化学プラントにおける安全システムProSafe-RSの適用事例

Application of the ProSafe-RS to Chemical Plants

五十嵐　英樹[*1]　青山　貴征[*2]　内田　盛康[*3]
IGARASHI Hideki　AOYAMA Takayuki　UCHIDA Moriyasu

三菱化学株式会社殿では，千代田化工建設株式会社殿を契約先として，分解炉の増設を実施した。その増設において，緊急遮断装置に当社のプロセス用統合型安全計装システムProSafe-RSを導入した。ProSafe-RSは，国際安全規格IEC61508の安全度水準SIL3の認証を受けた国産初のプロセス向け安全システムである。今回のプロジェクトでは，このProSafe-RSの特長を活かし，高安全性と高稼働率を兼ね備えた緊急遮断システムを構築した。また，同設備の制御システムに導入された当社の統合生産制御システムCENTUM CS 3000 R3との統合オペレーションを可能とし，緊急遮断装置の監視・操作機能の飛躍的な向上を行った。本稿では，この分解炉の緊急遮断装置に導入されたProSafe-RSシステムを含む全システムの構成と特長を詳説する。

Mitsubishi Chemical Corporation contracted with Chiyoda Corporation to construct an additional fractioner in its ethylene plant. Mitsubishi elected to introduce Yokogawa's ProSafe-RS integrated safety instrumented system for industrial processes as the plant's emergency shutdown system. The ProSafe-RS is the first domestically-developed TÜV-certified safety instrumented system for the process industry. In this project, we have built an emergency shutdown system with a high degree of safety and availability and with the capability of true integration with the Yokogawa CENTUM CS 3000 RS. These are the main features of the ProSafe-RS safety instrumented system. This paper mainly discusses the features and configuration of the entire emergency shutdown system for the fractioner as well as its ProSafe-RS component.

1. はじめに

国際競争力の強化の一環として，三菱化学株式会社殿では多種多様な原料を処理するために，新しい分解炉の増設を決定した。そして，三菱化学株式会社殿/三菱化学エンジニアリング株式会社殿は，2004年5月に分解炉設備増設工事を千代田化工建設株式会社殿へ発注され，増設される分解炉設備の制御システムには，当社の統合生産制御システムCENTUM CS 3000 R3の採用を決定した。

一方，緊急遮断システムについては，三菱化学殿並びに千代田化工建設殿による技術面，保守面等の評価・検討が行われ，従来のリレーによる緊急遮断システムに替わり，緊急遮断システム，及びデコーキングシーケンス等のインターロックロジック構築用として，CENTUM CS 3000 R3とシームレスに統合できるプロセス用統合型安全計装システムProSafe-RSの導入を決定した。この決定の背景としては，以下の4点が挙げられる。

(1) 国際標準機能安全規格の普及
新しい安全のコンセプトに基づく国際安全規格IEC61508の制定。本規格は，1999年に制定され2000年にJISに制定された（JIS C 0508）。また本規格の応用規格としてプロセス産業向けのIEC61511が2003年に制定された（JISへの制定を検討中）。

(2) 新しい技術の積極的な採用
従来のリレーを主体とした緊急遮断装置からの脱却。

(3) プラントライセンサーからの定量的な安全性に関する要求
国際安全規格IEC61508に準拠し，安全度水準SIL3の要求を満たすシステムの構築。

(4) 緊急遮断装置の監視，操作機能の向上
制御システム（DCS）と安全計装システム（Safety Instrumented System: SIS）との統合操作と監視機能の実現。

今回，ProSafe-RSを採用し，国際安全規格IEC61508に準拠した緊急遮断装置を構築したので，それを紹介する。

*1 IA事業部システム事業センター 安全システム部
*2 三菱化学エンジニアリング株式会社 メンテナンス技術センター
*3 千代田化工建設株式会社 制御電気システム設計センター

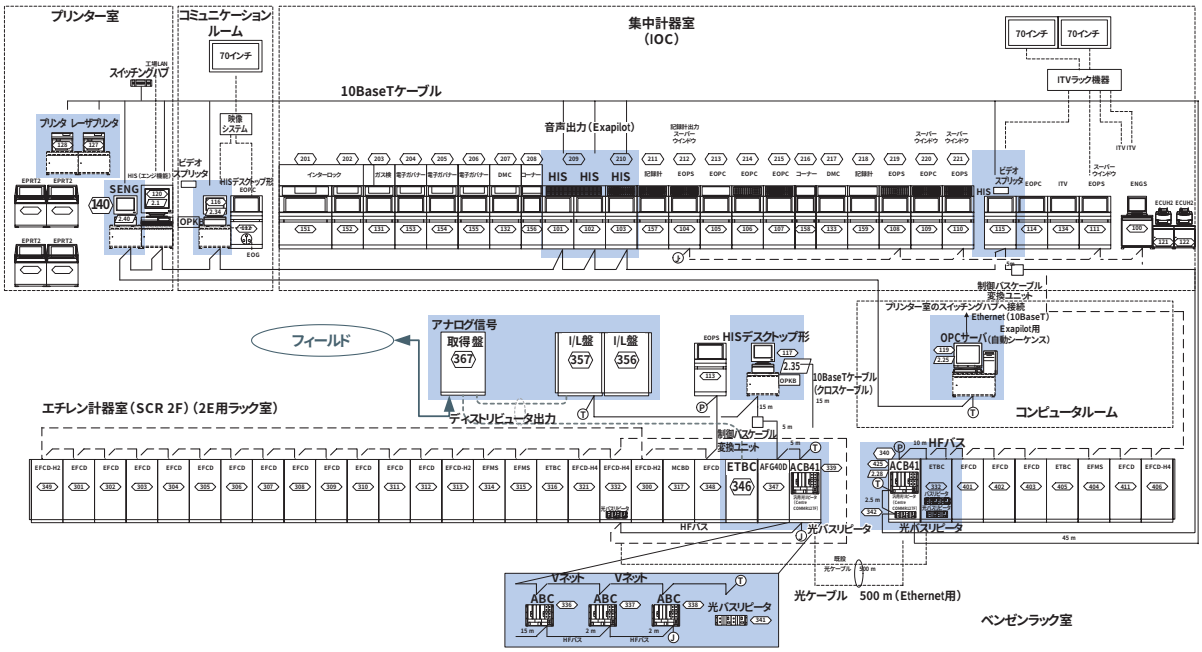

図1　全体構成図

2. システムの全体構成

システムの全体構成を，**図1**に示す。ここで網掛けされた部分が今回の設備増設で追加されたシステムである。その他の部分は従来からのシステムである。コンポーネント番号356，367がセーフティコントロールステーション(SCS)が収納されているキャビネットである。コンポーネント番号140は，ProSafe-RS用のセーフティエンジニアリングステーション(SENG)である。プラントの制御はCS 3000 R3が行い，緊急遮断に関する全てのインターロックについてはSCSが行っている。従って，緊急遮断に関するインターロックの入出力は，全てProSafe-RSに接続される。SCSとSENGは，CS 3000 R3の制御バスVnet上に接続され，Vnetを通じて互いの情報の受け渡しを行っている。同じVnet上に安全システムのProSafe-RSと制御システムのCS 3000 R3を直接接続するため，Human Interface Station(HIS)上で安全システムのデータを容易に監視･操作できるようになっている。

3. 安全システムのシステム構成

ProSafe-RSのシステム構成を，**図2**に示す。

今回のProSafe-RSのシステムは，セーフティコントロールステーション(SCS)1台とセーフティエンジニアリングステーション(SENG)1台から構成されている。SCSとSENGは，CS 3000 R3の制御バスVnetで接続されている。SCSは，CPUが実装されているCPUノード(SSC10D)と，各種I/Oモジュールが実装されている6台のI/Oノード(SNB10D)から構成されている。CPUノードと各I/Oノードは，ESBバスにより接続されている。ESBバスは，2重化された通信バスで，CPUと各I/Oモジュール間の通信に使用されている。

SENGは，汎用パーソナルコンピュータ(IBM PC/AT互換機)に専用のソフトウエアを搭載したものである。OSは，Microsoft社のWindows XP Professionalを使用している。SENGは，SCSのエンジニアリング機能，フォーシング機能(ロジック値を強制的に操作する機能)，SCSの状態表示，診断情報の表示，入出力値及びロジックの状態表示等の保守機能が備わっている。

SCSには，安全制御機能，シーケンスオブイベントレコーダ(SOER)機能，CS 3000 R3統合機能，及び他システムとのインタフェース機能(Modbus接続機能)を持つ。今回のSCSの構成では，CPUモジュール，I/Oモジュールとも2重化構成を採用している。SCSの電源は，標準で2重化構成の電源となっている。CPUモジュール，I/Oモジュールの2重化は，隣接するスロットに同じ種類のモジュールを装着することで実現されている。フィールドからの入出力信号は，専用の端子台に接続される。信号は専用端子台にて分岐，或いは突合わせされ，専用のケーブルにて各I/Oモジュールに接続されている。SCSへのDigital Input(DI)信号は無電圧接点である。またSCSからのDigital Output(DO)信号は，24 VDCの有電圧接点である。無電圧接点の入力或いは有電圧接点の出力のために，専用端子台には外部より24 VDC電源を供給している。この24 VDC電源はDC電源装置により100 VACから作られているが，今回のシステムではこの24 VDC電源も2重化構成にした。今回は，DOの負荷とな

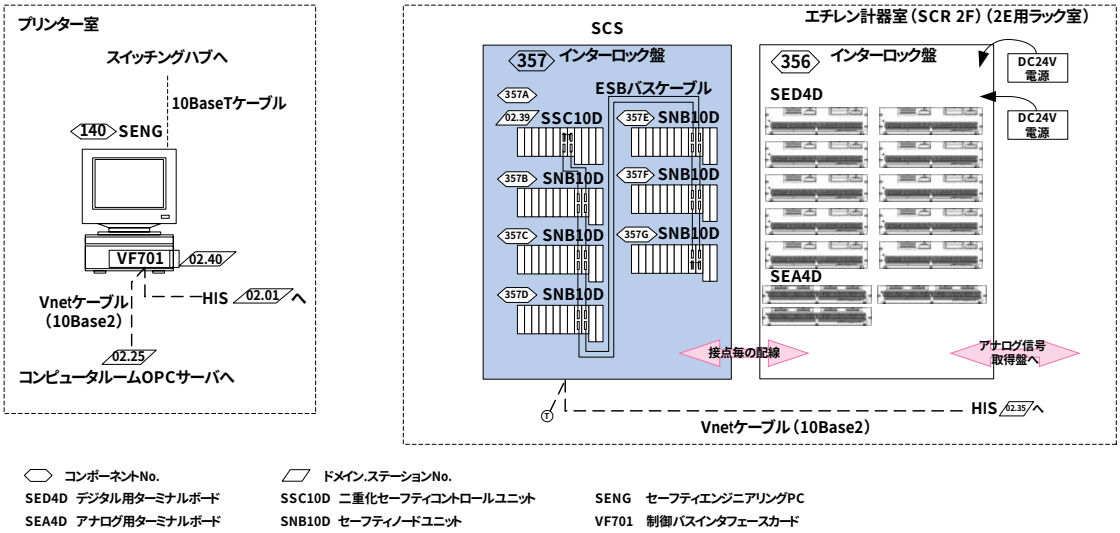

図2　安全システムのシステム構成

る電磁弁が100 VAC駆動タイプのため，DOにはセーフティリレーを接続し，その接点で電磁弁を駆動している。セーフティリレーは，TÜVの認証を得たリレーを使用している。Analog Input(AI)に関しては，制御用の信号と安全計装用の信号がそれぞれ別の伝送器より供給されており，安全に関する階層的防護の考え方に沿ったシステムとなっている。但し，一部のAIに関しては，安全計装システム側の信号の更なる冗長化(1 out of 1 を 2 out of 2 にする。)を行うために，制御用の伝送器からの入力をディストリビュータにて信号を分配し，CS 3000 R3 とSCSにそれぞれ入力させている。**図3**に，追加されたAIがディストリビュータにて分配され，安全計装システムに取り込まれる接続図を示す。

4.　安全計装システムの特長

本システムにおける安全計装システムの特長を以下に示す。

(1) アナログ入力の冗長化

今回のシステムでは，流量，温度，圧力等のアナログ量がプラントのシャットダウンの条件となっている。これらのアナログ入力は，2重化或いは3重化されSCSに取り込まれている。冗長化された入力信号は，同じアナログ入力モジュールのチャネルに割り当てず，異なるI/Oノードのアナログ入力モジュールのチャネルに割り当てている。これにより，アナログ入力モジュールの故障(今回のシステムではアナログ入力モジュールは2重化されているので，2重化した入力モジュールの同時故障を想定)，或いはI/Oノードの故障(例えば2重化された電源の同時故障等)に対しても，誤トリップ(安全計装システムの故障によるプラントのシャットダウン)することなく，高い稼働率を保てるシステム構成となっている。プリトリップアラームは，入力が3重化された場合には，1 out of 3のロジックで検出される。一方，シャットダウンのトリップのロジックは，2 out of 3のロジックで検出される。これは，プリトリップアラームの検出の信頼性を高めるとともに，シャットダウンに関しては，安全性と誤トリップ防止の調和を考慮したロジックの構成となっている。また，プリトリップアラームは，CS 3000 R3のHIS上に表示される。このアラーム表示はCS 3000 R3の表示と同じ形式で表示されるので，オペレータにとっては違和感なくアラームを監視することができる。

(2) CS 3000 R3 との統合機能

CS 3000 R3との統合により，以下の機能を実現した。

・HISのグラフィックへのSCSデータの表示

通常使用する制御用のグラフィック画面にSCSのデータを表示することにより，制御系のデータと安全システムのデータが同時に監視でき，プラントデータの一覧性が向上した。

・SCSからのデータの利用

従来パネルに取り付けられた機器で実現していたシャットダウン要因のファーストアウトアラーム機能をSCS内部のロジックで作成し，その結果をHISに表示することとした。また，バルブ等の手動操作も，HISから制御系の操作と同様な操作感覚で操作ができるようにした。

このように，CS 3000 R3との統合で，安全システムの監視・操作も従来の制御システムと同じ感覚で実現できるようになった。一方，制御システムとのシャットダウン発生の信号の受け渡しは，従来通りSCSのDOをCS 3000 R3のDIにハードワイヤーで

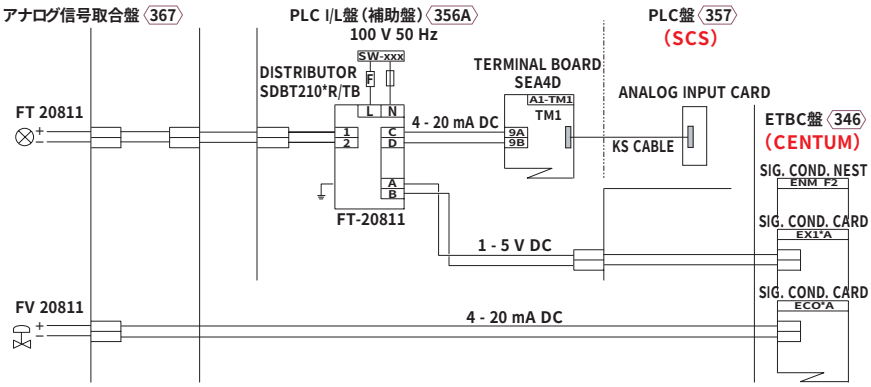

図 3　アナログ入力接続図

渡す方式とした。CS 3000 R3では，この信号によりシャットダウンが発生したことを知り，MV値（Manipulated Variable）を0%にするなどの必要な処置を行う。一方，シャットダウンのアラーム信号は，Vnet経由とした。このように，ProSafe-RSをVnet上に接続することで，ProSafe-RSとCS 3000 R3間の信号の受け渡しが，よりフレキシブルに選択できるようになった。

(3) SCS 異常時の動作選択

安全システムでは，一般的に，システム自身に異常が発生した場合，自身の出力をOffとするように設計されている。その出力により，安全計装システム全体として，安全システム異常時にプラントが安全方向に動作するように，システムの設計を行う。SCSも基本的にはこのような思想で作られているが，異常発生が検出されたら直ちに全出力 Off にするのではなく，異常発生箇所の出力の値のみを予め設定した値とすることができる。本システムでは，2重化している入力モジュールが同時故障した場合は，その入力値をプラントが安全方向に動作するように設定した。出力値も同様に，安全方向に動作するように設定した。この場合，予め設定した値になるのは当該モジュールのみで，その他の入出力モジュールの値は，故障の影響を受けることは無い。SCS は，万が一故障した場合でもその影響範囲を限定することにより，誤トリップの影響を小さくすることができる。もちろん，アプリケーションを作成して 2 重化している入力モジュールが同時故障した場合に，SCS の出力全てをOffにすることも可能である。ProSafe-RSでは，プラントの設備毎やシャットダウンループ毎にきめ細かくこれらの設定を行うことで，安全性を確保しながら誤トリップの影響を極力小さくできる。

5. 期待される導入効果

安全システムProSafe-RSを導入することにより，期待される効果を述べる。

(1) 安全性の向上

国際安全規格 IEC61508 の SIL3 に適合した安全システムProSafe-RSを採用することで，プラントの危険な事象が発生した時のシャットダウン動作がより確実に実行できるようになり，プラントの安全性が飛躍的に向上した。

(2) 信頼性の向上

ProSafe-RS は，安全性を確保しつつも，システム自身の異常による無用な誤トリップを最小にしたシステムである。特に今回採用した CPU モジュール，I/O モジュールとも 2 重化した本システムでは，殆どの場合の誤トリップを未然に防ぐことができる。

(3) CS 3000 R3 との統合化

ProSafe-RS と CS 3000 R3 との統合化により，CS 3000 R3 の HIS で ProSafe-RS の入出力，システム状態等を監視画面で監視でき，プラントの情報の一元管理がより進んだ。また，緊急時の操作等も，通常操作環境である HIS からできるようになり，緊急時の対処の確実性が向上した。

6. おわりに

本稿では，ProSafe-RSによる分解炉設備の安全計装システムの構築例を紹介した。今後，多くの国内プラントに安全計装システムを導入し，プラントの安全性の向上に寄与したいと考えている。

最後に，本稿を作成するに当たり，ご指導いただいた三菱化学エンジニアリング株式会社の青山様，千代田化工建設株式会社の内田様 他，関係者各位には，深く感謝申し上げる。