ProSafe-RS 安全システム生成・保守機能

System Generation and Maintenance Functions for the ProSafe-RS Safety System

佐藤　正仁[*1]　桑谷　資一[*2]
SATO Masahito　KUWATANI Motoichi

安全計装システム(Safety Instrumented System：SIS)の中核をなす当社の安全システム ProSafe-RS のシステム生成及び保守のためのパッケージを開発した。安全システム生成機能は，安全計装の分野で標準となっている国際標準規格IEC61131-3のファンクションブロック及びラダーを使ってアプリケーションロジック(ロジックソルバ)を正確に，かつ，効率良く作成する仕組みを持っている。保守機能は，CENTUM CS 3000 HISから安全機能を損なうことなく，容易に保守点検作業が実行できる“メンテナンスオーバライド”機能を有している。また，保守機能には，異常発生時に安全コントローラ(SCS)の状態をオペレータに的確にレポートし，機器やプロセスの異常が致命的になる前に通知し，更には万一の場合の故障やプロセスのシャットダウンにおいて，その復旧を迅速に行うことができる仕組みも併せ持っている。

We have developed system generation and maintenance functions for our ProSafe-RS safety system which forms the core of safety instrumented systems (SIS). The system generation function is designed to create application logic (logic solver) accurately and efficiently using IEC61131-3 (IEC standard)-compliant function block and ladder diagrams which are most commonly employed in the safety instrumentation area. The maintenance function has a "maintenance override" function which allows easy maintenance from the CENTUM CS 3000 HIS without affecting the safety functions of the ProSafe-RS. In addition, it accurately informs the operator of the status of safety controllers (SCS) when a fault is detected, annunciating device or process faults before they prove fatal. Furthermore, the maintenance function is systematized to promptly restore normal operation in case of a system failure or process shutdown.

1. はじめに

プラントを24時間365日効率的に動作させることを目的として，高信頼の分散型生産制御システムCENTUM CS 3000が全世界で導入されている。CS 3000は，プラントの異常を適切に処理し，異常になることを可能な限り防いでいる。一方で，CS 3000では防ぎきれないプラントの異常状態を見つけた場合，人命・環境・地域・装置・機器などにダメージを与えることなく清々とプラントを停止する国際規格に則った安全計装システム(SIS)のニーズが高まっており，そのなかで安全システムProSafe-RSが開発された。ProSafe-RSでは，シャットダウン信号に応じてプラントを停止(シャットダウン)させたり，防火・防ガス装置を起動させたりするため，安全コントローラ(SCS)内にアプリケーションロジック(ロジックソルバ)が必要となる。

ProSafe-RSでは，アプリケーションロジックを正確にかつ効率良く作成し，SCSへダウンロードするセーフティエンジニアリング機能を持っている。また，ProSafe-RSの保守機能には，CS 3000のHIS(Human Interface Station)から安全機能を損なうことなく容易に保守作業が実行できる“メンテナンスオーバライド”機能がある。また，SCSが異常なく動作していることを監視するため，異

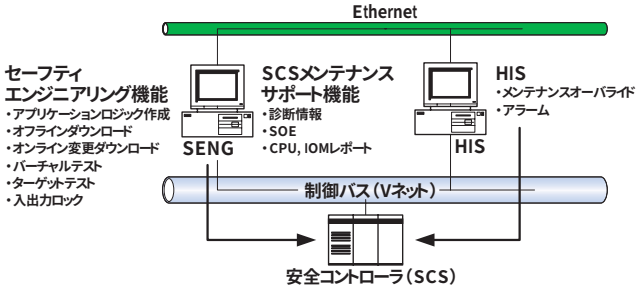

図1　ProSafe-RSのシステム構成

*1 IA事業部システム事業センター 第2技術部
*2 IA事業部システム事業センター プラットホーム開発部

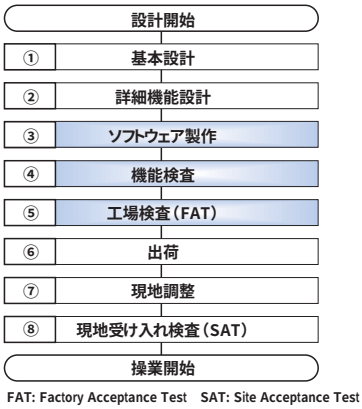

図2　エンジニアリング手順

常発生時のアラーム通知，異常発生後の復帰・復旧を正確にかつ効率良く行う“SCSメンテナンスサポート機能”がある。本システムでは，セーフティエンジニアリング機能とSCSメンテナンスサポート機能のパッケージが搭載されているPCをSENGと呼ぶ(**図1**)。

2. セーフティエンジニアリング機能

図2に，安全システムProSafe-RSの一般的なエンジニアリング手順を示す。ProSafe-RSセーフティエンジニアリング機能は，**図2**内の③ソフトウエア製作，④機能検査，⑤工場検査(FAT)で使用されることを想定して開発した。

2.1 特長

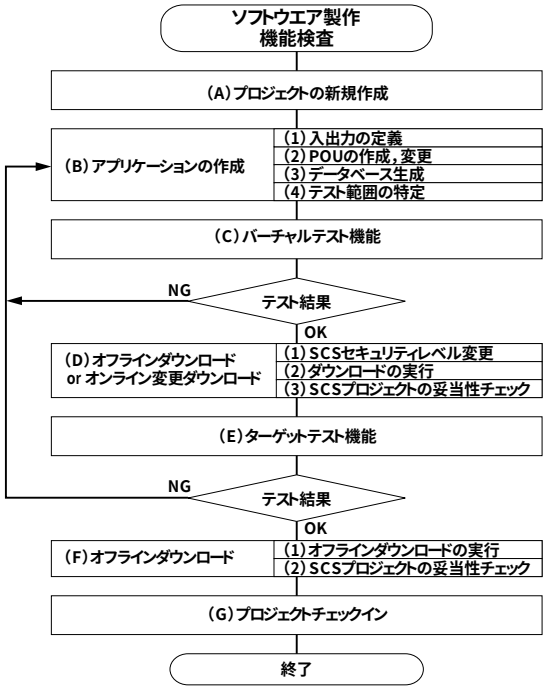

図3　ソフトウエア製作，機能検査手順

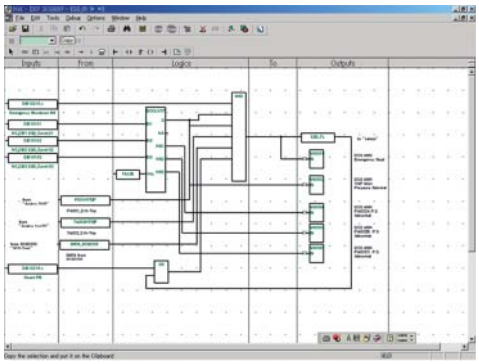

図4　マルチランゲージエディタ

アプリケーションロジックを正確に，かつ効率良く作成・管理するために，セーフティエンジニアリング機能に実装するソフトウエア製作と機能検査の手順(**図3**)に対比させて，主な特長を以下に述べる。

(1) 標準機能の採用

アプリケーションロジックの作成は，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)及びラダーダイアグラム(LD)を用いて行われる。特にFBDを作成するマルチランゲージエディタは，入力から出力までが一目で判るようにFBDを記述できるようにしている。実際には，Inputs(入力)-From(Program Organization Units：POU入力)-Logics(ロジック)-To(POU出力)-Outputs(出力)の領域を分けて記述できるようにしている(**図4**)。

この方式は，SISの分野で一般的に使用されており，下記の特長を持つ。

・設計フェーズで作成したFBDを，ほぼそのままの形で入力ができる。

・セルフドキュメント機能を使用して印刷することで，そのまま設計書として利用できる。

(2) テスト機能の充実

PC単体でFBD/LDをテストする機能(バーチャルテスト)と，SCS実機を使用してテストする機能(ターゲットテスト)が実装されている。

バーチャルテスト機能では，アプリケーションロジックを実行するためのシミュレータをPC上で動作させており，テスト機能の画面操作等は，バーチャルテストでもターゲットテストでも，ほぼ同じユーザインタフェース(UI)を持つ。

テスト機能では，アプリケーションロジックのデータ値の参照(モニタリング機能)や設定(フォーシング機能)，ブレークポイントの設定やワンショット実行等(デバッグ機能)が使用できる。**図5**は，BOOL値のTRUEを青色で，FALSEを赤色で表示するオンラインモニタリングの例である。

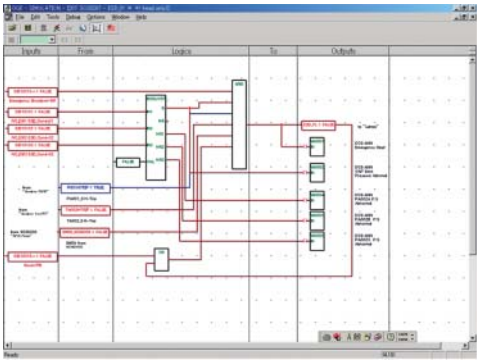

図5　テスト画面の一例

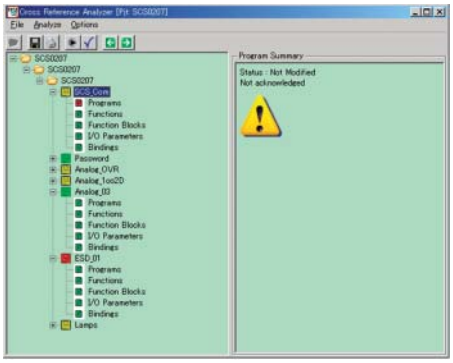

図6　Cross Reference Analyzer の例

(3) オンライン変更

SCSのCPUを停止することなく，アプリケーションロジックの変更を行うことができる(オンライン変更機能)。また，変更されたアプリケーションロジックのテストを正確にかつ効率良く行うためには，修正した箇所と修正によって影響を受けた箇所を特定し，その特定された箇所のみをテストするようにすれば効率が良い。

本セーフティエンジニアリング機能では，Cross Reference Analyzer(**図6**)と呼ばれる修正箇所と影響箇所を自動的にレポートするツールを用意している。Cross Reference Analyzerでは，修正されたアプリケーションロジックを赤色で，修正箇所の影響を受ける可能性があるアプリケーションロジックを黄色で表示するため，テスト範囲を限定することができる。緑色は一切の変更及び影響がないことを示すので，再テストを実施する必要がないことがわかる。

(4) 設計図，完成図の自動作成

セルフドキュメント機能を使用することで，作成したアプリケーションロジックなどを，A3用紙に指定したフッタ等を付けて印刷することができる。

(5) 容易なデータベース管理

作成したアプリケーションロジックは，SCS 毎に「SCSプロジェクト」と呼ばれるデータベース単位で管理される。バージョン管理は，SCS プロジェクト単位で，正確かつ効率良くデータベースを履歴管理することができる。

3. 保 守 機 能

安全計装システムは安全機能を確実に実行するために，DCS(Distributed Control System)などの他機能からの干渉がないことが求められている。一方，操作監視という視点ではDCSのHMIとの完全な統合が求められており，ProSafe-RSではSCS保守向け機能としてSCSメンテナンスサポート機能，DCSオペレータ向け機能としてCS 3000 HIS機能を提供している。

3.1 SCS メンテナンスサポート機能

SCSメンテナンスサポート機能は，SCSの保守し易さを目的に開発した機能である。本機能は故障部位の特定が容易なユーザインタフェースを持ち，解析に必要な保守データを診断情報メッセージ(UI)として，事象発生順に表示する。本機能を使用することで，保守員はSCS故障発生時の対処が迅速に行え，短期間でSCSを復旧できる。

SCSメンテナンスサポート機能の特長は，保守に必要なデータをSCS内部メモリに保持し，必要に応じてデータをSENG内のディスクに吸い上げる機能を実装したことである。SCSは保守作業に必要なデータ(診断情報や保守履歴，SOE(Sequence of Event)データ)をSCS内部メモリに保持している。このデータを必要に応じ，PC側にキャッシュデータとして吸い上げる機能(**図7**)がメッセージキャッシュ機能である。これにより，SENGがダウンしていても，保守に必要なデータの取りこぼしがない。

以下に，保守作業を高速化するウィンドウを示す(**図8**)。

(1) SCS 状態管理ウィンドウ

SCS状態管理ウィンドウは，SCSの各モジュールを階層付けて表示することに特徴がある。例えば入出力モジュールが故障した場合，当該入出力モジュールの箇所に診断情報マークが付く。これは階層構造になっているため，その上位のノードにも診断情報マークが付く。これにより，保守員は上位階層を見るだけで，下位も含めた故障の有無を一目で把握で

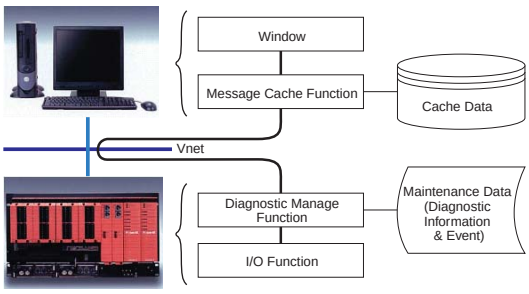

図7　メッセージキャッシュ機能

図 8　保守作業を高速化するウィンドウ

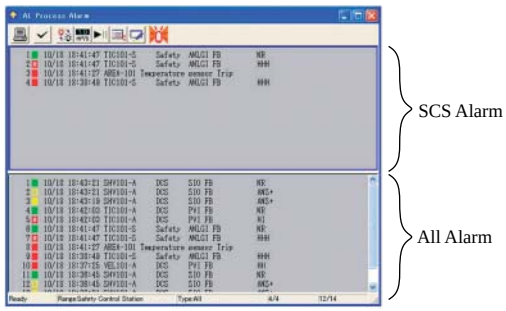

図 10　統合表示のアラームウィンドウ

きる。

(2) 診断情報ウィンドウ

SCS自らの診断結果とSCSに施した保守情報を診断情報メッセージとして表示する。保守員はSCSに施した作業が正しいか否かを診断情報メッセージで確認する。メッセージを確認し，削除をすれば，SCS状態管理ウィンドウから診断情報マークが消える。このユーザインタフェースにより，保守員はSCSが故障無く動作していると判断できる。削除済みメッセージをもう一度参照したい場合，ヒストリカルボタンを押すことで，下側ビューに削除済み診断情報メッセージが表示される。この仕組みにより，過去の保守履歴を簡単に表示できる。

(3) SOE ビューア

SCSには動作履歴を発生時刻順に記録するイベント記録機能がある。トリップ前後の動作履歴はSCS内の不揮発メモリに保管され，それをSENGにアップロードすることで，トリップ発生要因を解析できる。

3.2 CS 3000 HIS の ProSafe-RS 対応

CS 3000 HIS にはオペレータの視点で，SCS が出力したアラームを目立たせることと，SCS とフィールドコントロールステーション(FCS)のタグを容易に見分けられることが求められている。理由は，SCSが出力するアラームはプラントそのものの安全性を維持するために重要で，DCS よりもアラームの緊急度が高いからである。

(1) メンテナンスオーバライド

図 9 は，Safety 関連機器を切り離すために，ロジックの変数値を一時的に固定にする(Safety関連機器からの入力値をバイパスする)アプリケーションとそれを操作する画面である。ProSafe-RS と CS 3000 は V ネット上でシームレスに接続されているため，FCSと SCS のタグを同一画面上に表示することが可能である。そのため，保守員は画面上で装置全体の状態を監視しながら，Safety 関連機器の切り離し操作が行える。Safety関連機器の切り離し操作であるため，要求データにはCRCが付加されており，SCS側でデータの正当性が検査できる。この仕組みにより，SCS は誤った要求データを排除することが可能になる。

(2) アラームウィンドウ

安全計装システムからアラームが出力されている状況では，一般的にDCSからも多数のアラームが出力されていると考えられる。SCS が出力するアラームを確実にオペレータへ通知するために，上下にビューを分けて表示(**図 10**)する。この仕組みにより，緊急度が高いアラームを見逃さずに表示することが可能になる。

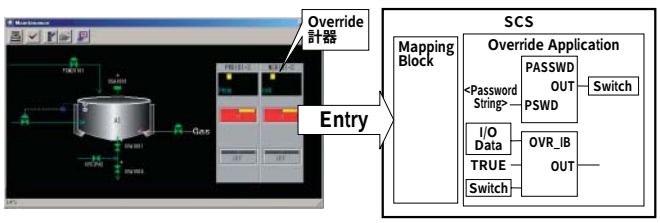

図 9　メンテナンスオーバライドの概要

4. おわりに

本稿では，セーフティエンジニアリング機能と保守機能を概観してきた。本機能は安全システムの中で正確に動作することが基本である。今後は作業の効率化，誤認や誤操作を事前に防ぐ機能， PRM(Plant Resource Manager)あるいはプラントエンジニアリングツールとの連携を行う機能などを実装し発展させていく所存である。

参考文献

(1) 佐藤正仁，“ CENTUM CS 3000 エンジニアリング機能 ”，横河技報，Vol. 43，No. 1，1999，p. 17-20