セーフティコントロールステーションにおける安全テクノロジー

Safety Technologies Incorporated in the Safety Control Station

江 守 敏 幸*1
EMORI Toshiyuki

当社は，機能安全の国際規格IEC61508で定義される安全度水準SIL3レベルに適合した安全システムProSafe-RSを開発し，ドイツの認証機関TÜVによる認証を取得した。セーフティコントロールステーション(SCS)は，ProSafe-RSの中核となる安全コントローラである。本稿では，SCSにおいて，SIL3の安全性を保証するために採用している安全機能と非安全機能間の干渉防御，安全通信など，いくつかのテクノロジーを紹介する。

We have developed the ProSafe-RS safety instrumented system, which has been certified by the TÜV German certification organization as meeting Safety Integrity Level (SIL) 3 specified in IEC 61508, the international standard for functional safety. The safety control station (SCS) is a safety controller that is a core component of the ProSafe-RS. This paper describes some of the technologies, including protection against interference between safety functions and non-safety functions, and safety communications, incorporated in the SCS to achieve SIL 3.

1. はじめに

従来の安全計装システム(SIS)では，分散型制御システム(DCS)からの干渉を排除して安全性を保証するために，DCSとは分離して設置されることが多かった。しかし，ユーザからは，安全コントローラの安全性は維持した上で，DCSとSISを統合したいとの要求が高まってきている。

ProSafe-RSの安全コントローラであるセーフティコントロールステーション(SCS)は，当社のDCSであるCENTUM CS 3000のフィールドコントロールステーション(FCS)と同一のアーキテクチャをベースとして採用し，FCSと同等の信頼性と上位通信インタフェースを継承している。さらに，安全機能と安全通信を実装し，CS 3000システムとの密な統合と同時に安全度水準SIL3レベルの安全性を実現し，ドイツの認証機関TÜVによる安全認証を取得している。

2. 安全ループとSCS

図1に，SCSの機能構成を示す。

SCSは安全ループ上に位置する安全ロジックソルバであり，センサからの入力データを取り込み，最終エレメントにフェイルセーフ出力する役割を持つ。

SCSは，安全ループに直接関係する安全機能(安全ロジック実行，I/O機能，診断機能など)と，直接安全ループと関係しない非安全機能(CS 3000接続，Modbus通信など)から構成されている。また，SCS間セーフティ通信を用いることで，制御ネットワークVネットを介して，複数のSCSをまたがった安全ループが構築できる。

3. SCSの安全機能

安全ロジックソルバとしての，SCSの基本的な安全機能に関して説明する。

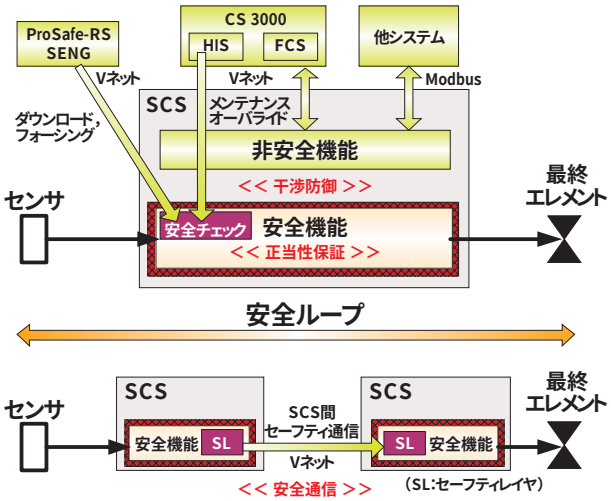

図1　SCSの機能構成

*1 IA事業部システム事業センター 第2技術部

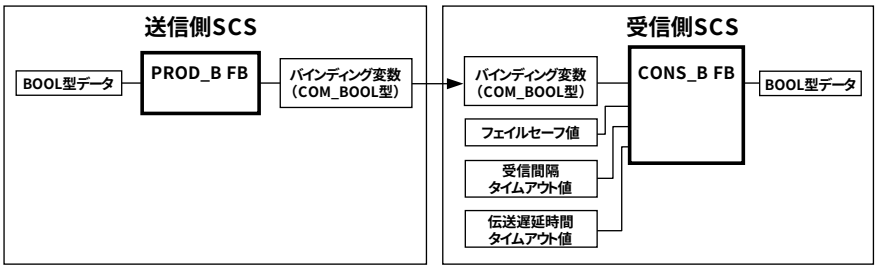

図2　SCS間セーフティ通信のロジック例

3.1 安全ロジック実行

SCSでは，国際標準規格IEC61131-3準拠のファンクションブロックダイアグラム(FBD)およびラダーダイアグラム(LD)で記述された安全ロジックが，指定されたスキャン周期で実行されている。センサからのデマンド(シャットダウンすべき要因)を検知すると，安全ロジックで記述されたシャットダウン処理が動作し，最終エレメント(シャットダウンバルブなど)に対して，シャットダウン信号を出力する。

3.2 異常検出時動作

SCSを構成するCPUモジュールおよび入出力モジュールでは，ハードウエアおよびソフトウエアにより定期的に自己診断が行われている。

以下に，各モジュールが，シングル動作時に故障が検出された時の動作を示す。モジュールが二重化で動作していれば，単一故障が発生してもシングルで動作を継続し，シャットダウン処理は実行されない。故障箇所および故障要因はアラームで通知され，故障モジュールはオンラインで交換することができる。

(1) CPUモジュールの故障時動作
　シングルのCPUモジュールで故障が検出された場合，CPUモジュールを停止させ，全出力モジュールからは，予め指定されたフェイルセーフ値が出力される。

(2) 入力モジュールの故障時動作
　入力モジュールでは，フィールド配線診断，チャネル診断，モジュール共通部診断が，定期的に実施されており，故障を検知すると，安全ロジックに予め指定された異常時の入力値を通知することができ，デマンド発生時のロジックをそのまま共用して，故障時のシャットダウン処理を行わせることができる。

(3) 出力モジュールの故障時動作
　出力モジュールにおいても，フィールド配線診断，チャネル診断，モジュール共通部診断が定期的に実施されており，モジュールの共通部の故障が検出されると，この出力モジュールの全チャネルの出力を強制的にOFFとする。
　個々のチャネルで故障が発生した場合は，予め指定されたフェイルセーフ値を強制的に出力する。なお，出力チャネルが異常状態になったことを安全ロジックで監視して，別の出力チャネルにシャットダウン信号を出力させることもできる。

3.3 SCS間セーフティ通信

ProSafe-RSでは，CS 3000システムの制御ネットワークVネットを分離することなく，同一Vネット上で，SIL3レベルの認証を受けた安全通信と，従来からのCS 3000の制御通信を混在させた統合システムが，小規模から大規模，広域対応と柔軟な構成で構築できる。

SCS間セーフティ通信を行うために，専用のSCS間セーフティ通信用のファンクションブロック(FB)を使用して，ロジックを記述する(**図2**)。

通信によって発生しうる危険事象(データの破壊，抜け，遅延など)が，受信側ＳＣＳのＦＢ(**図2**の例ではCONS_B)で全てチェックされ，異常検知時は，指定されたフェイルセーフ値を出力するとともに，異常箇所を特定する情報と異常要因をアラームで通知する。

3.4 メンテナンスオーバライド

メンテナンスオーバライドは，特定の入力などの部分的保守の間に，安全ロジックでシャットダウン処理を実行しないように，バイパスさせる機能である。専用のオーバライドFBを使用してバイパス用のロジックを構築することで，CS 3000のヒューマンインタフェースステーション(HIS)からSCSに対して，安全にメンテナンスオーバライドを実施することができる(**図3**)。

通常はオーバライドFBに入力された値がそのまま出力されるが，HISからのオーバライド実行指令により，指定された値(**図3**のOVR_BのVAL)が出力される。

また，オーバライドFBには，オーバライド許可スイッチがあり(**図3**のOVR_BのSW)，許可状態でないとHISからのオーバライド実行ができないようになっている。専用のパスワードFBを組み合わせることで，HISからオーバライド許可も行うことが可能である。

4．SIL3安全性のためのテクノロジー

図1に示すように，安全機能と非安全機能が混在したシステムでSIL3レベルの安全性を満足させるためには，安全機能および安全通信の正当性の保証と，非安全機能が安全機能に干渉しないことを保証する必要がある。

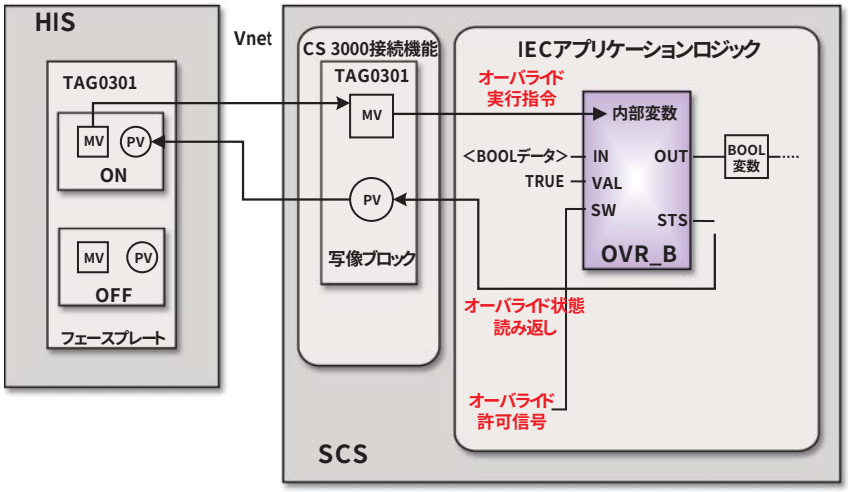

図3　HISからのメンテナンスオーバライドの例

4.1 安全機能の正当性保証

ProSafe-RSは，CS 3000と同等に厳格な開発標準に従って開発されており，高品質を保証している。さらに，発生しうるリスクに対して安全機能に及ぼす影響の分析を行い，以下に示すような異常検出のための種々の仕組みを実装し，ヒューマンエラーなどによるシステマティックフェイラーによって，危険な状態(デマンドが発生してもシャットダウンできない状態)に陥らないようにチェックしている。

(1) 安全ロジックの正当性保証

ユーザが作成した安全ロジックが，安全上正しく構築されているか，また，ロジックの修正に対しての影響箇所を，アナライザでチェックしてからでないと，SCSにダウンロードが実行できないようにしている。

(2) SENGからのデータの正当性チェック

SENGは，SCSのエンジニアリングと保守を行うためのコンポーネントであり，SCSと同一Vネット上に接続されている。SENGからSCSに対しての操作に関する通信に対して，以下のような仕組みで安全性を保証している。

・SENGからSCSへロードする個々のファイルおよび操作データにCRC (Cyclic Redundancy Check)コードを付加し，SCS側でデータが破壊されていないことをチェックしている。

・SENGからの操作に対して，送達確認のために，SCSがどの部分に対してどのような操作が行われたかをアラームで通知する。

(3) シーケンスモニタリング

SCS内で動作する安全ロジック，自己診断処理など安全機能に関連する処理が，決められた時間内に正しい順番で確実に実行されたかどうかを監視している。また，WDT (Watch-Dog Timer)によって，ソフトウエアが暴走していないことも監視している。

異常が発生した場合は，出力モジュールからフェイルセーフ値が出力されて，確実にプラントをシャットダウンさせることができる。

(4) データ空間モニタリング

SCSのプログラムおよび安全機能で使用されるデータベースは，SCS起動時にCRCが行われ正当性が確認される。また，定周期でも，安全関連のプログラムおよびデータベースが変更(破壊)されていないことを監視している。

4.2 非安全機能からの干渉防御

SCSでは，SCS内に同居する非安全機能，およびSCSと通信で接続される非安全な機器から，SCS内の安全機能への干渉を防御するために，以下のような仕組みを実装している。

(1) 安全機能領域に対してのメモリプロテクト

SCS内で安全機能が使用するメモリ領域に対して，非安全機能から書き込みができないようにプロテクトしている。

(2) 安全機能の実行を最優先とした設計

SCS内で安全機能の実行優先度を非安全機能よりも高く設定している。よって，もしも非安全機能がルーピングしたとしても，安全機能はスキャン周期毎に確実に実行することができる。

さらに，Vネット上のCS 3000ステーションからのSCSへの通信の集中によっても，安全機能の実行が阻害されないように考慮している。SCSでは，スキャン周期当たりに実行されたVネット通信の処理時間を計測し，設定された処理時間の上限を超えないようにコントロールしている。よって，もし，悪意を持ってSCSに通信アタックが行われたとしても，安全機能はスキャン周期毎に確実に実行できる。

(3) セキュリティレベル

SCSは，SENGからの安全機能への操作に対して，許可するためのセキュリティレベルを持っている。運転中のセキュリティレベルでは，SCSは，オフラインダウンロード，オンライン変更，フォーシング(安全ロジックのデータ値を強制的に固定・変更する操作)など，安全機能に対しての変更操作は受け付けない。SCSを保守する際には，SCS内に保持されてい

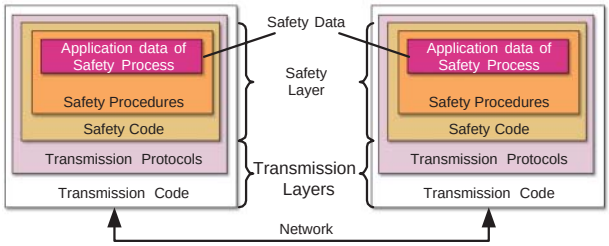

図4　安全通信の構成

るパスワードを入力してセキュリティレベルを保守レベルに変更する必要がある。

(4) メンテナンスオーバライドからの干渉防御

HISからのメンテナンスオーバライドは，SCSのセキュリティレベルが運転中のレベルでも実行できる特長がある。非安全な機器であるHISから直接SCSの安全ループのデータを変更するために，以下のような仕組みを実装し，安全性を保証している。

- オーバライドFBが許可状態でなければ，HISからのオーバライド実行指令は受け付けない。
- HISのオーバライド専用フェースプレートからのみ，SCSへのオーバライドを実行できる。このフェースプレートでは，操作状態とSCSからの読み返し状態が表示されるので，正しく実行できたことが確認できる。
- オーバライドFBの許可状態，実行状態が変化すると，SCSからHISにアラームが通知され，どのオーバライドFBが操作され，どの状態になったかが確認できる。
- HISからSCSへのオーバライド要求データにはCRCコードが付加されており，SCSでデータの正当性をチェックしている。
- オーバライド実行状態の解除忘れを防止するために，指定時間以上オーバライド状態が継続するとSCSからアラームを通知する。
- 同時にオーバライドが実行されている数も監視し，指定個数以上オーバライドを実行するとSCSからアラームを通知する。

4.3 SCSにおける安全通信

安全通信とは，既存の非安全な通信システム上で，安全関連データが，間違いなく確実に通信相手に受け渡されたことをチェックできる仕組みを持った通信方式のことである(安全通信に関する欧州規格EN50159を参照)。

安全通信では，通信のアプリケーションレイヤの部分にセーフティレイヤを配置し，セーフティレイヤで非安全な外界と安全機能を分離する。**図4**に，一般的な安全通信の構成を示す。

表1　SCS間セーフティ通信における伝送エラーに対するチェック方策

発生しうる伝送エラー	チェックするための方策			
	送信元と送信先を識別する情報を付加	送信毎に更新するシーケンス番号を付加	送信側で送信時のタイムスタンプを付加	データと左記の付加情報に対してCRCコード付加
同一メッセージの繰り返し	—	○	○	—
必要なメッセージが抜ける	—	○	—	—
期待していないメッセージが挿入	—	○	—	—
メッセージの順番が入れ替わる	—	○	○	—
メッセージが壊れている	—	—	—	○
メッセージの到着が遅れる	—	—	○	—
非安全な機器からのメッセージと混同する	○	—	—	—

(○:方策によりチェックできる伝送エラー，　—:方策によってチェックできない伝送エラー)

SCSでは，安全ロジックで実行するSCS間セーフティ通信FB(**図2**参照)内に，セーフティレイヤを配置し，安全通信を実現している。送信側のセーフティレイヤ(送信用FB)では，送信する安全データ毎にシーケンス番号，タイムスタンプ，CRCコードなどの情報を付加し，受信側のセーフティレイヤ(受信用FB)で伝送エラーを厳密にチェックしている。

表1に，通信で発生しうる伝送エラーとSCS間セーフティ通信で実施しているチェック方策を示す。

CS 3000システムの制御通信において，Vネットの高信頼性，高速応答性は実証済みである。SCS間セーフティ通信により，さらなる通信の信頼性の向上と，制御通信と混在環境下での安全性の保証が実現できた。

5. おわりに

ProSafe-RSでは，SCSに実装された安全対策の仕組みだけではなく，セーフティマニュアルやエンジニアリングガイドに，安全にエンジニアリングおよび操作するための注意点や運用手順なども明記し，多面的に安全性を保証し，安全認証を取得している。

当社としては，これからもDCSとSISを一体として開発を進め，ユーザに満足して頂けるトータルソリューションを提供し続けていく所存である。

参考文献

(1) 安藤忠明 他，“安全計装システムとProSafeシリーズの診断機能”，横河技報，Vol. 43，No. 4，1999，p. 175-180

(2) 江守敏幸 他，“CENTUM CS 制御用システムバス Vネット”，横河技報，Vol. 40，No. 2，1996，p. 59-62

(3) EN50159-1/-2：Railway applications－Communication, signaling and processing systems：Safety-related communication in closed/open transmission systems (March 2001)