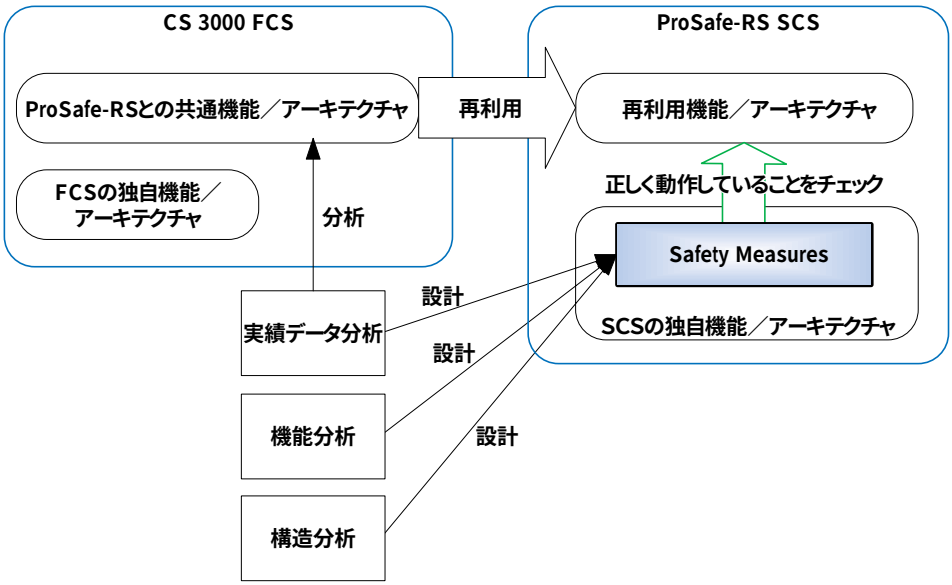

図2　再利用における共通原因故障と安全性

3.3 DCSとSISの統合と分離

DCSとSISを統合することにより，上記のようなメリットがある一方，国際安全規格ではDCSとSISの分離が求められている。これは複数の防護層によるリスク評価分析(LOPA)にも現れているように，コントロールの機能が失われても安全防護層の機能が失われないようにするためである。

ProSafe-RSでは，DCSとSISの機能の分離を確保した上で，Vnetで統合するシステム構成になっている。DCSとSISの分離を考える場合，DCSからSISへの干渉をどう防ぐか，および両者の共通原因故障をどう防ぐかがキーポイントとなる。以下に，ProSafe-RSではどのようにDCSからの干渉と共通原因故障を防いでいるかについて説明する。

・DCSからSISへの干渉の防御

例えば，互いにステーション間接続された2台のSCSと，3台のFCSが同一Vnetに直結されていた場合を考える。Vnetバス経由でFCSがSCSに干渉するケースとしては，大量データのVnetバスへの誤送信や不正フレームの誤送信によるSCSへのアタックなどが考えられる。しかし，VnetバスとFCSの信頼性は，CS 3000の実績データで証明されているため，FCSからSCSへの悪影響は，CS 3000と同程度の非常に低い確率でしか発生しないと考えられる。万が一Vnetバス異常が発生しても，Vnetバス異常に着目した安全対策機構(Safety Measures)により，通信アタックをプロテクトしたり，SCS間接続で構成されるセーフティループをシャットダウンしたりすることができる。これは，Vnet経由でのDCSからのどんな影響もProSafe-RSでは危険側故障を引き起こさないことを意味する。つまり，DCSからSISへの非干渉性(DCSからの影響により，SISの安全機能が働かなくなるような現象が発生しないこと)が保障される。

・DCSとSISの共通原因故障の防御

ProSafe-RSがCS 3000のアーキテクチャーをベースとして採用していることから，両者に共通のシステム欠陥(Systematic Failure)を仮定し，それが共通原因故障となりうる可能性と防御を考えることは重要である。**図2**に，共通原因故障を防ぐ基本的な考え方を示す。SCSのハードウエア，ソフトウエア共に，CS 3000と共通するモジュールの実績データを分析し，安全性に悪影響を与える可能性があると分析された部分に対しては，診断機構の実装や多重化するなどの安全対策機構(Safety Measures)を実装している。また，ProSafe-RSの機能およびアーキテクチャーの観点で，各部位に異常が発生した場合を仮定し，安全機能に悪影響を及ぼす可能性があると分析された場合には，同様にSafety Measuresを実装している。これらのSafety Measuresは，ProSafe-RSで新規に開発したものであり，これらのSafey Measuresの有効性と十分性が，認証機関(TÜV)と議論され認証されている。

つまり，万が一CS 3000とProSafe-RSに共通のSystematic Failureがあると仮定しても，ProSafe-RSではその故障(あるいはその原因によるエラー)を検出し，予め決めた動作を行うことができる。

4. シングルSIL3の安全性と信頼性

ProSafe-RSでは，一つのIOモジュールおよびCPUモジュールの内部に，二重系照合機構および自己診断機構を内蔵し，1コンポーネントでIEC61508で定義されるSIL3に適合するレベルを達成した。つまり，CPUモジュール，IOモジュール共にシングル構成で，SIL3を満たすセーフティループが実現できる。このことにより，以下のような，エンジニアリングの選択肢が増えるメリットがある。

・二重化構成時片側故障でも安全機能が損なわれない

ProSafe-RSは，シングル構成でSIL3を実現しているので，二重化構成時に片側CPUモジュールもしくは片側IOモジュールが故障しても，SIL3レベルの安全性は依然保たれる。

一般に冗長化構成でSIL3を実現するシステムにおいて片側故障が発生すると，修理が完了するまでの間，故障検出率が低下する。この場合，そのハードウエアを修理する時間の上限値(8 hなど)が決められており，その時間以内に修理しなければシステム全体の安全性が損なわれる。つまり，ユーザは規定時間以内に修理を完了させなければならない上に，完了できなかった場合には，プラントを手動で停止するなどの安全対策を実施しなければならない。従ってユーザは，エンジニアの待機や増員，短時間での故障部位特定，交換，テストを実施するための仕組みなど，修理時間を保証するためのランニングコストを運転期間全体に亘って考慮する必要がある。ProSafe-RSでは，この制限を排除できるため，安全性の人への依存度合いが縮小でき，かつ上記ランニングコストの削減が期待できる。さらに，保守し難い場所(遠い場所や井戸の中など)へ設置が可能になるなど，エンジニアリングの選択の幅が広がる。

・高い信頼性の実現

CPUモジュールの二重化構成でSIL3を満たすシステムでは，2つのCPUモジュールのデータ照合によって安全性を確保していることが多い。データ照合の不一致が検出された場合は，どちらのCPUモジュールが異常なのか判断できないため，通常両側故障と見なし，システムをシャットダウさせる方向に作用する。つまり，照合不一致を引き起こす故障は，1故障で誤トリップを引き起こす。

しかし，ProSafe-RSは，各モジュール内でSIL3レベルの診断が実施されているため，CPUモジュール間での比較照合は行われない。つまり，2つのCPUモジュールで同時に2故障発生しない限り誤トリップが発生することはなく，非常に高い信頼性が実現できている。

・シングル構成での柔軟な対応

ProSafe-RSでは，IOモジュールがシングル構成の時でも，IOモジュール故障時に誤トリップさせない機能を実装している。デジタル入力モジュール(DI)の場合，通常時1，プラント異常時0となる信号入力において，IOモジュールの当該チャネル故障を検知した時に1を入力するように定義することが可能である。この場合，IOモジュールの故障発生時にはシングル構成であっても誤トリップせず，故障の発生だけがアラームで通知されるためプラントの信頼性は保たれる。また，ユーザは規定された修理時間以内に故障部位を交換することにより，安全性を確保することができる。

5. IEC61131-3準拠のエンジニアリング機能

ProSafe-RSのエンジニアリング機能は，国際標準規格IEC61131-3準拠の言語をサポートしている。これにより，階層構造のアプリケーションが作成でき，再利用性，パーツ化などのIEC61131-3が持つメリットが享受できる。

ProSafe-RSでは，さらに効率のよいエンジニアリングおよび保守のために，以下の機能をサポートしている。

・IEC61131-3言語とCS 3000の統合ツール

CS 3000統合のための機能として，IEC61131-3のファンクションブロックとCS 3000タグの対応付けを行い，CS 3000のエンジニアリング機能と連携するツールをサポートすることで，CS 3000統合エンジニアリングの効率化を図っている。

・オンライン変更のサポート

ProSafe-RSでは，Safetyコントローラを停止させることなく，つまりプラントをシャットダウンせずにアプリケーションを変更し，運転を継続する機能が正式に認証されている。

さらに，オンライン変更時にテストすべき箇所を極小化するためのエンジニアリングツール(Cross Reference Analyzer)を用意することで，SISで認証上強制されている，アプリケーションの部分的変更後の全アプリケーションの多かった再テストが不要になっている。

・迅速な保守作業のための機能

SCSのハードウエア故障時に，故障部位の特定を簡単にするために，保守専用のHMI(SCSメンテナンスサポート機能)をサポートしている。

6. おわりに

本稿では，ProSafe-RSの特長を，そのねらいを交えて概観した。ProSafe-RSは，安全計装とDCSのトータルソリューションのための強力なプラットフォームを提供する。今後の課題としては，さまざまなユーザニーズに応えるべく，以下のような点に着目した機能拡張を検討中である。

・IOバラエティ拡張やフィールド機器との連携
・エンジニアリングコスト削減のための機能拡張
・オペレータの訓練環境などの付加価値機能のサポート

参考文献

(1) 関口隆，佐藤吉信，機械安全 / 機能安全実用マニュアル，日刊工業新聞，2001，271p.
(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. 149-158
(3) 安全システム特集，横河技報，Vol. 49，No. 4，2005，p. 147-158